Third Edition

Introduction to Reliability Engineering

James E. Breneman
Chittaranjan Sahay • Elmer E. Lewis

with website

WILEY

Introduction to Reliability Engineering

Introduction to Reliability Engineering

Third Edition

James E. Breneman
Manager, Engineering Technical University,
Retired, Pratt & Whitney Corporation
Division of Raytheon Technologies

Chittaranjan Sahay
Professor of Mechanical Engineering
University of Hartford

Elmer E. Lewis
Professor Emeritus
Department of Mechanical Engineering
Northwestern University

WILEY

This edition first published 2022

Edition History
1st edition (9780471811992) 1987, by John Wiley & Sons, Inc.
2nd edition (9780471018339) 1996, by John Wiley & Sons, Inc.

Registered Office
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Breneman, James E., author. | Sahay, Chittaranjan,
author | Lewis, E. E. (Elmer Eugene), 1938– author.
Title: Introduction to reliability engineering / J.E. Breneman, Director of Advanced Engineering
Processes Manager, Engineering Technical University, Retired, Pratt &
Whitney Corporation, Chittaranjan Sahay, Professor of Mechanical
Engineering, University of Hartford, Hartford, Connecticut, Elmer E. Lewis, Professor
Emeritus, Department of Mechanical Engineering, Northwestern University,
Evanston, Illinois.
Description: Third edition. | Hoboken, NJ : John Wiley & Sons, Inc., 2022.
| Includes bibliographical references and index.
Identifiers: LCCN 2021038736 (print) | LCCN 2021038737 (ebook) | ISBN
9781119640561 (cloth) | ISBN 9781119640622 (adobe pdf) | ISBN
9781119640653 (epub)
Subjects: LCSH: Reliability (Engineering)
Classification: LCC TA169 .L47 2022 (print) | LCC TA169 (ebook) | DDC
620/.00452–dc23
LC record available at https://lccn.loc.gov/2021038736
LC ebook record available at https://lccn.loc.gov/2021038737

Cover image: © Wikimedia Commons
Cover design by Wiley

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

10 9 8 7 6 5 4 3 2 1

To Our Wives and Families

Contents

Preface

The objective of this text is to provide an elementary and reasonably self-contained overview of reliability engineering that is suitable for an upper-level undergraduate or first-year graduate course for students of any engineering discipline. In addition, the third edition has added material for the "beginning" reliability engineer who is in the field and transferred to the reliability/safety discipline. The materials reflect the inherently interdisciplinary character of reliability considerations and the central role played by probability and statistical analysis in presenting reliability principles and practices.

The examples and exercises are drawn from a variety of engineering and some nonengineering fields. They can be understood, however, with only the knowledge from the physics, chemistry, and basic engineering courses contained in the first years of nearly all engineering curricula. Likewise, the reader is presumed to have completed only the standard mathematics sequence, through ordinary differential equations, required of most engineering students. No prior knowledge of probability or statistics is assumed; the development of the required concepts is contained within the text.

Since the second edition, at least two major changes have taken place that are incorporated into this new edition. The first is the increased industrial emphasis on quality in the product development cycle and the vital role that reliability plays in providing an overall reliable and safe product. The second is the rapid advances that have taken place in not only personal computer software but the extent to which that software has penetrated the engineering profession in all arenas, thus lending more time for thinking about the data and *then thinking* about the results of the analysis rather than spending so much time "computing" the solutions. The reader will find many instances in this edition where computer software is used not only to produce solutions to specific problems but also to the generation of tables of values (normal probability, t tables, chi-square tables, etc.).

For each appropriate example in this edition, the necessary steps for obtaining a solution are indicated using readily available software. EXCEL™ is augmented in many cases with MINITAB®. These two programs were chosen because they are widely available, and instructions for their use are also widely available. There are other statistical software packages other than MINITAB that can do most of the analyses (SAS™, SAS/JMP™, RELIASOFT++™, SUPERSMITH™, and others) that are referenced in the third edition. The problems and solutions are amenable to all these software packages as well as others.

A number of additional improvements have been incorporated into the new edition. Reliability Basics and the Exponential Distribution are introduced in Chapter 3; Chapter 4, Continuous Distributions, Part 1, introduces the normal and lognormal distributions. The Weibull and extreme value distributions are treated in Chapter 5, Continuous Distributions, Part 2. Chapter 6 is dedicated to the topic of reliability testing. It is expanded from the second edition to include many options for setting up reliability testing along with the analysis of the data, thus emphasizing the importance of the Weibull distribution in the practice of reliability engineering. Chapter 7 is dedicated to FMEA (Failure Modes and Effects Analysis), an indispensable tool in reliability in all areas, not just design but virtually EVERY process in any industry including the medical and most "soft" industries in terms of process FMEA. Chapter 8 on Loads, Capacity, and Reliability; Chapter 9 on Maintained Systems; and Chapter 10 on Failure Interactions are basically unchanged from the second edition. Two sections have been added to the System Safety Analysis (now Chapter 11) on FMECA (Failure Modes, Effects, and Criticality Analysis) and Safety Risk Analysis and the Use of Monte Carlo Simulation.

Finally, the text now contains over 150 solved examples and well over 300 exercises, many of which are new. The answers to the odd-numbered exercises are given at the end of the book.

The text contains more material than can be treated in detail in a normal one-semester undergraduate course, providing some latitude in the topics that may be emphasized. If the students have had some previous exposure to elementary probability, Chapter 2 can be somewhat telescoped because those probability concepts that are more specific to reliability analysis are set forth in Chapter 3. The statistical treatment of data contained mainly in Chapters 4, 5, 6, and 7 is essential to a well-rounded undergraduate course in reliability engineering. The materials in the remaining chapters may be covered independently in an advanced undergraduate or graduate course. For example, the quantitative analysis of the effects of load and capacities contained in Chapter 8 is critical to the understanding of failure mechanisms, but the reliability systems considerations concentrated in Chapters 9 and 11 may be read independently of it. Finally, the system safety analysis contained in Chapter 11 may be understood without first covering the Markov analysis methods developed in Chapter 10.

In addition to the continued thanks owed to the students and colleagues who provided their advice and assistance with previous editions, we would like to acknowledge the help of specific individuals in encouraging the authors to include the reliability engineering professionals in this book's prospective audience:

My sincere thanks to:

As well as the students at Northwestern University who have ferreted out errors in the first edition and made constructive criticisms and suggestions for improvements. George Coons of the Motorola Corporation has been particularly helpful in providing materials and suggestions related to the treatment of quality issues, and Jim Lookabaugh of Northwestern designed the data acquisition system and obtained the light bulb reliability results that serve as the basis for several examples in Chapters 5 and 8. Finally, I would like to express my appreciation for the continued understanding of my wife and children while I monopolized the family computer.

Elmer Lewis

My sincere thanks to:

- all my colleagues at Pratt & Whitney, especially Dr. Bob Abernethy, Wes Annas, Dave McDermott, Steve Luko, and in particular, my P&W Engineering mentor Jack Sammons, without whose

encouragement I would not have explored the needs at P&W in Weibull Risk & Reliability Analysis.

- Many former UTC divisions (Carrier, Otis, and Sikorsky) and many other companies I have consulted for as well as university students who had the fortitude to listen to my advice and take the many Reliability, Statistics, and Safety courses I have taught – thanks for helping me become a better listener and teacher.
- My SAE, ASA, and ASQ professional associates have provided me with their ideas and support: in particular, Wes Fulton, Paul Barringer, Jim McLinn, and Trevor Craney.

Jim Breneman

Prof. Alan Hadad and Dr. Louis Manzione for their support in always helping me pursue my goals. My portion of the materials in the book are influenced by discussions with my students over the years at the University of Hartford and the State University of New York at Binghamton. I received encouragement from my teacher, Prof. Rajendra Dubey of the University of Waterloo. I am grateful to my industry collaborators who have transformed my approach to engineering education. In particular, Jim Breneman, coauthor of the book, was an inspiration while serving as the point of contact for University relations at Pratt and Whitney. I owe the most of thanks to my wife, Saraswati Sahay, and my children, who stood by me and helped me stay focused.

Chittaranjan Sahay

Jim Breneman, Vergennes, VT, USA
Chittaranjan Sahay, West Hartford, CT, USA
Elmer Lewis, Evanston, IL, USA
December 2021

About the Author

James E. Breneman, received a B.S. in mathematics from University of North Carolina, Chapel Hill, and an M.S. in mathematics and statistics from N.C. State, Raleigh, North Carolina. He served in the US Army during the Vietnam war and is a former director of Advanced Engineering Processes and the founder and manager of Pratt & Whitney's Engineering Technical University. He has worked over 45 years in the reliability and statistical arena and 35 years at Pratt & Whitney (Division of Raytheon Technologies) in reliability and safety risk analysis. He is a Pratt & Whitney Fellow as well as SAE Fellow in reliability, a recipient of the ASQ Grant medal, and other professional awards. He is a coauthor of the USAF Weibull Analysis Handbook and numerous (published and unpublished) papers and handbooks in reliability and safety. He is a consultant to various aerospace and nonaerospace industries in the areas of reliability, statistics, and risk.

Chittaranjan Sahay, Received a B.Sc. in Mechanical Engineering from Regional (now, National) Institute of Technology, Jamshedpur in India, and a Ph.D. from Indian Institute of Technology, Delhi, India. He was a post-doctoral fellow at the University of Waterloo and University of Ottawa in Canada before moving to the State University of New York at Binghamton. He has served as Visiting Faculty at Cornell University, Birla Institute of Technology, Mesra Ranchi as B.M. Birla Professor of Mechanical Engineering, and at Indian Institute of Technology, Patna. He is a Fellow of the American Society of Mechanical Engineers. He is the Vernon D. Roosa Distinguished Professor of Manufacturing Engineering, a professor of Mechanical Engineering, and the Director for Center of manufacturing and Metrology at the University of Hartford.

Elmer E. Lewis is professor emeritus and former chairman of the Department of Mechanical Engineering, Northwestern University. He received his B.S. in engineering physics and an M.S. and Ph.D. in nuclear engineering at the University of Illinois, Urbana. He served as a captain in the US Army and as a Ford Foundation fellow and an assistant professor at MIT before joining Northwestern's faculty. He has also held appointments as visiting professor at the University of Stuttgart and guest scientist at the Nuclear Research Center at Karlsruhe, Germany, and has served as a consultant to Argonne, Los Alamos, and Oak Ridge National Laboratories and to a number of industrial firms. A fellow of the American Nuclear Society and winner of its Eugene P. Wigner Reactor Physics and Arthur Holly Compton Awards, his research has been focused on reliability modeling, radiation transport, and the physics and safety of nuclear systems. He is the author or coauthor of over 200 publications including the Wiley books, *Nuclear Power Reactor Safety, Computational Methods of Neutron Transport*, and the first two editions of *Introduction to Reliability Engineering*.

About the Companion Website

This book is accompanied by a companion website:

www.wiley.com/go/breneman/relabilityengineering3e

The instructor site will include:

- Answers to end-of-chapter exercises
- PowerPoints
- Project ideas

The student site will include:

- Excel files of the exercises

1

Introduction

> "When an engineer, following the safety regulations of the Coast Guard or the Federal Aviation Agency, translates the laws of physics into the specifications of a steamboat boiler or the design of a jet airliner, he is mixing science with a great many other considerations all relating to the purposes to be served. And it is always purposes in the plural — a series of compromises of various considerations, such as speed, safety economy and so on."
>
> *Source*: D. K Price, The Scientific Estate, 1968

1.1 Reliability Defined

The world demands that the performance of products and systems be improved while at the same time reducing their cost. The requirement to minimize the probability of failures, whether those failures simply increase costs and irritation or gravely threaten the public safety, has placed increased emphasis on reliability and safety. The formal body of knowledge that has been developed for analyzing such failures and minimizing their occurrence cuts across virtually all engineering disciplines, providing the rich variety of contexts in which reliability considerations appear. Indeed, deeper insight into failures and their prevention is to be gained by comparing and contrasting the reliability characteristics of systems of differing characteristics: computers, electromechanical machinery, energy conversion systems, chemical and materials processing plants, and structures, to name a few.

In the broadest sense, reliability is associated with dependability, with successful operation, and with the absence of breakdowns or failures. It is necessary for engineering analysis, however, to define reliability quantitatively as a probability.

Thus, *reliability is defined as the probability that a system will perform its intended function for a specified period of time under a given set of conditions*. System is used here in a generic sense so that the definition of reliability is also applicable to all varieties of products, subsystems, equipment, components, and parts.

A product or system is said to fail when it ceases to perform its intended function. When there is a total cessation of function – an engine stops running, a structure collapses, a piece of communication equipment goes dead – the system has clearly failed. Often, however, it is necessary to define failure quantitatively in order to take into account the more subtle forms of failure, through deterioration or instability of function. Thus, a motor that is no longer capable of delivering a specified torque, a structure that exceeds a specified deflection, a part that is seriously corroded or eroded (yet

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

still working), or an amplifier that falls below a stipulated gain has failed. Intermittent operation or excessive drift in electronic equipment and the machine tool production of out-of-tolerance parts may also be defined as failures.

The way in which time is specified in the definition of reliability may also vary considerably, depending on the nature of the system under consideration. For example, in an intermittently operated system one must specify whether calendar time or the number of hours of operation is to be used. If the operation is cyclic, such as that of a switch, time is likely to be cast in terms of the number of operations. Some subsystems of the same system (e.g. jet engine) may have different time criteria that drives their failure. If reliability is to be specified in terms of calendar time, it may also be necessary to specify the frequency of starts and stops and the ratio of operating to total time.

In addition to reliability itself, other quantities are used to characterize the reliability of a system. The mean time to failure and failure rate are examples, and in the case of repairable systems, so also are the availability and mean time to repair. The definition of these and other terms will be introduced as needed.

1.2 Performance, Cost, and Reliability

Much of engineering endeavor is concerned with designing and building products for improved performance. We strive for lighter and therefore faster aircraft, for thermodynamically more efficient energy conversion devices, for faster computers, and for larger, longer lasting structures. The pursuit of such objectives, however, often requires designs incorporating features that more often than not may tend to be less reliable than older, lower performance systems, at least initially when the customer receives them. The trade-offs between performance, reliability, and cost are often subtle, involving loading, system complexity, and the employment of new materials and concepts.

Load is most often used in the mechanical sense of the stress on a structure. But here we interpret it more generally so that it also may be the thermal load caused by high temperature, the electrical load on a generator, or even the information load on a telecommunications system. Whatever the nature of the load on a system or its components may be, performance is frequently improved through increased loading. Thus, by increasing the weight of an aircraft, we increase the stress levels in its structure; by going to higher – thermodynamically more efficient – temperatures we are forced to operate materials under conditions in which there are heat-induced losses of strength and more rapid corrosion/erosion. By allowing for ever-increasing flows of information in communications systems, we approach the frequency limits at which switching or other digital circuits may operate.

As the physical limits of systems or their components are approached in order to improve performance, the number of failures increase unless appropriate countermeasures are taken. Thus, specifications for a purer material, tighter dimensional tolerance, and a host of other measures are required to reduce uncertainty in the performance limits and thereby permit one to operate close to those limits without incurring an unacceptable probability of exceeding them (i.e. failure). But in the process of doing so, the cost of the system is likely to increase. Even then, adverse environmental conditions, product deterioration, and manufacturing flaws all lead to higher failure probabilities in systems operating near their limit loads.

System performance may often be increased at the expense of increased complexity, the complexity usually being measured by the number of required components or parts. Once again, reliability will be decreased unless compensating measures are taken, for it may be shown that if nothing else is changed, reliability decreases with each added component. In these situations, reliability can only be maintained if component reliability is increased or if component redundancy is built into the system. But each of these remedies, in turn, must be measured against the incurred costs.

Probably the greatest improvements in performance have come through the introduction of entirely new technologies. For, in contrast to the trade-offs faced with increased loading or complexity, more fundamental advances may have the potential for both improved performance and greater reliability. Certainly, the history of technology is a study of such advances; the replacement of wood by metals in machinery and structures, the replacement of piston with jet aircraft engines, and the replacement of vacuum tubes with solid-state electronics all led to fundamental advances in both performance and reliability while costs were reduced. Any product in which these trade-offs are overcome with increased performance and reliability, without a commensurate cost increase, constitutes a significant technological advance.

With any major advance, however, reliability may be diminished, particularly in the early stages of the introduction of new technology. The engineering community must proceed through a learning experience to reduce the uncertainties in the limits in loading on the new product, to understand its susceptibilities to adverse environments, to predict deterioration with age, and to perfect the procedures for fabrication, manufacture, and construction. Thus, in the transition from wood to iron, the problem of dry rot was eliminated, but failure modes associated with brittle fracture had to be understood. In replacing vacuum tubes with solid-state electronics the ramifications of reliability loss with increasing ambient temperature and vibration had to be appreciated.

Whether in the implementation of new concepts or in the application of existing technologies, the way trade-offs are made between reliability, performance and cost, and the criteria on which they are based is deeply imbedded in the essence of engineering practice, for the considerations and criteria are as varied as the uses to which technology is put. The following examples illustrate this point.

- Consider an air conditioner. What is the worst that can happen if it quits? The customer is warm. So, when developing air conditioners, safety is not paramount, reliability is considered, but cost is "king." Hence, copper tubing for A/C units has given way to aluminum. Plastics for metal wherever possible for weight saving, less testing, and lower confidence levels in the testing are used.
- At the opposite extreme is the design of a commercial airliner, where mechanical breakdown could well result in a catastrophic accident. In this case, reliability is the overriding design consideration; degraded speed, payload, and fuel economy are accepted in order to maintain a very small probability of catastrophic failure. An intermediate example might be in the design of a military aircraft, for here the trade-off to be achieved between reliability and performance is more equally balanced. Reducing reliability may again be expected to increase the incidence of fatal accidents. Nevertheless, if the performance of the aircraft is not sufficiently high, the number of losses in combat may negate the aircraft's mission, with a concomitant loss of life.

Hence, reliability of many products may be viewed primarily in economic terms. The design of a piece of machinery, for example may involve trade-offs between the increased capital costs entailed if high reliability is to be achieved and the increased costs of repair and of lost production that will be incurred from lower reliability. Even here, more subtle issues come into play. For consumer products, the higher initial price that may be required for a more reliable item must be carefully weighed against the purchaser's annoyance with the possible failure of a less-reliable item as well as the cost of replacement or repair. For these wide classes of products, it is illuminating to place reliability within the wider context of product quality.

1.3 Quality, Reliability, and Safety Linkage

In competitive markets there is little tolerance for poorly designed and/or shoddily constructed products. Thus, since the middle 1980s increasing emphasis has been placed on product quality improvement as manufacturers have striven to satisfy customer demands. In very general terms, *quality may be defined as the totality of features and characteristics of a product or service that bear on its ability to satisfy given needs*. Thus, while product quality and reliability invariably are considered to be closely linked, the definition of quality implies performance optimization and cost minimization as well. Therefore, it is important to delineate carefully the relationships between quality, reliability, and safety. We approach this task by viewing the three concepts within the framework of the design and manufacturing processes, which are at the heart of the engineering enterprise.

In the product development cycle, careful market analysis is first needed to determine the desired performance characteristics and quantify them as design criteria. In some cases, the criteria are upper limits, such as on fuel consumption and emissions, and in others they are lower limits, such as on acceleration and power. Still others must fall within a narrow range of a specified target value, such as the brightness of a video monitor and the release pressure of a door latch. In conceptual or system design, creativity is brought to the fore to formulate the best system concept and configuration for achieving the desired performance characteristics at an acceptable cost. Detailed design is then carried out to implement the concept. The result is normally a set of working drawings and specifications from which prototypes are built. In designing and building prototypes, many studies are carried out to optimize the performance characteristics.

If a suitable concept has been developed and the optimization of the detailed design is successful, the resulting prototype should have performance characteristics that are highly desirable to the customer. In this process, the costs that eventually will be incurred in production must also be minimized. The design may then be said to be of high quality or more precisely of high characteristic quality. Building a prototype that functions with highly desirable performance characteristics, however, is not in and of itself sufficient to assure that the product is of high quality; the product must also exhibit low variability in the performance characteristics.

The customer who purchases an engine with highly optimized performance characteristics, for example, will expect those characteristics to remain close to their target values as the engine is operated under a wide variety of environmental conditions of temperature, humidity, dust, and so on. Likewise, satisfaction will not be long lived if the performance characteristics deteriorate prematurely with age and/or use. Finally, the customer is not going to buy the prototype but a mass produced engine. Thus, each engine must be very nearly identical to the optimized prototype if a reputation of high quality is to be maintained; variability or imperfections in the production process that lead to significant variability in the performance characteristics should not be tolerated. Even a few “lemons” will damage a product’s reputation for high quality.

To summarize, two criteria must be satisfied to achieve high quality. First, the product design must result in a set of performance characteristics that are highly optimized to customer desires. Second, these performance characteristics must be robust. That is, the characteristics must not be susceptible to any of the three major causes of performance variability: (i) variability or defects in the manufacturing process, (ii) variability in the operating environment, and (iii) deterioration resulting from wear or aging.

In what we refer to as product dependability, our primary concern is in maintaining the performance characteristics in the face of manufacturing variability, adverse environments, and product deterioration. In this context, we may distinguish between quality, reliability, and safety.

- Any variability of performance characteristics concerning the target values entails a loss of quality.
- Reliability engineering is primarily concerned with variability that is so severe as to cause product failure.
- Safety engineering is focused on those failures that create hazards.

To illustrate these relationships, consider an automatic transmission for an automobile. Among the performance characteristics that have been optimized for customer satisfaction are the speeds at which gears automatically shift. The quality goal is then to produce every transmission so that the shift takes place at as near as possible to the optimum speed, under all environmental conditions, regardless of the age of the transmission and independently of where in the production run it was produced. In reality, these effects will result in some variability in the shift speeds and other performance characteristics. With increased variability, however, quality is lost. The driver will become increasingly displeased if the variability in shift speed is large enough to cause the engine to race before shifting or low enough that it grinds from operating in the higher gear at too low a speed. With even wider variability the transmission may fail altogether, by one of a number of modes, for example by sticking in either the higher or lower gear, or by some more catastrophic mode, such as seizure.

Just as failures studied in reliability engineering may be viewed as extreme cases of the performance variability closely associated with quality loss, *safety analysis deals with the subset of failure modes that may be hazardous*. Consider again our engine example. If it is a lawn mower engine, most failure modes will simply cause the engine to stop and have no safety consequences. A safety problem will exist only if the failure mode can cause the fuel to catch fire, the blades to fly off, or some other hazardous consequence. Conversely, if the engine is for a single-engine aircraft, reliability and safety considerations clearly are very closely linked.

In reliability engineering, the primary focus is on failures and their prevention. The foregoing example, however, makes clear the intimate relationship among quality loss, performance variability, and failure. Moreover, as will become clearer in succeeding chapters, there is a close correlation between the three causes of performance variability and the three failure mode categories that permeate reliability and safety engineering.

- Variability due to manufacturing processes tends to lead to failures concentrated early in product life. In the reliability community, these are referred to as early or infant mortality failures.
- The variability caused by the operating environment leads to failures designated as random, since they tend to occur at a rate which is independent of the product's age.
- Finally, product deterioration leads to failures concentrated at longer times and is referred to in the reliability community as aging or wear failures.

The common pocket calculator provides a simple example of the classes of variability and of failure. Loose manufacturing tolerances and imprecise quality control may cause faulty electrical connections, misaligned keys, or other imperfections that are most likely to cause failures early in the design life of the calculator. Inadvertently stepping on the calculator, dropping it in water, or leaving it next to a strong magnet may expose it to environmental stress beyond which it can be expected to tolerate. The ensuing failure will have little correlation to how long the calculator has been used, for these are random events that might occur at any time during the design life. Finally, with use and the passage of time, the calculator key contacts are likely to become inoperable, the casing may become brittle and crack, or other components may eventually cause the calculator to fail from age.

To be sure, these three failure mode classes often subtly interact. Nevertheless, they provide a useful framework within which we can view the quality, reliability, and safety considerations taken up in succeeding chapters.

1.4 Quality, Reliability, and Safety Engineering Tasks

The focus of the activities of quality, reliability, and safety engineers, respectively, differs significantly as a result of the nature and amount of data that is available. This may be understood by relating the performance characteristics to the types of data that engineers working in each of these areas must deal with frequently. Quality engineers must relate the product performance characteristics back to the design specifications and parameters that are directly measurable, the dimensions, material compositions, electrical properties, and so on. Their task includes both setting those parameters and tolerances so as to produce the desired performance characteristics with a minimum of variability and ensuring that the production processes conform to the goals. Thus, corresponding to each performance characteristic there are likely to be many parameters that must be held to close conformance. With modern instrumentation, data on the multitude of parameters and their variability may be generated during the production process. The problem is to digest the vast amounts of raw data and put it to useful purposes rather than being overwhelmed by it. The processes of robust design and statistical quality control deal with utilizing data to decrease performance characteristic variability.

Reliability data is more difficult to obtain, for it is acquired through observing the failure of products or their components. Most commonly, this requires life testing in which a number of items are tested until a significant number of failures occur. Unfortunately, such tests are often expensive, since they are destructive, and to obtain meaningful statistics substantial numbers of the test specimens must fail. They are also time consuming, since unless unbiased acceleration methods are available to greatly compress the time to failure, the test time may be comparable or longer to the normal product life. Reliability data, of course, is also collected from field failures once a product is put into use. But this is a lagging indicator and is not nearly as useful as results obtained earlier in the development process. It is imperative that the reliability engineer be able to relate failure data back to performance characteristic variability and to the design parameters and tolerances. In products that have evolved over many decades (e.g. airplanes, jet engines, and rocket engines) using previous "Lessons Learned" from the basic failures of similar parts, subsystems, and systems can be a beginning guide for a current design effort. Reviews of designs by EXPERIENCED Reliability, Safety, and Quality engineers can point out possible areas of concern in a new design and recommend actions to prevent the failures from occurring.

The paucity of data is even more severe for the safety engineer, for with most products, safety hazards are caused by only a small fraction of the failures. Conversely, systems whose failures by their very nature cause the threat of injury or death are designed with safety margins and maintenance and retirement policies such that failures are rare. In either case, if an acceptable measure of safety is to be achieved, the prevention of hazardous failures must rely heavily on more qualitative methods. Hazardous design characteristics must be eliminated before statistically significant data bases of injuries or death can develop. Thus, the study of past accidents and of potential unanticipated uses or environments, along with failure modes and effects analysis and various other "what if" techniques, finds extensive use in identifying potential hazards and eliminating them. Careful attention must also be paid to field reports for signs of hazards incurred through product use – or misuse – for often it is only through careful detective work that hazards can be identified and eliminated.

1.5 Preview

In the following chapter, we first introduce a number of concepts related to probability and discrete distributions. Chapter 3 introduces the engineer to the Basics of Reliability and the Exponential Distribution (since until the late 1950s/early 1960s the exponential distribution was virtually the only distribution used in reliability studies). The bathtub curve is introduced as well, and the relationships of reliability to failure modes, component failures, and replacements are discussed. Chapters 4 and 5 cover the continuous distributions important to reliability in the current world: normal, lognormal, and Weibull/extreme value.

In Chapter 6, we investigate reliability testing and its prominent place in setting up and analyzing data from laboratory tests as well as field test data. Accelerated life testing and its relationship to failure rates and other phenomena where time is of the essence in the product development cycle is covered extensively.

Chapter 7 covers the reliability engineering tool of Failure Modes and Effects Analysis (FMEA) in Design and Process. As discussed earlier in the Introduction, processes are just as (and evidence exists that they are *more*) important in producing a reliable and hence highly safe and quality product.

In contrast, Chapter 8 concerns the relationships between reliability, the loading on a system, and its capacity to withstand those loads. This entails, among other things, an exposition of the probabilistic treatment of safety factors and design margins. The treatment of repetitive loading allows the time dependence of failure rates on loading, capacity, and deterioration to be treated explicitly.

Chapters 9 and 10 deal with the reliability of more complex systems. Chapter 9 concentrates on maintained systems, examining the effects of both preventive and corrective maintenance and then focusing on maintainability and availability concepts for repairable system. In Chapter 10, the treatment of complex systems and their failures is brought together through an introduction to continuous-time Markov analysis.

Chapter 11 concludes the text with an introduction to system safety analysis. After discussions of the nature of hazards caused by equipment failures and by human error, quantitative methods for safety analysis are reviewed. The FMEA reliability engineering tool of Chapter 7 is expanded to Failure Modes and Effects Criticality Analysis (FMECA), which can be used, in conjunction with safety hazard analysis, to prioritize which failure modes are most hazardous in the design phase and later in the early test, production, and field phases of a product. The construction and analysis of fault tree analysis methods are then treated in some detail. Chapter 11 is completed with examples of safety risk analyses using Monte Carlo simulation.

Bibliography

Brockley, D. (ed.) (1992). *Engineering Safety*. London: McGraw-Hill.

Green, A.E. and Bourne, A.J. (1972). *Reliability Technology*. New York: Wiley.

Haviland, R.D. (1964). *Engineering Reliability and Long Life Design*. New York: Van Nostrand.

Kapur, K.C. and Lamberson, L.R. (1977). *Reliability in Engineering Design*. New York: Wiley.

Lewis, E.E. (2014). *How Safe Is Safe Enough? Technological Risk: Perceptions and Realities*. New York: Carell Books/Simon & Schuster.
McCormick, N.J. (1981). *Reliability and Risk Analysis*. New York: Academic Press.
Mitra, A. (1993). *Fundamentals of Quality Control and Improvement*. New York: Macmillan.
Smith, D.J. (1993). *Reliability, Maintainability and Risk*, 4th ed. Oxford: Butterworth-Heinemann.

2

Probability and Discrete Distributions

"Probability Theory is Nothing but Common Sense Reduced to Calculation"

–Laplace

2.1 Introduction

Fundamental to all reliability considerations is an understanding of probability, for reliability is defined as the *probability* that a system will not fail under some specified set of circumstances. In this chapter, we discuss the logic by which probabilities can be combined and manipulated. Although quite elementary, the notions presented will be shown to have immediate applicability to a variety of reliability considerations ranging from the reliability of parts to subsystems to the reliability of a system.

2.2 Probability Concepts

We denote the probability of an event, say a failure, A, as $P(A)$. This probability has the following interpretations:

There are three approaches to probability:

Relative Frequency

Counts the number of times an event (A) actually occurs, so that

$$P(A) = \frac{\text{number of times } A \text{ occurs}}{\text{number of times } A \text{ occurs} + \text{number of times it did not occur}} \tag{2.1a}$$

Example 2.1 Suppose that we perform an experiment in which we test 100 light bulbs. By the end of the test, six light bulbs failed. The probability that a light bulb fails the test is the relative frequency with which failure occurs. In this case

$$P(A) = \frac{\text{number of times } A \text{ occurs}}{\text{number of times } A \text{ occurs} + \text{number of times it did not occur}} = \frac{6}{6+94} = \frac{6}{100}$$

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

Classical

Events have an equal chance of occurring, so that

$$P(A) = \frac{\text{number of times } A \text{ occurs}}{\text{number of different sample events}} \tag{2.1b}$$

Example 2.2 In some situations, symmetry or other theoretical arguments also may be used to define probability. For example, one often assumes that you have a "fair" coin, then the probability of a coin flip resulting in "heads" is ½. Theoretically, in the long run, as you flip more and more times, the probability of a "heads" will *approach* ½. So, if you flip a fair coin 100 times, *on the average* you would expect

$$P(A) = \frac{\text{number of times } A \text{ occurs}}{\text{number of different sample events}} = \frac{50}{100} = \frac{1}{2}$$

Closer to reliability considerations, if one has two pieces of equipment, A and B, which are chosen from a lot of equipment of the same design and manufacture, one may assume that the probability that A fails before B is 1/2. If the hypothesis is doubted in either case, one must verify that the coin is true or that the pieces of equipment are identical by performing a large number of tests to which Eq. (2.2) may be applied.

Subjective

$P(A)$ is estimated based on previous experience, i.e. no way of counting the number of times A occurred, nor are all events of equal probability.

Example 2.3 It often happens in industry that when a new design is being started, and the reliability and safety implications are being

reviewed, no data is available. In situations like that, the experienced judgment of engineers will be used to give a subjective answer to questions such as

"how often will the temperature go beyond the limit of the part's capability during operation?"

or "Based on your judgment which of these suppliers has the least chance (read smallest probability) of producing a bad part?" These will be subjective judgments, to be used initially, and updated as testing and other data become available.

In reliability engineering, you will use probability at one time or another in all three of these approaches.

Therefore, in general terms, we can define the probability of X in any of the above forms, if N is the number of samples, and r is the number of failures, as repeated samples are taken:

$$P(X) = \lim_{N\to\infty} \frac{r}{N} \tag{2.2}$$

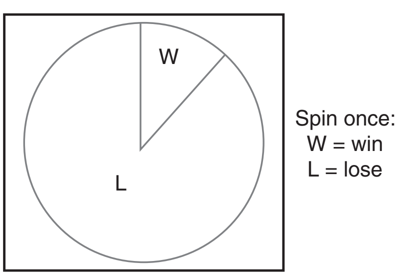


Figure 2.1 Spinner sample space with two outcomes (win, lose).

***Sample space* (*S*) = set of all possible outcomes**

e.g.

So, the set of all possible outcomes = sample space $(S) = (W, L)$, e.g. toss a fair coin (assume two faces per coin) (Figure 2.1)

S = (Heads, Tails)

***Outcome* (*e*) = an element of the sample space**

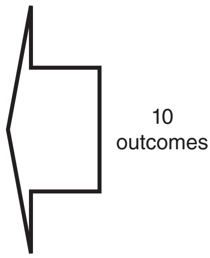
So, in the spin once example:

W is an outcome

L is also an outcome.

Table 2.1 Select 10 parts for inspection at random from a bin of parts.

Part	Defective	Good
1		×
2	×	
3		×
4		×
5		×
6		×
7	×	
8		×
9		×
10		×



In the toss coin example:

Tails is an outcome
Heads is another outcome.

Typical sample space in manufacturing (Table 2.1):

***Event* = A subset of outcomes**
Using the spin once example,

Define the sample space for spin twice:
Spin twice sample space (S) = (WW, WL, LW, LL)
where the outcomes are= WW, WL, LW, & LL
Now, an event is a subset of outcomes, and suppose that we use
Symbols A, B, C, D... for events. We can define events for the “spin twice” sample space.
For example, let
Event A = at least one W = (WW, WL, LW)
Event B = both spins are L = (LL)

In terms of probability, if all outcomes were equally likely,
$P(A) = 3/4$
$P(B) = 1/4$

Probability Axioms

$$\text{Probability}(outcome) \geq 0 \tag{2.3}$$

$$\sum \text{Prob}(all\ outcomes) = 1 \tag{2.4}$$

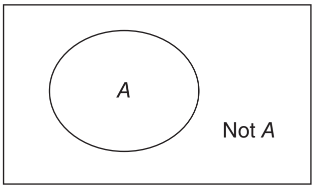


Figure 2.2 Complement of A, $(\overline{A})$ = NOT A

So, all probabilities are between 0 and 1 (Figures 2.2–2.5).

$$\text{Law of complement}: P(A) = 1 - P(\overline{A}) \quad (2.5)$$

$$\text{Addition Law}: P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad (2.6)$$

If A, B are mutually exclusive, $P(A \cap B) = 0$
Note: If A and B are mutually exclusive

$$P(A \cup B) = P(A) + P(B) \quad (2.7)$$

If A, B are independent, then

$$P(A \cap B) = P(A)\, P(B) \quad (2.8)$$

Conditional probability, written $P(A|B)$, means the probability that A occurs, given the "condition" that event B has already occurred.

$$P(A \mid B) = P(A \cap B)/P(B) \quad (2.9a)$$

or

$$P(A \cap B) = P(B)^{*} P(A \mid B) \quad (2.9b)$$

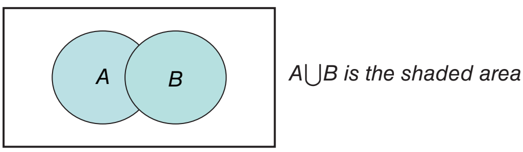


Figure 2.3 Union A ∪ B = A or B or both.

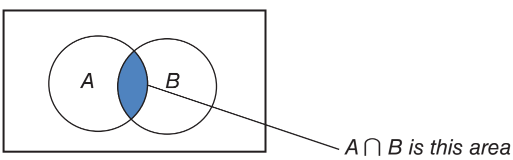


Figure 2.4 Intersection A ∩ B = A and B.

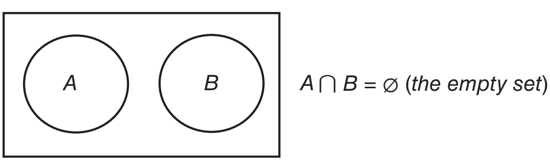


Figure 2.5 A and *B* are mutually exclusive means *A* and *B* cannot occur simultaneously.

Example 2.4 Suppose we know that the probability that the width of a machine-made part will be within specified bounds is 0.90, and the probability that its length will be within the bounds is 0.95. Suppose further that 80% of the parts are within specified bounds for length *and* width. Are the two events "width within bounds" and "length within bounds" independent?

Solution: Let $P(A) = 0.90$, $P(B) = 0.95$. Then, we need to check whether $P(A \cap B) = P(A)P(B)$ in this case.

Here, $(0.90)(0.95) = 0.855 \neq 0.80$. Therefore, the two events are not independent.

Example 2.5 An experiment results in one of the following events: $E1$, $E2$, $E3$, $E4$, or $E5$.

a) find $P(E3)$ if $P(E1) = 0.1$, $P(E2) = 0.3$, $P(E4) = 0.2$, $P(E5) = 0.1$
b) find $P(E3)$ if $P(E1) = P(E3)$, $P(E2) = 0.1$, $P(E4) = 0.2$, $P(E5) = 0.1$
c) find $P(E3)$ if $P(E1) = P(E2) = P(E4) = P(E5) = 0.1$

Solution:

Sum of all probabilities = 1; therefore,

$$P(E1) + P(E2) + P(E3) + P(E4) + P(E5) = 1$$

Then, a) $0.1 + 0.3 + P(E3) + 0.2 + 0.1 = 1$, so $P(E3) = 0.3$

b) $P(E1) + 0.1 + P(E3) + 0.2 + 0.1 = 1$, but $P(E1) = P(E3)$, $P(E3) + 0.1 + P(E3) + 0.2 + 0.1 = 1$, so $2P(E3) = 0.6$, and $P(E3) = P(E1) = 0.3$

c) $0.1 + 0.1 + P(E3) + 0.1 + 0.1 = 1$, $P(E3) = 0.6$.

Example 2.6

a) List the events in the sample space for this experiment (Figure 2.6).
b) Assign reasonable probabilities to the simple events.
c) Find the probability of each of the following events:
   A: (at least one system "works"),
   B: (Exactly one system works),
   C: (no system works)

Solution: (a) Sample space: where capital "W" indicates that a system "works," and capital "F" indicates that a system "fails."

(b) Eight outcomes, so the probability of each = 1/8.

(c) $P(A) = P$ (at least one system "works") = 7/8

$P(B) = P$ (exactly one system "works") = 3/8

$P(C) = P$ (no system "works") = 1/8.

(Moral of this example: if you can enumerate the sample space, you reduce your chances of an error!!).

See Table 2.2.

Figure 2.6 A machine consists of three linked systems: each system can "work" or "fail."

Table 2.2 All possible outcomes of a series of three components where each component either "fails" or "works."

	System	
X	Y	Z
W	W	W
W	W	F
W	F	W
W	F	F
F	W	W
F	W	F
F	F	W
F	F	F

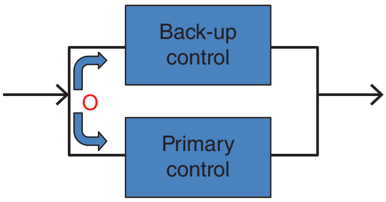


Figure 2.7 Primary and backup control configuration.

Example 2.7 Brand X aircraft manufacturing company has a backup control system that operates independently of the primary control. Each of the systems has a probability of 0.01 of failing on a particular mission. List the four events if we define the experiment to be observing the success or failure of the two operating systems. Now find the probability of the following events (Figure 2.7)**:**

A: (Both systems function properly)
B: (At least one of the systems fail)
C: (Exactly one of the systems fails)
D: (At least one system functions properly).

Solution: Construct a table with all outcomes of primary and backup control:

Primary control	Back-up control	P(System Working)
P(Works) = 0.99	P(Works) = 0.99	(0.99)*(0.99) = 0.9801
P(Works) = 0.99	P(Does not work) = 0.01	(0.99)*(0.01) = 0.0099
P(Does not work) = 0.01	P(Works) = 0.99	(0.01)*(0.99) = 0.0099
P(Does not work) = 0.01	P(Does not work) = 0.01	(0.01)*(0.01) = 0.0001

Figure 2.8 All possible outcomes for primary and backup control systems.

Then,

A: P(both systems functioning properly) $= 0.9801$
B: P(at least one of the systems failing) $= 1 - P$(none failing) $= 1 - 0.9801 = 0.0199$
C: P(exactly one of the systems failing) $= 0.0099 + 0.0099 = 0.0198$
D: P(at least one system functions properly) $= 1 - P$(none working) $= 1 - 0.0001 = 0.9999$

Example 2.7 Extended

Another useful way of tackling many probability problems is to draw a *probability tree*. For example, using the information on the backup and primary control, we illustrate the probability tree approach (Figure 2.9).

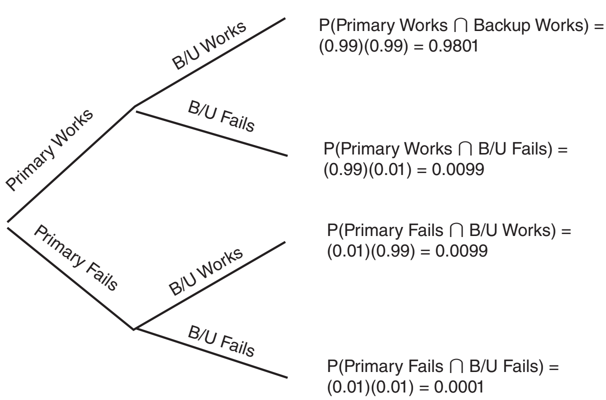


Figure 2.9 A probability tree approach works well when presenting results, in particular when there are more than two choices.

Example 2.8 The space shuttle had 12 O-rings. If any of the 12 rings fail, the shuttle would explode. If the probability of a single O-ring failing is 0.01, what is the probability of an explosion? Assume that the rings operate independently. Recalculate if the probability of a single O-ring failing is 0.001.

Solution:

(a) If P(O-ring failure) = 0.01

$$\begin{aligned}\text{Prob at least 1 O-ring fails} &= 1 - \text{Prob No O-rings fail}\\ &= 1 - [P(\text{O}_1\text{does not fail}) * P(\text{O}_2\text{does not fail}) * \cdots * P(\text{O}_{12}\text{does not fail})]\\ &= 1 - (0.99)^{12} \approx 0.113\\ &= 1 - (.99)^{12} \approx 0.113\end{aligned}$$

(b) If P(O-ring failure) = 0.001

$$\begin{aligned}\text{Prob at least 1 O-ring fails} &= 1 - \text{Prob No O-rings fail}\\ &= 1 - [P(\text{O}_1\text{does not fail}) * P(\text{O}_2\text{does not fail}) * \cdots * P(\text{O}_{12}\text{does not fail})]\\ &= 1 - (0.999)^{12} \approx 0.012\end{aligned}$$

When Challenger Flight 51-L exploded due to O-ring failure (January 28, 1986), there had been 1 failure in 25 missions, for a point estimate of 1/25 = 0.04. (Note: $0.113 > 0.04 > 0.012$.)

Example 2.9 A test was done on ultrasonic inspection kits to determine how effective they are in discovering microscopic cracks in aircraft parts. When a crack was present, the equipment signaled a crack of 98% of the time. There was a "false alarm" on 3% of the parts which had no cracks. Suppose that 5% of all the parts have a crack in them. If the percentages in the test can be assumed to be the true probabilities, find the probability that a part is really bad when a kit signals a crack.

Solution:

Let A = event that the part has a crack.
Let B vent ultrasonic inspection indicates a part has a crack.
Now,
$P(A) = 0.05$ (5 parts in 100 have a crack).
$P(B|A) = 0.98$ (the probability of a positive test, given a crack, is 0.98).
$P(B|\text{NOT } A) = 0.03$ (the probability of a false positive, given no crack, is 0.03).
$P(A|B)$ = ? (the probability of having a crack, given a positive test).

Table 2.3a Step one.

	A	Not A	Sum
B	$P(A \cap B)$	$P(\text{Not } A \cap B)$	$P(B)$
Not B	$P(A \cap \text{Not } B)$	$P(\text{Not } A \cap \text{Not } B)$	$P(\text{Not } B)$
	0.05	0.95	1.0

Table 2.3b Step two.

	A	Not A	Sum
B	0.049	0.0285	0.0775
Not B	$P(A \cap \text{Not } B)$	$P(\text{Not } A \cap \text{Not } B)$	$P(\text{Not } B)$
	0.05	0.95	1.0

Table 2.3c Final result.

	A	Not A	Sum
B	0.049	0.0285	0.0775
Not B	0.001	0.9215	0.9225
	0.05	0.95	1.0

The easiest way to visualize this the solution is in Table 2.3a

First, $P(A \cap B) = P(B|A)P(A) = (0.98)(0.05) = 0.049$

$P(\text{Not } A \cap B) = P(B|\text{Not } A)P(\text{Not } A) = (0.03)(0.95) = 0.0285$

After filling in the information from the two above equations into Table 2.3a, we have Table 2.3b and, finally Table2.3c is the finished calculation for this conditional probability problem.

Finally, the probability that a part is really bad, given an ultrasonic inspection indicates a crack:

$$P(A \mid B) = P(A \cap B)/P(B) = 0.049/0.0775 = 0.6322$$

Not intuitive, but given the data, when you have a positive test means that there is only a 63% chance of a crack in this case!

Example 2.10 Two circuit breakers of the same design each have a failure-to-open-on-demand probability of 0.02. It takes both to fail before the system fails. What is the probability of the system failure (a) if the failures are independent, and (b) if the probability of a second failure is 0.1, given the failure of the first? (c) In part a, what is the probability of one or more breaker failures on demand? (d) In part b, what is the probability of one or more failures on demand?

Solution: Let X = failure of first circuit breaker

Y = failure of second circuit breaker

Then, $P(X) = P(Y) = 0.02$

$$P(X \cap Y) = \; = P(X)P(Y) = 0.0004.$$

a) $P(Y|X) = 0.1$, so

$$P(X \cap Y) = P(Y \mid X)P(X) = 0.1 \times 0.02 \quad = 0.002.$$

$$P(X \cup Y) = P(X) + P(Y) - P(X)P(Y)$$
$$= 0.02 + 0.02 - (0.02)2 = 0.0396\,^{\cdot}$$

$$P(X \cup Y) = P(X) + P(Y) - P(Y \mid X)P(X)$$
$$= 0.02 + 0.02 - 0.1 \times 0.02 \quad = 0.038\,^{\cdot}$$

Example 2.11 A critical seam in an aircraft wing must be reworked if any one of the 28 identical rivets is found to be defective. Quality control inspections find that 18% of the seams must be reworked. (a) Assuming that the defects are independent, what is the probability that a rivet will be defective? (b) To what value must this probability be reduced if the rework rate is to be reduced below 5%?

Solution:

(a) Let x_i represent the failure of the ith rivet.

Then, since $P(x_1) = P(x_2) = \cdots = P(x_{28})$:

$$P(\text{at least 1 rivet being defective}) = 1\text{-}P(\text{no rivets being defective})$$
$$= 1\text{-}\{1\text{-}P(x_1)\}\{\{1\text{-}P(x_2)\}\cdots\{1\text{-}P(x_{28})\}$$
$$0.18 = 1\text{-}\{1\text{-P}(\text{x}_1)\}^{28}$$
$$0.82 = \{1\text{-P}(\text{x}_1)\}^{28}$$
$$P(x_1) = 1\text{-}(0.82)^{1/28} = 0.0071$$

(b) Since $0.05 = 1\text{-}\{1 - P(x_1)\}^{28}$

$$P(x_1) = 1\text{-}(0.95)^{1/28} = 0.0018$$

More Than Two Events

The foregoing equations state the axioms of probability and provide us with the means of combining two events. The procedures for combining events may be extended to three or more events, and the relationships may again be presented graphically as Venn diagrams. For example, in Figure 2.8a,b is shown, respectively, the intersection of *X, Y,* and *Z*, $X \cap Y \cap Z$, and the union of *X, Y,* and Z, $X \cup Y \cup Z$. The probabilities $P(X \cap Y \cap Z)$ and $P(X \cup Y \cup Z)$ may be interpreted as the cross-hatched areas.

The following observations are often useful in dealing with combinations of two or more events. Whenever we have a probability of a union of events, it may be reduced to an expression involving only the probabilities of the individual events and their intersection. The probability of the union of two events is an example of this ... $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. Similarly, probabilities of more complicated combinations involving unions and intersections may be reduced to expressions involving only probabilities of intersections. The intersections of events, however, may be eliminated only by expressing them in terms of conditional probabilities, as in $P(A \cap B = P(B|A)P(A)$, or if the independence may be assumed, they may be expressed in terms of the probabilities of individual events as in Eq. (2.8) (Figure 2.10).

The treatment of combinations of events is streamlined by using the rules of Boolean algebra listed in Table 2.4. If two combinations of events are equal according to these rules, their probabilities are equal. Thus, since according to Rule la (Table 2.4), $X \cap Y = Y \cap X$, we also have $P(X \cap Y) = P(Y \cap X)$. The communicative and associative rules are obvious. The remaining rules may be verified from a Venn diagram. For example, in Figure 2.11a, b, respectively, we show the distributive laws for $X \cap (Y \cup Z)$ and $X \cup (Y \cap Z)$.

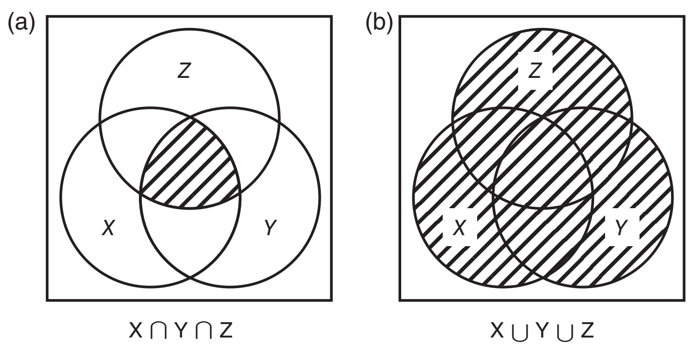


Figure 2.10 Venn diagrams for the intersection and union of three events.

Table 2.4 Rules of Boolean algebra.

(1a) $X \cap Y = Y \cap X$	Commutative law
(1b) $X \cup Y = Y \cup X$	
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$	Associative law
(2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	Distributive law
(3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	
(4a) $X \cap X = X$	Idempotent law
(4b) $X \cup X = X$	
(5a) $X \cap (X \cup Y) = X$	Law of absorption
(5b) $X \cup (X \cap Y) = X$	
(6a) $X \cap \widetilde{X} = \varphi^{a}$	Complementation
(6b) $X \cup \widetilde{X} = I^{a}$	
(6c) $\widetilde{\left(\widetilde{X}\right)} = X$	
(7a) $(\widetilde{X \cap Y}) = \widetilde{X} \cup \widetilde{Y}$	de Morgan's theorem
(7b) $(\widetilde{X \cup Y}) = \widetilde{X} \cap \widetilde{Y}$	
(8a) $\emptyset \cap X = \emptyset$	Operations with I
(8b) $\emptyset \cup X = X$	
(8c) $I \cap X = X$	
(8d) $I \cup X = I$	
(9a) $X \cup \left(\widetilde{X} \cap Y\right) = X \cup Y$	These relationships are unnamed
(9b) $\widetilde{X} \cap \left(X \cup \widetilde{Y}\right) = \widetilde{X} \cap \widetilde{Y} = (\widetilde{X \cup Y})$	

[a] $\emptyset$, null set; I, universal set.
Source: Adapted from Roberts et al. (1981).

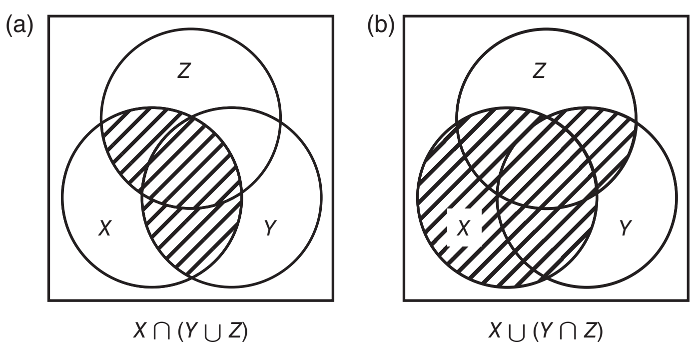


Figure 2.11 Venn diagrams for combinations of three vents.

Note that in Table 2.4, φ is used to represent the null event for which $P(\varphi) = 0$, and I is sometimes used to represent the universal event for which $P(I) = 1$.

Probabilities of combinations involving more than two events may be reduced to sums of the probabilities of intersections of events. If the events are also independent, the intersection probabilities may further be reduced to products of probabilities. These properties are illustrated with the following two examples.

Example 2.12 Express $P(X \cap (Y \cup Z))$ in terms of the probabilities of intersections of X, Y, and Z. Then, assume that X, Y, and Z are independent events and express the result in terms of $P(X)$, $P(Y)$, and $P(Z)$.

Solution: Rule 3a: $P(X \cap (Y \cup Z)) = P((X \cap Y) \cup (X \cap Z))$.

This is the union of two composites $X \cap Y$ and $Y \cap Z$. Therefore, from Eq. (2.6):

$$P(X \cap (Y \cup Z)) = P(X \cap Y) + P(X \cap Z) - P((X \cap Y) \cap (X \cap Z))$$

Associative rules 2a and 2b allow us to eliminate the parenthesis from the last term by first writing $(X \cap Y) \cap (X \cap Z) = (Y \cap X) \cap (X \cap Z)$ and then using Rule 4a to obtain

$$(Y \cap X) \cap (X \cap Z) = Y \cap (X \cap X) \cap Z = Y \cap X \cap Z = X \cap Y \cap Z$$

Utilizing these intermediate results, we have

$$P(X \cap (Y \cup Z)) = P(X \cap Y) + P(X \cap Z) - P(X \cap Y \cap Z)$$

If the events are independent, we may employ Eq. (2.6) to write

$$P(X \cap (Y \cup Z)) = P(X)P(Y) + P(X)P(Z) - P(X)P(Y)P(Z)$$

Example 2.13 Repeat Example 2.12 for $P(X \cup Y \cup Z)$.

Solution: From the associative law, $P(X \cup Y \cup Z) = P(X \cup (Y \cup Z))$. Since this is the union of event X and $(Y \cup Z)$, we use Eq. (2.6) to obtain $P(X \cup Y \cup Z) = P(X) + P(Y \cup Z) - P(X \cap (Y \cup Z))$ and again to expand the second term on the right as

$$P(Y \cup Z) = P(Y) + P(Z) - P(Y \cap Z)$$

Finally, we may apply the result from Example 2.2 to the last term, yielding $P(X \cup Y \cup Z) = P(X) + P(Y) + P(Z) - P(X \cap Y) - P(X \cap Z) - P(Y \cap Z) + P(X \cap Y \cap Z)$.

Applying the product rule for the intersections of independent events, we have

$P(X \cup Y \cup Z) = P(X) + P(Y) + P(Z) - P(X)P(Y) - P(X)P(Z) - P(Y)P(Z) + P(X)P(Y)P(Z)$

Often, we will have occasion to deal with intersections and unions of large numbers of n independent events: $X_1, X_2, X_3, ...X_n$. For intersections, the treatment is straightforward through the repeated application of the product rule:

$$P(X_1 \cap X_2 \cap \cap X_3 \cap \cdots \cap X_n) = P(X_1)P(X_2)P(X_3)\cdots P(X_n) \tag{2.10}$$

To obtain the probability for the union of these events, we first note that the union may be related to the intersection of the nonevents/complements

$$P(X_1 \cup X_2 \cup X_3 \cup \cdots X_n) + P\left(\overline{X}_1 \cup \overline{X}_2 \cup \overline{X}_3 \cup \cdots \overline{X}_n\right) = 1 \tag{2.11}$$

which may be visualized by drawing a Venn diagram for three or four events.

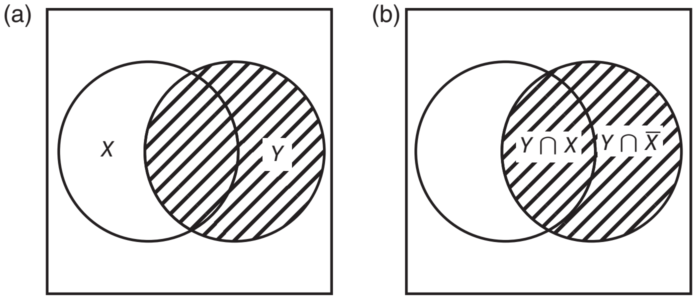


Figure 2.12 Venn diagram for total probability law.

Now, if we apply Eq. (2.9) to the independent $\overline{X}_i$, we obtain, after rearranging terms

$$P(X_1 \cup X_2 \cup X_3 \cup \cdots X_n) = 1 - P(\overline{X}_1)P(\overline{X}_2)P(\overline{X}_3)\cdots P(\overline{X}_n) \tag{2.12}$$

Finally, from Eq. (2.3) we must have for each $\overline{X}_i$,

$$P(\overline{X}_i) = 1 - P(X_i) \tag{2.13}$$

Thus, we have,

$$(X_1 \cup X_2 \cup X_3 \cup \cdots X_n) = 1 - [1 - P(X_1)][1 - P(X_2)] \\ [1 - P(X_3)]\cdots[1 - P(X_n)] \tag{2.14}$$

or more compactly

$$P(X_1 \cup X_2 \cup X_3 \cup \cdots X_n) = 1 - \prod_{i=1}^{n}[1 - P(X_i)] \tag{2.15}$$

This expression may also be shown to hold for the $\overline{X}$.

One other expression is very useful in the solution of certain reliability problems. It is sometimes referred to as the law of "total probability." Suppose that we divide a Venn diagram into regions of X and X as shown in Figure 2.12. We can always decompose the probability of Y, denoted by the circle, into two mutually exclusive contributions:

$$P(Y) = P(Y \cap X) + P(Y \cap \overline{X}) \tag{2.16}$$

Thus, using Eqs. (2.9a) and (2.9b), we have

$$P(Y) = P(Y \mid X)P(X) + P(Y \mid \overline{X})P(\overline{X}) \tag{2.17}$$

Example 2.14 A motor-operated relief valve opens and closes intermittently on demand to control the coolant level in an industrial process. An auxiliary battery pack is used to provide power for the approximately 1/2% of the time when there are plant power outages. The demand failure probability of the valve is found to be 3×10^{-5} when operated from the plant power and 9×10^{-5} when operated from the battery pack. Calculate the demand failure probability assuming that the number of demands is independent of the power source. Is the increase due to the battery pack operation significant?

Solution:

Let X signify a power outage. Then $P(X) = 0.005$ and $P(\overline{X}) = 0.995$.

Let Y signify value failure. Then $P(Y \mid \overline{X}) = 3 \times 10^{-5}$ and $P(Y|X) = 9 \times 10^{-5}$.
From Eq. (2.16), the value failure per demand is,

$$P(Y) = 9 \times 10^{-5} \times 0.005 + 3 \times 10^{-5} \times 0.095 = 3.03 \times 10^{-5}$$

The net increase in the failure probability over operation entirely with plant power is 1%.

Combinations and Permutations

We will be discussing arrangements of objects and the combinations and permutations of objects.
First, arrangements:

The number of ways of arranging *n* unlike objects in a line.

The number of ways of arranging n unlike independent objects in a line is $n!$*

For example, consider the letters A, B, C, and D. The number of ways of arranging the four letters is 4! = 24 (Figures 2.13a and 2.13b).

Checking this, the arrangements are:

ABCD ABDC ACBD ACDB ADCB ADBC
BCDA BCAD BDAC BDCA BACD BADC
CDBA CDAB CABD CADB CBAD CBDA
DABC DACB DBCA DBAC DCAB DCBA

Next, the number of ways of arranging in a line of n objects, of which ps are alike, is $n!/p!$. For example, given the letters A, A, A, and D, the 24 arrangements listed previously reduce to AAAD AADA ADAA DAAA or using the formula 4!/3! = 4.

$^*\mathbf{n}! = \mathbf{1} \times \mathbf{2} \times \mathbf{3} \times \cdots \times \mathbf{n}$

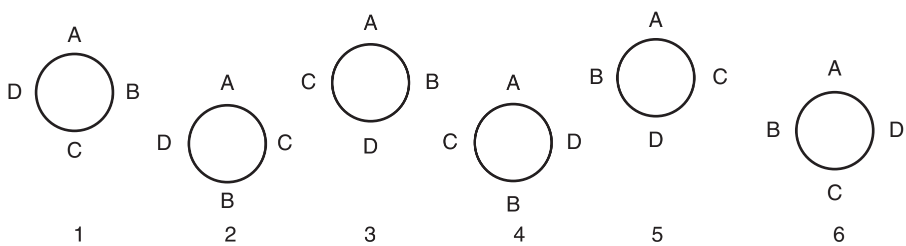
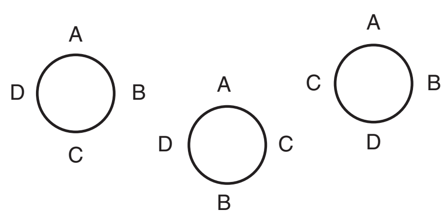


Figure 2.13a Illustration of the number of ways of arranging *A*, *B*, *C*, and *D* in a circle if clockwise and counterclockwise arrangements are considered different.

Figure 2.13b Illustration of the number of ways of arranging *A*, *B*, *C*, and *D* in a circle if clockwise and counterclockwise arrangements are considered the same.



Further, the number of ways of arranging in a line of n objects, of which ps of one type are alike, qs of a second type are alike, rs of a third type are alike, and so on, is $n!/(p!q!r!...)$.

Another step further, the number of ways of arranging n unlike objects in a ring when clockwise and counterclockwise arrangements are different is $(n-1)!$

For example, consider four people A, B, C, and D, who are seated at a round table. To find the number of different arrangements, we fix A and then consider the number of ways of arranging B, C, D, or $(4-1)! = 3! = 6$.

One more step: Notice that in the above example, we have six arrangements, but 1&6, 2&4, and 3&5 are simply clockwise–counterclockwise of each other.

When this happens, the number of ways of arranging n unlike objects in a ring, when clockwise and counterclockwise arrangements are the same, is $(n-1)!/2$.

Example 2.15 Given a "rainbow" wheel of 36 blades, with 4 different vendors (9 blades each):

1. How many ways can these 36 blades be arranged in this wheel?

Solution: $(36-1)!/2 = 35!/2$.

2. How many ways can these 36 blades be arranged in this wheel, considering the 4 vendors?

Solution: $(36-1)!/(9!9!9!8!)$.

Bladed disk[1]

A *permutation* of N different objects taken R at a time is an arrangement of R out of the N objects *with* ***attention given to the order of arrangement.***

Written:

$$_NP_R = \frac{N!}{(N-R)!}, \textit{where } N! = 1 \times 2 \times 3 \times \cdots \times \text{N}, \quad \text{and } 1! = 1 \text{ and } 0! = 1 \tag{2.18}$$

Example 2.16 How many ways can five parts be selected randomly from a bin of 100 parts when order is important?

(Note: $P_{11}\ P_{23}\ P_{41}\ P_{68}\ P_{96}$ and $P_{96}\ P_{23}\ P_{41}\ P_{68}\ P_{11}$ are different events.)

Solution:

$$_{100}P_5 = \frac{100!}{(100-5)!} = \frac{100!}{95!} = \frac{100 \times 99 \times 98 \times 97 \times 96 \times 95!}{95!} = 903,450,240$$

A *combination* of N different objects taken R at a time is a selection of R out of the N objects with **NO attention given to the order of arrangement**.

1 en.wikipedia.org

Written:

$$
{}_N C_R = \frac{N!}{R!(N-R)!}, \text{where } N! = 1 \times 2 \times 3 \times \cdots \times \text{N}, \\
\text{and } 1! = 1 \text{ and } 0! = 1 \tag{2.19}
$$

Example 2.17 How many ways can 5 parts be selected randomly from a bin of 100 parts when order is NOT important?

(Note: $P_{11}\ P_{23}\ P_{41}\ P_{68}\ P_{96}$ and $P_{96}\ P_{23}\ P_{41}\ P_{68}\ P_{11}$ are the same event.)

Solution:

$$
{}_{100}C_5 = \frac{100!}{5!(100-5)!} = \frac{100!}{5!95!} = \frac{100 \times 99 \times 98 \times 97 \times 96 \times 95!}{(1 \times 2 \times 3 \times 4 \times 5)95!} = 7,528,752
$$

2.3 Discrete Random Variables

Frequently, in reliability considerations, we need to know the probability that a specific number of events will occur, or we need to determine the average number of events that are likely to take place. For example, suppose that we have a computer with N memory chips, and we need to know the probability that none of them, that one of them, two of them, and so on, will fail during the first year of service. Or suppose that there is a probability p that a Christmas tree light bulb will fail during the first 100 hours of service. Then, on a string of 25 lights, what is the probability that there will be n $(0 \leq n \leq 25)$ failures during this 100-hour period? To answer such reliability questions, we need to introduce the properties of discrete random variables. We do this first in general terms, before treating two of the most important discrete probability distributions.

Properties of Discrete Variables

A discrete random variable is a variable that can only take on a countable number of values. We refer to such a variable with the bold-faced character $\boldsymbol{x}$, and denote by x_n the values to which it may be equal. In most cases, these values are integers so that $x_n = n$. By random variables, we mean that there is associated with each x_n a probability $f(x_n)$ that $\mathbf{x} = x_n$. We denote this probability as

$$
f(x_n) = P(\mathbf{x} = x_n) \tag{2.20}
$$

We will, for example often be concerned with counting numbers of failures (or of successes). Thus, we may let $\mathbf{x}$ signify the number n of failures in N tests. Then, $f(0)$ is the probability that there will be no failure, $f(1)$ the probability of one failure, and so on. Based on what we have shown in the probability axioms, the probabilities of all the possible outcomes must add to one

$$
\sum f(x_n) = 1 \tag{2.21}
$$

where the sum is taken over all possible values of $x_{n.}$ Eq. (2.21) is often referred to as the *normalization condition*.

The function $f(x_n)$ is referred to as the probability mass function (**PMF**) of the discrete random variable **x**. A second important function of the random variable is the *cumulative distribution function* **(CDF)** defined by

$$F(x_n) = P(\mathbf{x} \leq \mathbf{x_n}) \tag{2.22}$$

the probability that the value of x will be less than or equal to the value x.

Clearly, it is just the sum of probabilities:

$$F(x_n) = \sum_{i=0}^{n} f(x_i) \tag{2.23}$$

Closely related is the *complementary cumulative distribution function* (CCDF), defined by

$$\overline{F}(x_n) = 1 - F(x_n) = 1 - \sum_{i=0}^{n} f(x_i) = \sum_{i=n+1}^{N} f(x_i), \tag{2.24}$$

where x_N is the largest value for which $f(x_n) > 0$.

It is often convenient to display discrete random variables as bar graphs of the PMF. Thus, if we have, for example the discrete random variable

$$f(0) = 0, f(l) = 1/16, f(2) = ¼, f(3) = 3/8, f(4) = ¼, f(5) = 1/16$$

whose PMF may be plotted as in Figure 2.14a. Similarly, from Eq. (2.23) the bar graph for the CDF appears as in Figure 2.14b.

Several important properties of the random variable **x** are defined in terms of the PMF $f(x_n)$.

The mean value, μ, of **x is**

$$\mu = \sum_n x_n f(x_n) \tag{2.25}$$

and the variance of x is

$$\sigma^2 = \sum_n (x_n - \mu)^2 f(x_n) = \sum_n x_n^2 f(x_n) - \mu^2 \tag{2.26}$$

The mean is a measure of the expected value or central tendency of **x** when a very large sampling is made of the random variable, whereas the variance is a measure of the scatter or dispersion of the individual values of x_n about μ. It is also sometimes useful to talk about the most probable value of **x**, the *mode*, the value of x_n for which the largest value of $f(x_n)$ occurs, assuming that there is only one largest value. Finally, the median value is defined as that value $\mathbf{x} = x_n$ for which the probability of obtaining a smaller value is 1/2:

$$\sum_{i \geq n} f(x_i) = \frac{1}{2}, \text{ and also, } \sum_{i \leq n} f(x_i) = \frac{1}{2} \tag{2.27}$$

Example 2.18 A discrete probability distribution is given by

$$f(x_n) = An \quad \text{for } n = 0, 1, 2, 3, 4, 5$$

a) Determine A.
b) What is the probability that $x \leq 3$?
c) What is μ?
d) What is σ?

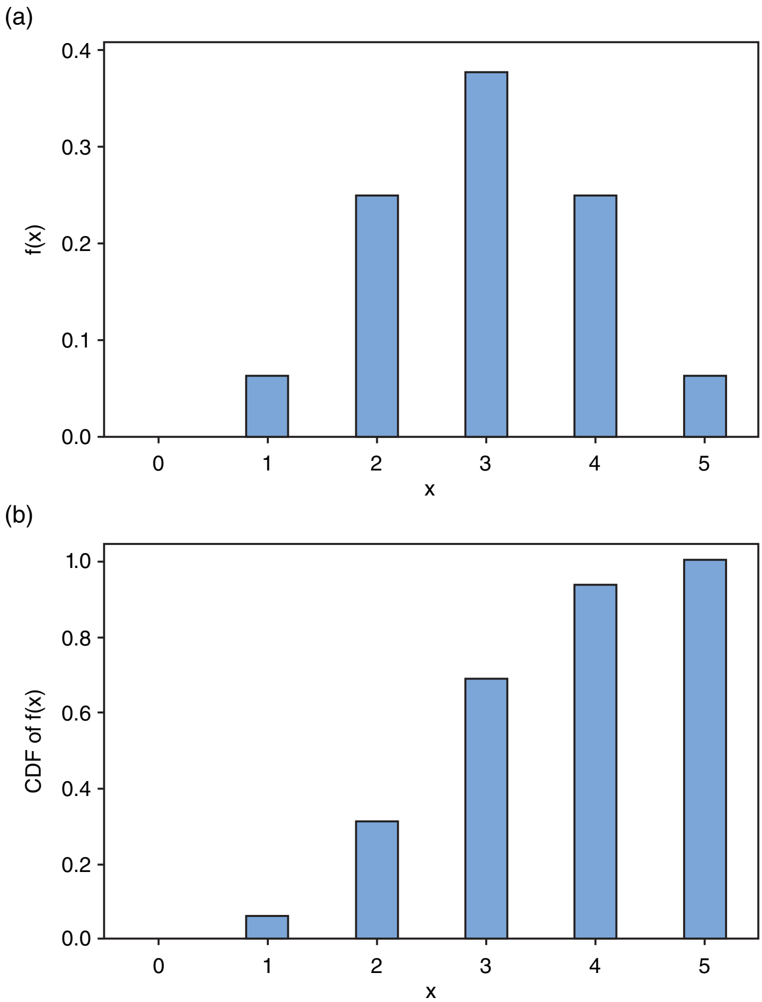


Figure 2.14 Discrete probability distribution: (a) probability mass function (PMF) and (b) the corresponding cumulative distribution function (CDF).

Solution:

(a) From Eq. (2.21):

$$1 = \sum_{n=0}^{5} An = A(0 + 1 + 2 + 3 + 4 + 5) = 15A$$

$$A = \frac{1}{15}$$

(b) From Eqs. (2.22) and (2.23):

$$P\{x \le 3\} = F(3) = \sum_{n=0}^{3} \frac{n}{15} = \frac{1}{15}(0 + 1 + 2 + 3) = \frac{6}{15} = \frac{2}{5}$$

(c) From Eq. (2.25): $\mu = \sum_{n=0}^{5} n\left(\frac{n}{15}\right) = \frac{1}{15}(0 + 1 + 4 + 9 + 16 + 25) = \frac{11}{3}$.

(d) Using Eq. (2.26),

$$\sigma^2 = \sum_n (x_n - \mu)^2 f(x_n) = \sum_n x_n^2 f(x_n) - \mu^2$$

First,

$$\sum_{n=0}^{5} x_n^2 f(x_n) = \sum_{n=0}^{5} n^2 An = \sum_{n=0}^{5} n^3 \frac{1}{15} = \frac{1}{15}(0 + 1 + 8 + 27 + 64 + 125) = 15$$

Then,

$$\sigma^2 = 15 - \mu^2 = 15 - \left(\frac{11}{3}\right)^2 = 1.555$$

$$\sigma = 1.247$$

The idea of the expected value is an important one. In general, if there is a function $g(x_n)$ of the random variable x, the expected value $E(g)$ is defined for a discrete random variable as

$$E(g) = \sum_i g(x_i) f(x_i) \tag{2.28}$$

Thus, the mean and variance given by Eqs. (2.22) and (2.23) may be written as

$$\mu = E(x) = \sum_n x_n f(x_n) \tag{2.29}$$

$$\sigma^2 = E\{(x - \mu)^2\} = \sum_n (x_n - \mu)^2 f(x_n) \tag{2.30a}$$

or

$$\sigma^2 = \sum_n x_n^2 f(x_n) - \mu^2 = E(x^2) - \mu^2 \tag{2.30b}$$

The quantity $\sigma = \sqrt{\sigma^2}$ is referred to as the standard deviation of the distribution. The notion of expected value and variance is also applicable to the continuous random variables discussed in the following chapter.

The Binomial Distribution

The binomial distribution is the most widely used discrete distribution in reliability engineering. To derive it, suppose that p is the probability of failure for some piece of equipment in a specified test and

$$q = 1 - p \tag{2.31}$$

is the corresponding success (i.e. nonfailure) probability. If such tests are truly independent of one another, they are referred to as Bernoulli trials. A discrete random variable is a Bernoulli trial if it can take on only the values zero and one. Bernoulli random variables are used to model events having two possible outcomes. For example:

- Coin toss ($p = 0.5$, $q = 0.5$)
- O-ring failure on Space Shuttle Solid Rocket booster ($p = 0.04$, $q = 0.96$)

In summary, a series of Bernoulli trials, each independent of the other trials, and each having the same probability of success, makes up a binomial distribution. With parameters:

n = number of trials
p = probability of failure
$q = 1 - p$ = probability of success
If such tests are truly independent of one another, they are referred to as Bernoulli trials.
We wish to derive the probability

$$f(n) = P\{\mathbf{n} = n \mid N, p\} \tag{2.32}$$

that in N independent tests, there are n failures. To arrive at this probability, we first consider the example of the test of two units of identical design and construction. The tests must be independent in the sense that success or failure in one test does not depend on the result of the other. There are four possible outcomes, each with an associated probability: qq is the probability that neither unit fails, pq the probability that only the first unit fails, qp the probability that only the second unit fails, and pp the probability that both units fail. Since these are the only possible outcomes of the test, the sum of the probabilities must equal 1. Indeed,

$$p^2 + 2pq + q^2 = (p + q)^2 = 1 \tag{2.33}$$

and by the definition of Eq. (2.2)

$$f(0) = q^2,\ f(1) = 2pq,\ f(2) = p^2 \tag{2.34}$$

In a similar manner, the probability of n independent failures may also be covered for situations in which a larger number of units undergo testing. For example, with $N = 3$, the probability that all three units fail independently is obtained by multiplying the failure probabilities of the individual units together. Since the units are identical, the probability that none of the three fails is qqq. There are now three ways in which the test can result in one unit failing: the first fails, pqq; the second fails, qpq; or the third fails, qqp. There are also three combinations that lead to two units failing: units 1 and 2 fail, ppq; units 1 and 3 fail, pqp; or units 2 and 3 fail, qpp. Finally, the probability of all three units failing is ppp.

In the three-unit test, the probabilities for the eight possible outcomes must again add to 1. This is indeed the case, for by combining the eight terms into four, we have

$$q^3 + 3q^2p + 3qp^2 + p^3 = (q + p)^3 = 1 \tag{2.35}$$

The probabilities of the test resulting in 0, 1, 2, or 3 failures are just the successive terms on the left:

$$f(0) = q^3, \quad f(1) = 3q^2p, \quad f(2) = 3qp^2, \quad f(3) = p^3 \tag{2.36}$$

The foregoing process may be systematized for tests of any number of units. For N units, Eq. (2.36) generalizes to

$$_NC_0q^N + {}_NC_1pq^{N-1} + {}_NC_2p^2q^{N-2} + \cdots + {}_NC_{N-1}p^{N-1}q + {}_NC_Np^N = (q + p)^N = 1 \tag{2.37}$$

since $q = 1 - p$. For this expression to hold, it may be shown that the $_NC_n$ must be the binomial coefficients. These are given by

$$_NC_n = \frac{N!}{(N-n)!n!}, \quad \textit{where}\ \ N!(\text{“}N\text{”factorial}) = 1 \times 2 \times 3 \times \cdots \times N \tag{2.38}$$

Table 2.5 Pascal's triangle.

								1									$N = 0$
							1		1								$N = 1$
						1		2		1							$N = 2$
					1		3		3		1						$N = 3$
				1		4		6		4		1					$N = 4$
			1		5		10		10		5		1				$N = 5$
		1		6		15		20		15		6		1			$N = 6$
	1		7		21		35		35		21		7		1		$N = 7$
1		8		28		56		70		56		28		8		1	$N = 8$

A convenient way to tabulate these coefficients is in the form of Pascal's triangle; this is shown in Table 2.5. Just as in the case of $N = 2$ or 3, the $N + 1$ terms on the left-hand side of Eq. (2.37) are the probabilities that there will be 0, 1, 2,..., N failures. *Thus, the PMF for the binomial distribution is*

$$f(n) = {}_NC_n p^n (1 - p)^{N-n}, \quad n = 0, 1, \ldots, N \tag{2.39}$$

That the condition Eq. (2.21) is satisfied follows from Eq. (2.37). *The CDF corresponding to f(n) is*

$$F(n) = \sum_{n'=0}^{n} {}_NC_{n'} p^{n'} (1 - p)^{N-n'} \tag{2.40}$$

and of course if we sum over all possible values of n' as indicated in Eq. (2.21), we must have

$$\sum_{n=0}^{n} {}_NC_n p^n (1 - p)^{N-n} = 1 \tag{2.41}$$

The mean of the binomial distribution is

$$\mu = Np \tag{2.42}$$

and the variance is

$$\sigma^2 = Np(1 - p) \tag{2.43}$$

The proof of Eqs. (2.42) and (2.43) requires some manipulation of the binomial terms. From Eqs. (2.25) and (2.39), we see that

$$\mu = \sum_{n=1}^{N} (n)_N C_n p^n (1 - p)^{N-n} \tag{2.44}$$

where the $n = 0$ term vanishes and therefore is eliminated. Making the substitutions $M = N - 1$ and $m = n - 1$, we may rewrite the series as

$$\mu = p \sum_{m=0}^{N} (m + 1)_{M+1} C_{m+1} p^m (1 - p)^{M-m} \tag{2.45}$$

Since it is easily shown that

$$(m + 1)_{M+1} C_{m+1} = (M + 1)_M C_m \tag{2.46}$$

we may write

$$\mu = (M+1)p \sum_{m=0}^{M} {}_M C_m p^m (1-p)^{M-m} \tag{2.47}$$

However, Eq. (2.41) indicates that the sum on the right is equal to 1. Therefore, noting that $M + 1 = N$, we obtain the value of the mean given by Eq. (2.42).

To obtain the variance, we begin by combining Eqs. (2.26), (2.39), and (2.42)

$$\sigma^2 = p \sum_{n=1}^{N} n^2 {}_N C_n p^n (1-p)^{N-n} - N^2 p^2 \tag{2.48}$$

Employing the same substitutions for N and n, and utilizing Eq. (2.46), we obtain

$$\sigma^2 = (M+1)p \left\{ \sum_{m=0}^{M} m {}_M C_m p^m (1-p)^{M-m} + \sum_{m=0}^{M} {}_M C_m p^m (1-p)^{M-m} \right\} - N^2 p^2 \tag{2.49}$$

But from Eqs. (2.41) and (2.44), we see that the first of the two sums is just equal to Mp, and the second is equal to 1. Hence,

$$\sigma^2 = (M+1)p(Mp+1) - N^2 P^2 \tag{2.50}$$

Finally, since $M = N - 1$, this expression reduces to Eq. (2.43).

Example 2.19 Suppose that $N = 10$, p = probability of the event = 0.08, q = probability of no event = 1 − p = 0.92, $\mu = Np = 10(0.08) = 0.8$, and variance = $Npq = 10(0.08)(0.92) = 0.736$.

So, $\sigma = (0.736)^{0.5} = 0.858$

Let us look at $P(x \text{ out of N}) = \frac{N!}{x!(N-x)!} p^x q^{(N-x)}$ for $x = 0$ to 10:

P(0 in 10)	=	$(1)(0.08)^0(0.92)^{10}$	=	0.434
P(1 in 10)	=	$(10)(0.08)^1(0.92)^9$	=	0.378
P(2 in 10)	=	$(45)(0.08)^2(0.92)^8$	=	0.148
P(3 in 10)	=	$(120)(0.08)^3(0.92)^7$	=	0.034
P(4 in 10)	=	$(210)(0.08)^4(0.92)^6$	=	0.005
P(5 in 10)	=	$(252)(0.08)^5(0.92)^5$	=	0.001
P(6 in 10)	=	$(210)(0.08)^6(0.92)^4$	=	0.000
P(7 in 10)	=	$(120)(0.08)^7(0.92)^3$	=	0.000
P(8 in 10)	=	$(45)(0.08)^8(0.92)^2$	=	0.000
P(9 in 10)	=	$(10)(0.08)^9(0.92)^1$	=	0.000
P(10 in 10)	=	$(1)(0.08)^{10}(0.92)^0$	=	0.000
		$\sum$ all Probabilites	=	1.000 ✔

Note: With an expected value of 0.8, the P(0 events) = 0.43. So, the probability of 1 or more events = 1 − 0.43 = 0.57.

Note: The sum of every probability distribution must be 1.0 (Eq. 2.4).

Example 2.20 Ten compressors with a failure probability $p = 0.1$ are tested. (a) What is the expected number of failures $E(n)$? (b) What is σ^2? (c) What is the probability that none will fail? (d) What is the probability that two or more will fail?

Solution:

(a)

$$E(n) = \mu = Np = 10 \times 0.1 = 1$$

(b)

$$\sigma^2 = Np(1-p) = 10 \times 0.1(1-0.1) = 0.9$$

(c)

$$P(n = 0 \mid 10, p) = f(0) = {}_{10}C_0(p)^0(q)^{(10\text{-}0)} = 1 \times 1 \times (0.9)^{(10\text{-}0)} = 0.349$$

(d)

$$P(n^3 2 \mid 10, p) = \text{1-}P(n < 2 \mid 10, p) = \text{1-}\sum_{i=0}^{x} {}_nC_i(p)^i(q)^{(n-i)}$$
$$= \text{1-}{}_{10}C_0(0.1)^0(0.9)^{(10\text{-}0)} + {}_{10}C_1(0.1)^1(0.9)^{(10\text{-}1)}$$
$$= \text{1-}\{0.349 + 10(0.1)(0.387)\} = 0.264$$

Example 2.21 A parts manufacturer has determined that 30% of all parts installed last year are defective.

If 15 parts are inspected at random from all parts installed last year, what is the probability that more than 10 of the 15 will have defects?

Solution:

$$\text{P}(> 10 \text{ are defective}) = \sum_{i=11}^{15} {}_{15}C_i(.3)^i(.7)^{15-i} = {}_{15}C_{11}.3^{11}.7^4 + {}_{15}C_{12}.3^{12}.7^3 +$$
$${}_{15}C_{13}.3^{13}.7^2 + {}_{15}C_{14}.3^{14}.7^1 + {}_{15}C_{15}.3^{15}.7^0 = .000672$$

Using EXCEL™: $N = 15$, $p = 0.3$.
Type this in any cell: =1-BINOMDIST(10,15,0.30,TRUE).
TRUE indicates that cumulative answer will appear in the cell: =0.00067223.

The Poisson Distribution

Situations in which the probability of failure p becomes very small, but the number of units tested, N, is large, are frequently encountered. The binomial distribution can be approximated by the Poisson distribution, when N is very large and p is very small such that their product Np is a finite quantity. For practical purposes, N has to be greater than 30, and p has to be smaller than 0.1.

Poisson distribution was introduced by the French mathematician, engineer, and physicist Simeon Denis. Poisson is a distribution of rare events, i.e. the events whose probability of occurrence is very small, but the number of trials, which could lead to the occurrence of the event, are very large. Generally speaking, the Poisson distribution is used to model the probability of a given number of events occurring in a fixed interval of time or space if these events occur with a known constant rate and independently of the time since the last event. The Poisson distribution can also be used for the number of events in other specified intervals such as distance, area, and volume.

Specific examples of the use of the Poisson modeling include (1) the number of commercial air accidents in a year, (2) the number of telephone calls coming into a large office every minute, (3) the defects per square foot in a composite sheet of material, (4) the number of horse kick deaths in the Prussian Cavalry, and (5) the number of bacteria in a certain amount of liquid.

The Poisson distribution may be shown to result from taking the limit of the binomial distribution as $p \to 0$ and $N \to \infty$, with the product Np remaining constant. To obtain the distribution we first multiply the binomial PDF given by Eq. (2.39) by N^n/N^n and rearrange the factors to yield

$$f(n) = \left\{\frac{N!}{(N-n)!N^n}\right\}(1-p)^{-n}\frac{(Np)^n}{n!}(1-p)^N \tag{2.51}$$

Now assume that $p \ll 1$ so that we may write $\ln(1-p) \approx -p$, and hence, the last factor becomes

$$(1-p)^N = \exp[N\ln(1-p)] \approx e^{-Np} \tag{2.52}$$

Likewise, as p becomes vanishingly small $(1 - p) - n \to 1$ for finite n, and as $N \to \infty$, we have

$$\frac{N!}{(N-n)!N^n} = \left(1-\frac{n-1}{N}\right)\left(1-\frac{n-2}{N}\right)\dots\left(1-\frac{1}{N}\right)1 \to 1 \tag{2.53}$$

Hence, as $p \to 0$ and $N \to \infty$, with $Np = \mu$, Eq. (2.51) reduces to

$$f(n) = \frac{\mu^n}{n!}e^{-\mu} \tag{2.54}$$

which is the PMF for the Poisson distribution.

Unlike the binomial distribution, the Poisson distribution can be expressed in terms of a single parameter, μ. Thus, $f(n)$ may be written as the probability

$$P\{\mathbf{n} = n \mid \mu\} = \frac{\mu^n}{n!}e^{-\mu}, \quad n = 0, 1, 2, 3, \dots \tag{2.55}$$

The normalization condition, Eq. (2.21), must, of course, be satisfied. This may be verified by first recalling the power series expansion for the exponential function

$$e^{\mu} = \sum_{n=0}^{\infty}\frac{\mu^n}{n!} \tag{2.56}$$

Thus, we have

$$\sum_{n=0}^{\infty} f(n) = \sum_{n=0}^{\infty}\frac{\mu}{n!}e^{-\mu} = e^{\mu}e^{-\mu} = 1 \tag{2.57}$$

In the foregoing equations, we have chosen $Np = \mu$ because it may be shown to be the mean of the Poisson distribution. From Eqs. (2.54) and (2.56), we have

$$\sum_{n=0}^{\infty} nf(n) = \sum_{n=0}^{\infty} n\frac{\mu}{n!}e^{-\mu} = \mu \tag{2.58}$$

Likewise, since it may be shown that

$$\sum_{n=0}^{\infty} n^2 f(n) = \sum_{n=0}^{\infty} n^2\frac{\mu}{n!}e^{-\mu} = \mu(\mu+1) \tag{2.59}$$

we may use Eq. (2.30b) to show that the variance is equal to the mean,

$$\sigma^2 = \mu \tag{2.60}$$

Example 2.22 Horse kick deaths in Polish Cavalry.

Event: A cavalry man being killed by a horse kick per year per army corps. Data: 122 deaths in 200 corps years, enumerated in Table 2.6a.

Does a Poisson distribution explain this data?

Solution:

Table 2.6a Observed deaths by corp year.

Obs deaths/army corps/year	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Corps years with Obs deaths	109	65	22	3	1	0	0

Ten army corps, 20 years = 200 corps years.

Average $= \mu = 122/200 = 0.61$

Probability Calculation	Expected Number
$P(0) = \quad e^{-0.61} = 0.543$	$0.543 \times 200 = 109$
$P(1) = 0.61\,e^{-0.61} = 0.331$	$0.331 \times 200 = 66.3$
$P(2) = \dfrac{0.61^2}{2!}e^{-0.61} = 0.101$	$0.101 \times 200 = 20.2$
$P(3) = - - - - - = 0.021$	$0.021 \times 200 = 4.1$
$P(4) = - - - - - = 0.003$	$0.003 \times 200 = 0.6$

Table 2.6b shows that the Poisson distribution is a good predictor of horse kick deaths in the Polish Cavalry.

Table 2.6b Summary comparison of observed vs Poisson predicted.

Obs deaths/army corps/year	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Corps years with Obs deaths	109	65	22	3	1	0	0
Poisson expected	109	66.3	20.2	4.1	0.6	0	0

Example 2.23 Do the preceding 10-compressor example (Example 2.20) approximating the binomial distribution by a Poisson distribution. Compare the results.

Solution:

a) $\mu = Np = 1$.
b) $\sigma^2 = \mu = 1$ **(0.9 for binomial)**.
c) $P(\mathbf{n} = 0|\mu = 1) = e^{-\mu} = 0.3678$ **(0.3874 for binomial)**.
d) $P(n \geq 2|\mu = 1) = 1 - f(0) - f(1) = 1 - 2e^{-\mu} = 0.2642$ **(0.2639 for binomial)**.

Example 2.24 Suppose that a Lyme disease has an incidence of 1 in 1000 person-years. Assuming that members of the population are affected independently, find the probability of exactly 0, 10, or 20 cases in a population of 10,000 (over the next year).

Table **2.7** EXCEL solution to Example 2.24.

x	*P* (exactly *x*)	*P*(Σ(0 – *X*)Poisson)
0	4.53999E−05	4.53999E−05
10	0.125110036	0.58303975
20	0.001866081	0.998411739
Showing equations		
x	Exactly *x*	Cumulatively by *x*
0	POISSON(H17, 10, FALSE)	POISSON(H17, 10, TRUE)
10	POISSON(H18, 10, FALSE)	POISSON(H18, 10, TRUE)
20	POISSON(H19, 10, FALSE)	POISSON(H19, 10, TRUE)

Solution:

The expected value (mean) = $\mu = (1/1000) \times 10{,}000 = 10$.

Ten new cases expected in this population over the next year,

$$f(x) = \frac{e^{-\mu}\mu^x}{x!}$$

$$\text{for } x = 0,\ f(0) = \frac{e^{-10}10^0}{0!} = 0.0000454$$

$$\textit{for } x = 10, f(10) = \frac{e^{-10}10^{10}}{10!} = 0.125$$

$$\textit{for } x = 20, f(20) = \frac{e^{-10}10^{20}}{20!} = 0.0019$$

The solution is shown in Table 2.7.

Confidence Intervals

Motivation for Confidence Intervals

Suppose that we want to estimate the failure probability p of a system and also gain some idea of the precision of the estimate. Our experiment consists of testing N units for failure, with the assumption that the N units are drawn randomly from a much larger population. If there are r failures, the failure probability, defined by Eq. (2.2), may be estimated by

$$\hat{p} = r/N \tag{2.61}$$

We use the caret to indicate that $\hat{p}$ is an estimate, rather than the true value p. It is referred to as a *point estimate* of p, since there is no indication of how close it may be to the true value.

The difficulty, of course, is that if the test is repeated, a different value of r, and therefore of $\hat{p}$, is likely to result. The number of failures is a random variable that obeys the binomial distribution discussed in the preceding section. Thus, $\hat{p}$ is also a random variable. We may define a PMF as

$$P\{\hat{\mathbf{p}} = \hat{p}_r \mid N, p\} = f(\hat{p}_r) \quad r = 0, 1, 2, \ldots N \tag{2.62}$$

where $\hat{p}_n = r/N$ is just the value taken on by $\hat{\mathbf{p}}$ when there are r failures in N trials. The PMF is just the binomial distribution given by Eq. (2.34)

$$f(\hat{p}_r) = C_r^N p^r (1-p)^{N-r} \tag{2.63}$$

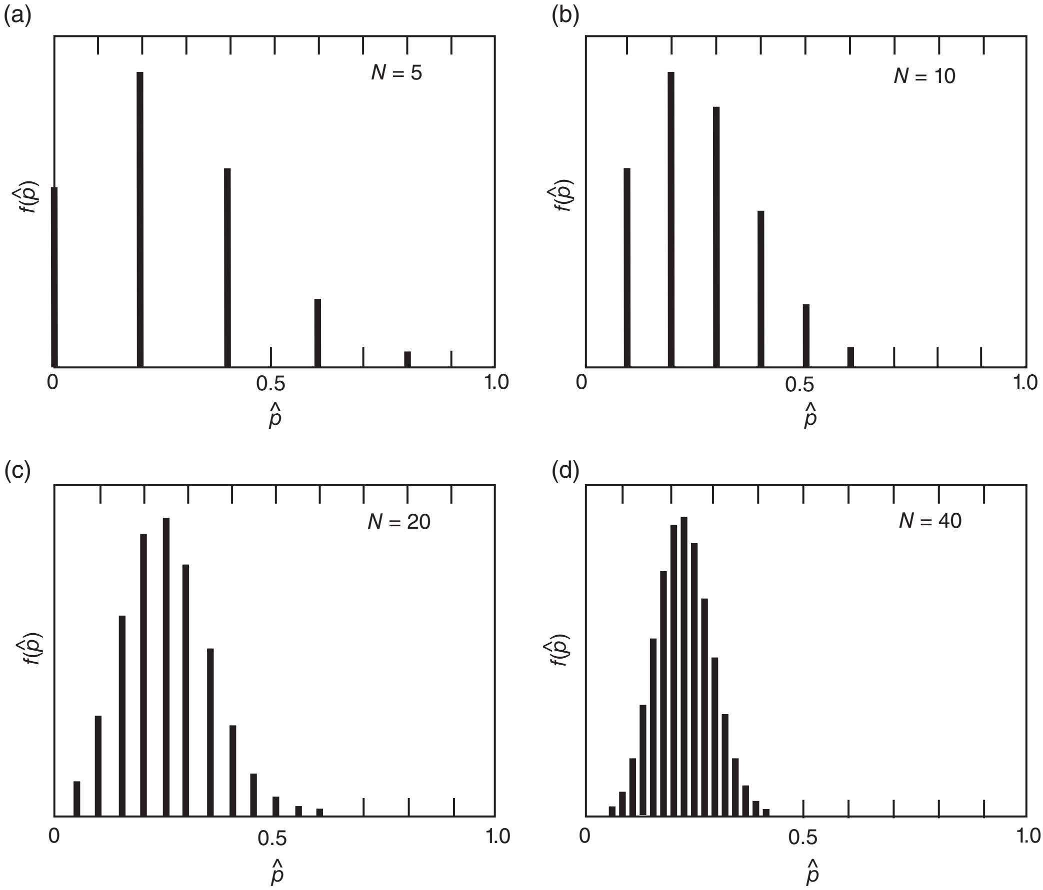


Figure 2.15 Probability mass function for binomial distribution where $p = 0.25$.

This PMF indicates that the probability for obtaining a particular value $\hat{p}_r$ from our test is just $f(\hat{p}_r)$, given that the true value is p.

For a specified value of p, we may gain some idea of the precision of the estimate for a given sample size N by plotting the $f(\hat{p}_r)$. Such plots are shown in Figure 2.15 for $p = 0.25$ with several different values of N. We see – not surprisingly – that with larger sample sizes the distribution bunches increasingly about p, and the probability of obtaining a value of $\hat{p}$ with a large error becomes smaller. With $p = 0.25$, the probability that $\hat{p}$ will be in error by more than 0.10 is about 50% when $N = 10$, about 20% when $N = 20$, and only about 10% when $N = 40$.

We may show that Eq. (2.61) is an unbiased estimator: If many samples of size N are obtained, the mean value of the estimator (i.e. the mean taken over all the samples) converges to the true value of p. Equivalently, we must show that the expected value of p is equal to p. Thus, for $\hat{p}$ to be unbiased we must have $E\{\hat{p}_r\} = p$. To demonstrate this, we first note by comparing Eqs. (2.34) and (2.63) that$f(\hat{p}_r) = f(r)$. Thus, with $\hat{p}_r = r/N$, we have

$$\mu_{\hat{p}} \equiv E\{\hat{p}\} = \sum_r \hat{p}_r f(\hat{p}_r) = \frac{1}{N}\sum_r r f(r) \tag{2.64}$$

The sum on the right, however, is just Np, the mean value of r. Thus, we have

$$\mu_{\hat{p}} = p \tag{2.65}$$

The increased precision of the estimator with increased N is demonstrated by observing that the variance of the sampling distribution decreases with increased N. From Eq. (2.26), we have

$$\sigma_{\hat{p}}^2 = \sum_n \hat{p}_n^2 f(\hat{p}_n) - \hat{\mu}_{\hat{p}}^2 \tag{2.66}$$

Inserting $\hat{\mu} = Np, \hat{p} = n/N$, and $f(\hat{p}_n) = f(n)$, we have

$$\sigma_{\hat{p}}^2 = \frac{1}{N^2}\left\{\sum_n n^2 f(n) - \boldsymbol{\mu}^2\right\} \tag{2.67}$$

but since the bracketed term is just $Np(1 - p)$, the variance of the binomial distribution, we have

$$\sigma_{\hat{p}}^2 = \frac{1}{N} p(1-p) \tag{2.68}$$

or equivalently

$$\sigma_{\hat{p}} = \frac{1}{\sqrt{N}} \sqrt{p(1-p)} \tag{2.69}$$

Unfortunately, we do not know the value of p beforehand. If we did, we would not be interested in using the estimator to obtain an approximate value. Therefore, we would like to estimate the precision of $\hat{p}$ without knowing the exact value of p. For this, we must introduce the somewhat more subtle notion of the confidence interval.

Introduction to Confidence Intervals

The confidence interval is the primary means by which the precision of a point estimator can be determined. It provides lower and upper confidence limits to indicate how tightly the sampling distribution is compressed around the true value of the estimated quantity. We will treat confidence interval more extensively in Chapter 5. Here, we confine our attention to determining the values of

$$P^- = \hat{p} - A \quad \text{where } P^- \text{ indicates the lower confidence bound and } \hat{p} = \frac{r}{N} \tag{2.70}$$

and

$$p^+ = \hat{p} + B \tag{2.71}$$

where these lower and upper confidence limits are associated with the point estimator $\hat{p}$.

To determine A and B, and therefore the limits, we first choose a risk level designated by α: $\alpha = 0.05$, which, for example would be a 5% risk. Suppose that we are willing to accept a risk of $\alpha/2$ in which the estimated lower confidence limit p^- will turn out to be larger than p, the true value of the failure probability. This may be stated as the probability

$$P\{p^- > p\} = \alpha/2 \tag{2.72}$$

which means we are $1 - \alpha/2$ confident that the calculated lower confidence limit will be less or equal to the true value:

$$P\{p^- \leq p\} = 1 - \alpha/2 \tag{2.73}$$

To determine the lower confidence limit, we first insert Eq. (2.70) and rearrange the inequality to obtain

$$P\{\hat{p}^- \leqslant p + A\} = 1 - \alpha/2 \tag{2.74}$$

But this is just the CDF for the sampling distribution evaluated at $p + A$. Thus, from the definition of the CDF given in Eq. (2.23), we may write

$$\sum_{\hat{p}_r \leqslant p + A} f(\hat{p}_r) = 1 - \alpha/2 \tag{2.75}$$

Recalling that $\hat{p}_r = r/N$ and copying the PMF explicitly from Eq. (2.63), we have

$$\sum_{r=0}^{N(p+A)} C_r^N p^r (1-p)^{N-r} = 1 - \alpha/2 \tag{2.76}$$

Thus, to find the lower confidence limit, we must determine the value of A for which this condition is most closely satisfied for specified α, N, and p.

Similarly, to obtain the upper limit at the same confidence, we require

$$P\{p \leqslant p^+\} = 1 - \alpha/2 \tag{2.77}$$

which upon insertion of Eq. (2.71) yields

$$P\{\hat{p} > p - B\} = 1 - \alpha/2 \tag{2.78}$$

and leads to the analogous condition on B,

$$\sum_{r=N(p+B)}^{N} C_r^N p^r (1-p)^{N-r} = 1 - \alpha/2 \tag{2.79}$$

To express the confidence interval more succinctly, the combined results of the foregoing equations are frequently expressed as the probability

$$P\{p^- \leqslant p \leqslant p^+\} = 1 - \alpha \tag{2.80}$$

Solutions for Eqs. (2.71) and (2.74) have been presented in convenient graphical form for obtaining p^+ and p^- from the point estimator $\hat{p}_n = n/N$. A graphical depiction of this for 95% confidence is depicted in Figures 2.16–2.18.

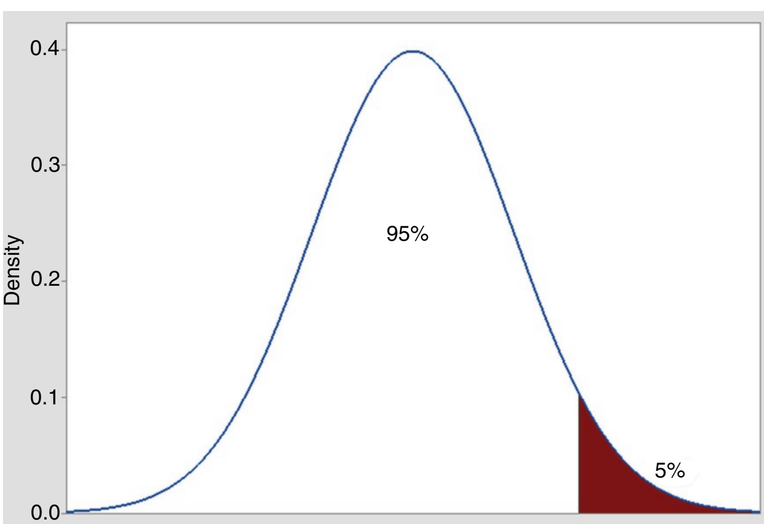


Figure 2.16 Upper 95% bound.

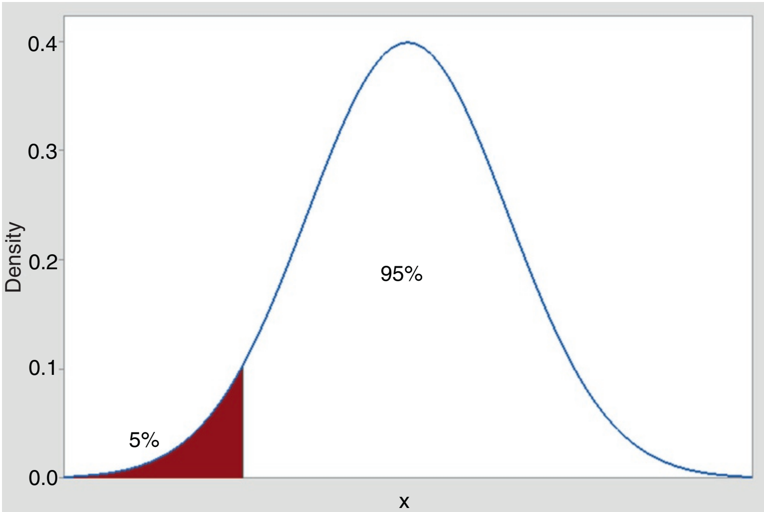


Figure 2.17 Lower 95% bound.

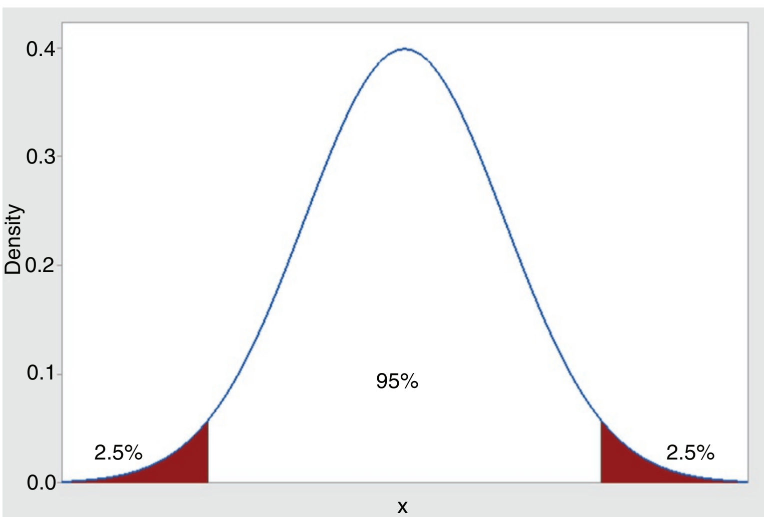


Figure 2.18 Illustration of 95% "two-sided" confidence bound.

Binomial Confidence Intervals

While the chances of a value being between an upper and lower bound is shown in Figure 2.18.

For those times when a quick approximate bound is needed for a binomial ratio of r/N, a plot of failure probability vs observed proportion can be useful. These are shown for a 95% confidence interval, corresponding to $\alpha/2 = 0.025$, in Figure 2.19 for values of N ranging from 10 to 1000. The corresponding graphs for other confidence intervals are given in Appendix B.

The results in Figure 2.19 indicate the limitations of classical sampling methods if highly accurate estimates are required, particularly when small failure probabilities are under considerations. Suppose, for example, that 10 items are tested with only one failure, our 95% confidence interval is then $0.001 < p < 0.47$.

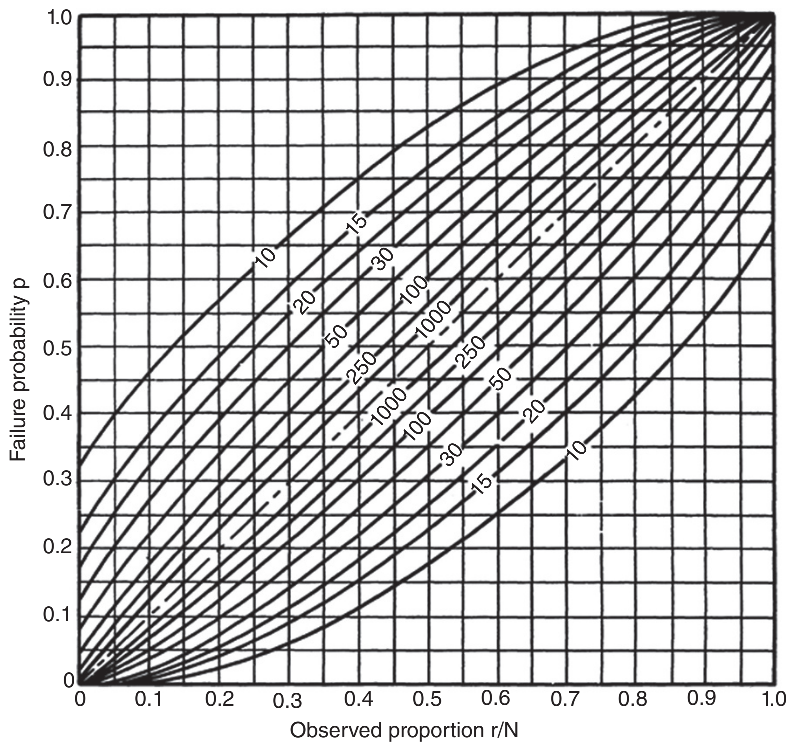


Figure 2.19 A 95% confidence interval for binomial sampling. *Source*: From Pearson and Clopper (1934). Public Domain.

With that in mind, what follows is a method to estimate more accurately confidence intervals for small numbers of failures and/or small sample sizes.

As we will show you in Chapter 4, the confidence limits for the binomial where $Np \geq 5$ or $N(1-p) \geq 5$ are easily solved using the normal approximation to the binomial.

However, for small numbers of failures or small sample sizes ($Np < 5$ or $N(1-p) < 5$), the approximations are not as useful as they have too much error for some applications. The following will show how to achieve exact intervals in those situations.

To construct a two-sided confidence interval at the $100(1-\alpha)\%$ confidence level for the true proportion defective p where r defects are found in a sample of size N, follow the steps below.

The equations to solve for a two-sided confidence interval $100(1-\alpha)\%$ for the true proportion defective p where N_d defects were found in a sample of size N:

1. Solve the equation:

$$\sum_{\mathrm{k}=0}^{N_d} {}_N C_k p_U^k (1-p_U)^{N-k} = \frac{\alpha}{2} \tag{2.81}$$

for p_U to obtain the upper $100(1-\alpha)\%$ confidence limit for p.

2. Solve the equation:

$$\sum_{\mathrm{k}=0}^{N_d-1} {}_N C_k p_L^k (1-p_L)^{N-k} = 1-\frac{\alpha}{2} \tag{2.82}$$

for p_L to obtain the upper $100(1-\alpha)\%$ confidence limit for p.

This interval (p_L, p_U) is an exact 100(1 – α)% confidence limit for p.

However, it is not symmetric about the observed proportion defective, $\hat{p} = \frac{r}{N}$.

Solving these equations can be done using EXCEL's Solver add-in, but this can take a bit of time each time you want to find an upper and lower bound on a binomial proportion where $\hat{p}$ *is small*. But a solution using a shortcut "Nomograph" called a *Thorndike chart* can yield quicker results.

Cumulative Sums of the Poisson Distribution (Thorndike Chart)

No discussion of binomial confidence bounds, and the Poisson approximation to binomial confidence bounds, would be complete without bringing up the only Nomograph that the author uses to this day.

The Thorndike chart (Figure 2.20) is used to find the probability that an event will occur at least c times in a large group of trials for which the average number of occurrences is μ' or Np. In addition, it is often used for a quick answer during the heat of a team meeting to the question of "What are the confidence bounds on the expected."

The Thorndike chart probability scale is proportional to the normal probability integral (see Chapter 3), while the x-axis is a logarithmic scale.

Example 2.25 Given that based on other analyses you expect (μ') incidents over a specific length of time of 2.3.

a) What is the probability of having seen 0 incidents?
b) What is the probability of 1 or more incidents?
c) What are the 80% confidence bounds on 2.3 failures?

Solution:

a) Entering the x-axis of Figure 2.20 at 2.3, and proceeding up to the "$C = 1$" line, you will follow that point of intersection to the y-axis and read 0.1. So, having observed 2.3 incidents on the average, you can be assured that your chance of seeing 0 incidents is <10%.
b) Since your chance of 0 incidents is <0.10, your probability (more than 1) = 1.0 − 0.1 = 0.9.
c) Moving up the x-axis scale from 2.3, you read off the 0.9 probability and 0.1 probability y-axis lines at 1 incident and ~4.8, respectively. If the average of 2.3 was based on 100 samples you could then use these numbers to state a 0.023 (failure rate) with 80% bounds (0.01, 048).

In Chapter 5, we will discuss risk analysis and use the Thorndike chart to be able to quickly answer confidence-bound questions when time is of the essence (e.g. customer or management meetings).

Example 2.26 Five of a batch of 100 computer chips fail the final screening test. Estimate the failure probability and the 90% confidence interval.

Again, in Chapter 4, we will introduce an approximation to confidence bounds for larger samples, and in Chapter 6, we will introduce exact confidence bounds for binomial testing.

Solution: $\hat{p} = 5/100 = 0.05$. Using Figure 2.21 and the dotted lines for 90% bounds and solid line at $Np = 5$, the 90% confidence bounds are ~(2.2, 9.3), and therefore, the 90% confidence bounds on 0.05 are ~(0.022, 0.093).

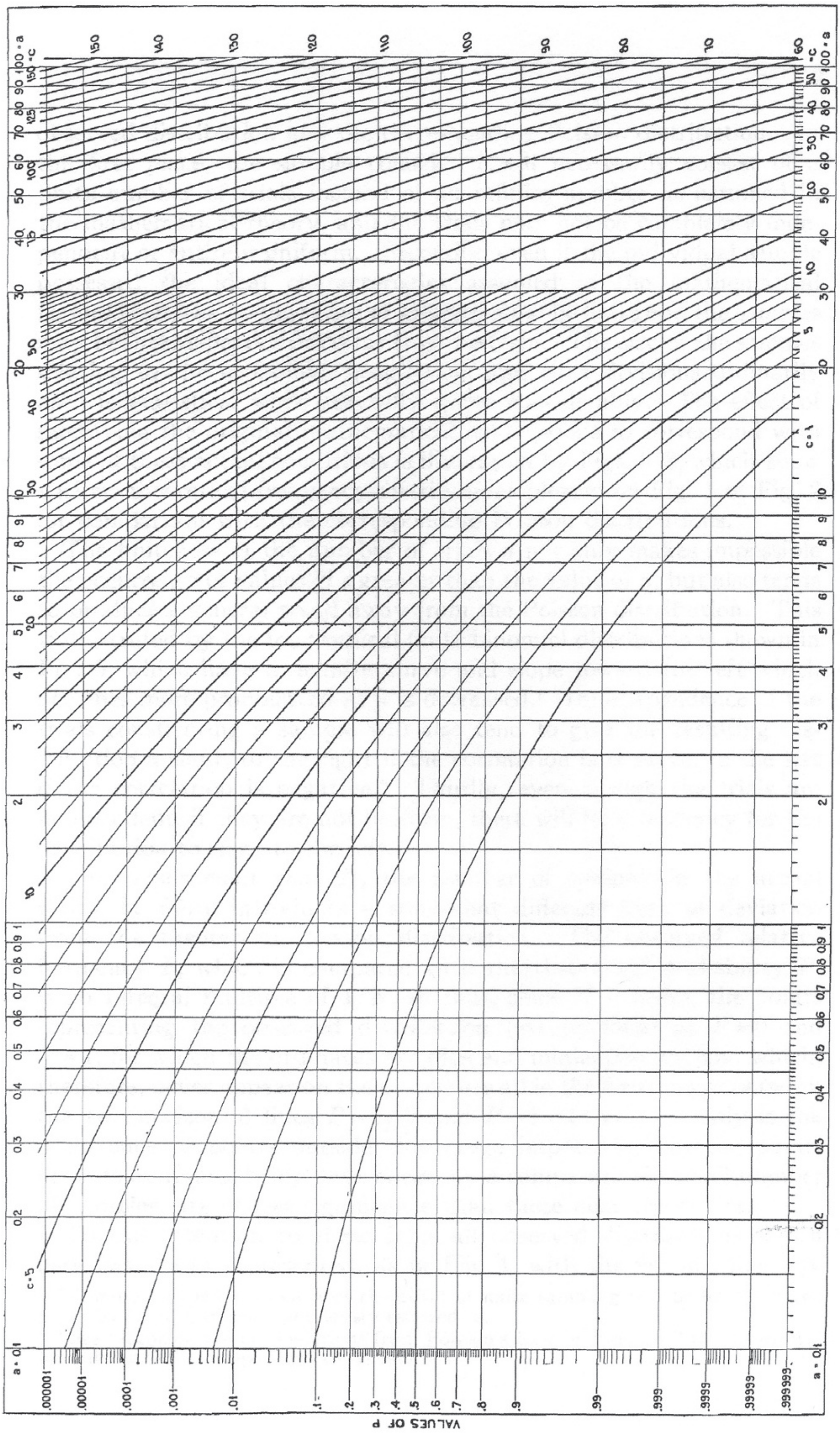


Figure 2.20 The Thorndike chart. *Source:* Reused with permission of Nokia Corporation and AT&T archives.

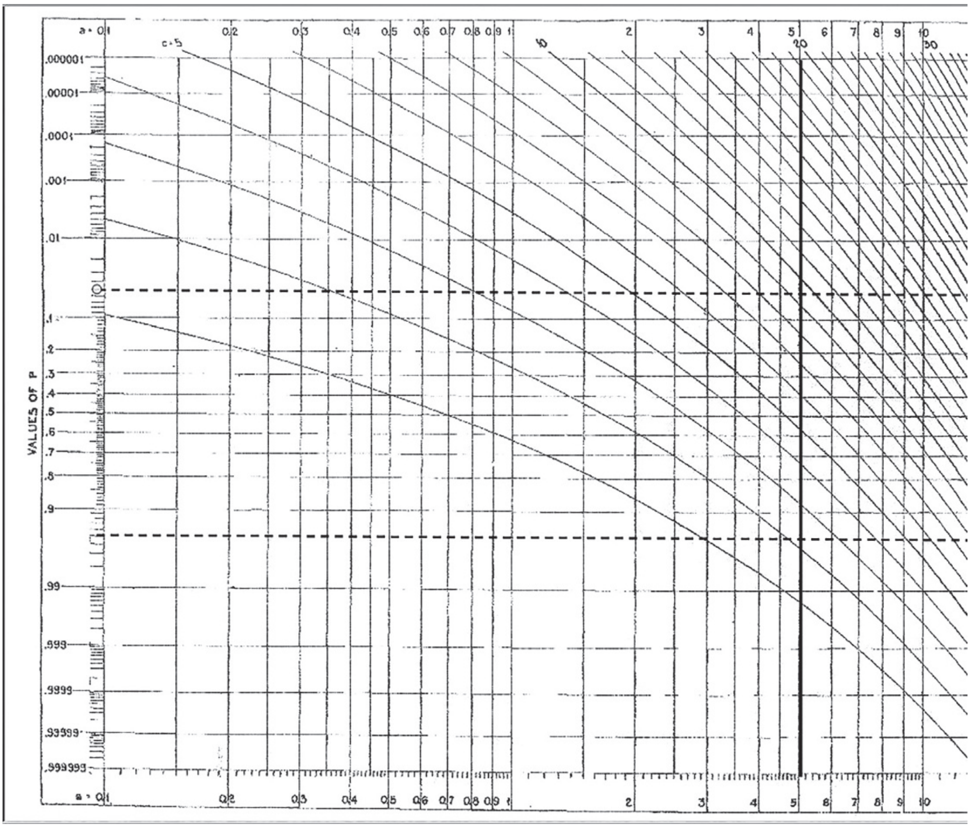


Figure 2.21 Illustrating the solution to Example 2.25.

Bibliography

Feigenbaum, A.Y. (1983). *Total Quality Control*, 3e. New York: McGraw-Hill.
http://statpages.info/ Internet page of statistical algorithms advanced texts in probability.
https://www.itl.nist.gov/div898/handbook/prc/section2/prc241.r (NIST online Handbook in Statistics).
Ireson, W., Coombs, C., and Moss, R. (1995). *Reliability Handbook*, 2e. New York: McGraw-Hill.
Lapin, L.L. (1998). *Probability and Statistics for Modern Engineering*, 2e. IL: Waveland Pr Inc.
Montgomery, D.C. and Runger, G.C. (1994). *Applied Statistics and Probability for Engineers*. New York: Wiley.
Pieruschkà, E. (1963). *Principles of Reliability*. Englewood Cliffs, NJ: Prentice-Hall.
Thorndike, F. (1926). Applications of Poisson's probability summation. *Bell System Technical Journal* **V**: 604–624.

Advanced texts in Probability

Dudley, R.M. (2004). *Real Analysis and Probability*. Cambridge Press.
Feller, W. (1948). *An Introduction to Probability Theory and It's Application*, vol. **Vol I**. Wiley.
Feller, W. (1965). *An Introduction to Probability Theory and It's Application*, vol. **Vol II**. Wiley.

Hoel, P., Port, S., and Stone, C. (1972). An Introduction to Probability. *Houghton-Mifflin* .
Pearson, E.S. and Clopper, C.J. (1934). The use of confidence or fiducial limits illustrated in the case of the binomial. *Biometrika* **26**: 404.
Roberts, H.R., Vesley, W.E., Haastand, D.F., and Goldberg, F.F. (1981). *Fault tree Handbook, NUREG-0492*. U.S. Nuclear Regulatory Commission.

Exercises

2.1 Suppose that $P(X) = 0.32$, $P(Y) = 0.44$, and $P(X \text{ U } Y) = 0.58$.
a) Are the events mutually exclusive?
b) Are they independent?
c) Calculate $P(X|Y)$
d) Calculate $P(Y|X)$

2.2 Suppose that X and Y are independent events with $P(X) = 0.28$ and $P(Y) = 0.41$. Find (a) $P(\overline{X})$, (b) $P(X \cap Y)$, (c) $P(\overline{Y})$, (d) $P(X \cap \overline{Y})$, (e) $P(X \cup Y)$, and (f) $P(\overline{X} \cap \overline{Y})$.

2.3 Suppose that $P(A) = 1/2$, $P(B) = 1/4$, and $P(A \cap B) = 1/8$. Determine $P(A|B)$, (b) $P(B|A)$, (c) $P(A \cup B)$, and (d) $P(\overline{A} \mid \overline{B})$.

2.4 Given: $P(A) = 0.4$, $P(A \cup B) = 0.8$, and $P(A \cap B) = 0.2$.
Determine (a) $P(B)$, (b) $P(A|B)$, and (c) $P(B|A)$.

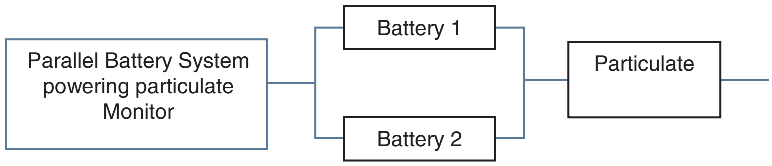
2.5 Two relays with demand failures of $p = 0.15$ are tested.
a) What is the probability that neither will fail?
b) What is the probability that both will fail?

2.6 For each of the following, draw a Venn diagram and shade the indicated areas: (a) $(X \cup Y) \cap \overline{Z}$, (b) $\overline{X} \cap \overline{Y} \cap Z$, (c) $(\overline{X} \cup \overline{Y}) \cap Z$, and (d) $(X \cap \overline{Y}) \cup Z$).

2.7 An aircraft-landing gear has a probability of 10^{-5} per landing of being damaged from excessive impact. What is the probability that the landing gear will survive a 10,000 landing design life without damage?

2.8 Consider events A, B, and C. If $P(A) = 0.8$, $P(B) = 0.3$, $P(C) = 0.4$, $P(A|B \cap C) = 0.5$, and $P(B|C) = 0.6$:
a) Determine whether events B and C are independent.
b) Determine whether events B and C are mutually exclusive.
c) Evaluate $P(A \cap B \cap C)$.
d) Evaluate $P(B \cap C|A)$.

2.9 A particulate monitor has a power supply consisting of two batteries in parallel (see diagram). Either battery is adequate to operate the monitor. However, since the failure of one battery places an added strain on the other, the conditional probability that the second battery will fail, given the failure of the first, is greater than the probability that the first will fail. On the basis of testing it is known that 7% of the monitors in question will have at least one battery failed by the end of their design life, whereas in 1% of the monitors, both batteries will fail during the design life.



a) Calculate the battery failure probability under normal operating conditions.
b) Calculate the conditional probability that the battery will fail, given that the other has failed.

2.10 Two pumps operating in parallel supply secondary cooling water to a condenser. The cooling demand fluctuates, and it is known that each pump is capable of supplying the cooling requirements 80% of the time in case the other fails. The failure probability for each pump is 0.12; the probability of both failing is 0.02. If there is a pump malfunction, what is the probability that the cooling demand can still be met?

2.11 For the discrete PMF,

$f(x_n) = Cx_n^2$, where $x_n = 1, 2, 3.$

a) Find C. (b) find $F(x_n)$. (c) calculate μ and σ.

2.12 Repeat Exercise 2.11 for

$f(x_n) = Cx_n(6 - x_n)$, where $x_n = 0, 1, 2, ..., 6.$

2.13 Consider the discrete random variable defined by

x_n	0	1	2	3	4	5
$f(x_n)$	$\frac{11}{36}$	$\frac{9}{36}$	$\frac{7}{36}$	$\frac{5}{36}$	$\frac{3}{36}$	$\frac{1}{36}$

Compute the mean and the variance.

2.14 A discrete random variable x takes on the values 0, 1, 2, and 3 with probabilities 0.4, 0.3, 0.2, and 0.1, respectively. Compute the expected values of x, x^2, $2x + 1$, and e^{-x}.

2.15 Evaluate the following:

a) ${}_5C_3$, (b) ${}_9C_2$, (c) ${}_{12}C_7$, (d)${}_{20}C_{19}$.

2.16 A discrete PMF is given by $f(0) = 1/6$,

$f(1) = 1/3, f(2) = 1/2$

a) Calculate the mean value μ.
b) Calculate the standard deviation σ.

2.17 Ten engines undergo testing. If the failure probability for an individual engine is 0.10, what is the probability that more than two engines will fail the test?

2.18 A boiler has four identical relief valves. The probability that an individual relief valve will fail to open on demand is 0.06. If the failures are independent:
a) What is the probability that at least one valve will fail to open?
b) What is the probability that at least one valve will open?

2.19 If the four relief valves were to be replaced by two valves in the preceding problem, to what value must the probability of an individual valve's failing be reduced if the probability that no valve will open is not to increase?

2.20 The discrete uniform distribution is

$$f(n) = 1/N, \quad n = l, 2, 3, 4, \ldots N$$

a) Show that the mean is $(N + 1)/2$.
b) Show that the variance is $(N^2 - 1)/12$.

2.21 The probability of an engine's failing during a 30-day acceptance test is 0.3 under adverse environmental conditions. Eight engines are included in such a test. What is the probability of the following? (a) None will fail. (b) All will fail. (c) More than half will fail.

2.22 The probability that part A causes a failure is 3/1000.
Determine:
a) The probability that no failure is involved in 30 events reported.
b) The probability that four failures are included in 20 events.

2.23 A manufacturer produces 1000 ball bearings. The failure probability for each ball bearing is 0.002.
a) What is the probability that more than 0.1% of the ball bearings will fail?
b) What is the probability that more than 0.5% of the ball bearings will fail?

2.24 Suppose that there is a disease that infects 1 out of 1000 people in a population and there is a test for this disease. If a person has the disease, the test comes back positive 99% of the time. BUT about 2% of uninfected patients also test positive. Now, you just tested positive. What are your chances of having the disease?

2.25 Suppose that the probability of a diode's failing an inspection is 0.006.
a) What is the probability that in a batch of 500, more than 3 will fail?
b) What is the mean number of failures per batch?
(Note: Use the Poisson distribution.)

2.26 The geometric distribution is given by

$$f(n) = p(1-p)^{n-1} \quad n = 1, 2, 3, \ldots \infty$$

show that $\sum_n f(x_n) = 1$ is satisfied

a) Show that Eq. (2.21) is satisfied.
b) Find that the expected value of n is $1/p$.
c) Show that the variance of $f(n)$ is $(1-p)/p^2$.
(Note: The summation formulas in Appendix A may be useful.)

2.27 One thousand capacitors undergo testing. If the failure probability for each capacitor is 0.0010, what is the probability that more than two capacitors will fail the test?

2.28 Let p equal the probability of failure, and n be the trial upon which the first failure occurs. Then, n is a random variable governed by the geometric distribution given in Exercise 2.26. An engineer wanting to study the failure mode proof tests on a new chip. Since there is only one test setup, she must run them one chip at a time. If the failure probability is $p = 0.2$:

a) What is the probability that the first chip will not fail?
b) What is the probability that the first three trials will produce no failures?
c) How many trials will she need to run before the probability of obtaining a failure reaches 1/2?

2.29 A manufacturer of 16K byte memory boards finds that the reliability of the manufactured boards is 0.98. Assume that the defects are independent. Assume $R_n = e^{-np}$ is the reliability formula.

a) What is the probability of a single byte of memory being defective?
b) If no changes are made in the design or manufacture, what reliability may be expected from 128K byte boards?

(Note: 16K bytes = 2^{14} bytes and 128K bytes = 2^{17} bytes.)

2.30 A problem of great concern to a manufacturer is the cost of repair and replacement required under a guarantee agreement. Assume that it is known that 10% of all units are returned for repair while their guarantee is still in effect. If the manufacturer sells 25 units, what is the probability that five or more of these units will need repair while their guarantees are still in effect?

2.31 Diesel engines used for generating emergency power are required to have a high reliability of starting during an emergency. If the failure to start on demand probability of 1% or less is required, how many consecutive successful starts would be necessary to ensure this level of reliability with a 90% confidence?

2.32 An engineer feels confident that the failure probability on a new electromagnetic relay is less than 0.01. The specifications require, however, only that $p < 0.04$. How many units must be tested without failure to prove with 95% confidence that $p < 0.04$?

2.33 A supplier of parts claims it has a manufacturing process in which 90% of parts are defect free. To check this theory, a customer randomly samples 25 parts and finds seven that are defective.
If the supplier's claim is true, what is the probability that 7 or more of the 25 sampled parts are defective?

2.34 Let us assume that the probability of a hurricane eye going into Palm Beach County is 0.1 per season. How many hurricanes should you expect in a decade? What is the probability of 4 or more hurricanes in a decade?

2.35 Suppose that 100 pressure sensors are tested, and 14 of them fail the calibration criteria. Make a point estimate of the failure probability and then estimate the 90% and the 95% confidence interval using Figure 2.21.

90% bounds (on $\mu = Np = 14$) approx. (8.8, 20) or $(p_L, p_U) = (0.088, 0.20)$.
95% bounds (on $\mu = Np = 14$) approx. (7.7, 22) or $(p_L, p_U) = (0.07, 0.22)$.

2.36 Suppose that the average number of lions seen on a 1-day safari is 5. What is the probability that tourists will see fewer than four lions on the next 1-day safari?

2.37 As a management team, paying for performance, without regard to gender is an important, indeed essential, responsibility. Using some probability skills to answer these questions can be useful:

About 21% of the managers in a large firm are at the top salary level. It is further known that 40% of all managers at the firm are women. Also, 6.4% of all managers are women *and* are at the top salary level, Recently, a question arose among executives at the firm as to whether there is any evidence of salary inequity. Do the percentages reported above provide any evidence of salary inequity?

2.38 As an example of a spatial distribution of random points, consider the statistics of flying bomb hits in the south of London during World War II. The entire area is divided into a grid of $N = 576$ small areas of size one-quarter square kilometer each. The table below records the number of squares with 0, 1, 2, 3, etc. hits each. The total number of hits is 537. The average number of hits per square is then $537/576 = 0.9323$ hits per square. It can be shown that if the targeting is *completely random*, then the probability that a square is hit with 0, 1, 2, 3, etc. hits is governed by a Poisson distribution; i.e. the probability that a given square suffers k hits is Poisson distributed. Fill in the table below with the Poisson distribution fit and comment on the comparison to actual.

# of hits	0	1	2	3	4	5
# of hits per cell actual	229	211	93	35	7	1
Poisson fit predicted						

2.39 The probability that a golfer hits the ball onto the green if it is windy as he strikes the ball is 0.4, and the corresponding probability if it is not windy as he strikes the ball is 0.7. The probability that it will be windy is 0.3.

Find the probability that (a) he hits the ball on to the green and (b) it was not windy, given that he does not hit the ball onto the green.

Use a probability tree.

3

The Exponential Distribution and Reliability Basics

"A good scientist is a person with original ideas. A good engineer is a
person who makes a design that works with as few original ideas as possible"

– Unknown

3.1 Introduction

Generally, reliability is defined as the probability that a system will perform properly for a specified period of time under a given set of operating conditions. Implied in this definition is a clear-cut criterion for failure from which we may judge at what point the system is no longer functioning properly. Similarly, the treatment of operating conditions requires an understanding both of the loading to which the system is subjected and of the environment within which it must operate. Perhaps the most important variable to which we must relate reliability, however, is time. For it is in terms of the rates of failure that most reliability phenomena are understood.

In this chapter we examine reliability as a function of time, and this leads to the definition of the failure rate. Examining the time dependence of failure rates allows us to gain additional insight into the nature of failures – whether they be infant mortality failures, failures that occur randomly in time, or failures brought on by aging. Similarly, the time dependence of failures can be viewed in terms of failure modes in order to differentiate between failures caused by different mechanisms and those caused by different components of a system. This leads to an appreciation of the relationship between failure rate and system complexity. Finally, we examine the impact of failure rate on the number of failures that may occur in systems that may be repaired or replaced.

3.2 Reliability Characterization

We begin this section by quantitatively defining reliability in terms of the probability density function (PDF) and the cumulative distribution function (CDF) for the time to failure. The failure rate and the mean time to failure are then introduced. The failure rate is discussed in detail, for its characteristic shape in the form of the so-called bathtub curve provides substantial insight into the nature of the three classes of failure mechanisms: infant mortality, random failures, and aging.

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

Basic Definitions

Reliability is defined in Chapter 1 as the probability that a system survives for some specified period of time. It may be expressed in terms of the random variable **t,** the time to system failure. The PDF, $f(t)$, has the physical meaning

$$f(t)\,\Delta t = P\{t < \mathbf{t} \le t + \Delta t\} = \left\{ \begin{array}{l} \text{probabiltity that failure} \\ \text{takes place at a time} \\ \text{between } t \text{ and } t + \Delta t \end{array} \right\} \tag{3.1}$$

for vanishingly small Δt. From Eq. (3.1) we see that the CDF now has the meaning

$$F(t) = P\{\mathbf{t} \le t\} = \left\{ \begin{array}{l} \text{probability that failure} \\ \text{takes place at a time less} \\ \text{than or equal to } t \end{array} \right\} \tag{3.2}$$

We define the reliability as

$$R(t) = P\{\mathbf{t} > t\} = \left\{ \begin{array}{l} \text{probability that a system} \\ \text{operates without failure} \\ \text{for a length of time } t \end{array} \right\} \tag{3.3}$$

Since a system that does not fail for $\mathbf{t} \le t$ must fail at some $\mathbf{t} > t$, we have

$$R(t) = 1 - F(t) \tag{3.4}$$

or equivalently either

$$R(t) = 1 - \int_0^t f(t')\,dt' \tag{3.5}$$

or

$$R(t) = \int_t^{\infty} f(t')\,dt' \tag{3.6}$$

From the properties of the PDF, it is clear that

$$R(0) = 1 \tag{3.7}$$

and

$$R(\infty) = 0 \tag{3.8}$$

We see that the reliability is the complement of the CDF of t, that is $R(t) = \widetilde{F}(t)$. Similarly, since $F(t)$ is the probability that the system will fail before $\mathbf{t} = t$, it is often referred to as the unreliability or failure probability; at times, we may denote the unreliability as

$$\widetilde{R}(t) = 1 - R(t) = F(t) \tag{3.9}$$

Equation (3.5) may be inverted by differentiation to give the PDF of failure times in terms of the reliability:

$$f(t) = -\frac{d}{dt} R(t) \tag{3.10}$$

Insight is normally gained into failure mechanisms by examining the behavior of the failure rate. The *failure rate,* $\lambda(t)$*,* may be defined in terms of the reliability or the PDF of the time to failure as follows. Let $\lambda(t)\,\Delta t$ be the probability that the system will fail at some time $\mathbf{t} < t + \Delta t$, given that it has not yet failed at $\mathbf{t} = t$. Thus, it is the conditional probability

$$\lambda(t)\,\Delta t = P\{\mathbf{t} < t + \Delta t | \mathbf{t} > t\} \tag{3.11}$$

Using Eq. (2.9a), the definition of conditional probability, we have

$$P\{\mathrm{t} < t + \Delta t \,|\, \mathbf{t} > t\} = \frac{P\{(\mathbf{t} > t) \cap (\mathbf{t} < t + \Delta t)\}}{P\{\mathbf{t} > t\}} \tag{3.12}$$

The numerator on the right-hand side is just an alternative way of writing the PDF, that is

$$P\{(\mathbf{t} > t) \cap (\mathbf{t} < t + \Delta t)\} \equiv P\{t < \mathbf{t} < t + \Delta t\} = f(t)\,\Delta t \tag{3.13}$$

The denominator of Eq. (3.12) is just $R(t)$, as may be seen by examining Eq. (3.3). Therefore, combining equations, we obtain

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{3.14}$$

This quantity, the failure rate, is also referred to as the *hazard* or *mortality* rate.

The most useful way to express the reliability and the failure PDF is in terms of the failure rate. To do this, we first eliminate $f(t)$ from Eq. (3.14) by inserting Eq. (3.10) to obtain the failure rate in terms of the reliability,

$$\lambda(t) = -\frac{1}{R(t)}\frac{d}{dt}R(t) \tag{3.15}$$

Then, multiplying by dt, we obtain

$$\lambda(t)\,dt = -\frac{dR(t)}{R(t)} \tag{3.16}$$

Integrating between zero and t yields

$$\int_0^t \lambda(t')\,dt' = -\ln[R(t)] \tag{3.17}$$

since $R(0) = 1$. Finally, exponentiating results in the desired expression for the reliability

$$R(t) = \exp\left[-\int_0^t \lambda(t')\,dt'\right] \tag{3.18}$$

To obtain the PDF for failures, we simply insert Eq. (3.18) into Eq. (3.14) and solve for $f(t)$:

$$f(t) = \lambda(t)\exp\left[-\int_0^t \lambda(t')\,dt'\right] \tag{3.19}$$

Probably, the single most-used parameter to characterize reliability is the *mean time to failure* (or MTTF). It is just the *expected* or *mean value* $E\{t\}$ of the failure time t. Hence,

$$\mathrm{MTTF} = \int_0^\infty t f(t)\,dt \tag{3.20}$$

The MTTF may be written directly in terms of the reliability by substituting Eq. (3.10) into Eq. (3.20) and integrating by parts:

$$\text{MTTF} = -\int_0^\infty t\,\frac{dR}{dt}\,dt = -tR(t)\Big|_0^\infty + \int_0^\infty R(t)\ dt \tag{3.21}$$

Clearly, the $tR(t)$ term vanishes at $t = 0$. Similarly, from Eq. (3.18), we see that $R(t)$ will decay exponentially or faster, since the failure rate $\lambda(t)$ must be greater than zero. Thus, $tR(t) \to 0$ as $t \to \infty$. Therefore, we have

$$\text{MTTF} = \int_0^\infty R(t)\,dt \tag{3.22}$$

Example 3.1 An engineer approximates the reliability of a cutting assembly by

$$R(t) = \begin{cases} (1 - t/t_0)^2, & 0 \le t < t_0, \\ 0 & t \ge t_0. \end{cases}$$

a) Determine the failure rate.
b) Does the failure rate increase or decrease with time?
c) Determine the MTTF.

Solution (a) From Eq. (3.10),

$$f(t) = -\frac{d}{dt}(1 - t/t_0)^2 = \frac{2}{t_0}(1 - t/t_0),\ \ 0 \le t < t_0$$

and from Eq. (3.14),

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{2}{t_0(1 - t/t_0)}, \quad 0 \le t < t_0$$

(b) The failure rate increases from $2/t_0$ at $t = 0$ to infinity at $t = t_0$.
(c) From Eq. (3.22)

$$\text{MTTF} = \int_0^{t_0} dt(1 - t/t_0)^2 = t_0/3$$

The Bathtub Curve

The behavior of failure rates with time is quite revealing. Unless a system has redundant components, such as those discussed later in this chapter the failure rate curve usually has the general characteristics of a "bathtub" such as shown in Figure 3.1. The bathtub curve, in fact, is an ubiquitous characteristic of living creatures as well as of inanimate engineering devices, and much of the failure rate terminology comes from demographers' studies of human mortality distributions. In the biomedical community, for example reliability is referred to as the survivability and denoted as $S(t)$. Moreover, comparisons of human mortality and engineering failures add insight into the three broad classes of failures that give rise to the bathtub curve.

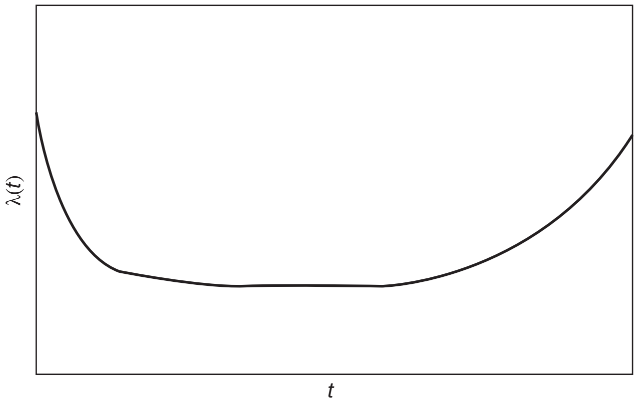


Figure 3.1 A "bathtub" curve representing a time-dependent failure rate.

The short period of time on the left-hand side of Figure 3.1 is a region of high but decreasing failure rates. This is referred to as the period of *infant mortality* or early failures. Here, the failure rate is dominated by infant deaths caused primarily by congenital defects or weaknesses. The death rate decreases with time as the weaker infants die and are lost from the population, or their defects are detected and repaired. Similarly, defective pieces of equipment, prone to failure because they were not manufactured or constructed properly, cause the high initial failure rates of engineering devices. Missing parts, substandard material batches, components that are out of tolerance, and damage in shipping are a few of the quality weaknesses that may cause excessive failure rates near the beginning of design life.

Early failures in engineering devices are nearly synonymous with the "product noise" quality loss stressed in the Taguchi methodology. The preferred method for eliminating such failures is through design and production quality control measures that will reduce variability and hence susceptibility to infant mortality failures. If such measures are inadequate, a period of time may be specified during which the device undergoes *wear-in/burn-in/run-in*. During this time, loading and use are controlled in such a way that weaknesses are likely to be detected and repaired without failure, or so that failures attributable to defective manufacture or construction will not cause inordinate harm or financial loss. Alternately, in environmental stress screening and in proof testing products are stressed beyond what is expected in normal use so that weak units will fail before they are sold or put in service (see Chapter 6-Reliability Testing)

The middle section of the bathtub curve contains the smallest and most nearly constant failure rates and is referred to as the *useful life*. This flat behavior is characteristic of failures caused by random events and hence referred to as *random failures*. They are likely to stem from unavoidable loads coming from without, rather than from any inherent defect in the device or system under consideration. Consequently, the probability that failure will occur in the next time increment is independent of the system's age. In human populations, deaths during this part of the bathtub curve are likely to be due to accidents or infectious disease. In engineering devices, the external loading may take a wide variety of forms, depending on the type of system under consideration: earthquakes, power surges, vibration, mechanical impact, temperature fluctuations, and moisture variation are some of the common causes. In the Taguchi quality methodology such loads are referred to as "outer noise."

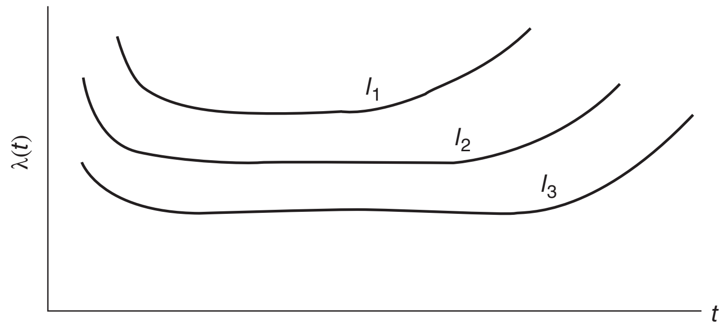


Figure 3.2 Time-dependent failure rates at different levels of loading: $l_1 > l_2 > l_3$.

Random failure can be reduced by improving designs: making them more robust with respect to the environments to which they are subjected. This may be accomplished by increasing the ratio of the components' capacities relative to the loads placed upon them (see Chapter 8). The net outcome may be visualized as in Figure 3.2, where for an assumed operating environment, the failure rate decreases as the component load is reduced. This procedure of deliberately reducing the loading is referred to as derating. The terminology stems from the deliberate reduction of voltages of electrical systems, but it is also applicable to mechanical, thermal, or other classes of loads as well. Conversely, the chance of component failure is decreased if the capacity or strength of the component is increased.

The right of the bathtub curve is a region of increasing failure rates. During this period of time *aging failures* become dominant. Again, with an obvious analogy to the loss of bone mass, arterial hardening, and other aging effects found in human populations, the failures tend to be dominated by cumulative effects such as corrosion, embrittlement, fatigue cracking, and diffusion of materials. The onset of rapidly increasing failure rates normally forms the basis for determining when parts should be replaced and for specifying the system's design life. Design with more durable components and materials, inspection and preventive maintenance, and control of deleterious environmental stresses are a few of the approaches in the enduring battle to produce longer lived products. In the Taguchi methodology, the causes of deterioration are referred to as "inner noise."

Although Figure 3.1 displays the general features present in failure rate curves for many types of devices, one of the three mechanisms may be predominant for a particular class of system. Examples of such curves are given in Figure 3.3. The curve in Figure 3.3a is representative of much

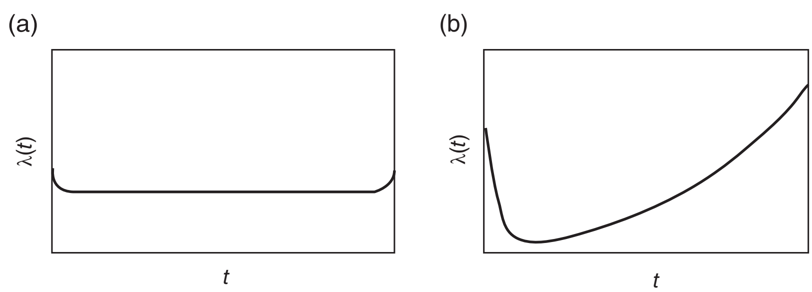


Figure 3.3 Representative failure rates for different classes of systems. (a) Electronic hardware. (b) Mechanical equipment.

computer and other electronic hardware. In particular, after a rather inconspicuous wear-in period, there is a long span of time over which the failure rate is essentially constant. For systems of this type, the primary concerns are with random failures and with methods for controlling the environment and external loading to minimize their occurrence.

The failure rate curve in Figure 3.3b is typical of valves, pumps, engines, and other pieces of equipment that are primarily mechanical in nature. Their initial wear-in period is followed by a long span of time with a monotonically increasing failure rate. In these systems, for which the primary failure mechanisms are fatigue, corrosion, and other cumulative effects, the central concern is in estimating safe and economical operating lives and in determining prudent schedules for preventive maintenance and for replacing parts.

Thus far, we have not discussed the reliability consequences of logical errors or oversights committed in the design of complex systems. These, for example may take the form of circuitry errors imbedded in microprocessor chips, bugs in computer software, or even equation mistakes in engineering reference books. Prototypes normally undergo extensive testing to find and eliminate such errors before a product is put into production. Nevertheless, it may be impossible – or at least impractical – to test a device against all possible combinations of inputs to assure that the correct output is produced in every case. Thus, there may exist untested sets of inputs that will cause the system to malfunction. In general, the resulting malfunctions may be expected to occur randomly in time, contributing to the time-independent component of the failure rate curve.

There is sometimes confusion with regard to failure rate definitions for computer software. This results from the common practice of finding and correcting bugs after, as well as before, the software is released for use. Such bugs tend to occur less and less frequently, giving rise to the notion of a decreasing failure rate. But that is not a failure rate in the sense in which it is defined here. In debugging, the software design is modified after each failure, whereas the definition used here is only valid for a product of fixed design. Hardware and software reliability growth attributable to test-fix debugging processes is taken up in Chapter 6.

In the following sections, models for representing failure rates with one, or at most a few parameters, are discussed. These are particularly useful when most of the failures are caused by early failures, random events, or aging effects. Even when more than one mechanism contributes substantially to the failure rate curve, however, these models can often be used to represent the combined failure modes and their interactions.

3.3 Constant Failure Rate Model

Random failures that give rise to the constant failure rate model are the most widely used basis for describing reliability phenomena. They are defined by the assumption that the rate at which the system fails is independent of its age. For continuously operating systems this implies a constant failure rate, whereas for demand failures it requires that the failure probability per demand be independent of the number of demands.

The constant failure rate approximation is often quite adequate even though a system or some of its components may exhibit moderate early failures or aging effects. The magnitude of early-failure effects is limited by strict quality control in manufacture and installation and may be further reduced by a wear-in period before actual operations are begun. Similarly, in many systems, aging effects can be sharply limited by careful preventive maintenance, with timely replacement of the parts or components in which the wear effects are concentrated. Conversely, if components are replaced as they fail, the overall failure rate of a "many-component system" will appear nearly constant, for the failure of the components will be randomly distributed in time as will the ages of the replacement parts. Finally, even though the system's failure rate may vary in time, we can use a constant failure rate that envelops the curve; this rate will be moderately pessimistic.

In the following sections, we first consider the exponential distribution. It is employed when constant failure rates adequately describe the behavior of continuously operating systems. We then examine two demand failure models, one in which the demands take place at equal time intervals, and the other in which the demands are randomly distributed in time. Both may be represented as constant failure rates. Finally, we formulate a composite model to describe the behavior of intermittently operating systems that may be subject to both operating and demand modes of failure.

The Exponential Distribution

The constant failure rate model for continuously operating systems leads to an exponential distribution. Replacing the time-dependent failure rate $\lambda(t)$ by a constant λ in Eq. (3.19) yields, for the PDF,

$$f(t) = \lambda e^{-\lambda t} \tag{3.23}$$

Similarly, the CDF becomes

$$F(t) = 1 - e^{-\lambda t} \tag{3.24}$$

and from Eq. (3.18), the reliability may be written as

$$R(t) = e^{-\lambda t} \tag{3.25}$$

Plots of $f(t)$, $R(t)$, and $\lambda(t)$ (the failure rate) are given in Figure 3.4. With the constant failure rate model, the resulting distributions are described in terms of a single parameter, λ. The MTTF and the variance of the failure times are also given in terms of λ. From Eq. (3.22), we obtain

$$\text{MTTF} = \frac{1}{\lambda} \tag{3.26}$$

and the variance is found from Eq. (3.16) to be

$$\sigma^2 = \frac{1}{\lambda^2} \tag{3.27}$$

A device described by a constant failure rate, and therefore by an exponential distribution of times to failure, has the following property of "memorylessness": The probability that it will fail

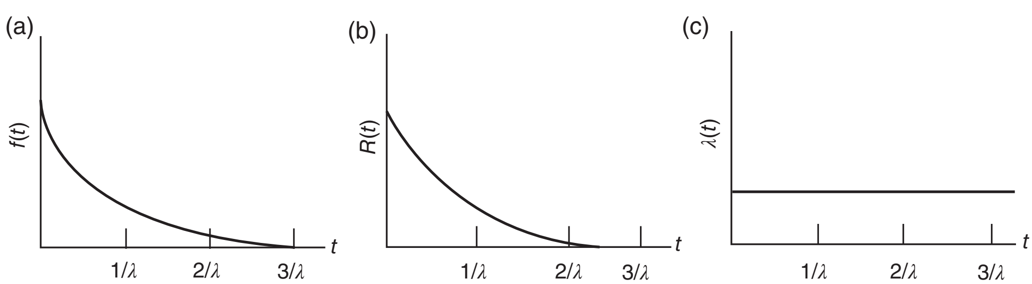


Figure 3.4 The exponential distribution. (a) Time to failure PDF, (b) reliability, and (c) failure rate.

during some period of time in the future is independent of its age. This is easily demonstrated by the following example.

Example 3.2 A device has a constant failure rate of $\lambda = 0.02$/hours.
(a) What is the probability that it will fail during the first 10 hours of operation?
(b) Suppose that the device has been successfully operated for 100 hours. What is the probability that it will fail during the next 10 hours of operation?

Solution (a) The probability of failure within the first 10 hours is

$$P\{\mathbf{t} \leq 10\} = \int_0^{10} f(t)\,dt = F(10) = 1 - e^{-0.02 \times 10} = 0.181$$

(b) From Eq. (2.9a), the conditional probability is

$$\begin{aligned} P\{\mathbf{t} \leq 100\,|\mathbf{t} > 100\} &= \frac{P\{(\mathbf{t} \leq 110) \cap (\mathbf{t} > 100)\}}{P\{\mathbf{t} = 100\}} = \frac{P\{100 \leq \mathbf{t} \leq 100\}}{P\{\mathbf{t} = 100\}} \\ &= \frac{\int_{100}^{110} f(t)\,dt}{1 - F(100)} \\ &= \frac{\int_{100}^{110} 0.02\,e^{-0.02t}\,dt}{1 - 1 + \exp\,(-0.02 \times 100)} \\ &= \frac{\exp\,(-0.02 \times 100) - \exp\,(-0.02 \times 110)}{\exp\,(-0.02 \times 100)} \\ &= 1 - \exp\,(-0.02 \times 10) = 0.181 \end{aligned}$$

That the probability of failure within a specified time interval is independent of the age of the device should not be surprising. Random failures are normally those caused by external shocks to the device; therefore, they should not depend on past history. For example, the probability that a satellite will fail during the next month owing to meteor impact would not depend on how long the satellite had already been in orbit. It would depend only on the frequency with which meteors pass through the orbit.

Demand Failures

The constant failure rate model has thus far been derived for a continuously operating system. It may also be shown to be applicable to a system exposed to a series of demands or shocks, each one of which has a small probability of causing failure. Suppose that each time a demand is made on a system, the probability of survival is r, giving a corresponding probability of failure of

$$p = 1 - r \tag{3.28}$$

The term demand here is quite general; it may be the switching of an electric relay, the opening of a valve, the start of an engine, or even the stress on a bridge as a truck passes over it. Whatever the application, there are two salient points. First, we must be able to count or at least infer the number of demands; and second, the probability of surviving each demand must be independent of the number of previous demands.

We define the reliability R_n as the probability that the system will still be operational after n demands. Let X_n signify the event of success in the nth demand. Then, if the probabilities of surviving each demand are mutually independent, R_n is given by Eq. (2.8) as

$$R_n = P\{X_1\}P\{X_2\}P\{X_3\}...P\{X_n\} \tag{3.29}$$

or since $P\{X_n\} = r$ for all n,

$$R_n = r^n \tag{3.30}$$

Then, using Eq. (3.28), we obtain

$$R_n = (1-p)^n \tag{3.31}$$

We may put this result in a more useful approximate form. First, note that the exponential of

$$ln\, R_n = \; ln\,(1-p)^n = n \; ln\,(1-p) \tag{3.32}$$

is

$$R_n = e^{n\ln(1-p)} \tag{3.33}$$

If the probability for failure on demand is small, we may make the approximation

$$\ln(1-p) \approx -p \tag{3.34}$$

for $p \ll 1$, yielding

$$R_n = e^{-np} \tag{3.35}$$

Since $p \ll 1$ is often a good approximation, we see that the reliability decays exponentially with the number of demands. If the rate at which demands are made on the system is roughly constant, we may express the number of demands occurring before time t as

$$n = \gamma t \tag{3.36}$$

where γ is the frequency at which demands arrive. Thus, if they arrive at time intervals Δt we have $\gamma = 1/\Delta t$. We may then calculate the reliability $R(t)$, defined as the probability that the system will still be operational at time t, as

$$R(t) = e^{-\lambda t} \tag{3.37}$$

where the failure rate λ is now given by

$$\lambda = \gamma p \tag{3.38}$$

Equation (3.35) indicates that the exponential distribution arises for systems that are subjected to many independent shocks or demands, each of which creates only a small probability of failure. If we drop the assumption that the demands appear at equal time intervals Δt, and assume that the shocks arrive at random intervals, the same result is obtained without assuming that the probability p of failure per shock is small. Let γ represent the mean number of demands per unit time. Then,

$$\mu = \gamma t \tag{3.39}$$

is the mean number of demands over a time interval t. If the demands appear randomly in time obeying a Poisson process, we may represent the probability that there will be n demands per unit time with the Poisson probability mass function given in Eq. (2.59):

$$f(n) = \frac{(\gamma t)^n}{n!} e^{-\gamma t} \tag{3.40}$$

Since the reliability after n independent demands is just r^n, the reliability at time t will just be the expected value of r^n at t. Using Eq. (2.25) for the expected value, we have

$$R(t) = \sum_{n=0}^{\infty} r^n f(n) \tag{3.41}$$

which yields in combination with Eq. (3.40):

$$R(t) = \sum\nolimits_{n=0}^{\infty} \frac{(r\gamma t)^n}{n!} e^{-\gamma t} \tag{3.42}$$

We next note that upon moving $e^{-\gamma t}$ outside the sum, we obtain a power series for $e^{r\gamma t}$. Thus, the reliability simplifies to

$$R(t) = e^{(r-1)\gamma t} \tag{3.43}$$

and upon inserting Eq. (3.28), we again obtain

$$R(t) = e^{-\gamma p t} \tag{3.44}$$

where the failure rate is given by Eq. (3.38).

Example 3.3 A telecommunications leasing firm finds that during the one-year warranty period, 6% of its telephones are returned at least once because they have been dropped and damaged. An extensive testing program earlier indicated that in only 20% of the drops should telephones be damaged. Assuming that the dropping of telephones in normal use is a Poisson process, what is the MTBD (mean time between drops)? If the telephones are redesigned so that only 4% of drops cause damage, what fraction of the phones will be returned with dropping damage at least once during the first year of service?

Solution (a) The fraction of telephones not returned is $R = e^{-\gamma p t}$ or $0.94 = e^{-\gamma \times 0.2 \times 1}$. Therefore,

$$\gamma = \frac{1}{0.2 \times 1} \ln\left(\frac{1}{0.94}\right) = 0.3094/\text{year}$$

$$\text{MTBD} = \frac{1}{\gamma} = 3.23\ \text{years}$$

(b) For the improved design, $R = e^{-\gamma p t} = e^{-0.3094 \times 0.04 \times 1} = 0.9877$. Therefore, the fraction of the phones returned at least once is

$$1 - 0.9877 = 0.0123 \text{ or } 1.23\%$$

Time Determinations

Careful attention must be given to the determination of appropriate time units. Is it operating time or calendar time? A warranty of 100,000 miles or 10 years, for example includes both, since the 100,000 miles is converted to an equivalent operating time. Two failure rates are then relevant, one for when the vehicle is operating, and another presumably smaller one for when it is not. A third consideration is the number of start–stop cycles that the vehicle is likely to undergo, for the related stress and thermal cycling may aggravate some failure mechanisms. Whatever the situation, we must clearly state what measure of time is being used. If the reliability is to be expressed in calendar time rather than operating time, the duty cycle or capacity factor c, defined as the fraction of time that the engine is running, must also enter the calculations.

Consider as an example a refrigerator motor that runs some fraction c of the time; the failure rate is λ_0 per unit operating time. The contribution to the total failure rate from failures while the refrigerator is operating will then be $c\lambda_0$ per unit calendar time. If the demand failure is also to be taken into account, we must know how many times the motor is turned on. Suppose that the average length of time that the motor runs when it comes on is $\bar{t}_0$. Then, the average number of times that the motor is turned on per unit operating time is $1/\bar{t}_0$. The average number of times that it is turned on per unit calendar time is $m = c/\bar{t}_0$. To obtain the total failure rate, we add the demand and operating failure rates. Consequently, the composite failure rate to be used in Eqs. (3.23) through (3.27) is

$$\lambda = \frac{c}{t_0}p + c\lambda_0 \tag{3.45}$$

In the foregoing development we have neglected the possibility that the motor may fail while it is not operating, that is while it is in a standby mode. Often, such failure rates are small enough to be neglected. However, for systems that are operated only a small fraction of the time, such as an emergency generator, failure in the standby mode may be quite significant. To take this into account, we define λ_s as the failure rate in the standby mode. Since the system in our example is in the standby mode for a fraction $1-c$ of the time, we add a contribution of $(1-c)\lambda_s$ to the composite failure rate in Eq. (3.45):

$$\lambda = \frac{c}{t_0}p + c\lambda_0 + (1-c)\lambda_s \tag{3.46}$$

Example 3.4 A pump on a volume control system at a chemical process plant operates intermittently. The pump has an operating failure rate of 0.0004/hour and a standby failure rate of 0.00001/hour. The probability of failure on demand is 0.0005. The times at which the pump is turned on t_u and turned off t_d over a 24-hour period are listed in Tables 3.1a and 3.1b.

Assuming that these data are representative: (a) Calculate a composite failure rate for the pump under these operating conditions. (b) What is the probability of the pump's failing during any one-month (30-day) period?

Table 3.1a Chemical process plant t_{ui} (uptime) and t_{di} (downtime).

t_{ui}	0.78	1.69	2.89	3.92	4.71	5.97	6.84	7.76
t_{di}	1.02	2.11	3.07	4.21	5.08	6.31	7.23	8.12
t_{ui}	8.91	9.81	10.81	11.87	12.98	13.81	14.87	15.97
t_{di}	9.14	10.08	11.02	12.14	13.18	14.06	15.19	16.09
t_{ui}	16.69	17.71	18.61	19.61	20.56	21.49	22.58	23.61
t_{di}	16.98	18.04	19.01	19.97	20.91	21.86	22.79	23.89

Table 3.1b Uptime and downtime in a 24-hour period.

t_{ui}	t_{di}	Down/up	Uptime	Downtime	t_{ui}	t_{di}	Down/up	Uptime	Downtime
0	0.78	Down			12.98	13.18	Up	0.2	0.84
0.78	1.02	Up	0.24	0.78	13.81	14.06	Up	0.25	0.63
1.69	2.11	Up	0.42	0.67	14.87	15.19	Up	0.32	0.81
2.89	3.07	Up	0.18	0.78	15.97	16.09	Up	0.12	0.78
3.92	4.21	Up	0.29	0.85	16.69	16.98	Up	0.29	0.6
4.71	5.08	Up	0.37	0.5	17.71	18.04	Up	0.33	0.73
5.97	6.31	Up	0.34	0.89	18.61	19.01	Up	0.4	0.57
6.84	7.23	Up	0.39	0.53	19.61	19.97	Up	0.36	0.6
7.76	8.12	Up	0.36	0.53	20.56	20.91	Up	0.35	0.59
8.91	9.14	Up	0.23	0.79	21.49	21.86	Up	0.37	0.58
9.81	10.08	Up	0.27	0.67	22.58	22.79	Up	0.21	0.72
10.81	11.02	Up	0.21	0.73	23.61	23.89	Up	0.28	0.82
11.87	12.14	Up	0.27	0.85	23.89	24	Down		0.11

Solution (a) From the data given, we first calculate:

$$\sum_{i=1}^{M} t_{di} = 326.28 \quad \text{and} \quad \sum_{i=1}^{M} t_{ui} = 318.34$$

where $M = 24$ is the number of operations. The average operating time $\bar{t}_0$ of the pump is estimated for the data to be

$$\bar{t}_0 = \frac{1}{M}\sum_{i=1}^{M}(t_{di} - t_{ui}) = \frac{1}{M}\left(\sum_{i=1}^{M} t_{di} - \sum_{i=1}^{M} t_{ui}\right)$$
$$= \frac{1}{24}(326.28 - 318.34) = 0.33083 \text{ hours}$$

Then, the capacity factor is

$$c = \frac{M\bar{t}_0}{24} = \frac{24 \times 0.33083}{24} = 0.33083$$

Thus, the failure rate from Eq. (3.46) is

$$\lambda = \frac{c}{t_0}p + c\lambda_0 + (1-c)\lambda_s = \frac{0.33083}{0.33083} \times 0.0005 + 0.33083 \times 0.0004$$
$$+ (1 - 0.33083) \times 0.0001 = 0.000699 \text{ per hour}$$

(b) The reliability is

$$R = \exp(-\lambda \times 24 \times 30) = \exp(-0.50328) = 0.60454$$

yielding a 30-day failure probability of

$$1 - R = 0.395453$$

Example 3.5 An automobile was driven for a total of 120,000 km. It had 11 failures at the odometer readings as listed in Table 3.2[1]:

Does the failure distribution follow an exponential distribution?

Solution:

Using MINITAB®, find MTBF and discuss the least-squares fit to the data (Figure 3.5).

Example 3.6 An electronic system in an aircraft showed the following table of failures (Table 3.3).

As a system it has historically followed an exponential distribution. Is this failure data fit by an exponential distribution?

What is the MTBF?

Table 3.2 Failures over 120,000-km test course.

4123	27720	63582
4497	28,496	66,057
10,506	40,887	100,763
12,317	48,323	

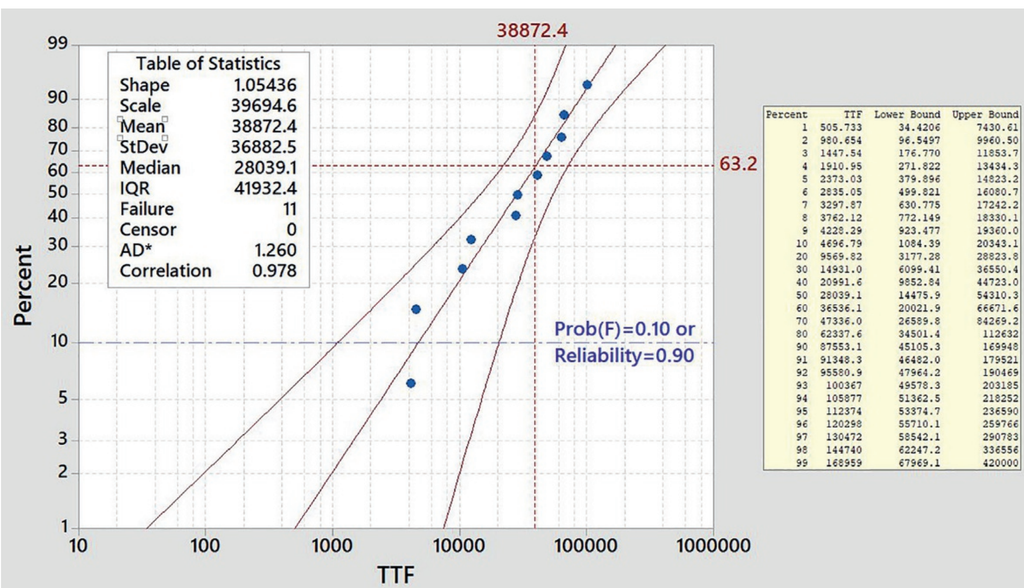


Figure 3.5 Exponential distribution fit to test course failures. Notice how closely the data follows the straight line fit on "exponential" paper. (See Appendix D "Exponential Distribution" for background on how the probability plot is generated.)

1 Kapur & Lamberson, Wiley, p. 270.

Table 3.3 Electronic system failures.

1100	13,489	33180	50545	98674
6697	16,818	35,367	60,280	101,702
8238	23,885	39,703	67,084	102,829
9766	24,323	49,412	70,740	158,880
10,455	27,987	49,729	76,039	206,640

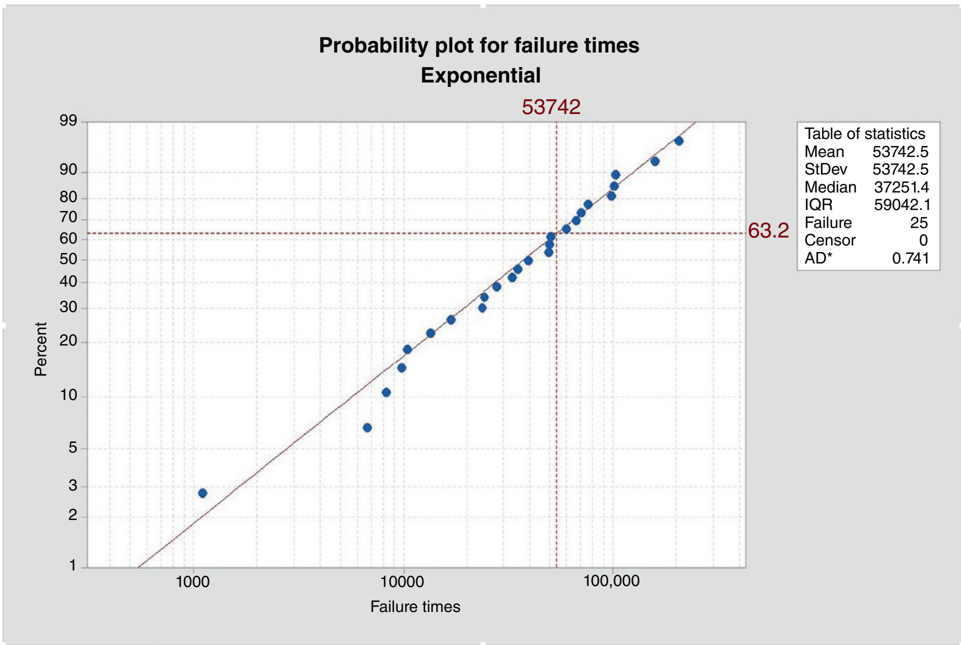


Figure 3.6 Weibull of electronic system failures.

Solution

Using MINITAB, the following exponential probability plot was generated:

By eye: The data shows a very good fit to the exponential line with an MTBF = 53,742 hours.

The p-value being >0.95 also indicates that the exponential distribution fits this data (Figure 3.6).

3.4 Time-Dependent Failure Rates

A variety of situations in which the explicit treatment of early failures or aging effects, or both, require the use of time-dependent failure rate models. This may be illustrated by considering the effect of the accumulated operating time T_0 on the probability that a device can survive for an additional time t. Suppose that we define $R(t|T_0)$ as the reliability of a device that has previously been operated for a time T_0. We may therefore write

$$R(t|\,T_0) = P\{\mathbf{t}' > T_0 + t|\mathbf{t}' > T_0\} \tag{3.47}$$

where $t' = T_0 + t$ is the time elapsed at failure since the device was new. From the definition of conditional probability given in Eq. (2.9), we may write the conditional probability as

$$P\{\mathbf{t}' > T_0 + t|\mathbf{t}' > T_0\} = \frac{P\{\mathbf{t}' > T_0 + t \cap \mathbf{t}' > T_0\}}{P\{\mathbf{t}' > T_0 + t\}} \tag{3.48}$$

However, since $\mathbf{t}' > T_0 + t \cap \mathbf{t}' > T_0 = \mathbf{t}' > T_0 + t\,\mathbf{t}' > T_0 + t$, we may combine equations to obtain

$$R(t|T_0) = \frac{P\{\mathbf{t}' > T_0 + t\}}{P\{\mathbf{t}' > T_0\}} \tag{3.49}$$

The reliability of a new device is then just

$$R(t) = R(t|T_0 = 0) = P\{\mathbf{t}' > t\} \tag{3.50}$$

and we obtain

$$R(t|T_0) = \frac{R(t + T_0)}{R(T_0)} \tag{3.51}$$

Finally, using Eq. (3.18), we obtain

$$R(t|T_0) = e^{-\int_{T_0}^{t+T_0} \lambda(t\prime)dt\prime} \tag{3.52}$$

The significance of this result may be interpreted as follows. Suppose that we view T_0 as a wear-in time undergone by a device before being put into service and t as the service time. Now, we ask whether the wear-in time decreases or increases the service life reliability of the device. To determine this, we take the derivative of $R(t|T_0)$ with respect to the wear-in period and obtain

$$\frac{\partial}{\partial T_0} R(t|T_0) = -[\lambda(T_0) - \lambda(T_0 + t)]R(t|T_0) \tag{3.53}$$

Increasing the wear-in period thus improves the reliability of the device only if the failure rate is decreasing (i.e. $\lambda(T_0) > \lambda(T_0 + t)$). If the failure rate increases with time, wear-in only adds to the deterioration of the device, and the service life reliability decreases.

To model early failures or wear effects more explicitly, we must turn to specific distributions of the time to failure. In contrast to the exponential distribution used for random failures, these distributions must have at least two parameters. Although the normal and lognormal distributions are frequently used to model aging effects, the Weibull distribution is probably the most universally employed. With it we may model early failures and random failures as well as aging effects. We will cover the Weibull distribution in Chapter 5.

3.5 Component Failures and Failure Modes

In Sections 3.3 and 3.4 the quantitative behavior of reliability is modeled for situations with constant and time-dependent failure rates, respectively. In real systems, however, failures occur through a number of different mechanisms, causing the failure rate curve to take a bathtub shape too complex to be described by any single one of the distributions discussed thus far. The mechanisms may be physical phenomena within a single monolithic structure, such as the tread wear, puncture, and defective sidewalls in an automobile tire, or physically distinct components of a system, such as the processor unit, disk drives, and memory of a computer, may fail. In either case, it is usually possible to separate the failures according to the mechanism or the components that caused them. It is then possible, provided that the failures are independent, to generalize and treat the system reliability in terms of mechanisms or component failures. We refer to these collectively as independent failure modes.

Failure Mode Rates

Whether we refer to component failure or failure modes – and the distinction is sometimes blurred – we may analyze the reliability of a system in terms of the component or mode failures, provided they are independent of one another. Independence requires that the probability of failure of any mode is not influenced by that of any other mode. The reliability of a system with *M* different failure modes is

$$R(t) = P\{X_1 \cap X_2 \cap X_3 \cdots X_M\} \tag{3.54}$$

where X_i is the event in which the *i*th failure mode does *not* occur before time *t*. If the modes are independent, we may write the system reliability as the product of the mode survival probabilities:

$$R(t) = P\{X_1\}P\{X_2\}\,P\{X_3\}\cdots P\{X_M\} \tag{3.55}$$

where the mode *i* reliability is

$$R_i(t) = P\{X_i\} \tag{3.56}$$

yielding

$$R(t) = \prod_{i=1}^{i=M} R_i(t) \tag{3.57}$$

Naturally, if mode *i* is the failure of component *i*, then $R_i(t)$ is just the component reliability.

This is illustrated by a three-component *block diagram* of a simple computer system in Figure 3.7.

A reliability block diagram (RBD) is a graphical depiction of a system's components that can be used to determine the overall system reliability.

In this case, the components are independent of and describe the computer system as a *series* system whose reliability (using Eq. (3.57)) is

$$R(\text{system}) = R_1 \times R_2 \times R_3$$

For each mode, we may define a PDF for time to failure, $f_i(t)$, and an associated failure rate, $\lambda_i(t)$. The derivation is exactly the same as in Section 3.2, yielding

$$R_i(t) = 1 - \int_0^t f_i(t')dt' \tag{3.58}$$

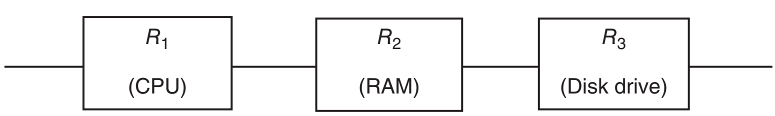


Figure 3.7 Simple computer system block diagram. R_1 is the reliability of the CPU, R_2 is the reliability of the RAM, and R_3 is the reliability of the disk drive.

$$\lambda_i(t) = \frac{f_i(t)}{R_i(t)} \tag{3.59}$$

$$R_i(t) = e^{-\int_0^t \lambda_i(t\prime)dt\prime} \tag{3.60}$$

and

$$f_i(t) = \lambda_i(t)e^{-\int_0^t \lambda_i(t\prime)dt\prime} \tag{3.61}$$

Combining Eqs. (3.55) and (3.56) with Eq. (3.60) then yields

$$R(t) = \exp\left[-\int_0^t \lambda(t')\,dt'\right] \tag{3.62}$$

where

$$\lambda(t) = \sum_{i=1}^{i=M} \lambda_i(t) \tag{3.63}$$

Thus, to obtain the system reliability, we simply add the mode failure rates.

For situations in which independent failure modes may be approximated by constant failure rates, $\lambda_i(t) \to \lambda_\iota$, the reliability is given by Eq. (3.25) with

$$\lambda = \sum \lambda_i \tag{3.64}$$

and Eq. (3.26) may be used to determine the system's mean time to failure. If we define the mean time to failure as

$$\text{MTTF}_i = \frac{1}{\lambda_i} \tag{3.65}$$

the system mean time to failure is related by

$$\frac{1}{\text{MTTF}} = \sum \frac{1}{\text{MTTF}_i} \tag{3.66}$$

In our simple computer system, this would become

$$\begin{aligned}
&R_{system} = e^{-\lambda_1 t} \times e^{-\lambda_2 t} \times e^{-\lambda_3 t} = e^{-(\lambda_1+\lambda_2+\lambda_3)t}\\
&\text{so}, e^{-\lambda_{system} t} = e^{-(\lambda_1+\lambda_2+\lambda_3)t}\\
&\text{then}, \lambda_{system} = \lambda_1 + \lambda_2 + \lambda_3\\
&\text{and}, \frac{1}{\text{MTTF}_{\text{system}}} = \frac{1}{\text{MTTF}_1} + \frac{1}{\text{MTTF}_2} + \frac{1}{\text{MTTF}_3}
\end{aligned} \tag{3.67}$$

Component Counts

The ability to add failure rates is most widely applied in situations in which each failure mode corresponds to a component or part failure. Often, failure rate data may be available at a component level but not for an entire system. This is true, in part, because several professional organizations collect and publish failure rate estimates for frequently used items, whether they be diodes, switches, and other electrical components; pumps, valves, and similar mechanical devices; or a number of other types of components. At the same time, the design of a new system may involve new configurations and numbers of such standard items. The foregoing equations then allow reliability estimates to be made before the new design is built and tested. In this chapter, we first considered only systems without redundancy. Without redundancy, failure of any component implies system failure. In systems with redundant components, the idea of a failure mode is still applicable in a more general sense. We will treat such systems later in this chapter.

When component failure rates are available, the most straightforward, but crudest, estimate of reliability comes from the parts count method. We simply count the number n_j of parts of type j in the system. The system's failure rate is then

$$\lambda = \sum_{j=1}^{j=M} n_j \lambda_j \tag{3.68}$$

where the sum is over the part types in the system.

Example 3.7 A computer-interface circuit card assembly for airborne application is made up of interconnected components in the quantities listed in the first column of Table 3.4. If the assembly must operate in a 50 °C environment, the component failure rates are as given in column 3 of Table 3.4. Calculate

a) the assembly failure rate,
b) the reliability for a 12-hour mission, and
c) the MTTF

Table 3.4 Components and failure rates for computer circuit card.

Component type	Quantity	Failure rate/10^6 hour	Total failure rate/10^6 hour
Capacitor tantalum	1	0.0027	0.0027
Capacitor ceramic	19	0.0025	0.0475
Resistor	5	0.0002	0.0010
J—K, M—S flip flop	9	0.4667	4.2003
Triple Nand gate	5	0.2456	1.2286
Diff line receiver	3	0.2738	0.8214
Diff line driver	1	0.3196	0.3196
Dual Nand gate	2	0.2107	0.4214
Quad Nand gate	7	0.2738	1.9166
Hex invertor	5	0.3196	1.5980
8-bit shift register	4	0.8847	3.5388
Quad Nand buffer	1	0.2738	0.2738
4-Bit shirt register	1	0.8035	0.8035
And-or-inverter	1	0.3196	0.3196
PCB connector	1	4.3490	4.3490
Printed wiring board	1	1.5870	1.5870
Soldering connections	1	0.2328	0.2328
Total	67		21.6616

Source: Reprinted from Ling (1981) (Arithmetic errors corrected).

Solution (a) We have calculated the total failure rate $n_j\lambda_j$ for each component type with Eq. (3.89) and listed them in the third column of Table 3.4. For a nonredundant system, the assembly failure rate is just the sum of these numbers, or as indicated, $\lambda = 21.6610 \times 10^{-6}$/hour.

(b) The 12-hour reliability is calculated from $R = e^{-\lambda t}$ to be

$$R(12) = \exp\left(-21.6610 \times 12 \times 10^{-6}\right) = 0.9997$$

(c) For constant failure rates, the MTTF is

$$\text{MTTF} = \frac{1}{\lambda} = \frac{10^6}{21.6610} = 46,165.9 \text{ hours}$$

The parts count method, of course, is no better than the available failure rate data. Moreover, the failure rates must be appropriate to the particular conditions under which the components are to be employed. For electronic equipment, extensive computerized databases have been developed that allow the designer to take into account the various factors of stress and environment as well as the quality of manufacture. For military procurement, such procedures have been formalized as the parts stress analysis method.

In parts stress analysis, each component failure rate, λ_i, is expressed as a base failure rate, λ_b, and as a series of multiplicative correction factors:

$$\lambda_i = \lambda_b \Pi_E \Pi_Q \cdots \Pi_N \tag{3.69}$$

The base failure rate, λ_b, takes into account the temperature at which the component operates as well as the primary electrical stresses (i.e. voltage, current, or both) to which it is subjected. Figure 3.8 shows qualitatively the effects these variables might have on a particular component type.

The correction factors, indicated by the $\prod$s in Eq. (3.69), take into account the environmental, quality, and other variables that are designated as having a significant impact on the failure rate. For example, the environmental factor Π_E accounts for environmental stresses other than temperature; it is related to the vibration, humidity, and other conditions encountered in operation. For purposes of military procurement, there are nine environmental categories, as listed in Table 3.5. For each component type, there is a wide range of values

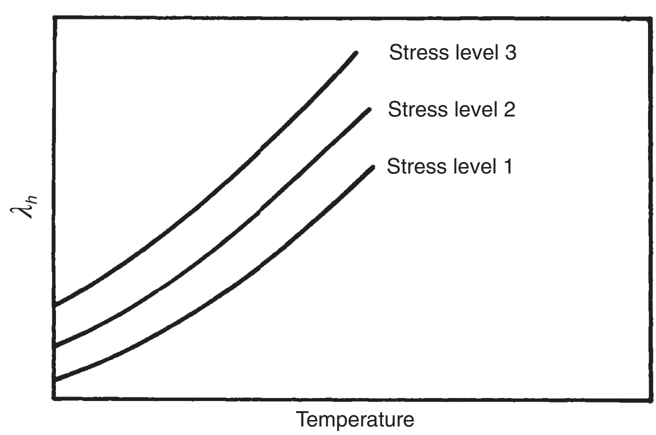


Figure 3.8 Failure rate versus temperature for different levels of applied stress (power, voltage, etc.).

Table 3.5 Environmental symbol identification and description.

Environment	π_e symbol	Nominal environmental conditions	π_e value[a]
Ground, benign	G_B	Nearly zero environmental stress with optimum engineering operation and maintenance.	0.2
Space, flight	S_F	Earth orbital. Approaches G_B conditions without access for maintenance. Vehicle neither under powered flight nor in atmospheric reentry	0.2
Ground, fixed	G_F	Conditions less than ideal: installation in permanent racks with adequate cooling air, maintenance by military personnel, and possible installation in unheated buildings	1.0
Ground, mobile (and portable)	G_M	Conditions less favorable than those for G_F, mostly through vibration and shock. The cooling air supply may be more limited, and maintenance less uniform	4.0
Naval, sheltered	N_s	Surface ship conditions similar to G_F but subject to occasional high levels of shock and vibration	4.0
Naval, unsheltered	N_v	Nominal surface shipborne conditions but with repetitive high levels of shock and vibration	5.0
Airborne, inhabited	A_t	Typical cockpit conditions without environmental extremes of pressure, temperature, shock, and vibration	4.0
Airborne, uninhabited	A_v	Bomb bay, tail, or wing installations, where extreme pressure, temperature, and vibration cycling may be aggravated by contamination from oil, hydraulic fluid, and engine exhaust	3.0
Missile, launch	M_L	Severe noise, vibration, and other stresses related to missile launch, boosting space vehicles into orbit, vehicle reentry, and landing by parachute. Conditions may also apply to installation near main rocket engines during launch operations	10.0

[a] Values for monolithic microelectronic devices.
Source: From Anderson (1976).

of $\prod_E$; for example, for microelectronic devices, II_E ranges from 0.2 for "ground, benign" to 10.0 for "missile launch."

Similarly, the quality multiplier $\prod_Q$ takes into account the level of specification and therefore the level of quality control under which the component has been produced and tested. Typically, $II_Q = 1$ for the highest levels of specification and may increase to 100 or more for commercial parts procured under minimal specifications. Other multiplicative corrections are also used. These include $\prod_A$, the application factor to take into account stresses found in particular applications, and factors to take into account cyclic loading, system complexity, and a variety of other relevant variables.

3.6 Replacements

Thus far, we have considered the distribution of the failure times, given that the system is new at $t = 0$. In many situations, however, failure does not constitute the end of life. Rather, the system is immediately replaced or repaired, and operation continues. In such situations, a number of new pieces of information became important. We may want to know the expected number of failures over some specified period of time in order to estimate the costs of replacement parts. More important, it may be necessary to estimate the probability that more than a specific number of failures N will occur over a period of time. Such information allows us to maintain an adequate inventory of repair parts.

In modeling these situations, we restrict our attention to the constant failure rate approximation. In this, the failure rate is often given in terms of the *mean time between failures* (MTBF), as opposed to the mean time to failure, or MTTF. In fact, they are both the same number if when a system fails, it is assumed to be repaired immediately to an as-good-as-new condition. In what follows, we use the constant failure rate model to derive $p_n(t)$, the probability of there being n failures during a time interval of length t. The derivation leads again to the Poisson distribution introduced in Chapter 2. From it we can calculate the numbers of failures and replacement requirements.

We first consider the times at which the failures take place and therefore the numbers that occur within any given span of time. Suppose that we let **n** be a discrete random variable representing the number of failures that take place between $t = 0$ and a time t. Let

$$p_n(t) = P\{n = n|t\} \tag{3.70}$$

be the probability that exactly n failures have taken place before time t. Clearly, if we start counting failures at time zero, we must have

$$p_0(0) = 1 \tag{3.71}$$

$$p_n(0) = 0, \quad n = 1, 2, 3, \dots, \infty \tag{3.72}$$

In addition, at any time

$$\sum_{n=0}^{\infty} p_n(t) = 1 \tag{3.73}$$

For small Δt, let failure $\lambda \Delta t$ be the probability that the $(n + 1)$th failure will take place during the time increment between t and $t + \Delta t$, given that exactly n failures have taken place before time t. Then, the probability that no failure will occur during Δt is $1 - \lambda \Delta t$. From this we see that the probability that no failures have occurred before $t + \Delta t$ may be written as

$$p_0(t + \Delta t) = (1 - \lambda \Delta t) p_0(t) \tag{3.74}$$

Then, noting that

$$\frac{d}{dt} p_n(t) = \lim_{\Delta t \to 0} \frac{p_n(t + \Delta t) - p_n(t)}{\Delta t} \tag{3.75}$$

we obtain the simple differential equation

$$\frac{d}{dt} p_0(t) = -\lambda p_0(t) \tag{3.76}$$

Using the initial condition, Eq. (3.71), we find

$$p_0(t) = e^{-\lambda t} \tag{3.77}$$

With p_0(t) determined, we may now solve successively for $p_n(t)$, $n = 1, 2, 3, \dots$ in the following manner. We first observe that if n failures have taken place before time t, the probability that the $(n+1)$th failure will take place between t and $t+\Delta t$ is $\lambda\Delta t$. Therefore, since this transition probability is independent of the number of previous failures, we may write

$$p_n(t+\Delta t) = \lambda\Delta t p_{n-1}(t) + (1-\lambda\Delta t)p_n(t) \tag{3.78}$$

The last term accounts for the probability that no failure takes place during Δt. For sufficiently small Δt we can ignore the possibility of two or more failures taking place.

Using the definition of the derivative once again, we may reduce Eq. (3.78) to the differential equation

$$\frac{d}{dt}p_n(t) = -\lambda p_n(t) + \lambda p_{n-1}(t) \tag{3.79}$$

This equation allows us to solve for $p_n(t)$ in terms of $p_{n-1}(t)$. To do this, we multiply both sides by the integrating factor $\exp(\lambda t)$. Then, noting that

$$\frac{d}{dt}\left[e^{\lambda t}p_n(t)\right] = e^{\lambda t}\left[\frac{d}{dt}p_n(t) + \lambda p_n(t)\right] \tag{3.80}$$

we have

$$\frac{d}{dt}\left[e^{\lambda t}p_n(t)\right] = \lambda p_{n-1}(t)e^{\lambda t} \tag{3.81}$$

Multiplying both sides by dt and integrating between 0 and t, we obtain

$$e^{\lambda t}p_n(t) - p_n(0) = \lambda\int_0^t p_{n-1}(t')e^{\lambda t'}dt' \tag{3.82}$$

But, since from Eq. (3.72) $p_n(0) = 0$, we have

$$p_n(t) = \lambda e^{-\lambda t}\int_0^t p_{n-1}(t')e^{\lambda t'}dt' \tag{3.83}$$

This recursive relationship allows us to calculate the p_n successively. For p_1, insert Eq. (3.98) on the right-hand side and carry out the integral to obtain

$$p_1(t) = \lambda t e^{-\lambda t} \tag{3.84}$$

Repeating this procedure for $n = 2$ yields

$$p_2(t) = \frac{(\lambda t)^2}{2}e^{-\lambda t} \tag{3.85}$$

and so on. It is easily shown that Eq. (3.83) is satisfied for all $n \geq 0$ by

$$p_n(t) = \frac{(\lambda t)^n}{n!}e^{-\lambda t} \tag{3.86}$$

and these quantities in turn satisfy the initial conditions given by Eqs. (3.71) and (3.72).

The probabilities $p_n(t)$ are the same as the Poisson distribution $f(n)$, provided that we set $\mu = \lambda t$. We may therefore use Eqs. (2.25) through (2.26) to determine the mean and the variance of the number n of events occurring over a time span t. Thus, the expected number of failures during time t is

$$\mu_n = E\{n\} = \lambda t \tag{3.87}$$

and the variance of n is

$$\sigma_n{}^2 = \lambda t \tag{3.88}$$

Of course, since $p_n(t)$ are the probability mass functions of a discrete variable **n,** we must have, according to Eq. (2.21),

$$\sum_{n=0}^{\infty} p_n(t) = 1 \tag{3.89}$$

The number of failures can be related to the MTBF by

$$\mu_n = \frac{1}{\text{MTBF}} \tag{3.90}$$

We have derived the expression relating μ_n and the MTBF assuming a constant failure rate. It has, however, much more general validity (see e.g., Barlow and Proschan 1965). Although the proof is beyond the scope of this book, it may be shown that Eq. (3.90) is also valid for time-dependent failure rates in the limiting case that $t \gg$ MTBF. Thus, in general, the MTBF may be determined from

$$\text{MTBF} = \frac{t}{n} \tag{3.91}$$

where n, the number of failures, is large.

We may also require the probability that more than N failures have occurred. It is

$$P\{\boldsymbol{n} > N\} = \sum_{n=N+1}^{\infty} \frac{(\lambda t)^n}{n!} e^{-\lambda t} \tag{3.92}$$

Instead of writing this infinite series, however, we may use Eq. (3.89) to write

$$P\{\boldsymbol{n} > N\} = 1 - \sum_{n=0}^{N} \frac{(\lambda t)^n}{n!} e^{-\lambda t} \tag{3.93}$$

Example 3.8 In an industrial plant there is a dc power supply in continuous use. It is known to have a failure rate of $\lambda = 0.40$/year. If replacement supplies are delivered at six-month intervals, and if the probability of running out of replacement power supplies is to be limited to 0.01, how many replacement power supplies should the operations engineer have on hand at the beginning of the six-month interval.

Solution First calculate the probability that the supply will have more than n failures with $t = 0.5$ year,

$$\lambda t = 0.4 \times 0.5 = 0.2; \quad e^{-0.2} = 0.819$$

Now use Eq. (3.93)

$$P\{\mathbf{n} > 0\} = 1 - e^{-\lambda t} = 0.181$$
$$P\{\mathbf{n} > 1\} = 1 - e^{-\lambda t}(1 + \lambda t) = 0.018$$
$$P\{\mathbf{n} > 2\} = 1 - e^{-\lambda t}\left[1 + \lambda t + \frac{1}{2}(\lambda t)^2\right] = 0.001$$

There is less than a 1% probability of more than two power supplies failing. Therefore, two spares should be kept on hand.

3.7 Redundancy

It is a fundamental tenet of reliability engineering that as the complexity of a system increases, the reliability will decrease, unless compensatory measures are taken. Since a frequently used measure of complexity is the number of components in a system, the decrease in reliability may then be expressed in terms of the product rule derived in Eq. (3.57). To recapitulate, if the component failures are mutually independent, the reliability of a system with N nonredundant component is

$$R = R_1 R_2 \ldots R_n \ldots R_N \quad (3.94)$$

where R_n is the reliability of the nth component. The dramatic deterioration of system reliability that takes place with increasing numbers of components is illustrated graphically by considering systems with components of identical reliabilities. In Figure 3.9, system reliability versus component reliability is plotted, each curve representing a system with a different number of components. It is seen, for example that as the number of components is increased from 1 to 2, where each component has a reliability of 0.85, the system reliability is decreased from 0.85 to 0.921.

An alternative to the requirements for increased component reliability is to provide redundancy in part or all of a system. In what follows, we examine a number of different redundant configurations and calculate the effect on system reliability and failure rates. We also discuss specifically several of the trade-offs between different redundant configurations as well as the increased problem of common-mode failures in highly redundant systems.

The graphical presentation of systems provided by (Reliability Block Diagrams) RBDs adds clarity to the discussion of redundancy. In these diagrams, which have their origin in electric circuitry, a signal enters from the left, passes through the system, and exits on the right. Each component is represented as a block in the system; when enough blocks fail so that all the paths by which the

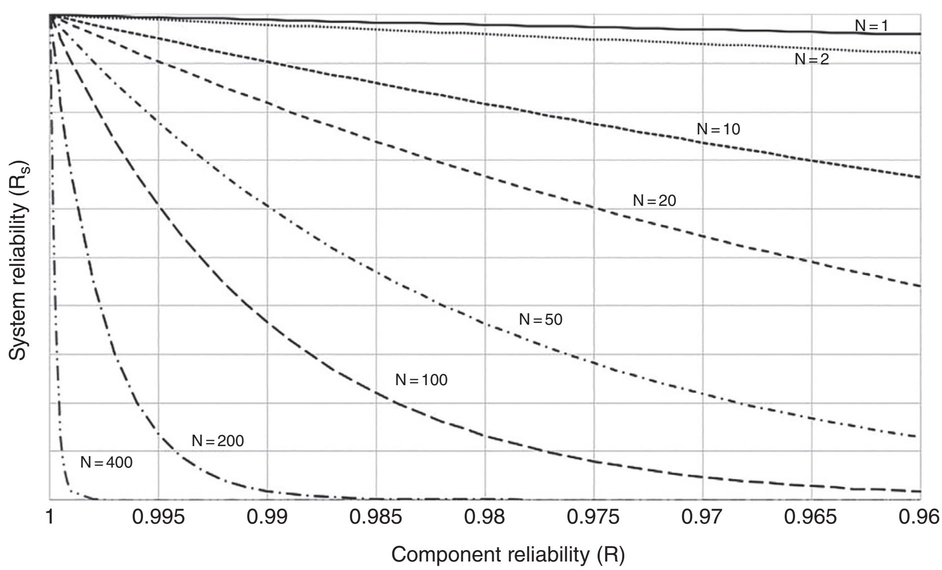


Figure 3.9 As complexity of a series system increases, reliability decreases.

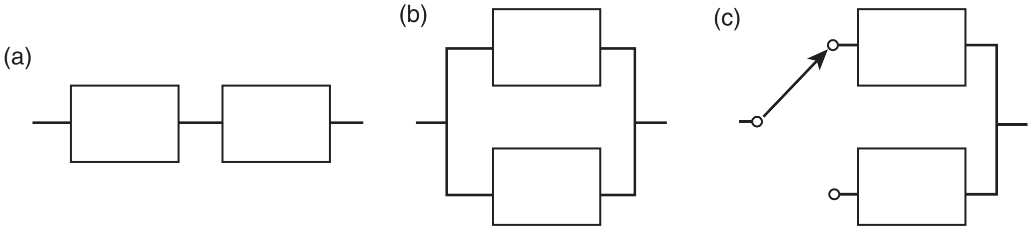


Figure 3.10 Reliability block diagrams: (a) series, (b) active parallel, and (c) standby parallel.

signal may pass from left (input) to right (output) are cut, the system is said to fail. The RBD of a nonredundant system is the series configuration shown in Figure 3.10a; the failure of either block (unit) clearly causes system failure. The simplest redundant configurations are the parallel systems shown in Figure 3.10b,c. In the active-parallel system shown in Figure 3.10b both blocks (units) must fail to cut the signal path and thus cause system failure. In the standby parallel system shown in Figure 3.10c the arrow switches from the upper block (the primary unit) to the lower block (the standby unit) upon failure of the primary unit. Thus, both units must fail for the system to fail. More general redundant configurations may also be represented as RBDs and will be discussed later in this chapter.

Active and Standby Redundancy

We begin our examination of redundant systems with a detailed look at the two-unit parallel configurations pictured in Figure 3.10. They differ in that both units in active parallel are employed and therefore subject to failure from the onset of operation, whereas in a standby parallel the second unit is not brought into operation until the first fails and therefore cannot fail until a later time. In this section, we derive the reliabilities for the idealized configurations, and then in Section 3.7, we discuss some of the limitations encountered in practice. Similar considerations also arise in treating multiple redundancy with three or more parallel units, and in the more complex redundant configurations considered the subsequent sections.

Active Parallel

The reliability $R_a(t)$ of a two-unit active-parallel system is the probability that either unit 1 or unit 2 will not fail until a time greater than t. Designating random variables t_1 and t_2 to represent the failure times, we have

$$R_a(t) = P\{\mathbf{t}_1 > t \cup \mathbf{t}_2 > t\} \tag{3.95}$$

Thus, Eq. (2.6) yields

$$R_a(t) = P\{\mathbf{t}_1 > t\} + P\{\mathbf{t}_2 > t\} - P\{\mathbf{t}_1 > t\} \cap P\{\mathbf{t}_2 > t\} \tag{3.96}$$

Next, we make an important assumption. Assume that the failures are independent events and thus replace the last term in Eq. (3.96) by $P\{\mathbf{t}_1 > t\}P\{\mathbf{t}_2 > t\}$. Denoting the reliabilities of the units as

$$R_i(t) = P\{\mathbf{t}_i > t\} \tag{3.97}$$

we may then write

$$R_a(t) = R_1(t) + R_2(t) - R_1(t)R_2(t) \tag{3.98}$$

Standby Parallel

The derivation of the standby parallel reliability $R_s(t)$ is somewhat more lengthy since the failure time $\mathbf{t}_2$ or the standby unit is dependent on the failure time $\mathbf{t}_1$ of the primary unit. Only the second unit must survive to time t for the system to survive, but with the condition that it cannot fail until after the first unit fails. Hence, we may write

$$R_s(t) = P\{\mathbf{t}_2 > t\,|\mathbf{t}_2 > \mathbf{t}_1\} \tag{3.99}$$

There are two possibilities. Either the first unit does not fail, $\mathbf{t}_1 > t$, or the first unit fails, but the standby unit does not, $\mathbf{t}_1 < t \cap \mathbf{t}_2 > t$. Since these two possibilities are mutually exclusive, according to Eq. (2.7), we may just add the probabilities,

$$R_s(t) = P\{\mathbf{t}_1 > t\} + P\{\mathbf{t}_1 < t\} \cap P\{\mathbf{t}_2 > t\} \tag{3.100}$$

The first term is just $R_1(t)$, the reliability of the primary unit. The second term requires more careful attention. Suppose that the PDF for the primary unit is $f_1(t)$. Then, the probability of unit 1 failing between t' and $t' + dt'$ is $f_1(t')\,dt'$. Since the standby unit is put into operation at t', the probability that it will survive to time t is $R_2\,(t - t')$. Thus, the system reliability, given that the first failure takes place between t' and $t' + dt'$, is $R_2\,(t - t')f_1(t')\,dt'$. To obtain the second term in Eq. (3.100), we integrate primary failure time t' between zero and t:

$$P\{\mathbf{t}_1 < t\} \cap P\{\mathbf{t}_2 > t\} = \int_0^t R_2(t-t')f_1(t')\,dt' \tag{3.101}$$

The standby system reliability then becomes

$$R_s(t) = R_1(t) + \int_0^t R_2(t-t')\,f_1(t')\,dt' \tag{3.102}$$

or using Eq. (3.10) to express the PDF in terms of reliability, we obtain

$$R_s(t) = R_1(t) - \int_0^t R_2(t-t')\frac{d}{dt'}\,R_1(t')\,dt' \tag{3.103}$$

Constant Failure Rate Models

General expressions for active or standby systems reliability can be obtained by inserting Eq. (3.18) for the reliability with time-dependent failure rates into Eqs. (3.98) or (3.103). Comparisons are simplest, however, if we employ a constant failure rate model. Assume that the units are identical, each with a failure rate λ. Equation (3.25), $R = \exp(-\lambda t)$, may then be inserted to obtain

$$R_a(t) = 2e^{-\lambda t} - e^{-2\lambda t} \tag{3.104}$$

for *active parallel*, and

$$R_s(t) = (1 + \lambda t)\,e^{-\lambda t} \tag{3.105}$$

for *standby parallel*.

The system failure rate can be determined for each of these cases using Eq. (3.15). For the active system, we have

$$\lambda_a(t) = -\frac{1}{R_a}\frac{d}{dt}\,R_a = \lambda\left(\frac{1-e^{-\lambda t}}{1-0.5e^{-\lambda t}}\right) \tag{3.106}$$

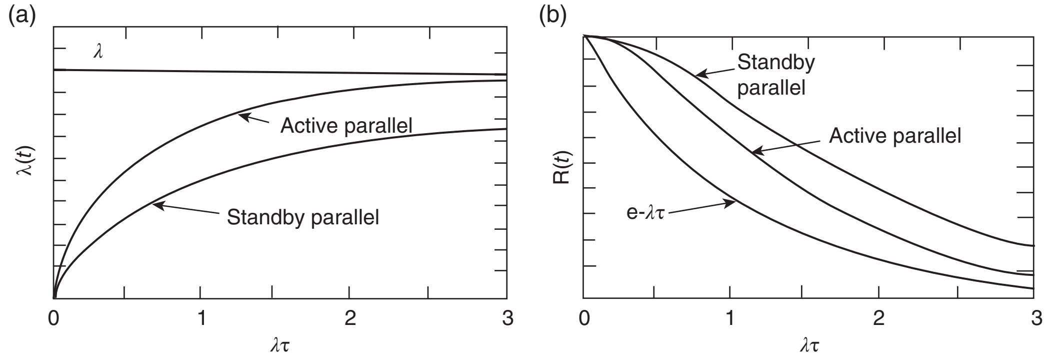


Figure 3.11 Properties of two-unit parallel systems: (a) reliability and (b) failure rate.

while for the standby system

$$\lambda_s(t) = -\frac{1}{R_s}\frac{d}{dt}R_s = \lambda\left(\frac{\lambda t}{1+\lambda t}\right) \tag{3.107}$$

Figure 3.11 shows both the reliability and the failure rate for the two parallel systems, along with the results for a system consisting of a single unit. The results for the failure rates are instructive. For even though the units' failure rates are constants, the failure rates of the redundant systems as a whole are functions of time. Characteristic of systems with redundancy, they have zero failure rates at $t = 0$. The failure rates then increase to an asymptotic value of λ, the value for a single unit. At intermediate times, the failure rate for the standby system is smaller than for the active-parallel system. This is reflected in a larger reliability for the standby system.

Two additional measures are useful in assessing the increased reliability that results from redundant configurations. These are the mean time to failure or MTTF and the rare-event estimate for reliability at times which are small compared to the MTTF of single units. The values of the MTTF for active and standby parallel systems of two identical units are obtained by substituting Eqs. (3.104) and (3.105) into Eq. (3.22). We have

$$\text{MTTF}_\text{a} = \frac{3}{2}\text{MTTF} \tag{3.108}$$

and

$$\text{MTTF}_\text{s} = 2\,\text{MTTF} \tag{3.109}$$

where $\text{MTTF} = 1/\lambda$ for each of the two units. Thus, there is a greater gain in MTTF for the standby than for the active system.

Frequently, the reliability is of most interest for times that are small compared to the MTTF, since it is within the small-time domain where the design life of most products falls. If the single unit reliability, $R = \exp(-\lambda t)$, is expanded in a power series of λt, we have

$$R(t) = 1 - \lambda t + \tfrac{1}{2}(\lambda t)^2 - \tfrac{1}{6}(\lambda t)^3 + \ldots \tag{3.110}$$

The rare-event approximation has the form of one minus the leading term in λt. Thus,

$$R(t) \approx 1 - \lambda t, \lambda t \ll 1 \tag{3.111}$$

for a single unit. Employing the same exponential expansion for the redundant configurations, we obtain

$$R_a(t) \approx 1 - (\lambda t)^2, \quad \lambda t \ll 1 \tag{3.112}$$

from Eq. (3.104) and

$$R_s(t) \approx 1 - \tfrac{1}{2}(\lambda t)^2, \quad \lambda t \ll 1 \tag{3.113}$$

from Eq. (3.105). Hence, for short times, the failure probability, $1 - R$, for a standby system is only one-half of that for an active-parallel system.

Example 3.9 The MTTF of a system with a constant failure rate has been determined. An engineer is to set the design life so that the end-of-life reliability is 0.9.

a) Determine the design life in terms of the MTTF.
b) If two of the systems are placed in active parallel, to what value may the design life be increased without causing a decrease in the end-of-life reliability?

Solution Let the failure rate be $\lambda \equiv 1/\text{MTTF}$.
(a) $R = e^{-\lambda T}$. Therefore, $T = (1/\lambda)\ \ln\ (1/R)$.

$$T = \ln\left(\frac{1}{R}\right) \times \text{MTTF} = \ln\left(\frac{1}{0.9}\right)\text{MTTF} = 0.105\ \text{MTTF}$$

(b) From Eq. (3.104), $R = 2e^{-\lambda T} - e^{-2\lambda T}$. Let $x \equiv e^{-\lambda T}$. Therefore, $x^2 - 2x + R = 0$. Solve the quadratic equation:

$$x = \frac{+\,2 \pm \sqrt{4 - 4R}}{2} = 1 - \sqrt{1 - R}$$

The "+" solution is eliminated, since x cannot be greater than 1. Since $x = e^{-\lambda T} = 1 - \sqrt{1 - R}$, then with $\lambda = 1/\text{MTTF}$,

$$\begin{aligned} T &= \ln\left[\frac{1}{(1 - \sqrt{1 - R})}\right] \times \text{MTTF} \\ &= \ln\left[\frac{1}{(1 - \sqrt{1 - 0.9})}\right] \times \text{MTTF} = 0.380\ \text{MTTF} \end{aligned}$$

Thus, the redundant system may have nearly four times the design life of the single system, even though it may be seen from Eq. (3.108) that the MTTF of the redundant system is only 50% longer.

3.8 Redundancy Limitations

The results for active and standby reliability presented thus far are highly idealized. In practice, a number of factors can significantly reduce the reliability of redundant systems. In reality, these factors and their mitigation often are dominant in determining the level of reliability which can be achieved. For active-parallel systems, common-mode failures and load-sharing phenomena tend to be of most concern. For standby systems, switching failures and failure of the standby unit before switching are important considerations.

Common-Mode Failures

Common-mode failures are caused by phenomena that create dependencies between two or more redundant components which cause them to fail simultaneously. Such failures have the potential for negating much of the benefit gained with redundant configurations. Common-mode failures may be caused by common electric connections, shared environmental stresses such as dust or vibration, common maintenance problems, or a host of other factors. In commercial aviation, for example a great deal of redundancy is employed, allowing high levels of safety to be achieved. Thus, when problems do occur frequently they may be attributed to common-mode failures: the dust rising from a volcanic eruption in Alaska that caused simultaneous malfunctioning of all of a commercial airliner's engines, or the pieces of a fractured jet engine turbine blade that cut all of the redundant hydraulic control lines and caused the crash of a DC10.

Viewed in terms of the RBDs in Figure 3.10, common-mode failure mechanisms have the same effect as putting in an additional component in series with the parallel configuration. For identical units with reliability R, the active-parallel reliability given by Eq. (3.98) becomes

$$R'_a = \left(2R - R^2\right)R' \tag{3.114}$$

where R' is the contribution to decreased reliability from common-mode failures. The effects are illuminated if we recast this equation in terms of the failure probability $p = 1 - R$, $p' = 1 - R'$, and $p'_a = 1 - R'_a$ corresponding to each of the reliabilities. Equation 3.114 may be written as

$$p'_a = p' + p^2 - p'p^2 \tag{3.115}$$

Suppose that we have an aircraft engine with a failure probability per flight of $p = 10^{-6}$ and a common-mode failure probability a thousand times smaller: $p' = 10^{-9}$. For a two-engine aircraft in the absence of common-mode failures, the failure probability would be $p^2 = 10^{-12}$, but from Eq. (3.115) we see that

$$p'_a = 10^{-9} + 10^{-12} - 10^{-21} \tag{3.116}$$

Thus, the system failure probability, $p'_a \approx 10^{-9}$, is totally dominated by common-mode failure, although it is still far more reliable than if a single engine had been used.

A great deal of the engineering of redundant systems is expended on identifying possible common-mode mechanisms and eliminating them. Nevertheless, some possibilities may be impossible to eliminate entirely, and therefore, reliability modeling must take them into account. Most commonly, such phenomena are modeled through the following constant failure rate model (Flemming and Raabe 1978). Suppose that λ is the total failure rate of a single unit. We divide λ into two contributions

$$\lambda = \lambda_I + \lambda_c \tag{3.117}$$

where λ_I is the rate of independent failure, and λ_c is the common-mode failure rate. These partial failure rates may be used to express common-mode failure rates in active-parallel systems as follows. *Define the factor* ζ as the ratio

$$\zeta = \lambda_c/\lambda \tag{3.118}$$

Each of the units then has a failure mode reliability of

$$R_I = e^{-\lambda_I t} \tag{3.119}$$

which accounts only for independent failures. Therefore, the system reliability for independent failure is determined using λ_I, in Eq. (3.104). We multiply this system reliability by $\exp(-\lambda_c t)$ to account for common-mode failures. Thus, for the two units in parallel

$$R_a(t) = \left(2e^{-\lambda_I t} - e^{-2\lambda_I t}\right)e^{-\lambda_c t} \tag{3.120}$$

or using $\lambda_c = \zeta\lambda$ and $\lambda_I = (1-\zeta)\lambda$, we may write

$$R_a(t) = \left[2 - e^{-(1-\zeta)\lambda t}\right] e^{-\lambda t} \tag{3.121}$$

The loss of reliability with the increase in the ζ factor is clearly seen by looking at the rare-event approximation at small λt, for we now have a term which is linear in λt:

$$R_a(t) \approx 1 - \zeta\lambda t - \left(1 - 2\zeta + \zeta^2/2\right)(\lambda t)^2 + \cdots \tag{3.122}$$

as opposed to $1 - (\lambda t)^2$ as in Eq. (3.112). The effect of common-mode failures can also be seen in the reduction in the meantime to failure:

$$\text{MTTF}_a = \left[2 - \frac{1}{2-\zeta}\right]\text{MTTF} \tag{3.123}$$

Example 3.10 Suppose that a unit has a design-life reliability of 0.95.

a) Estimate the reliability if two of these units are put in active parallel and there are no common-mode failures.
b) Estimate the maximum fraction ζ of common failures that is acceptable if the parallel units in *a* are to retain a system reliability of at least 0.99.

Solution From Eq. (3.131), take $\lambda t = 0.05$.
(a) $R \approx 1 - (\lambda T)^2$, $R = 0.9975$.
(b) From Eq. (3.122),

$$\widetilde{R} = 1 - R = 0.01 \approx \zeta\lambda T + \left(1 - 2\zeta + \frac{\zeta^2}{2}\right)(\lambda T)^2$$

Thus, with $\lambda T \approx 0.05$, we have

$$0.00125\zeta^2 + 0.045\zeta - 0.0075 = 0$$

Therefore,

$$\zeta = \frac{-0.045 \pm \left(2.0625 \times 10^{-3}\right)^{1/2}}{0.0025}$$

For ζ to be positive, we must take the positive root. Therefore, $\zeta \leq 0.166$.

Load Sharing

Load sharing is a second cause of reliability degradation in active-parallel systems. For redundant engines, motors, pumps, structures, and many other devices and systems, the failure of one unit will increase the stress level on the other and therefore increase its failure rate. A simple example is two flashlight batteries placed in parallel to provide a fixed voltage. Assume the circuit is designed so that if either fails, the other will supply adequate voltage. Nevertheless, the current through the remaining battery will be higher, and this will cause greater heating in the internal resistance. The net result is that the remaining battery will operate at a higher temperature and thus tend to deteriorate faster.

Fortunately, in a redundant system with sufficient capacity, the increased failure rate should not lead to unacceptable failure probabilities. If the first failure is detected, the system may be required to operate for only a short period of time before repairs are made. Thus, if one engine fails in a multiengine aircraft, it is only necessary that the flight continue to the nearest airfield without incurring a significant probability of a second engine failure. From this standpoint, the degradation is less serious than the potential for common-mode failures.

In Chapter 10, Markov methods are used to develop the following model for shared load redundancy with time-independent failure rates. Suppose that $\lambda^* > \lambda$ is the increased failure rate of the remaining unit after the first has failed. Then, in the absence of common-mode failures,

$$R_a(t) = (2\lambda - \lambda^*)^{-1}\left(2\lambda e^{-\lambda^* t} - \lambda^* e^{-2\lambda t}\right) \tag{3.124}$$

This may be seen to reduce to Eq. (3.104) in the limiting case that $\lambda^* = \lambda$. A conservative design procedure, which always gives an underestimate of the reliability, is to replace λ by λ^* in Eq. (3.104), thereby assuming that each unit is carrying the entire load of the system.

If λ^* becomes too large, all of the benefits of the redundancy may be lost, and in fact, the system may be less reliable than a single unit with failure rate A. For example, it may be shown that if $\lambda^* > 1.56\lambda$, the MTTF will be less than for a single unit. In the limit as $\lambda^* \to \infty$, Eq. (3.104) reduces to the reliability for the two units placed in series. This may be understood as follows: If either unit failing gives rise to the second unit failing almost instantaneously, then indeed the system failure rate will be twice that of a single unit. For in doubling the number of units, one increases the possibility of a first failure.

Example 3.11 In an active-parallel system, each unit has a failure rate of 0.002/hours.

a) What is the MTTF_a if there is no load sharing?
b) What is the MTTF_a if the failure rate increases by 20% as a result of increased load?
c) What is the MTTF_a if one simply (and conservatively) increased both the unit failure rates by 20%?

Solution

(a)

$$\text{MTTF}_a = \frac{3}{2}\text{MTTF} = \frac{3}{2\lambda} = \frac{3}{2 \times 0.002} = 750 \text{ hours}$$

(b)

$$\text{MTTF}_a = \int_0^\infty R_a(t)dt = \int_0^\infty (2\lambda - \lambda^*)^{-1}\left(2\lambda e^{-\lambda^* t} - \lambda^* e^{-2\lambda t}\right)dt$$

or

$$\text{MTTF}_a = \frac{1}{2\lambda}\left[1 + 2\left(\frac{\lambda}{\lambda^*}\right)\right]$$

Thus, with

$$\lambda* = 1.2 \times 0.002 = 0.0024/\text{hour}$$

we have

$$\text{MTTF}_a = \frac{1}{2 \times 0.002}\left(1 + 2x\,\frac{1}{1.2}\right) = 667\,\text{hours}$$

(c)

$$\text{MTTF}_a = \frac{3}{2\lambda*} = \frac{3}{2 \times 0.0024} = 625\,\text{hours}$$

Switching and Standby Failures

Common-mode failures are less likely for standby than for active-parallel configurations because the secondary system may be quite different from the primary. For example, the causes of the failure of electric power are likely to be quite different than those that may cause the diesel backup generator to fail. Nevertheless, care must also be exercised in the design and operation of systems with standby redundancy. Some smaller possibility of common-mode failure incapacitating both primary and secondary units may remain. In addition, two new failure modes, unique to standby configurations, must be addressed: switching failures and secondary unit failure while in the standby mode. The following illustration may be helpful in understanding these modes.

Suppose that power is supplied by a diesel generator. A second identical generator is used for backup. If there is some probability, p, that a switch cannot be made to the second generator upon failure of the primary unit, as derived in Chapter 10, the reliability of the system is obtained by multiplying the second term in Eq. (3.105) by $(1-p)$:

$$R_s(t) = [1 + (1-p)\lambda t]e^{-\lambda t} \tag{3.125}$$

One cause of switching failures is the failure of the control mechanism in sensing the primary unit failure and turning on the secondary unit. Time is also an important consideration, for in certain situations some delay can be tolerated before the backup unit takes over. For example, if a pump supplying coolant to a reservoir fails, it may only be necessary for the backup system to come on before the reservoir drains. On a shorter time scale, if a process control computer fails, there may be a period of seconds or less before the backup is required. If some time delay is tolerable, repeated attempts to switch the system may be made, or parts replaced.

Failure of the secondary unit to function may result not only from switching failures. The secondary system may also have failed in the standby mode before the primary system failure. Such failures are most prone to happen in situations where the secondary unit is called upon very infrequently and therefore may have been allowed to deteriorate while in the standby mode. In Chapter 10 an expression for reliability in which both failure modes are present is developed. The result is equivalent to affixing the multiplicative factor $(\lambda^{+}\,t)^{-1}\,(1-e^{-\lambda+t})$ to the second term in Eq. (3.125)

$$R_s(t) = \left[1 + (1-p)\frac{\lambda}{\lambda^{+}}\left(1 - e^{-\lambda^{+}t}\right)\right]e^{-\lambda t} \tag{3.126}$$

where λ^{+} is the failure rate of the secondary unit while in standby.

Example 3.12 An engineer designs a standby system with two identical units to have an idealized MTTF of 1000 days. To be conservative, she then assumes a switching failure probability of 10% and the failure rate of the unit in standby of 10% of the unit in operation.

Assuming constant failure rates, estimate the reduced MTTF_s of the system with switching and standby failures included.

Solution For the idealized MTTF, we have $\text{MTTF}_S = 2/\lambda$ or $\lambda = 2/1000$ days $= 0.002$/day.

For the reduced MTTF_s, we have

$$\text{MTTF}_s = \int_0^\infty R_s(t)dt = \int_0^\infty \left\{ \left[1 + (1-p)\frac{\lambda}{\lambda^+}\left(1 - e^{-\lambda^+ t}\right)\right] e^{-\lambda t} \right\} dt$$

or

$$\text{MTTF}_s = \frac{1}{\lambda}\left[1 + (1-p)(1 + \lambda^+/\lambda)^{-1}\right]$$

Thus, with $p = 0.1$ and $\lambda^+/\lambda = 0.1$, we have

$$\text{MTTF}_s = \frac{1}{0.002}\left[1 + (1-0.1)(1 + 0.1)^{-1}\right] = 909 \text{ days}$$

Cold, Warm, and Hot Standby

The trade-off between switching failures and failure in standby must be considered in the design of standby redundancy; it is the primary consideration in determining whether cold, warm, or hot standby is to be used. In cold standby, the secondary unit is shut down until needed. This typically reduces the value of λ^+ to a minimum. However, it tends to result in the largest values of p. Thus, in our example of the diesel generator, it is most likely not to have failed if it has not been operating. However, coming from cold startup to a fully loaded operation on short notice may cause sufficient transient stress to result in a significant demand failure probability. In warm standby, the transient stresses are reduced by having the secondary unit continuously in operation but in an idling or unloaded state. In this case, p may be expected to be smaller, at the expense of a moderately increased value of λ^+. Even smaller values of p are achieved by having the secondary unit in hot standby, that is continuously operating at a full load. In this case – for identical units – the failure rate will equal that of the primary system, $\lambda^+ = \lambda$, causing Eq. (3.126) to reduce to

$$R_s(t) = (2-p)e^{-\lambda t} - (1-p)e^{-2\lambda t} \tag{3.127}$$

We see from this equation that if the switching failure can be made very small, which is the object of hot standby, the equation is equivalent to an active-parallel system. Thus, the reliability is markedly less than for an idealized standby system. In many instances of warm or hot standby, however, secondary unit failures in standby can be detected and repaired fairly rapidly. The modeling of such repairable systems is taken up in Chapters 9 and 10.

Redundant computer control systems present a somewhat different situation than that encountered with motors, engines, pumps, or other energy or mass delivery systems. In order to start from cold standby not only must the computer be powered, but the current data must also be loaded to memory. Hot standby is particularly advantageous in these cases where switching the output from the primary to the secondary computer is a relatively simple matter. There is, however, one difficulty. A means must be established for detecting which computer is wrong. This is straightforward if the computer stops functioning altogether. However, if the failure mode is a type that caused the computer to give incorrect but plausible output, then a means for knowing where the incorrect information is being produced is a necessity. For these situations the 2/3 voting systems discussed in the following section are widely used.

3.9 Multiply Redundant Systems

The reliability of a system can be further enhanced by placing increased numbers of components in parallel. Such redundancy can take either active or standby form. In $1/N$ and m/N redundancy, respectively, one or m of the A units must function for the system to function. Consider $1/N$ redundancy first for active and then for standby parallel. In either of these configurations, the probability of system malfunction becomes increasingly small, and as a result, increased attention must be given to the complications discussed in Section 3.7.

1/*N* Active Redundancy

Suppose that we have N components in parallel; if any one of them functions, the system will function successfully. Thus, in order for the system to fail, all the components must fail. This may be written as follows. Let X_i denote the event of the ith component failure, and X the system failure. Thus, for a system of N parallel components, we have

$$X = X_1 \cap X_2 \cap \cdots \cap X_N \tag{3.128}$$

and the system reliability is

$$R_a = 1 - P\{X_1 \cap X_2 \cap \cdots \cap X_N\} \tag{3.129}$$

If the failures are mutually independent, we may use the definition of independence to write

$$R_a = 1 - P\{X_1\}P\{X_2\}\cdots P\{X_N\}, \text{where } P\{X_i\} = 1 - R_i \tag{3.130}$$

The $P\{X_i\}$ are the component failure probabilities; therefore, they are related to the reliabilities by

$$P\{X_i\} = 1 - R_i \tag{3.131}$$

Consequently, we have for $1/N$ active redundancy

$$R_a = 1 - \prod_i (1 - R_i) \tag{3.132}$$

For identical components this may be simplified. Suppose that all the R_is have the same value, $R_i = R$. Equation (3.131) then reduces to

$$R_a = 1 - (1 - R)^N \tag{3.133}$$

The degree of improvement in system reliability brought about by multiple redundancy is indicated in Figure 3.12, where system reliability is plotted versus component reliability for different numbers of parallel components. Two other characterizations of the increased reliability are given by the rare-event approximation and the MTTF. The expansion of Eq. (3.111) yields $1 - R \approx \lambda t$ for small λt and results in the reduction of Eq. (3.133) to

$$R_a(t) \approx 1 - (\lambda t)^N, \quad \lambda t \ll 1 \tag{3.134}$$

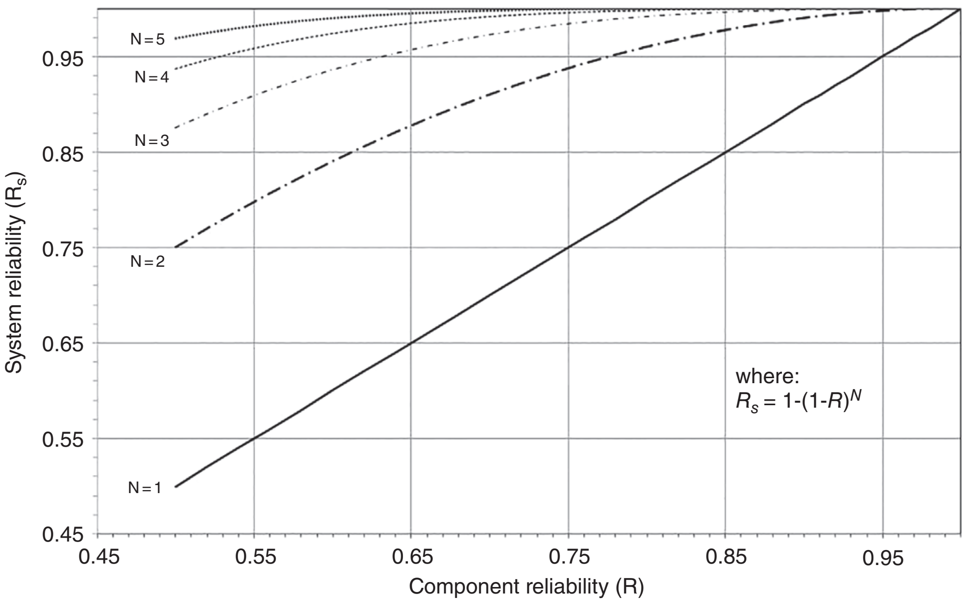


Figure 3.12 Reliability improvement by N parallel components.

We may use the binomial expansion, introduced in Chapter 2, to express the reliability in a form that is more convenient for evaluating the MTTF. The binomial coefficients allow us to write in general

$$(p+q)^N = \sum_{n=0}^{N} {}_NC_n P^{N-n} q^n \tag{3.135}$$

where the ${}_NC_n$ coefficients are given by ${}_NC_R = \frac{N!}{R!(N-R)!}$. Taking $p = 1$ and $q = -R$, we obtain

$$(1-R)^N = \sum_{n=0}^{N} {}_NC_n(-1)^n R^n \tag{3.136}$$

Therefore, since $C_0^N = 1$, we may write Eq. (3.152) as

$$R_a = \sum_{n=1}^{N} (-1)^{n-1} {}_NC_n R^n \tag{3.137}$$

We next assume a constant failure rate for each component and replace R with $e^{-\lambda t}$. Applying Eq. (3.22), to express the MTTF in terms of $R_a(t)$, we obtain

$$\text{MTTF}_a = \sum_{n=1}^{N} (-1)^{n-1} \frac{{}_NC_n}{n\lambda} \tag{3.138}$$

While the forgoing relationships indicate that in principle, reliabilities very close to 1 are obtainable, common-mode failures become an increasingly overriding factor when N is taken to be 3 or more. If the ζ factor method is applied, for example the loss of reliability may be dominated not by the $(\lambda t)^N$ of Eq. (3.133) but by a $\zeta\ \lambda t$ term as in Eq. (3.122). Likewise, the load-sharing phenomena become increasingly serious as additional units fail. A four-engine aircraft, flying on one engine, may be expected to be under higher stress than a two-engine aircraft flying on one.

Example 3.13 A temperature sensor is to have a design-life reliability of no less than 0.98. Since a single sensor is known to have a reliability of only 0.90, the design engineer decides to put two of them in parallel. From Eq. (3.98) the reliability should then be 0.99, meeting the criterion. Upon reliability testing, however, the reliability is estimated to be only 0.97. The engineer first deduces that the degradation is due to common-mode failures and then considers two options: (i) putting a third sensor in parallel and (ii) reducing the probability of common-mode failures.

a) Assuming that the sensors have constant failure rates, find the value of ζ that characterizes the common-mode failures.
b) Will adding a third sensor in parallel meet the reliability criterion if nothing is done about common-mode failures?
c) By how much must ζ be reduced if the two sensors in parallel are to meet the criterion?

Solution: If the design-life reliability of a sensor is $R_1 = e^{-\lambda t} = 0.9$, then $\lambda T = \ln(1/R_1) = \ln(1/0.9) = 0.10533$.

(a) Let $R_2 = 0.97$ be the system reliability for two sensors in parallel. Then, $\zeta$is found in terms of R_2 from Eq. (3.121) to be

$$\begin{aligned}\zeta &= 1 + \frac{1}{\lambda T}\ln\left(2 - R_2 e^{\lambda T}\right)\\ &= 1 + \frac{1}{0.10536}\ln\left(2 - \frac{0.97}{0.9}\right)\\ &= 0.2315\end{aligned}$$

(b) The reliability for three sensors in parallel is given by Eq. (3.133) with $N = 3$. Using $\lambda_1 = (1-\beta)\lambda$ and $\lambda_c = \zeta\lambda$, we may expand the bracketed term to obtain

$$R_3 = \left[3 - 3e^{-(1-\zeta)\lambda T} + e^{-2(1-\zeta)\lambda T}\right]e^{-\lambda T}$$

From a we have $(1-\zeta)\,\lambda T = (1 - 0.2315)\times 0.10536 = 0.08097$, and thus $e^{-(1-\zeta)\lambda T} = 0.92222$. Thus, the reliability is

$$R_3 = \left[3 - 3\times 0.92222 + (0.92222)^2\right]\times 0.9 = 0.975$$

Therefore, the criterion is not met by putting a third sensor in parallel.

(c) To meet the criterion with two sensors in parallel, we must reduce enough so that the equation in part a is satisfied with $R_2 = 0.98$. Thus,

$$\zeta = 1 + \frac{1}{0.10536}\ln\left(2 - \frac{0.98}{0.9}\right) = 0.1165$$

Therefore, ζ must be reduced by at least

$$1 - \frac{0.1165}{0.2315} \approx 50\%$$

1/*N* Standby Redundancy

We may derive expressions for $1/N$ standby reliability by noting that the derivation of the recursive equation, Eq. (3.103), is valid even if $R_1(t)$ represents a standby system. Thus, we may derive the reliability of a standby system of N identical units in terms of a system of $N-1$ units. Suppose that we denote the reliability of the n unit system as R_n, and thus of the $n-1$ system as R_{n-1} where the reliability of a single unit is $R_1 = R$. We may now rewrite Eq. (3.103) as

$$R_n(t) = R_{n-1}(t) - \int_0^t R_n(t-t')\frac{d}{dt'}R_{n-1}(t')\,dt' \tag{3.139}$$

Thus, R_2, in the constant failure rate approximation given by Eq. (3.105), may be shown to result from inserting $R = R_1 = e^{-\lambda t}$ into the right-hand side of this expression. Likewise, if Eq. (3.105) is inserted into the right-hand side of this expression, we obtain

$$R_3(t) = \left[1 + \lambda t + \frac{1}{2}(\lambda t)^2\right]e^{-\lambda t} \tag{3.140}$$

This expression can be inserted into the right of Eq. (3.139) to obtain R_4 and so on. In general, for N units in standby redundancy, we obtain

$$R_s(t) = \sum_{n=0}^{N-1}\frac{1}{n!}(\lambda t)^n e^{-\lambda t} \tag{3.141}$$

Equation (3.22) then yields a standby MTTF of

$$\text{MTTF}_s = N/\lambda \tag{3.142}$$

To calculate the rare-event approximation, we first note that the exponential expansion can be written as two sums:

$$e^{\lambda t} = \sum_{n=0}^{N-1}\frac{1}{n!}(\lambda t)^n + \sum_{n=N}^{\infty}\frac{1}{n!}(\lambda t)^n \tag{3.143}$$

Solving for the first sum, and inserting the result into Eq. (3.141), we obtain after simplification

$$R_s(t) = 1 - \sum_{n=N}^{\infty}\frac{1}{n!}(\lambda t)^n e^{-\lambda t} \tag{3.144}$$

Thus, taking the lowest order terms, we find for small λt that

$$R_s(t) \approx 1 - \frac{1}{\text{N!}}(\lambda t)^N \tag{3.145}$$

We see that the *1/N* standby configuration comes closer to 1 in the rare-event approximation than does Eq. (3.134) for the active-parallel system. Of course, switching failures and failures in the standby state must be included to make more realistic comparisons.

m/N Active Redundancy

In the $1/N$ systems considered thus far, if any one of the two or more units functions, the system operates successfully. We now turn to the *m/N* system in which m is the minimum number that must function for successful system operation. The *m/N* is popular for relief valves, pumps, motors, and other equipment that must have a specified capacity to meet the design criteria. In such systems it is often possible to increase reliability without a commensurate cost increase, for components of off-the-shelf sizes may meet capacity requirements while at the same time allowing for some degree of redundancy. In instrumentation and control systems *m/N* configurations are popular for two

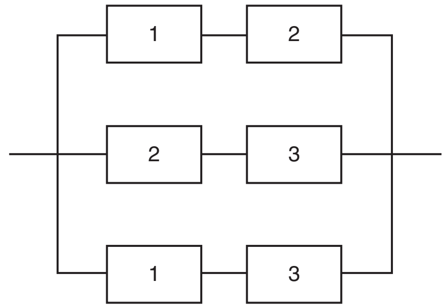


Figure 3.13 Reliability block diagram for a $\frac{2}{3}$ system.

reasons. The spurious fail-safe operation of a single unit is prevented from causing undesirable consequences. Likewise, voting can be applied to the output of redundant instruments or computers.

An *m/N* system may be represented in a RBD, as shown for a 2/3 system in Figure 3.13. Now, however, the block representing each component must be repeated in the diagram. Thus, the system reliability cannot be calculated as in earlier $1/N$ cases because the three parallel chains contain some of the same components and therefore cannot be independent of one another.

For identical components, the reliability of an *m/N* system may be determined by again returning to the binomial distribution. Suppose that p is the probability of failure over some period of time for one unit. That is

$$p = 1 - R \tag{3.146}$$

where R is the component reliability. From the binomial distribution, the probability that n units will fail is just

$$P\{\mathbf{n} = n\} = C_n^N p^n (1-p)^{N-n} \tag{3.147}$$

The *m/N* system will function if there are no more than $N - m$ failures. Thus,

$$P\{\mathbf{n} \le N-m\} = \sum_{n=0}^{N-m} C_n^N p^n (1-p)^{N-n} \tag{3.148}$$

is the reliability. Combining Eqs. (3.146) and (3.14) then yields

$$R_a = \sum_{n=0}^{N-m} C_n^N (1-R)^n R^{N-n} \tag{3.149}$$

Alternately, since

$$P\{\mathbf{n} > N-m\} = \sum_{n=N-m+1}^{N} C_n^N p^n (1-p)^{N-n} \tag{3.150}$$

is the probability that the system will fail, we may also write the system reliability as

$$R_a = 1 - \sum_{n=N-m+1}^{N} C_n^N (1-R)^n R^{N-n} \tag{3.151}$$

Equations (3.149) and (3.151) are identical in value. Depending on the ratio of m to N, one may be more convenient than the other to evaluate. For example, in a $1/N$ system, Eq. (3.151) is simpler to evaluate, since the sum on the right-hand side has only one term, $n = N$, yielding Eq. (3.133).

In dealing with redundant configurations, whether of the $1/N$ or m/N variety, we can simplify the calculations substantially with little loss of accuracy if the component failure probabilities are small (i.e. when the component's reliability approaches 1). In these situations, a reasonable approximation includes only the leading term in the summation of Eq. (3.151). To illustrate, suppose that R *is* very close to 1; we may replace it by 1 in the R^{N-n} term to yield

$$R_a \approx 1 - \sum_{n=N-m+1}^{N} C_n^N (1-R)^n \tag{3.152}$$

We note, however, that the terms in the $(1-R)^n$ series decrease very rapidly in magnitude as the exponent is increased. Consequently, we need to include only the term with the lowest power of $1-R$. Thus, the reliability is approximately

$$R_a \approx 1 - C_{N-m+1}^N (1-R)^{N-m+1} \tag{3.153}$$

If the rare-event approximation, $1 - R \approx \lambda t$, is employed, then

$$R_a \approx 1 - C_{N-m+1}^N (\lambda t)^{N-m+1} \tag{3.154}$$

Example 3.14 A pressure vessel is equipped with six relief valves. Pressure transients can be controlled successfully by any three of these valves. If the probability that any one of these valves will fail to operate on demand is 0.04, what is the probability on demand that the relief valve system will fail to control a pressure transient? Assume that the failures are independent.

Solution In this situation, the foregoing equations are valid if unreliability, $\widetilde{R}_a = 1 - R_a$, is defined as demand failure probability. Using the rare-event approximation, we have from Eq. (3.153), with $N = 6$ and $m = 3$, $0.04 = 1 - R$:

$$\widetilde{R}_a \approx C_4^6 (0.04)^4 = \frac{6!}{2!4!}(0.04)^4 = 15 \times 256 \times 10^{-8}$$
$$\widetilde{R}_a \approx 0.384 \times 10^{-4}$$

3.10 Redundancy Allocation

High reliability can be achieved in a variety of ways; the choice will depend on the nature of the equipment, its cost, and its mission. If we were to provide an emergency power supply for a hospital, an air traffic control system, or a nuclear power plant, for example the most cost-effective solution might well be to use commercially available diesel generators as the components in a redundant configuration. On the other hand, the use of redundancy may not be the optimal solution in systems in which the minimum size and weight are overriding considerations, for example in satellites or

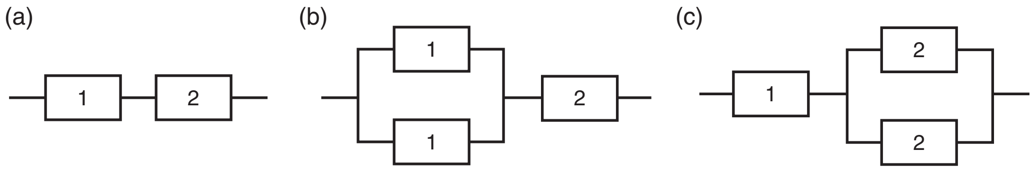


Figure 3.14 Redundancy allocation.

other space applications, in well-logging equipment, and in pacemakers and similar biomedical applications. In such applications, space or weight limitations may dictate an increase in component reliability rather than redundancy. Then, more emphasis must be placed on robust design, manufacturing quality control, and on controlling the operating environment.

Once a decision is made to include redundancy, a number of design trade-offs must be examined to determine how redundancy is to be deployed. If the entire system is not to be duplicated, then which components should be duplicated? Consider, for example the simple two-component system shown in Figure 3.14a. If the reliability $R_a = R_1R_2$ is not large enough, which component should be made redundant? Depending on the choice, the system in Figure 3.14b,c will result.

It immediately follows that

$$R_b = \left(2R_1 - R_1^2\right)R_2 \tag{3.155}$$

$$R_c = R_1\left(2R_2 - R_2^2\right) \tag{3.156}$$

Or taking the differences of the results, we have

$$R_b - R_c = R_1R_2(R_2 - R_1). \tag{3.157}$$

Not surprisingly, this expression indicates that the greatest reliability is achieved in the redundant configuration if we duplicate the component that is least reliable; if $R_2 > R_1$, then system R_b is preferable, and conversely. This rule of thumb can be generalized to systems with any number of nonredundant components; the largest gains are to be achieved by making the least reliable components redundant. In reality, the relative costs of the components also must be considered. Since component costs are normally available, the greatest impediment to making an informed choice is lack of reliability data for the components involved. Trade-offs in the allocation of redundancy often involve additional considerations. Two examples are those between high- and low-level redundancy, and those between fail safe and fail to danger consequences.

Example 3.15 Suppose that in the system shown in Figure 3.14 the two components have the same cost, and $R_1 = 0.7$, $R_2 = 0.95$. If it is permissible to add two components to the system, would it be preferable to replace component 1 by three components in parallel or to replace components 1 and 2 each by simple parallel systems?

Solution If component 1 is replaced by three components in parallel, then from Eq. (3.152)

$$R_a = \left[1 - (1 - R_1)^3\right] R_2 = 0.973 \times 0.95 = 0.92435$$

If each of the two components is replaced by a simple parallel system,

$$R_b = \left[1-(1-R_1)^2\right]\left[1-(1-R_2)^2\right] = 0.91 \times 0.9975 = 0.9077$$

In this problem, the reliability R_1 is so low that even the reliability of a simple parallel system, $2R_1 - R_1^2$, is smaller than that of R_2. Thus, replacing component 1 by three parallel components yields the higher reliability.

High- and Low-level Redundancy

One of the most fundamental determinants of component configuration concerns the level at which redundancy is to be provided. Consider, for example the system consisting of three subsystems, as shown in Figure 3.15. In high-level redundancy, the entire system is duplicated, as indicated in Figure 3.15a, whereas in low-level redundancy the duplication takes place at the subsystem or component level indicated in Figure 3.15b. Indeed, the concept of the level at which redundancy is applied can be further generalized to lower and lower levels. If each of the blocks in the diagram is a subsystem, each consisting of components, we might place the redundancy at a still lower component level. For example, computer redundancy might be provided at the highest level by having redundant computers, at an intermediate level by having redundant circuit boards within a single computer, or at the lowest level by having redundant chips on the circuit boards.

Suppose that we determine the reliability of each of the systems in Figure 3.15 with the component failures assumed to be mutually independent. The reliability of the system without redundancy is then

$$R_0 = R_a R_b R_c \tag{3.158}$$

The reliability of the two redundant configurations may be determined by considering them as composites of series and parallel configurations.

For the high-level redundancy shown in Figure 3.15a, we simply take the parallel combination of the two series systems. Since the reliability of each series subsystem is given by Eq. (3.158), the high-level redundant reliability is given by

$$R_{HL} = 2R_0 - R_0^2 \tag{3.159}$$

or equivalently,

$$R_{HL} = 2R_a R_b R_c - R_a^2 R_b^2 R_c^2 \tag{3.160}$$

Conversely, to calculate the reliability of the low-level redundant system, we first consider the parallel combinations of component types a, b, and c separately. Thus, the two components of type a in parallel yield

$$R_A = 2R_a - R_a^2 \tag{3.161}$$

and similarly,

$$R_B = 2R_b - R_b^2, \quad R_C = 2R_c - R_c^2 \tag{3.162}$$

The low-level redundant system then consists of a series combination of the three redundant subsystems. Hence,

$$R_{LL} = R_A R_B R_C \tag{3.163}$$

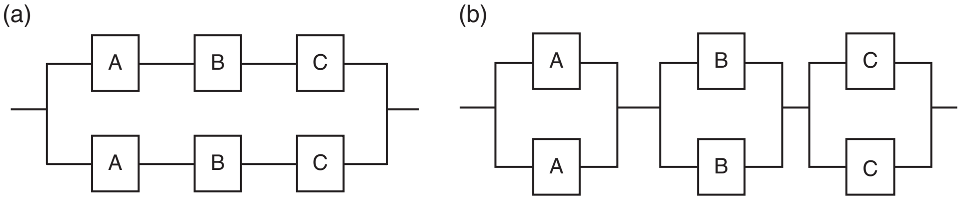


Figure 3.15 High- and low-level redundancy. (a) High-level redundancy and (b) low-level redundancy

or, inserting Eqs. (3.161) and (3.162) into this expression, we have

$$R_{LL} = \left(2R_a - R_a^2\right)\left(2R_b - R_b^2\right)\left(2R_c - R_c^2\right) \tag{3.164}$$

Both the high- and low-level redundant systems have the same number of components. They do not result, however, in the same reliability. This may be demonstrated by calculating the quantity $R_{LL} - R_{HL}$. For simplicity, we examine systems in which all the components have the same reliability, R. Then,

$$R_{HL} = 2R^3 - R^6 \tag{3.165}$$

and

$$R_{LL} = \left(2\mathrm{R} - R^2\right)^3 \tag{3.166}$$

After some algebra, we have

$$R_{LL} - R_{HL} = 6R^3(1 - R)^2 \tag{3.167}$$

Consequently, $R_{LL} > R_{HL}$.

Regardless of how many components the original system has in series, and regardless of whether two or more components are put in parallel, low-level redundancy yields higher reliability, but only if a very important condition is met. The failures must be truly independent in both configurations. In reality, common-mode failures are more likely to occur with low-level than with high-level redundancy. In high-level redundancy, similar components are likely to be more isolated physically and therefore less susceptible to common local stresses. For example, a faulty connector may cause a circuit board to overheat and then the two redundant chips on that board to fail. But if the redundant chips are on different circuit boards in a high-level redundant system, this common-mode failure mechanism will not exist. Physical isolation, in general, may eliminate many causes of common-mode failures, such as local flooding and overheating.

Some insight into common-mode failures may be gained as follows. Consider the same high- and low-level redundant systems for which the results are given by Eqs. (3.165) and (3.166), and let the component reliability be represented by $R = e^{-\lambda t}$. Suppose that because components in the high-level system are physically isolated, there are no significant common-mode failures. Then, we may write simply

$$R_{HL} = e^{-3\lambda t}\left(2 - e^{-3\lambda t}\right) \tag{3.168}$$

In the low-level system, however, we specify that some fraction, ζ, of the failure rate λ is due to common-mode failures. In this case, the quantities R_a, R_b, and R_c will no longer reduce to Eq. (3.166), or

$$R_{LL} = \left(2e^{-\lambda t} - e^{-2\lambda t}\right)^3 \tag{3.169}$$

where there are no common-mode failures. Rather, the ζ-factor model replaces Eqs. (3.161) and (3.162) by Eq. (3.121) to yield

$$R_A = R_B = R_C = 2e^{-\lambda t} - e^{-2\lambda t}e^{\beta\lambda t} \tag{3.170}$$

Then, from Eq. (3.163), we find that the low-level redundant system reliability is reduced to

$$R_{LL} = \left(2e^{-\lambda t} - e^{-2\lambda t}e^{\beta\lambda t}\right)^3 \tag{3.171}$$

This must be compared to Eq. (3.168) to determine how large β can become before the advantage of low level is lost. Consider the following example.

Example 3.16 Suppose that the design-life reliability of each of the components in the high- and low-level redundant systems pictured in Figure 3.15 is 0.99. What fraction of the failure rate in the low-level system may be due to common-mode failures, without the advantage of low-level redundancy being lost?

Solution Set $R_{\text{HL}} = R_{\text{LL}}$ using Eqs. (3.168) and (3.171) at the end of the design life:

$$e^{-3\lambda T}\left(2 - e^{-3\lambda T}\right) = \left(2e^{-\lambda T} - e^{-2\lambda T + \zeta\lambda T}\right)^3$$

Solving for ζ yields

$$\zeta = \frac{1}{\lambda T}\ln\left[2 - \left(2 - e^{-3\lambda T}\right)^{1/3}\right] + 1$$

Since $e^{-\lambda T} = 0.99$, $\lambda T = 0.01005$. Thus,

$$\zeta = \frac{1}{0.01005}\ln\left[2 - \left(2 - 0.99^3\right)^{1/3}\right] + 1 = 0.0197$$

Fail Safe and Fail to Danger

Thus far, we have lumped all failures together. There are situations, however, in which different failure modes can have quite different consequences. Judgment must then be exercised in allocating redundancy between modes. One of the most common examples occurs in the trade-off between fail safe and fail to danger encountered in the design of m/N alarm and safety systems.

Consider an alarm system. The alarm may fail in one of two ways. It may fail to function even though a dangerous situation exists, or it may give a spurious or false alarm even though no danger is present. The first of these is referred to as fail to danger and the second as fail safe. Generally, the fail-to-danger probability is made much smaller than the fail-safe probability. Even then, small fail-safe probabilities are also required. If too many spurious alarms are sounded, they will tend to be ignored. Then, when the real danger is present, the alarm is also likely to be ignored.

Two factors are central to the trade-offs between fail safe and fail to danger modes. First, many design alterations that decrease the fail-to-danger probability are likely to increase the fail-safe probability. Power supply failures, which are often a primary cause of failure of crudely designed safety systems, are an obvious example. Often, the system can be redesigned so that power supply failure will cause the system to fail safe instead of to danger. Specifically, instead of leaving the system unprotected following the failure, the power supply failure will cause the system to function spuriously. Of course, if no change is made in the probability of power supply failure, the amelioration of system fail to danger will result in an increased number of spurious operations.

Second, as increased redundancy is used to reduce the probability of fail to danger, more fail-safe incidents are likely to occur. To demonstrate this, consider a $1/N$ parallel system with which are associated two failure probabilities p_d and p_s for fail to danger and fail safe, respectively. The system fail-to-danger unreliability $\widetilde{R}_{dg}$ is found by noting that all units must fail. Hence,

$$\widetilde{R}_{dg} = p_d^N \tag{3.172}$$

However, the system fail-safe reliability is calculated by noting that any one-unit failure with probability p_s will cause the system to fail safe. Thus,

$$\widetilde{R}_{sf} = 1 - (1 - p_s)^N \tag{3.173}$$

If $p_s \ll 1$, then $(1 - p_s)^N \approx Np_s$, and we see that the fail-safe probability grows linearly with the number of units in parallel,

$$\widetilde{R}_{sf} \approx Np_s \tag{3.174}$$

The m/N configuration has been extensively used in electronic and other protection systems to limit the number of spurious operations at the same time that the redundancy provides high reliability. In such systems, the fail-to-danger unreliability is obtained from Eq. (3.1):

$$\widetilde{R}_{dg} = P\{\mathbf{n} \geq N - m\} = \sum_{n=N-m+1}^{N} {}_N C_n p_d^n (1 - p_d)^{N-n} \tag{3.175}$$

With the approximation that $p_d \ll 1$ this reduces to a form analogous to Eq. (3.154):

$$\widetilde{R}_{dg} \approx {}_N C_{N-m+1} p_d^{N-m+1} \tag{3.176}$$

Conversely, at least m spurious signals must be generated for the system to fail safe. Assuming independent failures with probability p_s, we have

$$\widetilde{R}_{sf} = P\{\mathbf{n} \geq m\} = \sum_{n=m}^{N} {}_N C_n p_s^n (1 - p_s)^{N-n} \tag{3.177}$$

Now, assuming that $p_s \ll 1$, we may approximate this expression by

$$\widetilde{R}_{sf} \approx {}_N C_m p_s^m \tag{3.178}$$

From Eqs. (3.176) and (3.178), the trade-off between fail to danger and spurious operation is seen. The fail-safe probability is decreased by increasing m, and the fail-to-danger probability is decreased by increasing $N - m$. Of course, as N becomes large, common-mode failures may severely limit further improvement.

Example 3.17 You are to design an *m/N* detection system. The number of components, *N*, must be as small as possible to minimize cost. The fail to danger and the fail safe probabilities for the identical components are

$$p_d = 10^{-2},\ \ p_s = 10^{-2}$$

Your design must meet the following criteria:

1) Probability of system fail to danger $<10^{-4}$.
2) Probability of system fail safe $<10^{-2}$.

What values of m and N should be used?

Solution Ans: At least four components are required to meet both criteria. They are met by a 2/4 system.

Voting Systems

In addition to the use of *m/N* redundancy to reduce the spurious operation of safety and alarm systems, it plays an important role in the design of computer control systems that must feed continuous streams of highly reliable output to guarantee safe operations (Table 3.6). Temperature controllers in chemical plants, automated avionics controls, controls for respirators, and other biomedical devices offer a few examples where accurate sensing and control often requires the use of redundancy.

In these situations the most frequent configuration is a 2/3 voting system. Three process computers or other instruments operate in parallel. A voter then compares the outputs of the three units, and if one differs from the other two, its output is ignored. The configuration reliability is then obtained by putting the voter reliability in series with the 2/3 result obtained from Eq. (3.149):

$$R_{sys} = \left(3R^2 - 2R^3\right)R_v \tag{3.179}$$

where R and R_v are the computer and voter reliabilities, respectively. Clearly, the voter must have a very small failure probability if the system is to operate satisfactorily. Fortunately, the voter is

Table 3.6 Make a table of unreliabilities (i.e. the failure probabilities) for fail safe and fail to danger using the rare-event approximations given by Eqs. (3.178) and (3.176).

m/N	$\tilde{R}_{sf}$ Eq. (3.178)	$\tilde{R}_{dg}$ Eq. (3.176)
1/1	$p_s = 10^{-2}$	$p_d = 10^{-2}$
1/2	$2p_s, = 2\times10^{-2}$	$p_d^2 = 10^{-4}$
2/2	$p_s^2 = 10^{-4}$	$2p_d = 2\times10^{-2}$
1/3	$3p_s = 3\times10^{-2}$	$p_s^3 = 10^{-6}$
2/3	$3p_s^2 = 3\times10^{-4}$	$3p_d^2 = 3\times10^{-4}$
3/3	$p_s^3 = 10^{-6}$	$3p_d = 3\times10^{-2}$
1/4	$4p_s, = 4\times10^{-2}$	$p_d^4 = 10^{-8}$
2/4	$6p_s^2 = 6\times10^{-4}$	$4p_d^3 = 4\times10^{-6}$
3/4	$4p_s^3 = 4\times10^{-6}$	$6p_d^2 = 6\times10^{-6}$
4/4	$p_s^4 = 10^{-8}$	$4p_d = 4\times10^{-2}$

typically a very simple device compared to the computer and therefore may be expected to have a much smaller failure probability.

In some situations the electronic voter may be replaced by an operator decision. Suppose, for example that three computers are used to calculate the pitch and yawl of an aircraft. The pilot and copilot might have the displays from two of the computers in front of them with a third placed to be readily visible by both of them. Therefore, comparisons can be made readily, and the malfunctioning computer switched out of the system. Of course, this system also creates an additional opportunity for pilot error.

More extensive voting systems may be required to achieve exceedingly small failure probabilities in computer-controlled systems. In one such configuration each of the computers has a spare, which may be kept in hot standby and switched into the circuit upon detection of a failure by the voter. An alternative configuration is a 3/5 majority vote system. In each of these configurations, at least three computers must fail before the system fails, but each requires that additional computers be purchased.

Example 3.18 Derive the MTTF and the rare-event approximation for

a) a 2/3 voting system,
b) a 3/5 voting system.

Assume that the failure probability of the voter can be neglected. How do the results compare to those for a single unit?

Solution (2/3) From Eq. (3.149), we have

$$R = e^{-\lambda t} : R_{2/3} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

Using the definition of MTTF given by Eq. (3.22) and evaluating the integrals, we have

$$\text{MTTF}_{2/3} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6}\text{MTTF}$$

For the rare-event approximation, Eq. (3.154) yields

$$R_{2/3} \approx 1 - {}_3C_2(\lambda t)^2 = 1 - 3(\lambda t)^2$$

(3/5) From Eq. (3.149), we have

$$R_{3/5} = \sum_{n=0}^{2} {}_5C_n(1-R)^n R^{5-n} = R^5 + 5(1-R)R^4 + 10(1-R)^2R^3$$

Thus,

$$R_{3/5} = 10R^3 - 15R^4 + 6R^5 = 10e^{-3\lambda t} - 15e^{-4\lambda t} + 6e^{-5\lambda t}$$

and we can again apply Eq. (3.22) to obtain

$$\text{MTTF}_{3/5} = \frac{10}{3\lambda} - \frac{15}{4\lambda} + \frac{6}{5\lambda} = \frac{47}{60}\text{MTTF}$$

For the rare-event approximation, Eq. (3.154) yields

$$R_{3/5} \approx 1 - {}_5C_3(\lambda t)^3 = 1 - 10(\lambda t)^3$$

Increased number of voting components decreases the system MTTF. However, at short times the rare-event approximations indicated that the reliability is increasingly close to 1. For example with $\lambda t = 0.1$, we have

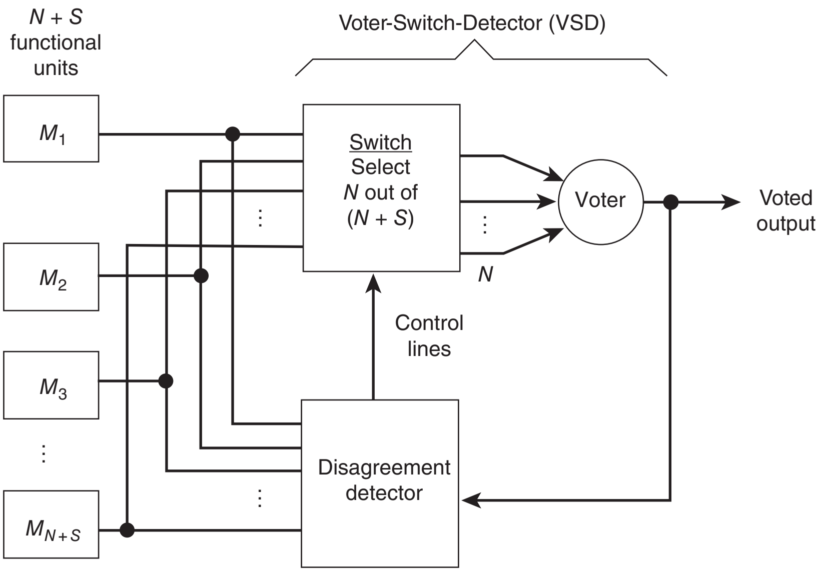


Figure 3.16 Basic organization of a hybrid redundant system. *Source*: From Elkind (1982).

$R_{1/1} \approx 0.90$, $R_{2/3} \approx 0.97$, and $R_{3/5} \approx 0.99$

Finally, it should be noted that in an electronic system, transient faults, which may last only a fraction of a second, are expected to occur more frequently than "hard" irrecoverable failure. Thus, in voting systems, software is often included to test for transient faults and restart the computer once the fault is corrected. If this is not done, the failure probability may be too large even if three or more faults must occur before the system will fail. In this case, the failure mode is referred to as "exhaustion of spares." Conversely, if the testing to determine whether a correctable fault or an irreparable failure has taken place takes a significant length of time, there is a small possibility that a fault will cause a second computer to malfunction before the spare can be switched in. The system is then said to have a fault handling or switching failure. The achievement of very small failure probabilities in systems such as shown in Figure 3.16 often hinges on balancing the gains and losses incurred with the use of such sophisticated fault-handling systems.

3.11 Redundancy in Complex Configurations

Systems may take on a variety of complex configurations. In what follows we examine the analysis of redundancy in two classes of systems: those that may be analyzed in terms of series and parallel configurations, and those in which the components are linked in such a way that they cannot. For brevity, we primarily treat configurations involving only active-parallel units. However, with proper care the analysis can be extended to systems containing standby configurations.

Series–Parallel Configurations

As long as a system can be decomposed into series and parallel subsystem configurations, the techniques of the preceding sections can be employed repeatedly to derive expressions for system reliability. As an example, consider the RBD shown for a system in Figure 3.17. Components a_1 through a_4 have reliability R_a, and components b_1 and b_2 have reliability R_b. For the following analysis to be valid, the failures of the components must be independent of one another.

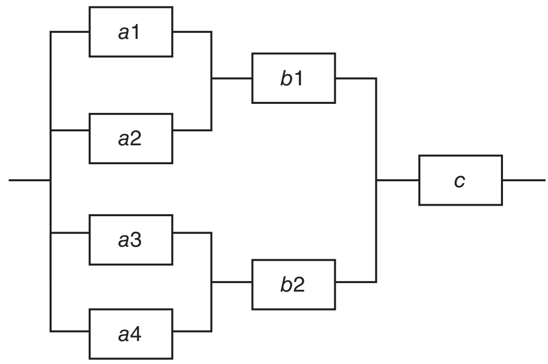


Figure 3.17 Reliability block diagram of a series–parallel configuration.

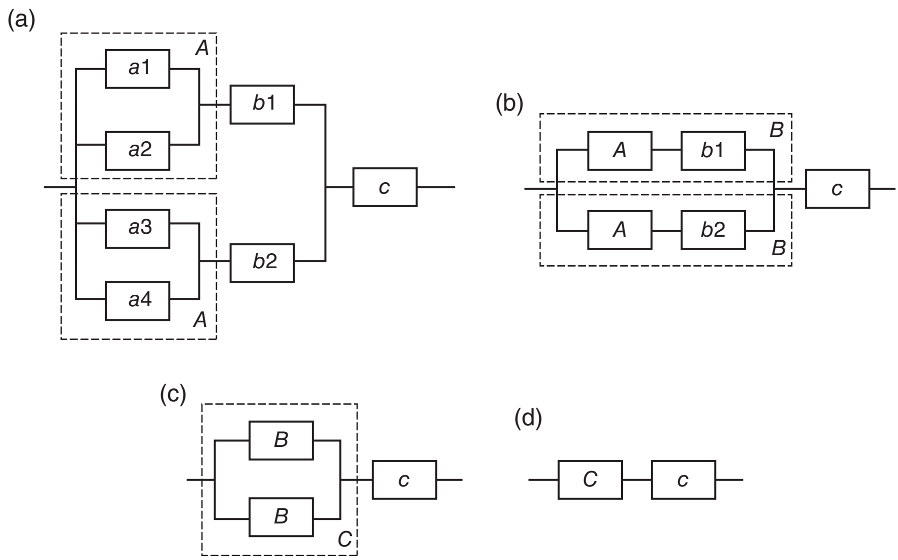


Figure 3.18 Decomposition of the system in Figure 3.17.

We begin by noting that there are two sets of subsystems with type a components, consisting of a simple parallel configuration as shown in Figure 3.18a. Thus, we define the reliability of these configurations as

$$R_A = 2R_a - R_a^2 \tag{3.180}$$

The system configuration then appears as the reduced block diagram shown in Figure 3.18b. We next note that each newly defined subsystem A is in series with a component of type b. We may therefore define a subsystem B by

$$R_B = R_A R_b \tag{3.181}$$

and the reduced block diagram then appears as in Figure 3.18c. Since the two subsystems B are in parallel, we may write

$$R_C = 2R_B - R_B^2 \tag{3.182}$$

to yield the simplified configuration shown in Figure 3.18d. Finally, the total system consists of the series of subsystems **C** and component *c*. Thus,

$$R = R_C R_c \tag{3.183}$$

Having derived an expression for the system reliability, we may combine Eqs. (3.180) through (3.183) to obtain the system reliability in terms of that of R_a, R_b, and R_c

$$R = \left(2R_a - R_a^2\right)R_b\left[2 - \left(2R_a - R_a^2\right)R_b\right]R_c \tag{3.184}$$

Standby configurations can also be included within series–parallel configurations. Suppose that components a_1 and a_2 are in a 1/2 standby configuration, and that components a_3 and a_4 are in the same configuration. In the constant failure rate approximation, we would simply replace R_A by R_s, given by Eq. (3.105), and proceed as before. We would obtain, instead of Eq. (3.184),

$$R = R_s R_b(2 - R_s R_b)R_c \tag{3.185}$$

Example 3.19 Suppose that in Figure 3.15, $R_a = R_b = e^{-\lambda} \equiv R_*$ and $R_c = 1$. Find R in the rare-event approximation.

Solution We simplify Eq. (3.184),

$$R = R_*^2(2 - R_*)\left[2 - (2 - R_*)R_*^2\right]$$

and write it as a polynomial in R_*:

$$R = 4R_*^2 - 2R_*^3 - 4R_*^4 + 4R_*^5 - R_*^6$$

Then, we expand $R_*^N = e^{-N\lambda t} \cong 1 - N\lambda t + \frac{1}{2}N^2(\lambda t)^2 - \cdots$ to obtain for small λt

$$R_*^N \cong 4\left[1 - 2\lambda t + 2(\lambda t)^2\right] - 2\left[1 - 3\lambda t + \frac{9}{2}(\lambda t)^2\right] - 4\left[1 - 4\lambda t + 8(\lambda t)^2\right] + 4\left[1 - 5\lambda t + \frac{1}{2}25(\lambda t)^2\right] - 1 - 6\lambda t + 18(\lambda t)^2 + \cdots$$

$$R \cong (4 - 2 - 4 + 4 - 1) - (8 - 6 - 16 + 20 - 6)(\lambda t) - (-8 + 9 + 32 - 50 + 18)(\lambda t)^2 + \cdots$$

$$R \cong 1 - (\lambda t)^2$$

Had the coefficient of the $(\lambda t)^2$ term also been zero, we would have needed to carry terms in $(\lambda t)^3$.

Linked Configurations

In some situations, the linkage of the components or subsystems is such that the foregoing technique of decomposing into parallel and series configurations cannot be applied directly. Such is the case for the system configuration shown in Figure 3.19, consisting of subsystem types 1, 2, and 3, with reliabilities R_1, R_2, and R_3.

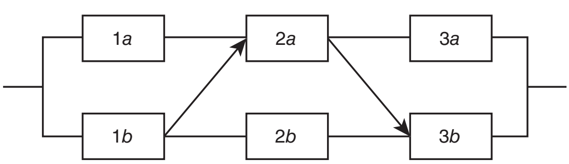


Figure 3.19 Reliability block diagram of a cross-linked system.

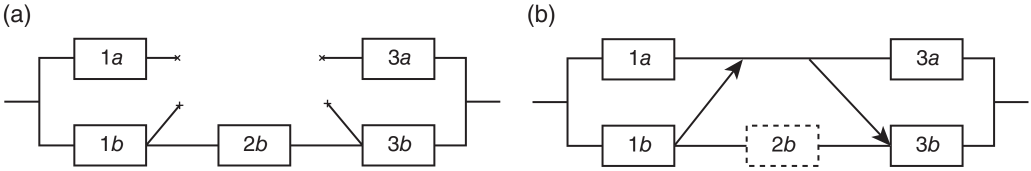


Figure 3.20 Decomposition of the system in Figure 3.19.

To analyze this and similar systems, we decompose the problem into a combination of series–parallels by utilizing the total probability rule given in Eq. (2.17):

$$P\{Y\} = P\{Y|X\}P\{X\} + P\left\{Y|\widetilde{X}\right\}P\left\{\widetilde{X}\right\} \tag{3.186}$$

Suppose that we let X be the event that subsystem $2a$ fails. Then, $P\{X\} = 1 - R_2$ and $P\left\{\widetilde{X}\right\} = R_2$. If we then let Y denote successful system operation, the system reliability is defined as $R = P\{Y\}$. Now suppose that we define the conditional reliabilities that the system function with subsystem $2a$ failed as

$$R^- = P\{Y|X\} \tag{3.187}$$

and with 2a operational as

$$R^+ = P\left\{Y|\widetilde{X}\right\} \tag{3.188}$$

Inserting these probabilities into Eq. (3.186), we may write the system reliability as

$$R = R^-(1 - R_2) + R^+ R_2 \tag{3.189}$$

We must now evaluate the conditional reliabilities R^+ and R^-. For R^- in which $2a$ has failed, we disconnect all the paths leading through $2a$ in Figure 3.19; the result appears in Figure 3.20a. Conversely, for R^+ in which $2a$ is functioning, we pass a path through $2a$, thereby bypassing $2b$ with the result shown in Figure 3.20b.

We see that when $2a$ is failed, the reduced system consists of a series of three subsystems, lb, $2b$, and $3b$; subsystems la and $3a$ no longer make any contribution to the value of R^-. We obtain

$$R^- = R_1R_2R_3 \tag{3.190}$$

When $2a$ is operating, we have a series combination of two parallel configurations, la and lb in the first and $3a$ and $3b$ in the second; since component $2b$ is always bypassed, it has no effect on R^+. Therefore, we have

$$R^+ = \left(2R_1 - R_1^2\right)\left(2R_3 - R_3^2\right) \tag{3.191}$$

Finally, substituting these expressions into Eq. (3.189), we find the system reliability to be

$$R = R_1R_2R_3(1 - R_2) + \left(2R_1 - R_1^2\right)\left(2R_3 - R_3^2\right)R_2 \tag{3.192}$$

Example 3.20 Evaluate Eq. (3.192) in the rare-event approximation with $R_n = e^{-\lambda t}$ for all n.

Solution Let $R_* = R_n$. Then, Eq. (3.192) becomes $R = R_*^3(1 - R_*) + \left(2R_* - R_*^2\right)^2 R_*$. Writing this expression as a polynomial in R_*, we have $R = 5R_*^3 - 5R_*^4 + R_*^5$. Now we expand $R_*^N = e^{-\lambda t} = 1 - N\lambda t + {}^1\!/_2 N^2(\lambda t)^2 - \cdots$ to obtain:

$$\begin{aligned} R = 5 - 15\lambda t &+ {}^1\!/_2 45(\lambda t)^2 - \cdots \\ -5 + 20\lambda t &+ {}^1\!/_2 80(\lambda t)^2 + \cdots \\ +1 - 5\lambda t &+ {}^1\!/_2 25(\lambda t)^2 - \cdots \end{aligned}$$

Hence,

$$R = 1 - 5(\lambda t)^2 + \cdots$$

If the $(\lambda t)^2$ term were zero, we would need to carry the $(\lambda t)^3$ term in the expansion.

Bibliography

Anderson, R.T. (1973). *Reliability Design Handbook*. U. S. Department of Defense Reliability Analysis Center.

Anderson, R.T. (1976). *Reliability Design Handbook RDH-376*. Griffiss Air Force Base, NY: Rome Air Development Center.

Barlow, R.E. and Proschan, F. (1965). *Mathematical Theory of Reliability*. New York: Wiley.

Bazovsky, I. (1961). *Reliability Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall.

Billinton, R. and Allan, R.N. (1983). *Reliability Evaluation of Engineering Systems*. New York: Plenum Press.

Dillon, B.S. and Singh, C. (1981). *Engineering Reliability*. New York: Wiley.

Elkind, S.A. (1982). Reliability and availability techniques. In: *The Theory and Practice of Reliable System Design* (ed. D.P. Siewiorek and R.S. Swarz). Bedford, MA: Digital Press.

Flemming, K.L. and Raabe, P.H. (1978). A comparison of three methods for the quantitative analysis of common cause failures. *General Atom. Rep*., GA-A14568.

Henley, E.J. and Kumamoto, H. (1981). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.

Ling, A.H.K. (1981). Mathematical modelling. In: *Reliability and Maintainability of Electronic Systems* (ed. J.A. Roberts and J.E. Arsenault). Rockville, Maryland: Computer Science Press, Inc.

Meeker & Escobar (1998). *Statistical Methods for Reliability Data*. Wiley.

MIL-HDBK-217D (1982). *Reliability Prediction of Electronic Equipment*. U. S. Department of Defense.

Proschan, F. (1963). Theoretical explanation of observed decreasing failure rate. *Technometrics* **5** (3): 375–383.

Roberts, N.H. (1964). *Mathematical Methods in Reliability Engineering*. New York: McGraw-Hill.

Sandler, G.H. (1963). *System Reliability Engineering*. Englewood Cliffs, NJ: Prentice-Hall.

Shooman, M.L. (1990). *Probabilistic Reliability: An Engineering Approach*. Malabar, FL: Krieger.

Siewiorek, D.P. and Swarz, R.S. (1992). *Reliable Computer Systems*, 2e. Digital Press.

Exercises

3.1 The PDF for the time to failure of an appliance is

$$f(t) = \frac{32}{(t+4)^3}, \quad t > 0$$

where t is in years

a) Find the reliability of $R(t)$.
b) Find the failure rate $\lambda(t)$.
c) Find the MTTF.

3.2 The reliability of a machine is given by

$$R(t) = \exp\left[-0.04t - 0.008\,t^2\right] \ (t \text{ in years})$$

a) What is the failure rate?
b) What should the design life be to maintain a reliability of at least 0.90?

3.3 The failure rate for a high-speed fan is given by

$$\lambda(t) = \left(2 \times 10^{-4} + 3 \times 10^{-6} t\right)/\text{hour}$$

where t *is* in hours of operation. The required design-life reliability is 0.95.
a) How many hours of operation should the design life be?
b) If, by preventive maintenance, the wear contribution to the failure rate can be eliminated, to how many hours can the design life be extended?
c) By placing the fan in a controlled environment, we can reduce the constant contribution to $\lambda(t)$ by a factor of 2. Then, without preventive maintenance, to how many hours may the design life be extended?
d) What is the extended design life when both reductions from (*b*) and (*c*) are made?

3.4 If the CDF for times to failure is

$$F(t) = 1 - \frac{100}{(t+10)^2}$$

a) Find the failure rate as a function of time.
b) Does the failure rate increase or decrease with time?

3.5 Repeat Exercise 3.3 but fix the design life at 100 hr and calculate the design-life reliability for conditions (a), (b), (c), and (d).

3.6 An electronic device is tested for two months and found to have a reliability of 0.990; the device is also known to have a constant failure rate.
a) What is the failure rate?
b) What is the mean time to failure?
c) What is the design-life reliability for a design life of four years?
d) What should the design life be to achieve a reliability of 0.950?

3.7 A device has a constant failure rate of 0.7/year.
a) What is the probability that the device will fail during the *second* year of operation?
b) If upon failure the device is immediately replaced, what is the probability that there will be more than one failure in three years of operation?

3.8 The failure rate on a new brake drum design is estimated to be

$$\lambda(t) = 1.2 \times 10^{-6} \exp\left(10^{-4} t\right)$$

per set, where t is in kilometers of normal driving. Forty vehicles are each test-driven for 15,000 km.
a) How many failures are expected, assuming that the vehicles with failed drives are removed from the test?
b) What is the probability that more than two vehicles will fail?

3.9 The failure rate for a hydraulic component is given empirically by

$$\lambda(t) = 0.001\left(1 + 2e^{-2t} + e^{t/40}\right)/\text{year}$$

where t is in years. If the system is installed at $t = 0$, calculate the probability that it will have failed by time t. Plot your results for 40 years.

3.10 A home computer manufacturer determines that his machine has a constant failure rate of $\lambda = 0.4$ year in normal use. For how long should the warranty be set if no more than 5% of the computers are to be returned to the manufacturer for repair?

3.11 A one-year guarantee is given based on the assumption that no more than 10% of the items will be returned. Assuming an exponential distribution, what is the maximum failure rate that can be tolerated?

3.12 There is a contractual requirement to demonstrate with 90% confidence that a vehicle can achieve a 100-km mission with a reliability of 99%. The acceptance test is performed by running 10 vehicles over a 50,000-km test track.

a) What is contractual MTTF?
b) What is the maximum number of failures that can be experienced on the demonstration test without violating the contractual requirement? (*Note:* Assume an exponential distribution and review Section 2.5.)

3.13 Suppose that the CDF for time to failure is given by

$$R(t) = \begin{cases} 1 - at^2, & t < 1/\sqrt{a} \\ 0, & t > 1/\sqrt{a} \end{cases}$$

Determine the following:

a) the PDF $f(t)$,
b) the failure rate,
c) the MTTF.

3.14 Suppose that amplifiers have a constant failure rate of $\lambda = 0.08$/month. Suppose that four such amplifiers are tested for six months. What is the probability that more than one of them will fail? Assume that when they fail, they are not replaced.

3.15 A device has a constant failure rate with an MTTF of two months. One hundred of the devices are tested to failure.

a) How many of the devices do you expect to fail during the second month?
b) Of the devices that survive two months, what fraction do you expect to fail during the third month?
c) If you are allowed to stop the test after 80 failures, how long do you expect the test to last?

3.16 A manufacturer determines that the average television set is used 1.8 hour/day. A one-year warranty is offered on the picture tube having an MTTF of 2000 hr. If the distribution is exponential, what fraction of the tubes will fail during the warranty period?

3.17 Ten control circuits are to undergo simultaneous accelerated testing to study the failure modes. The accelerated failure rate has previously been estimated to be constant with a value of 0.04/days.

a) What is the probability that there will be at least one failure during the first day of the test?
b) What is the probability that there will be more than one failure during the first week of the test?

3.18 The reliability of a cutting tool is given by

$$R(t) \equiv \begin{cases} (1-0.2t)^2, & 0<t<5 \\ 0, & t>5 \end{cases}$$

where t is in hours.
a) What is MTTF?
b) How frequently should the tool be changed if failures are to be held to no more than 5%?
c) Is the failure rate decreasing or increasing? Justify your result.

3.19 A motor-operated valve has a failure rate λ_0 while it is open and λ_c while it is closed. It also has a failure probability p_0 to open on demand and a failure probability p_c to close on demand. Develop an expression for the composite failure rate similar to Eq. (3.46) for the valve.

3.20 Night watchmen carry an industrial flashlight eight hours per night, seven nights per week. It is estimated that on the average the flashlight is turned on about 20 min per eight-hour shift. The flashlight is assumed to have a constant failure rate of 0.08/hour while it is turned on and 0.005/hour when it is turned off but being carried.
a) In working hours, estimate the MTTF of the light.
b) What is the probability of the light's failing during one eight-hour shift?
c) What is the probability of its failing during one month (30 days) of eight-hour shifts?

3.21 If waves hit a platform at the rate of 0.4/min and the "memoryless" failure probability is 10^{-6}/wave, estimate the failure rate in days^{-1}.

3.22 The one-month reliability on an indicator lamp is 0.95 with the failure rate specified as constant. What is the probability that more than two spare bulbs will be needed during the first year of operation? (Ignore replacement time.)

3.23 A part for a marine engine with a constant failure rate has an MTTF of two months. If two spare parts are carried,
a) What is the probability of surviving a six-month cruise without losing the use of the engine as a result of part exhaustion?
b) What is the result for part a if three spare parts are carried?

3.24 In Exercise 3.27, suppose that there are three watchmen on duty every night for eight hours.
a) How many flashlight failures would you expect in one year?
b) Assuming that the failures are not caused by battery or bulb wear-out (these are replaced frequently), how many spare flashlights would be required to be on hand at the beginning of the year, if the probability of running out of spares is to be less than 10%?

3.25 An electronics manufacture mixes 1000 capacitors with an MTTF of three months and 2000 capacitors with an MTTF of six months. Assuming that the capacitors have constant failures rates:

a) What is the PDF for the combined population?
b) Use Eq. (3.15) to derive an expression for the failure rate of the combined population.
c) What is the failure rate at $t = 0$?
d) Does the failure rate increase or decrease with time?
e) What is the failure rate at very long times?

3.26 A servomechanism has an MTBF of 2000 hours with a constant failure rate.

a) What is the reliability for a 125-hour mission?
b) Neglecting repair time, what is the probability that more than one failure will occur during a 125-hour mission?
c) That more than two failures will occur during a 125-hour mission?

3.27 Assume that the occurrence of earthquakes strong enough to be damaging to a particular structure is governed by the Poisson distribution. If the mean time between such earth quakes is twice the design life of the structure:

a) What is the probability that the structure will be damaged during its design life?
b) What is the probability that it will suffer more than one damaging earthquake during its design life?
c) Calculate the failure rate (i.e. damage rate due to earthquakes).

3.28 A relay circuit has an MTBF of 0.8 year. Assuming random failures,

a) Calculate the probability that the circuit will survive one year without failure.
b) What is the probability that there will be more than two failures in the first year?
c) What is the expected number of failures per year?

3.29 A logic circuit is known to have a decreasing failure rate of the form

$$\lambda(t) = \frac{1}{20}t^{-1/2}/\text{year}$$

where t is in years.

If the design life is one year, what is the reliability?

If the component undergoes wear-in for one month before being put into operation, what will the reliability be for a one-year design life?

3.30 The MTBF for punctures of truck tires is 150,000 miles. A truck with 10 tires carries 1 spare.

a) What is the probability that the spare will be used on a 10,000-mile trip?
b) What is the probability that more than the single spare will be required on a 10,000-mile trip?

3.31 Widgets have a constant failure rate with MTTF = 5 days. Ten widgets are tested for one day.

a) What is the expected number of failures during the test?
b) What is the probability that *more than one* will fail during the test?
c) For how long would you run the test if you wanted the expected number of failures to be five?

Redundancy

3.32 A nonredundant system with 100 components has a design-life reliability of 0.90. The system is redesigned so that it has only 70 components. Estimate the design life of the redesigned systems, assuming that all the components have constant failure rates of the same value.

3.33 At the end of one year of service, the reliability of a component with a constant failure rate is 0.95.
a) What is the failure rate (include units)?
b) If two of the components are put in active parallel, what is the one year reliability? (Assume no dependencies)
c) If 10% of the component failure rate may be attributed to common-mode failures, what will the one-year reliability be of the two components in active parallel?

3.34 Thermocouples of a particular design have a failure rate of $\lambda = 0.008$/hour. How many thermocouples must be placed in active parallel if the system is to run for 100 hours with a system failure probability of no more than 0.05? Assume that all failures are independent.

3.35 In an attempt to increase the MTTF, an engineer puts two devices in parallel and tests the resulting parallel system. The MTTF increases by only 40%. Assuming the device failure rate is a constant, what fraction of it, β, is due to common-mode failures of the parallel system?

3.36 A disk drive has a constant failure rate and an MTTF of 5000 hours.
a) What will the probability of failure be for one year of operation?
b) What will the probability of failure be for one year of operation if two of the drives are placed in active parallel and the failures are independent?
c) What will the probability of failure be for one year of operation if the common-mode errors are characterized by $\zeta = 0.2$?

3.37 Suppose that the design-life reliability of a standby system consisting of two identical units must be at least 0.95. If the MTTF for each unit is three months, determine the design life (assume constant failure rates and neglect switching failures, etc.).

3.38 Find the variance in the time to failure, assuming a constant failure rate λ:
a) For two units in series.
b) For two units in active parallel.
c) Which is larger?

3.39 A component has a one-year design-life reliability of 0.9; two such components are placed in active parallel. What is the one-year reliability of the resulting system:
a) In the absence of common-mode failures?
b) If 20% of the failures are common-mode failures?

3.40 Suppose that the PDF for time to failure for a single unit is uniform:

$$f(t) = \left\{ \begin{array}{ll} 1/T & 0 < t < T \\ 0 & \text{otherwise} \end{array} \right\}$$

a) Find and plot $R(t)$ for a single unit.
b) Find and plot $R(t)$ for two units in active parallel.
c) Find and plot $R(t)$ for two units in standby parallel.
d) Find the MTTF for parts *a, b,* and *c*.

3.41 An amplifier with constant failure rate has a reliability of 0.90 at the end of one month of operation. If an identical amplifier is placed in standby parallel and there is a 3% switching failure probability, what will the reliability of the parallel system be at the end of one year?

3.42 Consider the standby system described by Eq. (3.126)
a) Find the MTTF.
b) Show that your result from (a) reduces to Eq. (3.108) as $p \to 0$ and $\lambda^+ \to \to \lambda$.
c) Show that your result from (a) reduces to a single unit MTTF as $p \to 1$.
d) Find the rare-event approximation for Eq. (3.126).

3.43 Consider a system with three identical components with failure rate λ. Find the system failure rate:
a) For all three components in series.
b) For all three components in active parallel.
c) For two components in parallel and the third in series.
d) Plot the results for *a, b,* and *c* on the same scale for $0 \leq t \leq 5/\lambda$.

3.44 For a 1/2 parallel system with load sharing:
a) Show that $\lambda^*/\lambda > 1.56$ will have a smaller MTTF than a single unit.
b) Find the rare-event approximation for the case where $\lambda^*/\lambda = 1.56$.
c) Using rare-event approximations, compare reliabilities at $\lambda t = 0.05$ for a single unit, for $\lambda^*/\lambda = 1.56$ and for $\lambda^*/\lambda = 1.0$.
(d)Discuss your results.

3.45 In a 1/2 active-parallel system each unit has a failure rate of 0.05/day.
a) What is the system MTTF with no load sharing?
b) What is the system MTTF if the failure rate increases by 10% as a result of increased load?
c) What is the system MTTF if one increases both unit failure rates by 10%?

3.46 An engineer running a 1/2 identical unit system in cold standby finds the switching failure probability to be 0.2 while the failure rate in standby is negligible. He converts to hot standby and eliminates the switching failure probability but discovers that now the failure rate of the unit in standby is 30% of the active unit. As measured by system MTTF, has going from cold to hot standby improved or degraded the system? By how much?

3.47 Suppose that a system consists of two subsystems in active parallel. The reliability of each subsystem is given by the Rayleigh distribution

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

Assuming that common-mode failures may be neglected, determine the system MTTF.

3.48 Repeat Exercise 3.46 assuming that the failure rate of the unit in standby is only 20% of the active unit.

3.49 The design criterion for the ac power system for a reactor is that its failure probability be less than 2×10^{-5}/year. Off-site power failures may be expected to occur about once in five years. If the on-site ac power system consists of two independent diesel generators, each of which is capable of meeting the ac power requirements, what is the maximum failure probability per year that each diesel generator can have if the design criterion is to be met? If three independent diesel generators are used in active parallel, what is the value of the maximum failure probability? (Neglect common-mode failures.)

3.50 Consider a 1/3 system in active parallel, each unit of which has a constant failure rate λ.

a) Plot the system failure rate $\lambda(t)$ in units of λ versus λt from $\lambda t = 0$, to large enough λt to approach an asymptotic system failure rate.
b) What is the asymptotic value $\lambda(\infty)$?
c) At what interval should the system be shut down and failed components replaced if there is a criterion that $\lambda(t)$ should not exceed 1/3 of the asymptotic value?

3.51 An engineer designs a system consisting of two subsystems in series. The reliabilities are $R_1 = 0.98$ and $R_2 = 0.94$. The cost of the two subsystems is about equal. The engineer decides to add two redundant components. Which of the following would it be better to do?

a) Duplicate subsystems 1 and 2 in high-level redundancy.
b) Duplicate subsystems 1 and 2 in low-level redundancy.
c) Replace the second subsystem with 1/3 redundancy.
d) Justify your answer.

3.52 For a 2/3 system:

a) Express $R(t)$ in terms of the constant failure rates.
b) Find the system MTTF.
c) Calculate the reliability y when $\lambda t = 1.0$ and compare the result to a single unit and to a 1/2 system with the same unit failure rate.

3.53 Suppose that a system consists of two components, each with a failure rate A, placed in series. λ redundant system is built consisting of four components. Derive expressions for the system failure rates

a) for high-level redundancy,
b) for low-level redundancy.
c) Plot the results of a and b along with the failure rate of the nonredundant system for $0 \leq t \leq 2/\lambda$.

3.54 Suppose that in Exercise 9.21 one-fourth of the diesel generator failures are caused by common-mode effects and therefore incapacitate all the active-parallel systems. Under these conditions what is the maximum failure probability (i.e. random and common-mode) that is allowable if two diesel generators are used? If three diesel generators are used?

3.55 The failure rate on a jet engine is $\lambda = 10^{-3}$/hour. What is the probability that more than two engines on a four-engine aircraft will fail during a two-hour flight? Assume that the failures are independent.

3.56 The shutdown system on a nuclear reactor consists of four independent subsystems, each consisting of a control rod bank and its associated drives and actuators. Insertion of any three banks will shut down the reactor. The probability that a subsystem will fail is 0.2×10^{-4} per demand. What is the probability per demand that the shutdown system will fail, assuming that common-mode failures can be neglected?

3.57 Two identical components, each with a constant failure rate, are in series. To improve the reliability two configurations are considered:

a) for high-level redundancy,
b) for low-level redundancy.

Calculate the system MTTF in terms of MTTF of the system mean time to failure without redundancy.

3.58 Consider two components with the same MTTF. One has an exponential distribution, the other a Rayleigh distribution (see Exercise 9.19). If they are placed in active parallel, find the system MTTF in terms of the component MTTF.

3.59 A radiation-monitoring system consists of a detector, an amplifier, and an annunciator. Their lifetime reliabilities and costs are, respectively, 0.83 ($1200), 0.58 ($2400), and 0.69 ($1600).

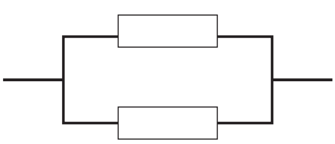
a) How would you allocate active redundancy to achieve a system lifetime reliability of 0.995?
b) What is the cost of the system?

3.60 For constant failure rates, evaluate R_{HL} and R_{LL} for high- and low-level redundancy in the rare-event approximation beginning with Eqs. (3.165) and (3.166).

3.61 A system consists of three components in series, each with a reliability of 0.96. A second set of three components is purchased and a redundant system is built. What is the reliability of the redundant system (a) with high-level redundancy and (b) with low-level redundancy?

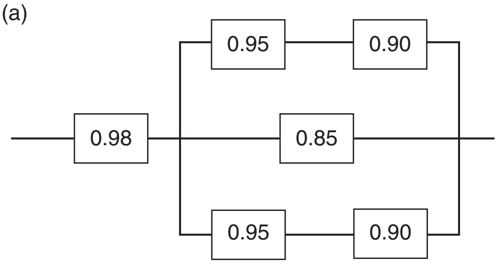
3.62 The identical components of the system below have fail-to-danger probabilities of $p_d = 10^{-2}$ and fail-safe probabilities of $p_s - 10^{-1}$.

a) What is the system fail-to-danger probability?
b) What is the system fail-safe probability?

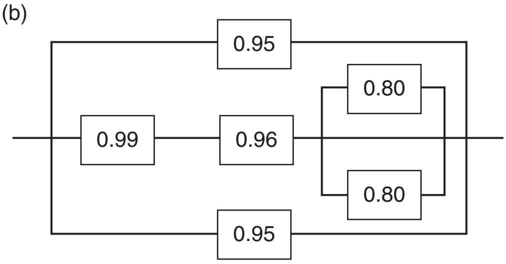


3.63 Calculate the reliabilities of the following systems:

(a)

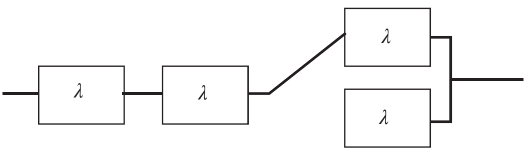


(b)

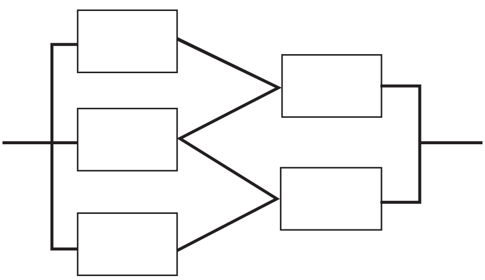


3.64 A device consists of two components in series with a (1/2) standby system as shown. Each component has the same constant failure rate.

a) What is $R(t)$?
b) What is the rare-event approximation for $R(t)$?
c) What is the MTTF?

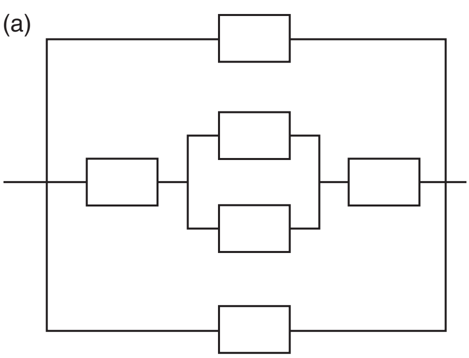


3.65 Calculate the reliability for the following system, assuming that all the component failure rates are equal. Then, use the rare-event approximation to simplify your result.

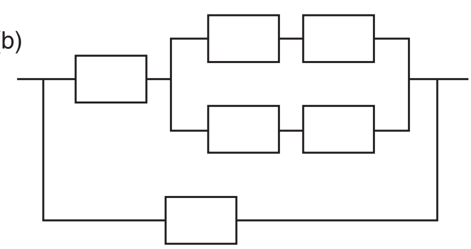


3.66 Calculate the reliability, $R(t)$, for the following systems, assuming that all the components have failure rate λ. Then, use the rare-event approximation to simplify the result.

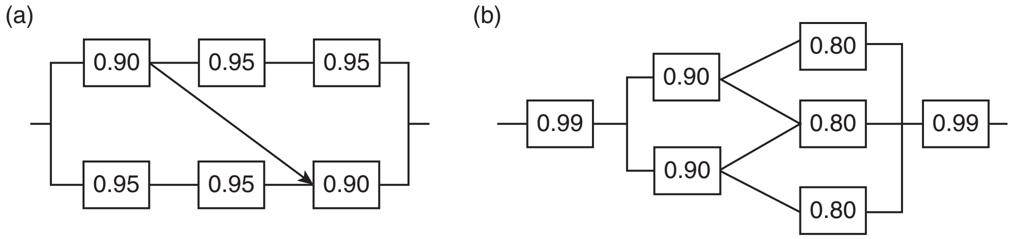
(a)



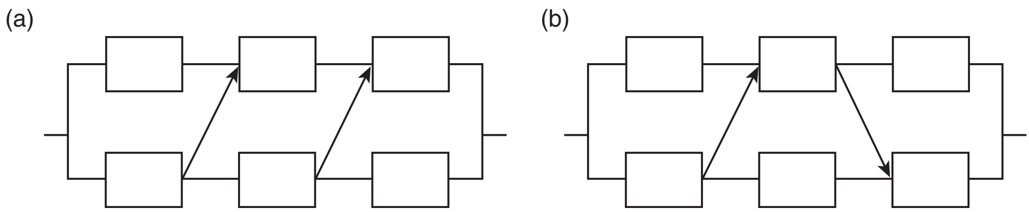
(b)



3.67 Given the following component reliabilities, calculate the reliability of the two systems.



3.68 Calculate the reliabilities of the following two systems, assuming that all the component reliabilities are equal. Then, determine which system has the higher reliability.



3.69 The PDF of the lifetime of an appliance is given by

$$f(t) = 0.25te^{-0.5t}, t \geq 0$$

where t is in years, (a) What is the probability of failure during the first year? (b) What is the probability of the appliances lasting at least five years? (c) If no more than 5% of the appliances are to require warranty services, what is the maximum number of months for which the appliance can be warranted?

4

Continuous Distributions – Part 1 Normal and Related Continuous Distributions

"All business proceeds on beliefs or judgments of probabilities and not just on certainties."
Source: Charles Eliot

4.1 Introduction

In Chapter 2, probabilities of discrete events, most frequently failures, were discussed. The discrete random variables associated with such events are used to estimate the number of events that are likely to take place. In order to proceed further with reliability analysis, however, it is necessary to consider how the probability of failure depends on a variety of other variables that are continuous: the duration of operation time, the strength of the system, the magnitudes of stresses, and so on. If the repeated measurement of such variables is carried out, however, the same value will not be obtained with each test. These values are referred to as continuous random variables for they cannot be described with certainty but only with the probability that they will take on values within some range. In Section 4.2, we first introduce the mathematical apparatus required to describe random variables. In Section 4.3, the Empirical cumulative distribution function (Empirical CDF) is introduced. The Empirical CDF assumes no distribution (sometimes referred to statistical texts as "nonparametric"). Section 4.4 introduces the simplest "parametric" distribution, the uniform distribution. The exponential distribution was introduced in Chapter 3, since it was used for most reliability calculations until computers became more generally available in the 1970s. Section 4.5 brings you back to the distribution family most used outside of reliability – the normal distribution and its associate, the lognormal distribution. The lognormal distribution does have its uses in reliability as well, but only in limited cases, as will be discussed.

In Chapter 5, the Weibull and extreme-value distributions are described in detail.

4.2 Properties of Continuous Random Variables

In this section, we examine some of the important properties of continuous random variables. We first define the quantities that determine the behavior of a single random variable. We then examine how these properties are transformed when the variable is changed.

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

Probability Distribution Functions

We denote a continuous random variable with bold-faced type as $\mathbf{x}$, and the values that $\mathbf{x}$ may take on are specified by x, that is in normal type. The properties of a random variable are specified in terms of probabilities. For example, $P\{\mathbf{x} < x\}$ is used to designate the probability that $\mathbf{x}$ has a value less than x. Similarly, $P\{a < \mathbf{x} < b\}$ is the probability that $\mathbf{x}$ has a value between a and b. Two particular probabilities are most often used to describe a random variable. The first one,

$$F(x) = P\{\mathbf{x} \le x\} \tag{4.1}$$

the probability that $\mathbf{x}$ has a value less than or equal to x, is referred to as the *cumulative distribution function* or CDF for short. The second, the probability that $\mathbf{x}$ lies between x and $x + \Delta\boldsymbol{x}$ as $\Delta\boldsymbol{x}$ becomes infinitesimally small, is denoted by

$$f(x)\,\Delta x = P\{x \le \mathbf{x} \le x + \Delta x\} \tag{4.2}$$

where $f(x)$ is the *probability density function*, referred to hereafter as the PDF. Since both $f(x)$ and $F(x)$ are probabilities, they must be greater than or equal to zero for all values of x.

These two functions of x are related. Suppose that we allow $\mathbf{x}$ to take on any values $-\infty \le \boldsymbol{x} \le \infty$. Then, the CDF is just the integral of the PDF over all $\mathbf{x} \le x$:

$$F(x) = \int_{-\infty}^{x} f(x')dx' \tag{4.3}$$

We also may invert this relationship by differentiating to obtain

$$f(x) = \frac{d}{dx}F(x) \tag{4.4}$$

The probability distributions $f(x)$ and $F(x)$ are normalized as follows: We first note that the probability that $\mathbf{x}$ lies between a and b may be obtained by integration

$$\int_{a}^{b} f(x)dx = P\{a \le x \le b\} \tag{4.5}$$

Now, $\mathbf{x}$ must have some value between $-\infty$ and $+\infty$. Thus,

$$P\{-\infty \le \boldsymbol{x} \le \infty\} = 1 \tag{4.6}$$

The combination of this relationship with Eq. (4.5) with $a = -\infty$ and $b = +\infty$ then yields the normalization condition

$$\int_{-\infty}^{\infty} f(x)dx = 1 \tag{4.7}$$

Then, setting $\mathbf{x} = \infty$ in Eq. (4.3), we find the corresponding condition on the CDF to be

$$F(\infty) = 1 \tag{4.8}$$

One more function that is often used is the *complementary cumulative distribution function* or CCDF, which is defined as

$$\widetilde{F}(x) = P\{\mathbf{x} > x\} \tag{4.9}$$

where we use the tilde to designate the complementary distribution, since $\mathbf{x} > x$ is the same as $\mathbf{x}$ *not* $\le x$. The definition of $f(x)$ and Eq. (4.7) allows us to write $\widetilde{F}(x)$ as

$$\widetilde{F}(x) = \int_x^{\infty} f(x')dx' = 1 - \int_{-\infty}^{x} f(x')dx' \tag{4.10}$$

or combining this expression with Eq. (4.3) yields

$$\widetilde{F}(x) = 1 - F(x) \tag{4.11}$$

Thus far, we have assumed that $\mathbf{x}$ can take on any value $-\infty \le \mathbf{x} \le +\infty$. In many situations, we must deal with variables that are restricted to a smaller domain. For example, time is most often restricted to $0 \le \mathbf{t} \le \infty$. In such cases, the foregoing relationships may be modified quite simply. For example, in considering only positive values of time, we have

$$F(t) = 0, \quad t < 0 \tag{4.12}$$

and therefore for time, Eq. (4.3) becomes

$$F(t) = \int_0^t f(t')dt' \tag{4.13}$$

Similarly, the condition of Eq. (4.7) becomes

$$\int_0^{\infty} f(t)dt = 1 \tag{4.14}$$

In Figure 4.1, the relation between $f(t)$ and $F(t)$ is illustrated for a typical random variable with the restriction that $0 \le \mathbf{t} \le \infty$. In what follows we retain the $\pm\infty$ limits on the random variables, with the understanding that these are to be appropriately reduced in situations in which the domain of the variable is restricted.

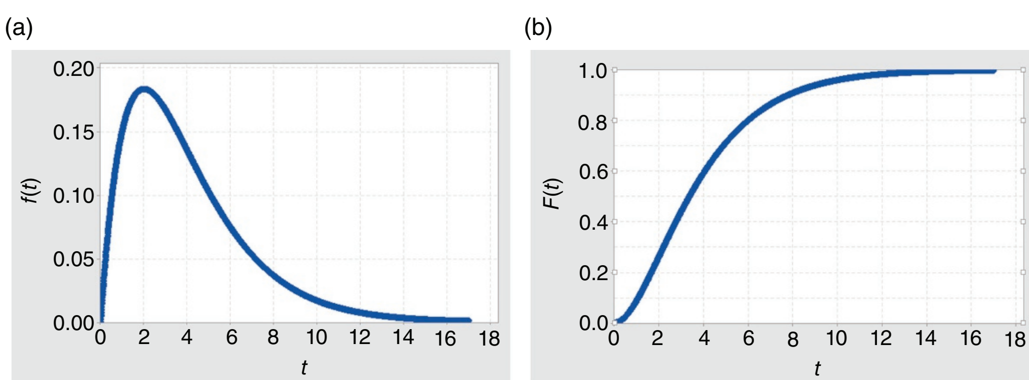


Figure 4.1 Continuous probability distribution: (a) probability density function (PDF) and (b) the corresponding cumulative distribution function (CDF).

Characteristics of a Probability Distribution

Sometimes it is not necessary, or possible, to know the details of the probability density function of a random variable. In many instances, it suffices to know certain integral properties. The two most important of these are the mean and the variance.

The mean or expectation value of **x** is defined by

$$\mu = \int_{-\infty}^{\infty} xf(x)dx \tag{4.15}$$

The variance is given by

$$\sigma^2 = \int_{-\infty}^{\infty} (x-\mu)^2 f(x)dx \tag{4.16}$$

The variance is a measure of the dispersion of values about the mean. Note that since the integrand on the right-hand side of Eq. (4.16) is always nonnegative, the variance is always nonnegative. In Figure 4.2, examples are shown of probability density functions with different mean values and with different values of the variance, respectively.

More general functions of a random variable can be defined. Any function, say $g(x)$, that is to be averaged over the values of a random variable we write as

$$E\{g(x)\} = \int_{-\infty}^{\infty} g(x)f(x)dx \tag{4.17}$$

The quantity $E\{g(x)\}$ is referred to as the expected value of $g(x)$. It may be interpreted more precisely as follows. If we sampled an infinitely large number of values of **x** from $f(x)$ and calculated $g(x)$ for each one of them, the average of these values would be $E\{g\}$. In particular, the nth moment of $f(x)$ is defined to be

$$E\{x^n\} = \int_{-\infty}^{\infty} x^n f(x)dx \tag{4.18}$$

With these definitions, we note that $E\{x^0\} = 1$, and the mean is just the first moment:

$$\mu = E\{x\} \tag{4.19}$$

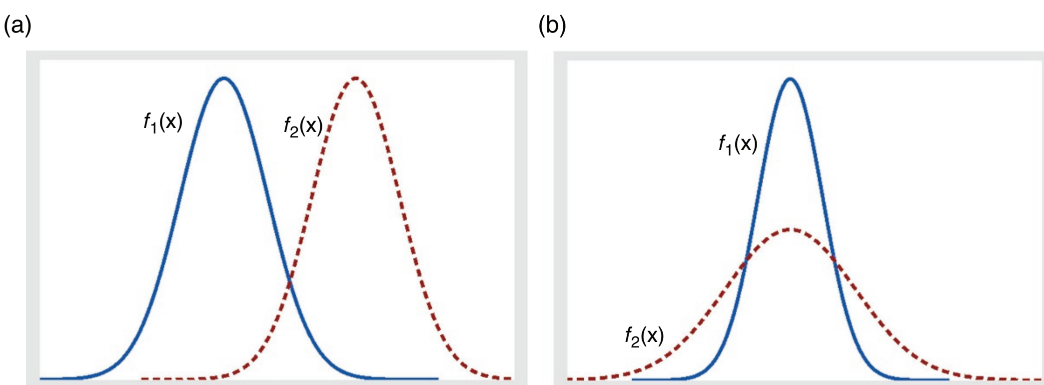


Figure 4.2 Probability density functions. (a) $\mu_1 < \mu_2$, $\sigma_1 = \sigma_2$. (b) $\mu_1 = \mu_2$, $\sigma_1 < \sigma_2$.

Similarly, the variance may be expressed in terms of the first and second moments. To do this, we write

$$\sigma^2 = E\{(x-\mu)^2\} = E\{x^2 - 2x\mu + \mu^2\} \tag{4.20}$$

But since μ is independent of x, it can be brought outside of the integral to yield

$$\sigma^2 = E\{x^2\} - 2E\{x\}\mu + \mu^2 \tag{4.21}$$

Finally, using Eq. (4.19), we have

$$\sigma^2 = E\{x^2\} - E\{x\}^2 \tag{4.22}$$

In addition to the mean and variance, two additional properties are sometimes used to characterize the PDF of a random variable, which are the skewness and the kurtosis. The skewness is defined by

$$\text{skewness(sk)} = \frac{1}{\sigma^3}\int_{-\infty}^{\infty}(x-\mu)^3 f(x)dx \tag{4.23}$$

It is a measure of the asymmetry of a PDF about the mean. In Figure 4.3 are shown two PDFs with identical values of μ and σ^2, but with values of the skewness that are opposite in sign but of the same magnitude. The kurtosis, similar to the variance, is a measure of the spread of $f(x)$ about the mean. It is given by

$$\text{kurtosis(ku)} = \frac{1}{\sigma^4}\int_{-\infty}^{\infty}(x-\mu)^4 f(x)dx \tag{4.24}$$

Example 4.1 A lifetime distribution has the form

$$f(t) = \alpha e^{-\alpha t}, \quad t \geq 0 \text{ and } \alpha > 0$$

where t is in hours. Find μ and σ^2 in terms of α.

Solution:

$$E(t) = \int_{-\infty}^{\infty} tf(t)dt$$

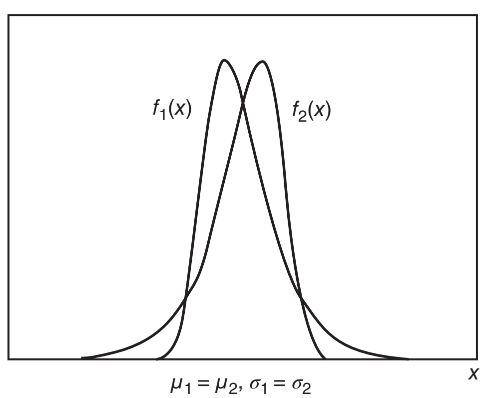


Figure 4.3 Probability density functions with skewness of opposite signs.

By definition, in this case

$$E(t) = \int_0^\infty t\,\alpha e^{-\alpha t}dt = t\left[\frac{\alpha e^{-\alpha t}}{-\alpha}\right]_0^\infty - \int_0^\infty 1\left[\frac{\alpha e^{-\alpha t}}{-\alpha}\right]dt$$

$$= 0 + \int_0^\infty e^{-\alpha t}dt = \left[\frac{e^{-\alpha t}}{-\alpha}\right]_0^\infty = \frac{1}{\alpha}$$

Since $\sigma^2 = E\{t^2\} - E\{t\}^2$:

$$E(t^2) = \int_0^\infty t^2\alpha e^{-\alpha t}dt = t^2\left[\frac{\alpha e^{-\alpha t}}{-\alpha}\right]_0^\infty - \int_0^\infty 2t\left[\frac{\alpha e^{-\alpha t}}{-\alpha}\right]dt$$

$$= 0 + \frac{2}{\alpha}\int_0^\infty t\alpha e^{-\alpha t}dt = \frac{2}{\alpha}E(x) = \frac{2}{\alpha}\left\{\frac{1}{\alpha}\right\} = \frac{2}{\alpha^2}$$

and therefore,

$$\sigma^2 = E\{t^2\} - E\{t\}^2 = \frac{2}{\alpha^2} - \left(\frac{1}{\alpha}\right)^2 = \frac{1}{\alpha^2}$$

and $\sigma = 1/\alpha$.

Sample Statistics

The sample statistics treated here are estimates of random variable properties that do not require the form of the underlying probability distribution to be known. We reconsider estimates for the mean, variance, skewness, and kurtosis defined above. Suppose that we have a sample of size N of a random variable x. Then, the mean can be estimated with

$$\hat{\mu} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4.25}$$

and the variance with

$$\hat{\sigma}^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2 \tag{4.26}$$

if the mean is known. If the mean is not known, but must be estimated from Eq. (4.25), then the variance is increased to

$$\hat{\sigma}^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \hat{\mu})^2 \tag{4.27}$$

The same technique which is applied to Eq. (4.20) may be employed to rewrite the variance as

$$\hat{\sigma}^2 = \frac{N}{N-1}\left[\frac{1}{N}\sum_{i=1}^{N}x_i^2 - \left(\frac{1}{N}\sum_{i}x_i\right)^2\right] \tag{4.28}$$

The estimators for the skewness and kurtosis are, respectively:

$$\widehat{s}_k = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-\hat{\mu})^3}{\left[\frac{1}{N}\sum_{i=1}^{N}(x_i-\hat{\mu})^2\right]^{3/2}}, \quad \widehat{k}_u = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-\hat{\mu})^4}{\left[\frac{1}{N}\sum_{i=1}^{N}(x_i-\hat{\mu})^2\right]^{2}} \tag{4.29}$$

These sample statistics are said to be point estimators because they yield a single number, with no specification as to how much in error that number is likely to be. They are unbiased in the following sense. If the same statistic is applied over and over to successive sets of N data points drawn from the same population, the grand average of the resulting values will converge to the true value as the number of data sets goes to infinity. In Section 4.6, the precision of point estimators is characterized by confidence intervals. Unfortunately, with the exception of the mean, given by Eq. (4.25), confidence intervals can only be obtained after the form of the distribution has been specified.

Transformations of Variables

Frequently, in reliability considerations, the random variable for which data are available is not the one that can be used directly in the reliability estimates. Suppose, for example that the distribution of speeds of impact $f(v)$ is known for a mechanical snubber. If the wear on the snubber, however, is proportional to the kinetic energy, $e = \frac{1}{2}mv^2$, the energy is also a random variable, and it is the distribution of energies $f_e(e)$ that is needed. Such problems are ubiquitous, for much of the engineering analysis is concerned with functional relationships that allow us to predict the value of one variable (the dependent variable) in terms of another (the independent variable).

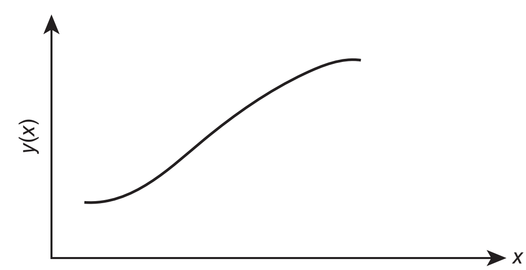
To deal with situations such as the change from speed to energy in the foregoing example, we need a means for transforming one random variable to another. The problem may be stated more generally as follows. Given a distribution $f_{\mathbf{x}}(x)$ or $F_{\mathbf{x}}(x)$ of the random variable $\mathbf{x}$, find the distribution $f_{\mathrm{y}}(y)$ of the random variable $\mathbf{y}$ that is defined by

$$y = y(x) \tag{4.30}$$

We then refer to $f_{\mathrm{y}}(y)$ as the derived distribution. Hereafter, we use subscripts $\mathbf{x}$ and $\mathbf{y}$ to distinguish between the distributions whenever there is a possibility of confusion. First, consider the case where the relation between y and x has the characteristics shown in Figure 4.4; that is, if $x_1 < x_2$, then $y(x_1) < y(x_2)$. Then, $y(x)$ is a monotonically increasing function of x; that is, $dy/dx > 0$. To carry out the transformation, we first observe that

$$P\{\mathbf{x} \le x\} = P\{\mathbf{y} \le y\} \tag{4.31}$$

Figure 4.4 Function of a random variable x.



or simply

$$F_x(x) = F_y(y) \tag{4.32}$$

To obtain the PDF $f_y(y)$ in terms of $f_x(x)$, we first write the preceding equation as

$$\int_{-\infty}^{x} f_x(x')dx' = \int_{-\infty}^{y(x)} f_y(y')dy' \tag{4.33}$$

Differentiating with respect to x, we obtain

$$f_x(x) = f_y(y)\frac{dy}{dx} \tag{4.34}$$

or

$$f_y(y) = f_x(x)\left|\frac{dx}{dy}\right| \tag{4.35}$$

Here, we have placed an absolute value about the derivative. With the absolute value, the result can be shown to be valid for either monotonically increasing or monotonically decreasing functions.

The most common transforms are of the linear form

$$y = ax + b \tag{4.36}$$

and the foregoing equation becomes simply

$$f_y(y) = \frac{1}{|a|} f_x\left(\frac{y-b}{a}\right) \tag{4.37}$$

Note that once a transformation has been made, new values of the mean and variance must be calculated, since in general

$$\int g(x) f_x(x) \neq \int g(y) f_y(y) \tag{4.38}$$

Example 4.2 Consider the distribution $f_x(x) = \alpha e^{-\alpha x}$, $0 \le x \le \infty$, $\alpha > 1$.

a) Transform to the distribution $f_y(y)$, where $y = e^x$.
b) Calculate μ_x and μ_y

Solution:

a) $dy/dx = e^x$; therefore, Eq. (4.35) becomes $f_y(y) = e^{-x} f_x(x)$. We also have $x = \ln y$. Therefore,

$$f_y(y) = e^{-\ln y}\alpha e^{-\alpha \ln y} = \frac{\alpha}{y^{\alpha+1}}, \quad 1 \le y \le \infty$$

b) $\mu_x = \int_0^{\infty} x\alpha e^{-\alpha x}dx = \frac{1}{\alpha}$,
$\mu_y = \int_1^{\infty} y\alpha y^{-(\alpha+1)}dy = \frac{\alpha}{\alpha-1}$

4.3 Empirical Cumulative Distribution Function (Empirical CDF)

Suppose that we have five lab-accelerated life failures (time in minutes): 90, 96, 30, 49, 82.

We can plot these five failures as probability vs time if we do the following: Rank all the failures by ordering the times from smallest to largest and then estimate the probability of failure:

$$\widetilde{F}(t) = r_i/N, \text{where } r_i \text{ is the rank of the failure, e.g. } 1, 2, 3, \text{and } N$$

For our data sample, we then have (Table 4.1):

Plotting probability of failure vs failure time, we have a "step function," which is represented in Figure 4.5. The mean and standard deviation/variance are calculated as

$\hat{\mu} = \frac{1}{N}\sum_{i=1}^{i=N} X_i$, sample variance, $s^2 = \frac{1}{N-1}\sum_{i=1}^{i=N}(X_i - \hat{\mu})^2$, and sample standard deviation,

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{i=N}(X_i - \hat{\mu})^2}$$

Table 4.1 Five lab-accelerated life failures plotted.

Failure number	Rank	Probability of failure	Failure time (min)
1	1	0.2	30
2	2	0.4	49
3	3	0.6	82
4	4	0.8	90
5	5	1	96

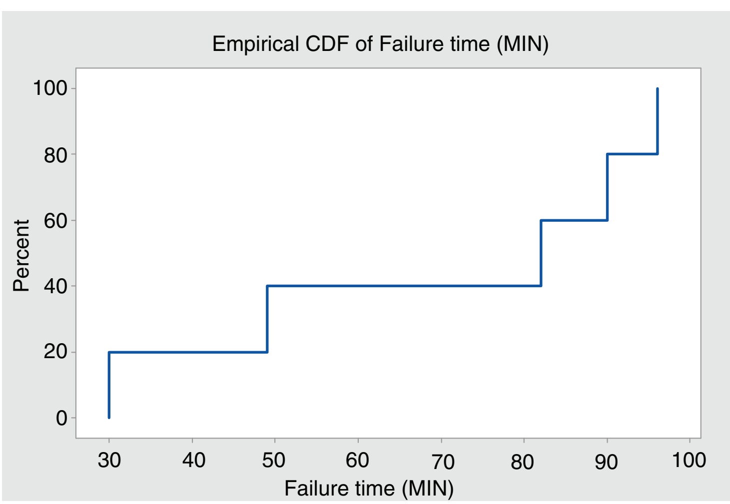


Figure 4.5 Empirical CDF of lab data.

Example 4.3 We have a sample of data from manufacturing, 16 times to failure (TTF) in terms of holes drilled by a drill bit (Table 4.2).

The 16 failures, along with the rank and calculated probability of failure, are listed in the table.

The empirical CDF is in Figure 4.6:

Table 4.2 Manufacturing data.

Rank	Time to failure	Prob = 1/*N*
1	450	0.0625
2	450	0.125
3	700	0.1875
4	700	0.25
5	900	0.3125
6	900	0.375
7	900	0.4375
8	1100	0.5
9	1400	0.5625
10	1400	0.625
11	1400	0.6875
12	1800	0.75
13	1800	0.8125
14	2050	0.875
15	2200	0.9375
16	2700	1

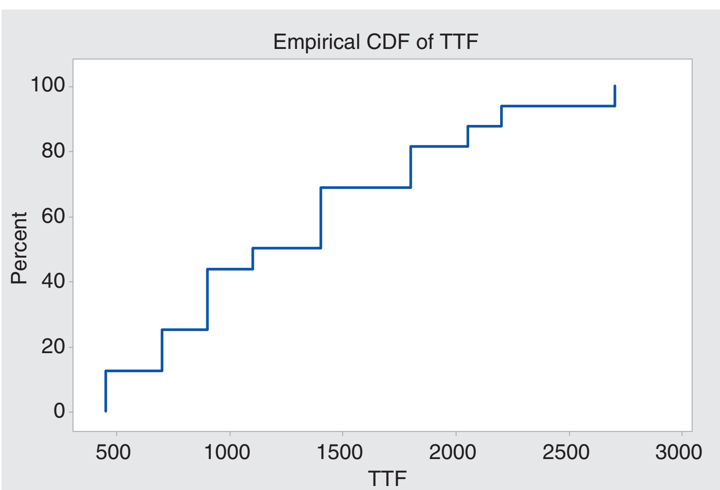


Figure 4.6 Manufacturing drill bit failures.

With sample statistics:

Variable	*N*	Mean	St. Dev
TTF	16	1303	661

Example 4.4 The empirical CDF and the histogram of failures are shown in Figure 4.7.

The empirical CDF shows that failures increase until about 600 hours and then level off until about 1000 hours and then increase again (Table 4.3). The histogram of failures shows that same

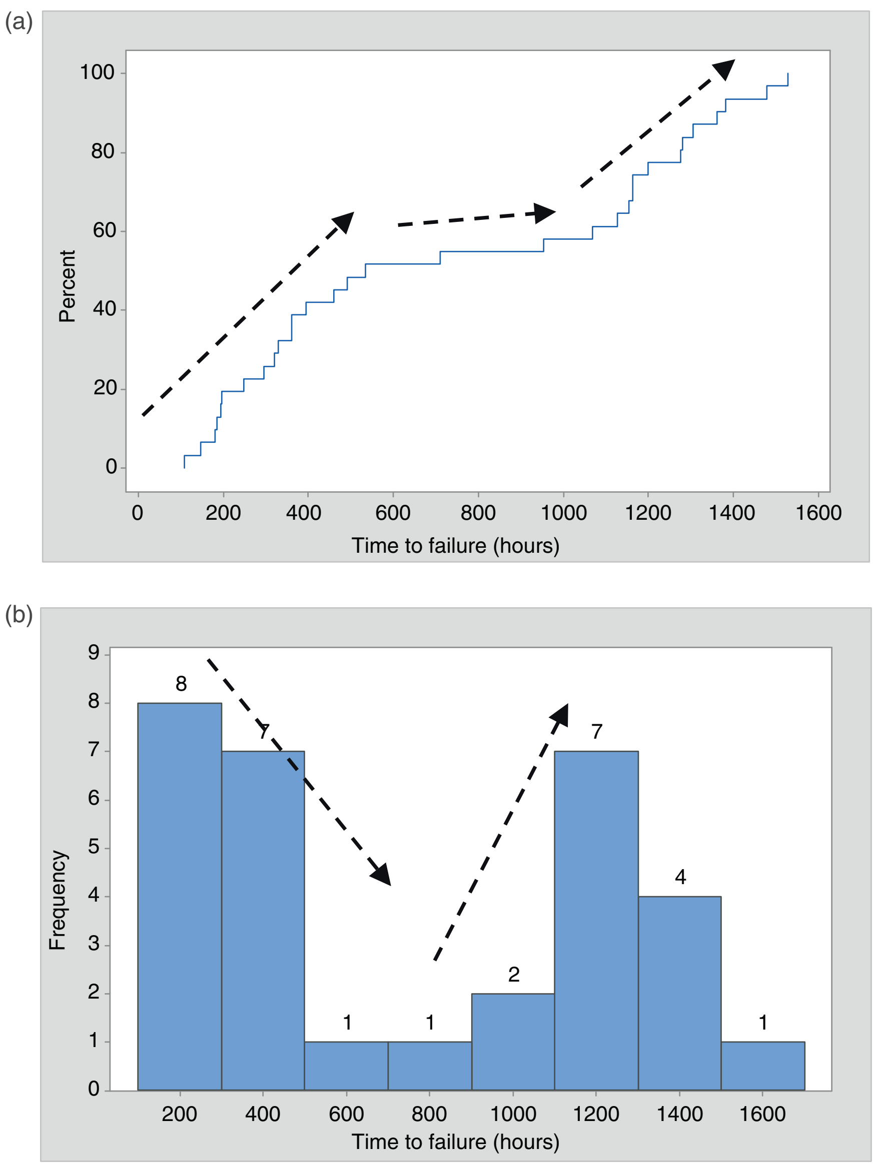


Figure 4.7 Empirical CDF and the histogram of part failures.

Table 4.3 31 failures of a compressor part have been reported from the field.

107.3	192.9	319.8	394.5	708.8	1154.7	1276.6	1381.4
147.2	197.7	328	459.2	952.8	1162.7	1280.5	1478.1
179.1	247.5	359.7	492.1	1067.4	1163.2	1305.1	1527.6
184.5	294.8	361.5	533.8	1126.1	1199	1361.3	

"valley" between 600 and 1000 hours. These two plots should give the engineering team some ideas of where to look for the cause of the leveling off. Some ideas: two different usages, two different locations, two different failure modes?

4.4 Uniform Distribution

The next step in "complexity" is the uniform distribution.

A uniform distribution is used to model events that have equal probability over all possible responses.

If X has a uniform distribution on the interval (a, b), then X has the pdf (probability density function) (Figure 4.8):

$$f(x) = \frac{1}{b-a} \text{ for } a < x < b \\ = 0 \text{ elsewhere} \tag{4.39}$$

The CDF of the uniform distribution is:

$$F(x) = \begin{cases} 0 & \text{for} \quad 0 < x < a \\ \dfrac{x-a}{b-a} & \text{for} \quad a < x < b \\ 0 & \text{for} \quad b < x \end{cases} \tag{4.40}$$

The mean of the uniform distribution is equal to:

$$\mu = \frac{a+b}{2} \tag{4.41}$$

and

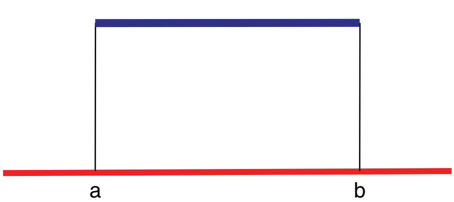


Figure 4.8 Uniform distribution.

$$\text{Variance}\ (\sigma^2) = \frac{(b-a)^2}{12} \tag{4.42}$$

$$\text{Standard Deviation} = \sqrt{\frac{(b-a)^2}{12}} \tag{4.43}$$

And the probability of an observation falling if any interval (*x*, *y*) is equal to:

$$P(a \le x \le b) = \frac{y-x}{b-a} \tag{4.44}$$

Example 4.5 The hardness of a certain alloy (measured on the Rockwell scale) is a random variable X with a uniform distribution from 55 to 80.

A. What is the probability density function for *X*?

Ans: $f(x) = 1/(b-a) = 1/(80–55) = 1/25$

B. Calculate μ and σ^2

Ans: $\mu = \frac{a+b}{2} = \frac{55+80}{2} = 67.5, \sigma^2 = \sqrt{\frac{(b-a)^2}{12}} = \sqrt{\frac{(80-55)^2}{12}} = \frac{25}{2\sqrt{3}}$ or ~ 7.22

C. What is the probability X is between 65 and 75?

Ans: $P(65 \le x \le 75) = \frac{75-65}{80-55} = \frac{10}{25} = 0.4$

D. What is the median hardness?

$$\int_{55}^{X_{Med}} \frac{1}{25} dx = 0.50 \rightarrow \left.\frac{X}{25}\right]_{55}^{X_{Med}} = 0.5$$

$$\frac{X_{Med}}{25} - \frac{55}{25} = 0.5 \rightarrow X_{Med} = 25(0.5) + 55 = 67.5$$

Ans:

The median and mean of this symmetric distribution are equal

Example 4.6 The daily use of jet fuel at a fighter base varies between 35,000 and 150,000 gallons. What is the probability the base will use more than 100,000 gallons on any day?

Ans: $P(100,000 \le x \le 150,000) = \frac{150,000-100,000}{150,000-35,000} = 0.435$

Example 4.7 We need to do a worst case study of the effect of the four parameters (Figure 4.9):

$$\text{Nominal max bending stress} = \frac{6WL}{BH^2} = 96\ \text{ksi}$$

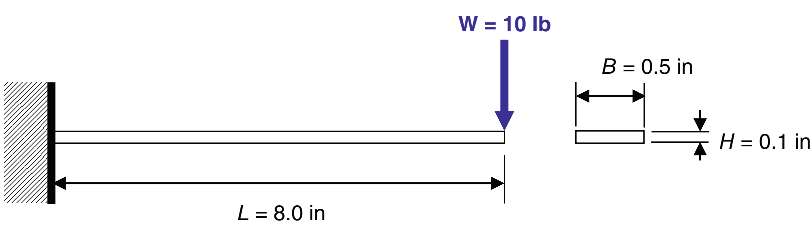


Figure 4.9 A cantilever beam supports an 10-lb load.

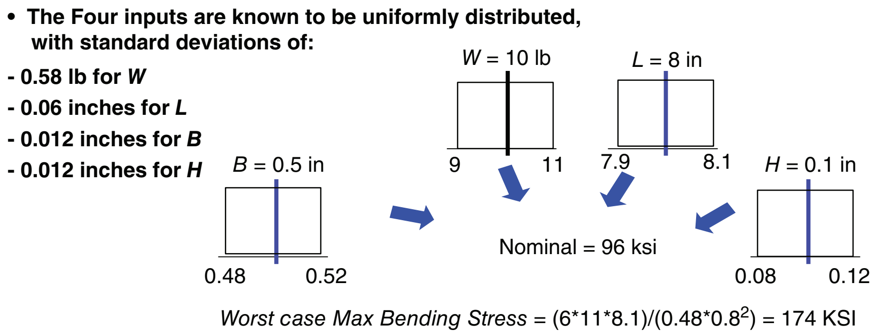


Figure 4.10 Illustration of calculation for max bending stress using uniform distribution assumption

Material yield stress = 140 ksi

$$\text{Margin} = \left(1 - \frac{96}{140}\right) \times 100 = 31\%$$

Since 171.2 ksi exceeds the material yield stress, a redesign is in order.
Ans: See Figure 4.10.

Another very important use of the uniform distribution is in the generation of random numbers, which we will cover in the Section 5.4 (Risk Analysis) and Chapter 11 (Safety Analysis) when we give examples of using Monte Carlo simulation.

4.5 Normal and Related Distributions

Continuous random variables find extensive use in reliability analysis for the description of survival times, system loads and capacities, repair rates, and a variety of other phenomena. Moreover, a substantial number of standardized probability distributions are employed to model the behavior of these variables. For the most part we introduce these distributions as they are needed for model reliability phenomena in the following chapters. We introduce here the normal distribution and the related lognormal and Dirac delta distributions, for they appear in a variety of different contexts throughout the book.

As will be mentioned in Chapter 5, while the Weibull distribution can fit approximately 95% (the author's experience over 45 years of reliability analysis) of *failure data* well, the lognormal is a reliability distribution that will sometimes fit a set of *failure data* better than the Weibull. The lognormal distribution can be derived from the "proportional-effect theory." The proportional effect theory of failure states that the crack growth between any two stages $X_i - X_{i-1}$ of a sequence of crack sizes $X_1 < X_2 \cdots < X_n$ is proportional to the crack size X_{i-1} of the preceding stage for all stages.

From this proportional effect theory, the lognormal distribution can be developed.

The normal distribution will, on the other hand, fit very few instances of *failure data* because it has a time scale that can go below zero, and hence when fitting life data a negative life is nonsensical.

The Normal Distribution

Unquestionably, the normal distribution is the most widely applied in *statistics* (nonfailure) data. It is frequently referred to as the Gaussian distribution. To introduce the normal distribution, we first consider the following function of the random variable **x**:

$$f(x) = \frac{1}{\sqrt{2\pi}b} e^{-\frac{1}{2}\left(\frac{x-a}{b}\right)^2} \text{ for } x, \quad -\infty \le x \le \infty \tag{4.45}$$

where a and b are parameters that we have yet to specify. It may be shown that $f(x)$ meets the conditions for a probability density function. First, it is clear that $f(x) \geq 0$ for all x. Second, by performing the integral

$$\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}b} e^{-\frac{1}{2}\left(\frac{x-a}{b}\right)^2} dx = 1 \tag{4.46}$$

it may be shown that the condition on the PDF given by Eq. (4.7) is met. The evaluation of Eq. (4.46) cannot be carried out by rudimentary means. Rather, the method of residues from the theory of complex variables must be employed. For convenience, some of the more common integrals involving the normal distribution are included in Appendix A.

A unique feature of the normal distribution is that the mean and variance appear explicitly as the two parameters a and b. To demonstrate this, we insert Eq. (4.45) into the definitions of the mean and variance, Eqs. (4.15) and (4.16). Using the evaluated integrals in Appendix A, we find

$$\mu = \int x f(x) dx = \int_{-\infty}^{\infty} x \frac{1}{\sqrt{2\pi}b} e^{-\frac{1}{2}\left(\frac{x-a}{b}\right)^2} dx = a \tag{4.47}$$

$$\sigma^2 = \int x^2 f(x) dx = \int_{-\infty}^{\infty} x^2 \frac{1}{\sqrt{2\pi}b} e^{-\frac{1}{2}\left(\frac{x-a}{b}\right)^2} dx = b^2 \tag{4.48}$$

Consequently, we may write the normal PDF directly in terms of the mean and variance as

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \quad -\infty \le x \le \infty \tag{4.49}$$

Similarly, the CDF corresponding to Eq. (4.34) is

$$F(x) = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x'-\mu}{\sigma}\right)^2} dx' \tag{4.50}$$

When we use the normal distribution, it is often beneficial to make a change of variables first in order to express $F(x)$ in a standardized form. To this end, we define the random variable **z** in terms of **x** by

$$z = \frac{x-\mu}{\sigma} \tag{4.51}$$

Recalling that PDFs transform according to Eq. (4.35), we have

$$f_z(z) = f(x)\left|\frac{dx}{dz}\right| = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} |\sigma| \tag{4.52}$$

which for $x = \mu + \sigma z$

$$f_z(z)\ \frac{1}{\sqrt{2\pi}}\ \exp\left(-\frac{1}{2}z^2\right) \tag{4.53}$$

This implies that for the reduced variate z, $\mu_z = 0$ and $\sigma_z^0 = 1$.

The PDF is plotted in Figure 4.11. Its appearance causes it to be referred to frequently as the bell-shaped curve. The standardized form of the CDF may also be found by applying Eq. (4.51) to $F(x)$,

$$F(z) \equiv \Phi\left[\frac{x-\mu}{\sigma}\right] \tag{4.54}$$

where the standardized error function on the right is defined as

$$\Phi(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{1}{2}\zeta^2}\, d\zeta \tag{4.55}$$

The integrand of this expression is just the standardized normal PDF. A graph of $\Phi(z)$ is given in Figure 4.12; note that each unit on the horizontal axis corresponds to one standard deviation σ, and that the mean value is now at the origin. A tabulation of $\Phi(z)$ is included in Appendix C. Although values for $z < 0$ are included in Appendix C, this is only for convenience, since for the normal distribution we may use the property $f(-z) = f(z)$ to obtain $\Phi(-z)$ from

$$\Phi(-z) = 1 - \Phi(z) \tag{4.56}$$

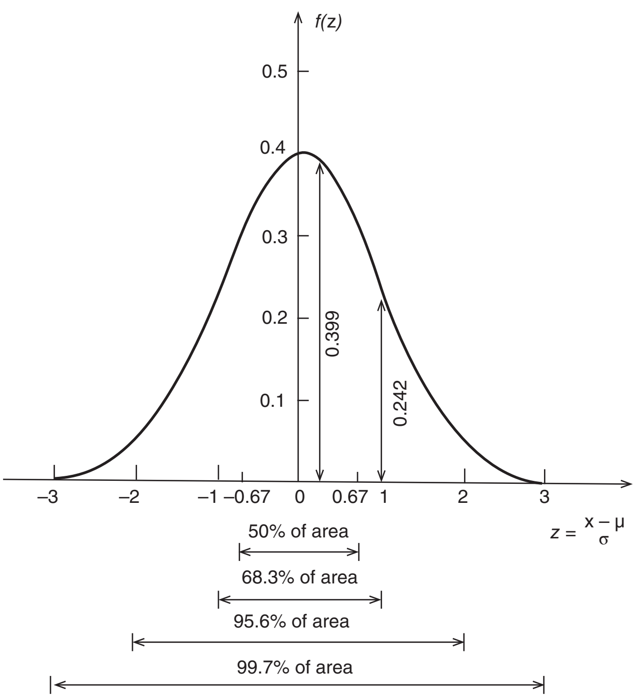


Figure 4.11 Probability density function for a standardized normal distribution.

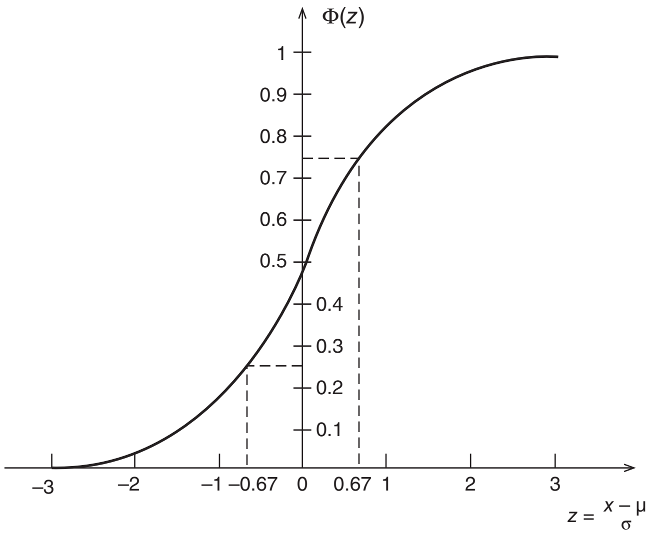


Figure 4.12 Cumulative distribution function for a standardized normal distribution.

Example 4.8 The time to wear out of a cutting tool edge is distributed normally with $\mu = 2.8$ hours and $\sigma = 0.6$ hours.

a) What is the probability that the tool will wear out in less than 1.5 hours?
b) How often should the cutting edges be replaced to keep the failure rate less than 10% of the tools?

Solution: a) $P\{t < 1.5\} = F_t(1.5) = \Phi(z)$, where

$$z = \frac{t-\mu}{\sigma}, \quad z = \frac{1.5-2.8}{0.6} = -2.1667$$

From Appendix C: $\Phi(-2.1667) = 0.0151$.
b) $P\{\mathbf{t} < t\} = 0.10$; $\Phi(z) = 0.10$. $-t + \mu = 1.28\sigma$, $t = \mu - 1.28\sigma$. Then, from Appendix C, $z \approx -1.28$. Therefore, we have

$$-t + \mu = 1.28\sigma, t = \mu - 1.28\sigma = 2.8 - 1.28 \times 0.6 = 2.03 \text{ hours}$$

The normal distribution arises in many contexts. It may be expected to occur whenever the random variable **x** arises from the sum of a number of random effects, no one of which dominates the total. It is widely used to represent measurement errors, dimensional variability in manufactured goods, material properties, and a host of other phenomena.

A specific illustration might be as follows. Suppose that an elevator cable consists of strands of wire. The strength of the cable is then

$$x = x_1 + x_2 + x_3 + \dots + x_N \tag{4.57}$$

where x_l is the strength of the ith strand. Even though the PDF of the individual strands x_l is not a normal distribution, the strength of the cable will be given by a normal distribution, provided that N, the number of strands, is sufficiently large.

The normal distribution also has the following property. If **x** and **y** are **independent** random variables that are normally distributed, then

$$u = ax + by \tag{4.58}$$

where a and b are constants, is also distributed normally. Moreover, it may be shown that the mean and variance of u are related to those of x and y by

$$\mu_u = a\mu_x + b\mu_y \tag{4.59}$$

and

$$\sigma_u{}^2 = a^2\sigma_x{}^2 + b^2\sigma_y{}^2 \tag{4.60}$$

The same relationships may be extended to linear combinations of three or more random variables.

Normal Distribution...... Cautions and Warnings!!

Often, the normal distribution is adopted as a convenient approximation, even though there may be no sound physical basis for assuming that the previously stated conditions are met. In some situations this may be justified on the basis that it is the limiting form of several other distributions, the binomial and the Poisson, to name two. More important, if one is concerned only with very general characteristics and not the details of the shape, the normal distribution may sometimes serve as a widely tabulated, if rough, approximation to empirical data. One must take care, however, not to pursue too far the idea that the normal distribution is generally a reasonable representation for empirical data. If the data exhibit a significant skewness, the normal distribution is not likely to be a good choice. Moreover, if one is interested in the "tails" of the distribution, where $|(x - \mu)/\sigma| > > 1$, improper use of the normal distribution is likely to lead to large errors. Extreme values of distribution must often be considered when determining safety factors and related phenomena. Distributions appropriate to such extreme-value problems (most notably the Weibull distribution) are taken up in Chapter 5.

Example 4.9 The Manufacturing floor has given you the following (Table 4.4):

Assuming the data is from a Normal distribution, what is the 0.01(1/100) probability of failure in terms of holes drilled?

Hint: Do a probability plot of the data

Table 4.4 Drill bit lifetimes for drilling holes through a superalloy, in terms of number of holes drilled:

54	134	199
55	141	224
60	167	239
99	172	24
127	199	

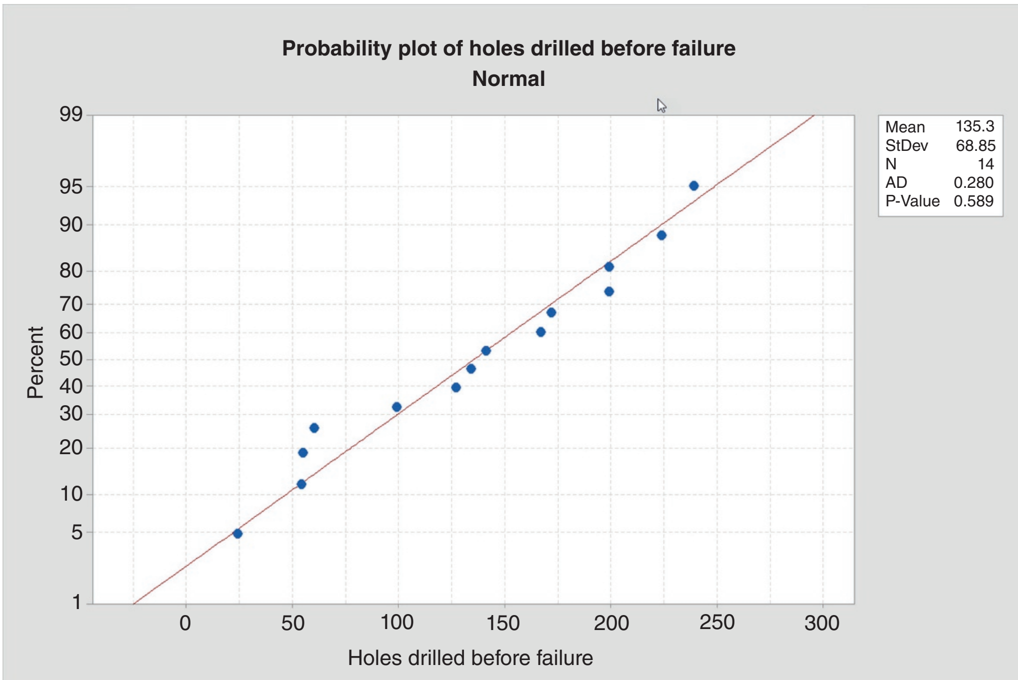


Figure 4.13 Normal probability plot of drill bit lifetimes.

Solution: Using MINITAB® (Figure 4.13):

OOPS, the 1/100 probability of failure in terms of holes drilled is <0 holes????

This is an illustration of a warning not to assume that the normal distribution will fit failure data. It seldom does.

Central Limit Theorem

Next, we address a concept that allows us to identify bounds on our reliability parameters and in general make inferences concerning the populations we are studying.

Statement of the Theorem:

If all possible simple random samples, each of size n, are taken from any population with a mean μ and a standard deviation σ, the sampling distribution of the sample means (averages) will:

1) Have mean $\mu_{\overline{X}} = \mu$
2) Have standard deviation $\sigma_{\overline{X}} = \dfrac{\sigma}{\sqrt{n}}$ (Standard deviation of the mean)
3) Be approximately normally distributed regardless of the shape of the parent population (normality improves with larger n).

How large is large enough? Generally speaking, a sample size of 30 or more is considered to be large enough for the central limit theorem to take effect. The closer the population distribution is to a normal distribution, the fewer samples needed to demonstrate the theorem.

Populations that are heavily skewed or have several modes may require larger sample sizes.

The statement of the central limit theorem can seem quite technical but can be understood if we think through the following steps. We begin with a simple random sample with n individuals from a population of interest. From this sample, we can easily form a sample mean that corresponds to the mean of what measurement we are curious about in our population.

A sampling distribution for the sample mean is produced by repeatedly selecting simple random samples from the same population and of the same size and then computing the sample mean for each of these samples. These samples are to be thought of as being independent of one another.

The central limit theorem concerns the sampling distribution of the sample means. We may ask about the overall shape of the sampling distribution. The central limit theorem says that this sampling distribution is approximately normal. This approximation improves as we increase the size of the simple random samples that are used to produce the sampling distribution.

The surprising fact is that this theorem says that a normal distribution arises regardless of the initial distribution. Even if our population has a skewed distribution, which occurs when we examine things such as manufacturing data, incomes, or people's weights, a sampling distribution for a sample mean with a sufficiently large sample size will be normal.

That fact can be illustrated as follows:

Start with a histogram of 1000 samples from a uniform distribution on [0,1], then successively take 1000 averages of 2 samples from the Uniform sample, then 1000 averages of 5 samples, 1000 averages of 25 samples, and 1000 averages of 100 samples from this same distribution. The result of drawing histograms of this simulation data is illustrated in Figure 4.14a. Note that as the number of samples in a mean of 2, then 5, then 25, and then 100 are approaching the mean of the original distribution, 0.5 (Figure 4.14a). In addition, the more samples that are averaged are giving a smaller variation around the mean. This simulation exercise illustrates the CLT.

In considering the above uniform distribution of 1000 averages of 100, redrawing the histogram and marking off 1σ, 2σ, and 3σ areas illustrates the standard deviation of the mean (Figures 4.14b and Figure 4.14c):

$$\text{Using CLT}, \sigma_{100} = \frac{\sigma_{orig}}{\sqrt{100}} = \frac{0.29}{10} = 0.029$$

Central Limit Theorem in Practice

Just a little work with some real-world data shows that outliers, skewness, multiple peaks, and asymmetry show up quite routinely. The use of an appropriate sample size and the central limit theorem help us to get around the problem of data from populations that are not normal.

Thus, even though we might not know the shape of the distribution where our data comes from, the central limit theorem says that we can treat the sampling distribution as if it were normal. Of course, in order for the conclusions of the theorem to hold, we do need a sample size that is large enough. We use the central limit theorem in later chapters to explain confidence intervals on various reliability parameters as well as on comparing population parameters for differences.

The Lognormal Distribution

As indicated earlier, if a random variable $\mathbf{x}$ can be expressed as a sum of the random variables, x_i, $i = 1, 2, ..., N$ where no one of them is dominant, then $\mathbf{x}$ can be described as a normal distribution, even though the $\mathbf{x}_i$ are described by normal distributions that may not even be the same for different

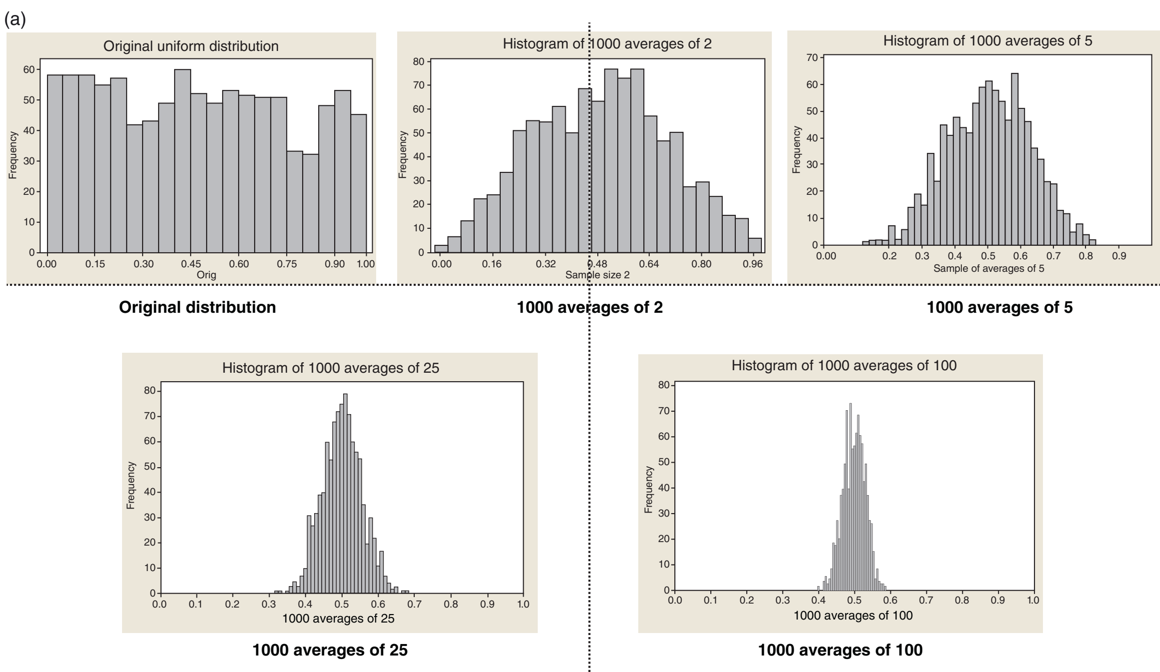


Figure 4.14a Demonstration of the central limit theorem using the uniform distribution.

(b)

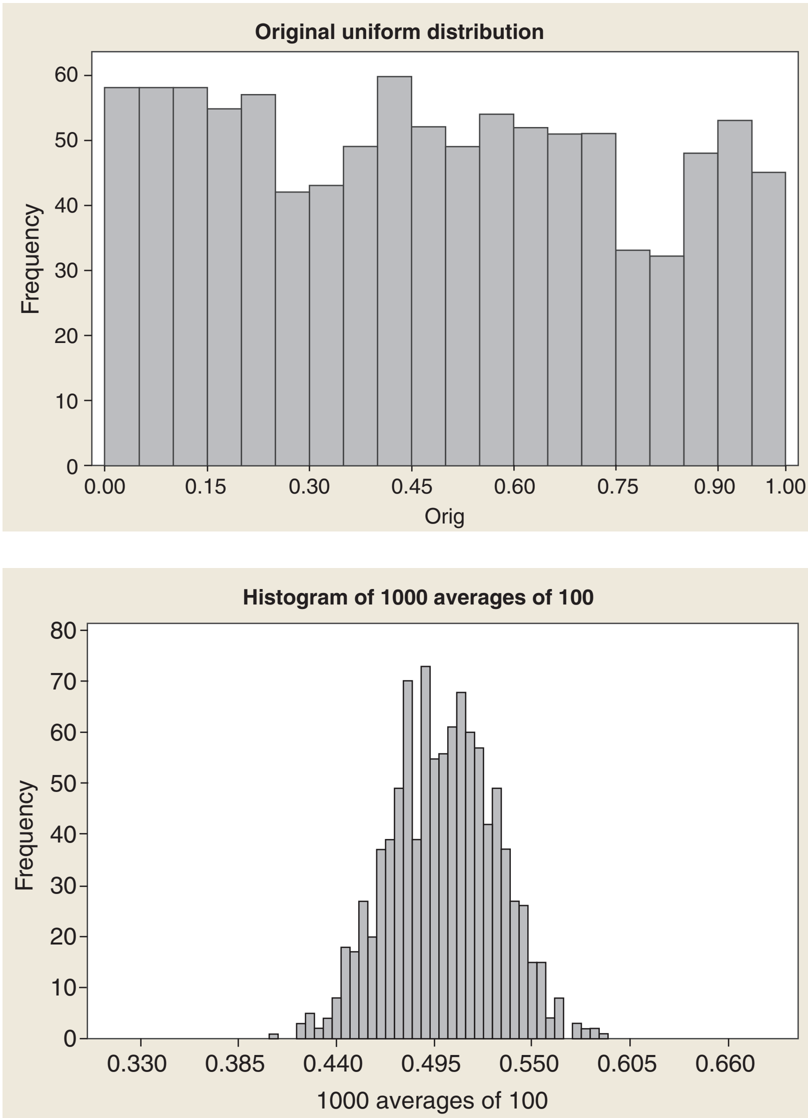


Figure 4.14b Demonstration of the mean and standard deviation of the original to 1000 averages of 100. Where original Uniform distribution μ = 0.477, σ = 0.29, *and 1000 averages of 100 from the Uniform Distribution* μ = 0.500, σ = 0.029.

values of i. A second frequently arising situation consists of a random variable $\mathbf{y}$ that is a product of the random variables $\mathbf{y}_l$:

$$y = y_1 y_2 \ldots y_n \tag{4.61}$$

For example, the wear on a system may be proportional to the product of the magnitudes of the demands that have been made on it. Suppose that we take the natural logarithm of Eq. (4.61):

$$\ln y = \ln y_1 + \ln y_2 + \cdots + \ln y_n \tag{4.62}$$

(c)

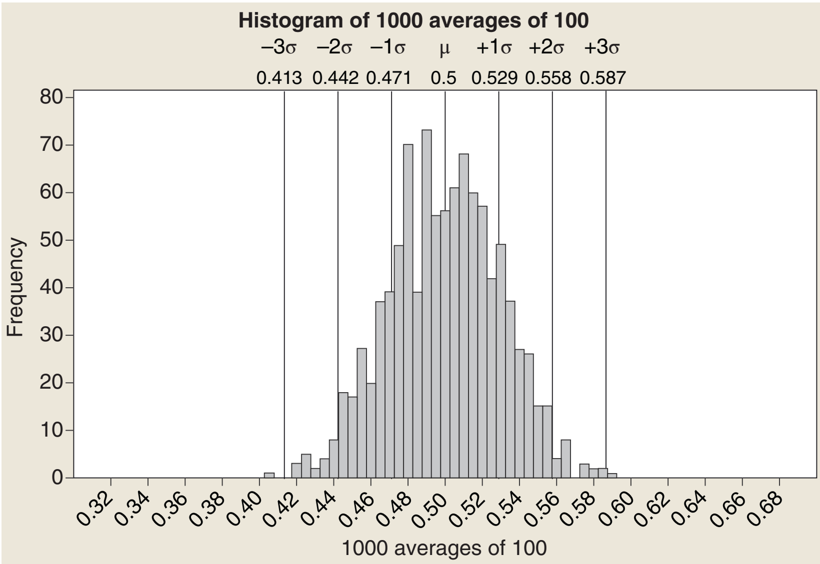


Figure 4.14c Demonstration of the standard deviation of 1000 averages of 100 from -3σ to $+3\sigma$.

The analogy to the normal distribution is clear. If no one of the terms on the right-hand side has a dominant effect, then In y should be distributed normally. Thus, if we define

$$x \equiv \ln y \tag{4.63}$$

then x is distributed normally, and y is said to be distributed lognormally.

To obtain the lognormal distribution for y, we first write the normal distribution for x,

$$f_x(x) = \frac{1}{\sqrt{2\pi}\sigma_x} e^{-\frac{1}{2}\left(\frac{x-\mu_x}{\sigma_x}\right)^2} - \infty \leq x \leq \infty \tag{4.64}$$

where μ_x is the mean value of $\mathbf{x}$, and $\sigma_\mathbf{x}^2$ is the variance of the distribution in $\mathbf{x}$. Now suppose that we let x be the natural logarithm of the variable y. In order to find the PDF in y, we must transform the distribution according to Eq. (4.35):

$$f_y(y) = f_x(x)\left|\frac{dx}{dy}\right| \tag{4.65}$$

Noting that

$$\frac{dx}{dy} = \frac{d}{dy}(\ln y) = \frac{1}{y} \tag{4.66}$$

and using $x = \ln y$ to eliminate x from Eqs. (4.64) and (4.65), we obtain *the PDF*:

$$f_y(y) = \frac{1}{\sqrt{2\pi}\omega y} e^{-\frac{1}{2\omega^2}\left(\ln\left(\frac{y}{y_0}\right)\right)^2} \tag{4.67}$$

where we have made the replacements

$$\mu_x = \ln y_0; \sigma_x = \omega \tag{4.68}$$

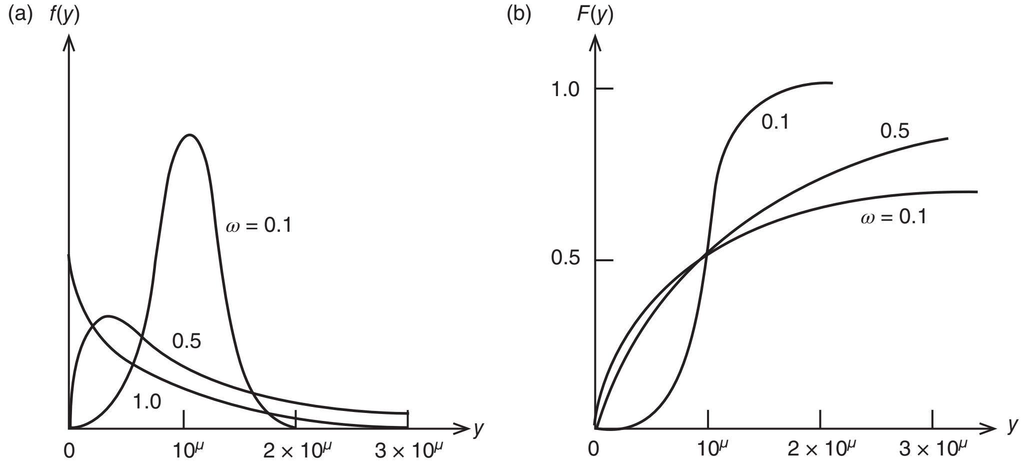


Figure 4.15 The lognormal distribution: (a) probability density function (PDF) and (b) cumulative distribution function (CDF).

The corresponding *CDF is* obtained by integrating over y with a lower limit of $y = 0$. The results can be expressed in terms of the standardized normal integral as

$$F_y(y) = \Phi\left[\frac{1}{\omega}\ln\left(\frac{y}{y_0}\right)\right] \tag{4.69}$$

The PDF and the CDF for the lognormal distribution are plotted as a function of y in Figure 4.15. Note that for small values of ω, the lognormal and normal distributions have very similar appearances.

The mean of the lognormal distribution may be obtained by applying Eq. (4.15) to Eqs. (4.67) and (4.68):

$$\mu_y = y_0 e^{\frac{\omega^2}{2}} = e^{\mu_x} e^{\frac{\sigma_x{}^2}{2}} = e^{\mu_x + \frac{\sigma_x{}^2}{2}} \tag{4.70}$$

Note that it is not equal to the parameter y_0 for which the distribution is a maximum. On the contrary, y_0 *may be shown to be the median value of* $\boldsymbol{y}$. Similarly, the *variance in* $\boldsymbol{y}$ *is not equal to* ω *but rather is*

$$\sigma_y{}^2 = y_0{}^2 e^{\omega^2}\left(e^{\omega^2} - 1\right) = e^{2\mu_x + \sigma_x^2}\left(e^{\sigma_x^2} - 1\right) \tag{4.71}$$

Lognormal distributions are widely applied in reliability engineering to describe failures caused by fatigue, uncertainties in failure rates, and a variety of other phenomena. It has the property that if variables x and y have lognormal distributions, the product random variable $z = xy$ is also lognormally distributed.

The lognormal distribution also finds use in the following manner. Suppose that the best estimate of a variable is y_0, and there is a 90% certainty that y_0 is known within a factor of n. That is, there is a probability of 0.9 that it lies between y_0/n and $y_0 n$, where $n > 1$. We then have

$$0.05 = \int_{-\infty}^{-\frac{1}{\omega}\ln n} \frac{1}{\sqrt{2\pi}\omega y} e^{-\frac{1}{2\omega^2}\left(\ln\left(\frac{y}{y_0}\right)\right)^2} dy \tag{4.72}$$

With the change of variables $\zeta = (1/\omega)\ \ln\ (y/y_0)$, Eq. (4.72) may be written as

$$0.05 = \int_{-\infty}^{-\frac{1}{\omega}\ln n} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2\omega^2}\zeta^2} d\zeta \tag{4.73}$$

This integral is the CDF for the standardized normal distribution, given by Eq. (4.55). Thus, we have

$$0.05 = \Phi\left[-\frac{1}{\omega}\ln n\right] \tag{4.74}$$

where Φ is the standardized normal CDF. Similarly, it may be shown that

$$0.95 = \Phi\left[+\frac{1}{\omega}\ln n\right] \tag{4.75}$$

From the table in Appendix C it is seen that the argument for which $\Phi = 0.05$ or 0.95 is ∓ 1.645. Thus, we have

$$\frac{1}{\omega}\ln n = 1.645 \tag{4.76}$$

Therefore, the parameter ω is given by

$$\omega = \frac{\ln n}{1.645} \tag{4.77}$$

With y_0 and ω determined, the μ_y can be determined from Eq. (4.70).

Example 4.10 Fatigue life data for an industrial rocker arm is fit to a lognormal distribution. The following parameters are obtained: $y_0 = 2 \times 10^7$ cycles, $\omega = 2.4$. (a) To what value should the design life be set if the probability of failure is not to exceed 1.0%? (b) If the design life is set to 1.0×10^6 cycles, what will the failure probability be?

Solution: (a) Let y be the number of cycles for which the failure probability is 1%. Then, from Eq. (4.69), we have

$$0.01 = F_y(y) = \Phi\left[\frac{1}{2.3}\ln\left(\frac{y}{2 \times 10^7}\right)\right]$$

From Appendix C, we find

$$\Phi(-2.32) \approx 0.01$$

Thus,

$$-2.32 = \frac{1}{2.3}\text{In}\left(\frac{y}{2 \times 10^7}\right)$$

and

$$y = 2 \times 10^7 \exp(-2.32 \times 2.3)$$
$$= 9.63 \times 10^4 \text{ cycles}$$

(b) In Eq. (4.69), we have

$$z \equiv \frac{1}{\omega} \ln\left(\frac{y}{y_0}\right) = \frac{1}{2.3} \ln\left(\frac{10^6}{2.0 \times 10^7}\right)$$
$$= -1.302$$

From Appendix C, $\Phi(-1.302) \approx 0.096$ so that
$F_y(y) = 0.096$ probability of failure.

Log Normal Distribution from a Physics of Failure Perspective

The log normal models a process where the time to failure results from a multiplication of effects. Progressive deterioration will be log normal. For example, a crack grows rapidly with high stress because the stress grows progressively as the crack grows (in other words, if the crack growth rate increases with the size of the crack, that failure phenomenon can be modeled by the lognormal distribution). See also Ireson (1966), pp. 2–8.

On the other hand, if the crack growth is linear with time as it may be in a low stress area, the Weibull distribution (Chapter 5) will be more appropriate.

Example 4.11 Jet engine turbine cover plate cracking. After a cover plate cracking failure mode appeared in the field, the physics of failure suggested a redesign of the cover plate. This redesign was lab tested on 20 redesigned cover plates (cycles to failure in the table) (Table 4.5):

The 1800 cycle probability of failure is desired.

Solution: Using MINITAB and producing a log-normal probability plot (Figure 4.16).

Table 4.5 Cover plate cracking lab data.

1989	2979	3853	5716
2160	3016	3916	5984
2569	3283	4294	6378
2758	3294	4462	6556
2813	3503	5178	7000

Source: Data from USAF Weibull Analysis Handbook, AFWAL-TR-83-2079, pp. 135–137.

Example 4.12 M60 torsion bar test data (Table 4.6)

Torsion bar life has been shown to be lognormally distributed. Using data in the table to the right: Find the median and 1/1000 life.

Find median life and 1/1000 life of this data.

Note: Example taken from AMMRCTR85-18, "Reliability and Life Prediction Methodology – M60 Torsion Bars." AD-A159 197, June 1985.

Solution: See Figure 4.17.

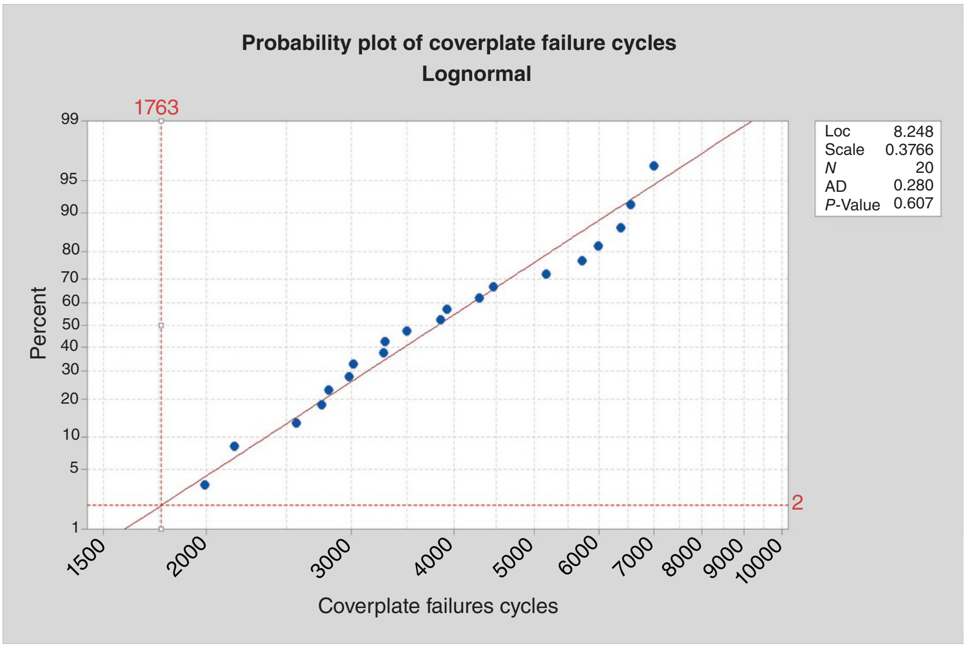


Figure 4.16 The probability of failure by ~1760 cycles is 0.02 (i.e. 2% of the cover plate population are predicted to be cracked by 1800 cycles). *Source:* Adapted from Abernethy et al. (1983).

Table 4.6 M60 torsion bar life data(cycles).

362,016	195,863	201,169	142,939	125,955
207,889	147,773	331,606	131,890	183,740
186,849	270,778	123,325	137,765	
181,344	239,396	219,715	221,500	
310,785	271,990	156,315	248,754	

4.6 Confidence Intervals

Point and Interval Estimates

The mean, variance, and other sample statistics introduced in Section 4.2 are often referred to as nonparametric point estimators. They are nonparametric because they may be evaluated without knowing the population distribution from which the sample was drawn, and they are point estimators because they yield a single number. Point estimates can also be made for the parameters of specific distributions, for example the shape and scale parameters of a Weibull distribution (discussed in Chapter 6). The corresponding interval estimates, which provide some level of confidence that a parameter's true value lies within a specified range of the point estimate, occupy a pivotal place in statistical analysis.

We begin our examination of interval estimates by expressing the sample static properties in terms of the probability concepts developed above. Suppose that we want to estimate a property

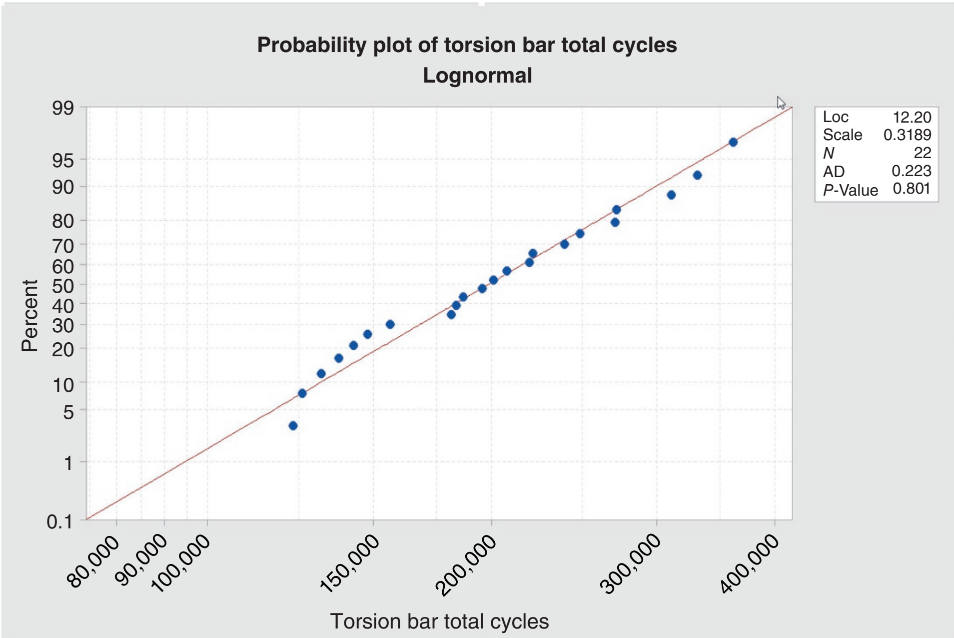


Figure 4.17 The median life is exp(12.2) = 198,789 cycles and 1/1000 life ~74,300 cycles (reading off the plot). *Source:* Adapted from Barsoum et al. (1985).

θ, where θ might be the mean, variance, or skewness, or a parameter associated with a specific distribution. The estimator $\hat{\theta}$ is itself a random variable with the sampling variability characterized by a PDF, referred to as a sampling distribution. Let the sampling distribution be denoted by $f_{\hat{\theta}}(\hat{\theta})$. If we repeatedly form $\hat{\theta}$ from samples of size N, and make a histogram of the values of $\hat{\theta}$, after many trials the sampling distribution $f_{\hat{\theta}}(\hat{\theta})$ will emerge. A sketch of a typical sampling distribution is provided in Figure 4.18a. If the estimator is unbiased, then $E\{\hat{\theta}\} = \theta$, which is to say that the mean value of the sampling distribution is the true value of θ:

$$\int_{-\infty}^{\infty} \hat{\theta} f_{\hat{\theta}}(\hat{\theta}) \ d\hat{\theta} = \theta. \tag{4.78}$$

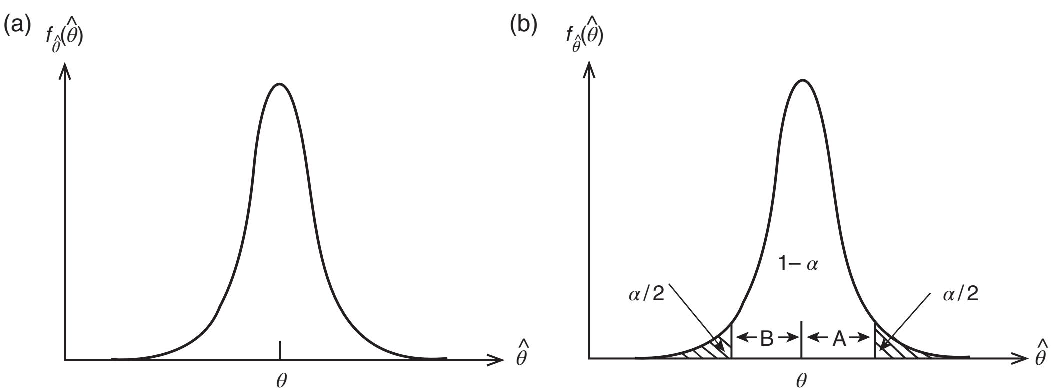


Figure 4.18 Sampling distribution.

Along with the value of the point estimate $\hat{\theta}$ we would like to gain some idea of its precision. For this, we calculate a *confidence interval* as follows. Suppose that we pick a value $\theta + A$ on the $\hat{\theta}$ axis in Figure 4.18b such that the probability that $\hat{\theta} \leq \theta + A$ is $1 - \alpha/2$, where α is typically a small number such as 1% or 5%. This condition may be written in terms of the sampling distribution as

$$P\{\hat{\theta} \leq \theta + A\} = \int_{-\infty}^{\theta + A} f_{\hat{\theta}}(\hat{\theta}) \; d\hat{\theta} = 1 - \alpha/2 \tag{4.79}$$

As shown in Figure 4.18b, the area under the sampling distribution to the right of $\theta + A$ is $\alpha/2$. Rearranging the inequality on the left, we have

$$P\{\hat{\theta} - A \leq \theta\} = \int_{-\infty}^{\theta + A} f_{\hat{\theta}}(\hat{\theta}) \, d\hat{\theta} = 1 - \alpha/2. \tag{4.80}$$

Likewise, if we choose a value B such that the probability that $\hat{\theta} \geq \theta - B$ is $1 - \alpha/2$, we obtain

$$P\{\hat{\theta} \geq \theta - B\} = \int_{\theta - B}^{\infty} f_{\hat{\theta}}(\hat{\theta}) \, d\hat{\theta} = 1 - \alpha/2, \tag{4.81}$$

and as indicated in Figure 4.18b, the area under the sampling distribution to the left $\theta - B$ is also $\alpha/2$. Rearranging the inequality on the left, we have

$$P\{\theta \leq \hat{\theta} + B\} = \int_{\theta - B}^{\infty} f_{\hat{\theta}}(\hat{\theta}) \, d\hat{\theta} = 1 - \alpha/2. \tag{4.82}$$

The probability that $\hat{\theta} - B \leq \theta \, and \, \theta \leq \hat{\theta} + A$ is just the area $1 - \alpha$ under the central section of the sampling distribution, or

$$P\{\hat{\theta} - A < \theta \leq \hat{\theta} + B\} = \int_{\theta - B}^{\theta + A} f_{\hat{\theta}}(\hat{\theta}) \, d\hat{\theta} = 1 - \alpha \tag{4.83}$$

The lower and upper confidence limits for estimates based on a sample size N are defined as

$$L_{\alpha/2,N} = \hat{\theta} - A \tag{4.84}$$

and

$$U_{\alpha/2,N} = \hat{\theta} + B \tag{4.85}$$

respectively. Hence, the $100(1 - \alpha)\%$ two-sided confidence interval is

$$P\{L_{\alpha/2,N} \leq \theta \leq U_{\alpha/2,N}\} = 1 - \alpha \tag{4.86}$$

We must be specific about the preceding probability statements, for they define the meaning of confidence intervals. Equation (4.87) may be understood with the aid of Figure 4.19 as follows. Suppose that a large number of samples each of size N are taken, and $\hat{\theta}$, $L_{\alpha/2,N}$, and $U_{\alpha/2,N}$ are calculated for each sample. These three quantities are random variables and in general will be different for each sample. In Figure 4.19, we have plotted them for 10 such samples. If $L_{\alpha/2,N}$ and $U_{\alpha/2,N}$ define the 90% confidence interval, then for 90% of the samples of size N the true value of θ will lie within the intervals indicated by the solid vertical lines. Conversely, there is an $\alpha = 0.1$ risk that the true value will lie outside of the confidence interval. For brevity, we frequently suppress the subscripts in Eqs. (4.84) and (4.85) and denote the lower and upper confidence limits by $\theta^{-} \equiv L_{\alpha/2,\,N}$ and $\theta^{+} \equiv U_{\alpha/2,N}$.

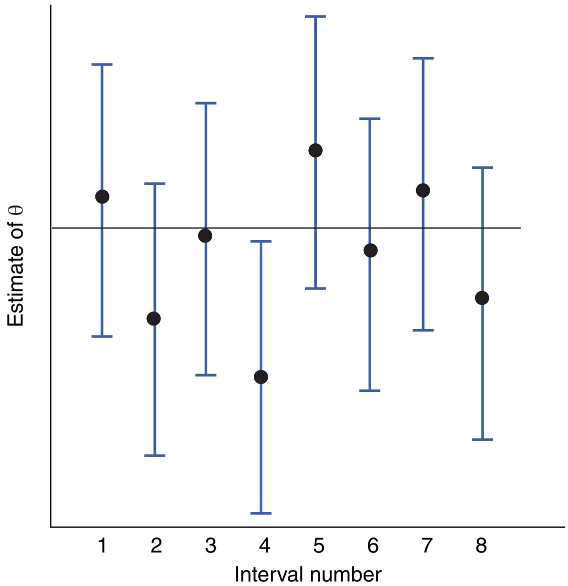


Figure 4.19 Confidence limits for repeated estimates of a parameter.

For the foregoing methodology to be applied to the computation of the confidence interval for a particular parameter, the properties of the corresponding sampling distribution, $f_{\hat{\theta}}(\hat{\theta})$, must be sufficiently well understood. In this respect, the situation is quite different for the mean, variance, skewness, and kurtosis, which may be defined for any distribution, and the specific parameters appearing in the normal, lognormal, Weibull, or other distribution. If the parent distribution is not designated, then a confidence interval can be determined only for the mean, μ, and then only if the sample size is sufficiently large, say $N > 30$. In this situation, the sampling distribution becomes normal, and as shown in the following subsection, the confidence interval can be estimated.

As was mentioned in Chapter 2, Section 2.3.4 on binomial confidence intervals, for $Np \geq 5$ or $N(1 - p) \geq 5$, the normal distribution (Eq. 4.86) can be used to approximate binomial confidence intervals.

If the parent distribution is known, then the point and interval estimates of the distribution parameters become the center of attention. Here, the situation differs markedly depending on whether *N*, the sample size, is large. For small or intermediate sample sizes taken from a normal distribution, the Student's *t* and the Chi-squared sampling distributions can be used to estimate the confidence interval for the mean and variance, respectively. The procedures are covered in elementary statistical texts. The more sophisticated procedures required for other parent distributions are found in the more advanced statistical literature but are increasingly accessible though statistical software packages. Large sample sizes, point estimates, and confidence intervals for distribution parameters may be expressed in more elementary terms; then, the sampling distributions approach the normal form, enabling the confidence intervals to be expressed in terms of the standard normal CDF. In subsequent subsections, the results compiled by Nelson (1982) are presented for point estimates and confidence intervals of the normal, lognormal, Weibull, and extreme-value parameters.

Estimate of the Mean

The sample mean given by Eq. 4.25, in addition to being the most ubiquitous statistic, has a unique property. An interval estimate is associated with the mean that is independent of the distribution from which the sample is drawn. Provided the sample size is sufficiently large, say $N > 30$, the central limit theorem provides a powerful result; the sampling distribution $f_{\hat{\mu}}(\hat{\mu})$ for μ becomes normal with a mean of μ and variance σ^2/N. Thus,

$$f_{\hat{\mu}}(\hat{\mu}) = \frac{\sqrt{N}}{\sqrt{2\pi}\sigma} \exp\left[-\frac{N}{2\sigma^2}(\hat{\mu}-\mu)^2\right] \tag{4.87}$$

Replacing θ with $\hat{\mu}$ in Eq. (4.83), we have

$$\int_{\mu-B}^{\mu+A} \frac{\sqrt{N}}{\sqrt{2\pi}\sigma} \exp\left[-\frac{N}{2\sigma^2}(\hat{\mu}-\mu)^2\right] d\hat{\mu} = 1-\alpha \tag{4.88}$$

or with the substitution $\xi = \sqrt{N}(\hat{\mu}-\mu)/\sigma$,

$$\int_{-\sqrt{N}B/\sigma}^{\sqrt{N}A/\sigma} \frac{1}{\sqrt{2\pi}} \exp\left[-\tfrac{1}{2}\xi^2\right] d\xi = 1-\alpha \tag{4.89}$$

Comparing this integral with the normal CDF given in standard form by Eq. (4.55), we see that

$$\Phi\left(\sqrt{N}A/\sigma\right) - \Phi\left(-\sqrt{N}B/\sigma\right) = 1-\alpha. \tag{4.90}$$

The standardized normal distribution is plotted in Figure 4.20. Recall that A is chosen so that the area under the sampling curve to the right is $\alpha/2$. We designate $z_{\alpha/2}$ to be the value of the reduced variate for which this condition holds. Thus, the area to the left of $z_{\alpha/2}$ is given by

$$\Phi(z_{\alpha/2}) = 1-\alpha/2 \tag{4.91}$$

The symmetry of the normal distribution results in the condition given by Eq. (4.56). Consequently, we also have

$$\Phi(-z_{\alpha/2}) = \alpha/2 \tag{4.92}$$

Thus, Eq. (4.90) is satisfied if we take

$$A = B = z_{\alpha/2}\sigma/\sqrt{N} \tag{4.93}$$

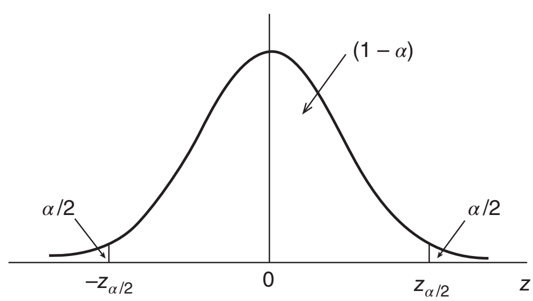


Figure 4.20 Standard normal distribution.

If we combine these conditions with Eqs. (4.84) and (4.85), and estimate σ from the sample variance given by Eq. (4.28), the 100(1 – α)% two-sided confidence interval for μ is given by

$$L_{\alpha/2,N} = \hat{\mu} - z_{\alpha/2}\frac{\hat{\sigma}}{\sqrt{N}} \tag{4.94}$$

and

$$U_{\alpha/2,N} = \hat{\mu} + z_{\alpha/2}\frac{\hat{\sigma}}{\sqrt{N}} \tag{4.95}$$

Some of the more commonly used confidence intervals are 80%, 90%, 95%, and 99%. These correspond to risks of $\alpha = 20\%$, 10%, 5%, and 1%, respectively. The corresponding values of $z_{\alpha/2}$ may be found from the CDF for the normal distribution tabulated in Appendix C. They are, respectively:

$$z_{0.1} = 1.28, \quad z_{0.05} = 1.648, \quad z_{0.025} = 1.96 \quad z_{0.005} = 2.58$$

Example 4.13 Find the 90% and the 95% confidence interval for the mean of the failures in Example 4.3.

Solution: The sample mean and variance obtained in Example 4.3 are $\hat{\mu} = 1303$ and $\hat{\sigma} = 661$. For two-sided 90% confidence, $Z_{\alpha/2} = 1.645$. Thus, $z_{\alpha/2}\hat{\sigma}/\sqrt{N} = 1.645 \times 661/4 = 271.8$, and thus, from Eqs. (4.94) and (4.95), $\hat{\mu} = 1303 \pm 271.8$ with 90% confidence. Likewise, for 95% confidence, $Z_{\alpha/2} = 1.960$ and $z_{\alpha/2}\hat{\sigma}/\sqrt{N} = 1.960 \times 661/4 = 323.9$.. Thus, $\hat{\mu} = 1303 \pm 323.9$ with 95% confidence.

To recapitulate, the interval estimate for the mean, μ, is nonparametric in that the distribution from which the sample of N derives need not be normal. The two-sided confidence limits can be used for any distribution so long as the variance exists, and N is sufficiently large, usually greater than $N = 30$. No distribution-free confidence intervals exist for the variance, skewness, or other properties.

4.7 Normal and Lognormal Parameters

Since the two parameters appearing in the normal distribution are just the mean and the standard deviation (i.e. the square root of the variance), the unbiased point estimators are given by Eqs. (4.25) and (4.27). For $N > 30$, the central limit theorem is applicable to the mean, and therefore, the confidence interval is given by Eqs. (4.94) and (4.95). The 100(1 − α)% two-sided confidence limits are thus

$$\mu^{\pm} = \hat{\mu} \pm z_{\alpha/2}\frac{\hat{\sigma}}{\sqrt{N}} \tag{4.96}$$

The confidence interval for the standard deviation for $N > 30$ may be estimated as

$$\sigma^{\pm} = \hat{\sigma} \pm z_{\alpha/2}\frac{\hat{\sigma}}{\sqrt{2(N-1)}} \tag{4.97}$$

Example 4.14 Find the point estimate and the 90% confidence interval for the mean and the standard deviation for the population of resistors coming from supplier 1 in Table 4.7.

Solution: Using MINITAB, we obtain:

Table 4.7 Resistor data.

48.47	48.84	49.29	49.39	49.52	49.75	49.96	50.44	50.77
48.49	49.14	49.30	49.43	49.54	49.78	50.03	50.57	50.87
48.66	49.27	49.32	49.49	49.69	49.93	50.06	50.70	51.87

Statistics:

	Total						
Variable	**Count**	**Mean**	**St. Dev**	**Variance**	**Minimum**	**Maximum**	**Range**
Resistor value	30	49.772	0.756	0.572	48.470	51.870	3.400

Since there are 30 data points, we may use the expressions for large sample size. For the mean, we use Eq. (4.96) to obtain

$$\hat{\mu} = 49.77 \pm 1.645 \times 0.756/\sqrt{30} = 49.77 \pm 0.227$$

For the standard deviation, we use Eq. (4.97) to obtain

$$\hat{\sigma} = 0.756 \pm 1.645 \times 0.756/\sqrt{2 \times 29} = 0.756 \pm 0.163$$

The CDF of a random variable y that is lognormally distributed is directly related to the standard normal distribution through the relationship $x = \ln(y)$ yielding the CDF

$$F(y) = \Phi\left[\frac{1}{\omega} \ln(y/y_0)\right] \tag{4.98}$$

Here, $\ln y_0$, the log mean, is estimated by

$$\ln \hat{y}_0 = \frac{1}{N}\sum_i \ln y_i \tag{4.99}$$

or solving for $\hat{y}_0$ and simplifying

$$\hat{y}_0 = \left(\prod_i y_i\right)^{1/N} \tag{4.100}$$

Likewise, we may write

$$\hat{\omega}^2 = \frac{N}{N-1}\left[\frac{1}{N}\sum_i (\ln\ y_i)^2 - \left(\frac{1}{N}\sum_t \ln\ y_i\right)^2\right] \tag{4.101}$$

The $100(1-\alpha)\%$ two-sided confidence limits are similarly obtained by transforming Eqs. (4.96) and (4.97)

$$y_0^{\pm} = \hat{y}_0 \exp\left(\pm z_{\alpha/2} \hat{\omega} N^{-1/2} \right) \tag{4.102}$$

and

$$\omega^{\pm} = \hat{\omega} \pm z_{\alpha/2} \frac{\hat{\omega}}{\sqrt{2(N-1)}} \tag{4.103}$$

Bibliography

Abernethy, R.B. (2006). *New Weibull Handbook*, 5e, 3–14.

Abernethy, R.B., Breneman, J.E., Medlin, C.H., and Reinman, G.L. (1983). *Weibull Analysis Handbook*. U.S. Air Force AFWAL-TR-83-2079.

AMMRCTR85-18 (1985). Reliability and Life Prediction Methodology – M60 Torsion Bars, AD-A159 197.

Ang, A.H.-S. and Tang, W.H. (1975). *Probability Concepts in Engineering Planning and Design*, vol. **1**. New York: Wiley.

Barlow, R. and Proschan, F. (1965). *Mathematical Theory of Reliability*. Wiley.

Barsoum, R.S. et al. (1985). *Reliability and Life Prediction Methodology – M60 Torsion Bars*. Massachusetts: Army Material and Mechanics Research Center.

Crowder, M.J., Kimber, A., Smith, T., and Sweeting, R. (1991). *Statistical Analysis of Reliability Data*. Chapman & Hall.

Green, A.E. and Bourne, A.J. (1972). *Reliability Technology*. NY: Wiley.

Haugen, E.B. (1980). *Probabilistic Mechanical Design*. New York: Wiley.

Ireson, W. (ed.) (1966). *Reliability Handbook*, 2–8. McGraw-Hill.

Kapur, K.C. and Lamberson, L.R. (1977). *Reliability in Engineering Design*. Wiley.

Lapin, L.L. (1984). *Probability and Statistics for Modern Engineering*. Belmont, CA: Brooks/Cole.

Montgomery, D.C. and Runger, G.C. (1994). *Applied Statistics and Probability for Engineers*. New York: Wiley.

Nelson, W. (1982). *Applied Life Data Analysis*. New York, NY: Wiley.

O'Connor, P.D.T. (2012). *Practical Reliability Engineering*, 5e. Wiley.

Olkin, I., Gleser, Z.J., and Derman, G. (1980). *Probability Models and Applications*. New York: Macmillan Co.

Pieruschka, E. (1964). *Principles of Reliability*. Englewood Cliffs, NJ: Prentice-Hall.

Vining, G. (1998). *Statistical Methods for Engineers*. Duxbury.

Walpole, R.E., Myers, R.L., Myers, S.H., and Ye, K. (2007). *Probability and Statistics for Engineers & Scientists*, 8e. Prentice-Hall.

Wikipedia, The Central Limit Theorem.

Exercises

4.1 For the PDF

$$f(x) = \begin{cases} bx(1-x), & 0 \le x \le 1, \\ 0, & \text{otherwise} \end{cases}$$

determine *b*, μ, and σ.

4.2 Consider the following PDF:

$$\begin{aligned} f(x) &= 1/2 \quad 0 < x < 2, \\ &= 0 \qquad \text{otherwise} \end{aligned}$$

Determine the mean and variance.

4.3 A motor is known to have an operating life (in hours) that fits the distribution

$$f(t) = \frac{a}{(t+b)^3}, \quad t \ge 0$$

The mean life of the motor has been estimated to be 3000 hours.

a) Find *a* and *b*.
b) What is the probability that the motor will fail in less than 2000 hours?
c) If the manufacturer wants no more than 5% of the motors returned for warranty service, how long should the warranty be?

4.4 For a random variable for which the PDF is

$$f(x) = \begin{Bmatrix} 0, & x < -1 \\ A, & -1 < x < 1 \\ 0, & x > 1 \end{Bmatrix}$$

determine (a) *A*, (b) μ, (c) σ^2, (d) sk, and (e) ku.

4.5 Suppose that

$$F(x) = 1 - e^{-0.2x} - 0.2xe^{-0.2x}, \quad 0 \le x \le \infty$$

a) Find *f*(*x*).
b) Determine μ and σ^2.
c) Find the expected value of e^{-x}.

4.6 Repeat Exercise 4.4 for $f(x) = A \exp(-|x|), -\infty \le x \le \infty$.

4.7 Suppose that the maximum flaw size in steel bars is given by

$$f(x) = 4xe^{-2x}, \quad 0 \le x \le \infty$$

where *x* is in microns.

a) What is the mean value of the maximum flaw size?

b) If flaws of lengths greater than 1.5 μm are detected and the bars rejected, what fraction of the bars will be accepted?
c) What is the mean value of the maximum flaw size for the bars that are accepted?

4.8 The following PDF has been proposed for the distribution of pit depths in a tailpipe of thickness x_0:

$$f(x) = A \sin h[\alpha(x_0 - x)], \quad 0 \le x \le x_0.$$

a) Determine A in terms of α.
b) Determine $F(x)$: the CDF.
c) Determine the mean pit depth. What is the probability that there will be a pit of more than twice the mean depth?

4.9 The PDF for the maximum depths of undetected cracks in steel piping is

$$f(x) = \frac{1}{\gamma}\frac{e^{-x/\gamma}}{(1 - e^{-\tau/\gamma})},$$

where τ is the pipe thickness, and $\gamma = 6.25$ mm.

a) What is the CDF?
b) For a 20-mm-thick pipe, what is the probability that a crack will penetrate more than half of the pipe thickness?

4.10 For a random variable for which the PDF is $f(x), -\infty \le x \le \infty$, find the following in terms of the moments $\overline{x^n} \equiv \int_{-\infty}^{+\infty} x^n f(x)\, dx$:
a) μ, (b) σ^2, (c) sk, and (d) ku.

4.11 Under design pressure, the minimum unflawed thickness of a pipe required to prevent failure is τ_0.

a) Using the maximum crack depth PDF from Exercise 4.9, show that if the probability of failure is to be less than ε, the total pipe thickness must be at least

$$\tau = \gamma \operatorname{In}\left[1 - \frac{1}{\varepsilon}\left(e^{\tau_0/\gamma} - 1\right)\right].$$

b) For γ = 6.25 mm and a minimum unflawed thickness of τ_0 = 4 cm, what must the total thickness be if the probability of failure is 0.1%?
c) Repeat part *b* for a probability of failure of 0.01%.
d) Show that for $\tau_0 \gg \gamma$ and $\varepsilon \ll 1$, τ is approximately $\tau_0 + \gamma$ In $(1/\varepsilon)$.

4.12 Suppose that

$$f_{\mathbf{x}}(x) = \left\{\begin{array}{ll} 0, & x < 0 \\ 1, & 0 < x < 1 \\ 0, & x > 1 \end{array}\right\}$$

a) If $y = x^2$, find $f_y(y)$. (b) If $z = 3x$, find $f_z(z)$.

4.13 Express the skewness in terms of the moments $E\{x^n\}$.

4.14 The beta distribution is defined by

$$f(x) = \frac{1}{B}x^{r-1}(1-x)^{t-r-1}, \quad 0 \le x \le 1.$$

show

a) that if t and r are integers,

$$B = \frac{(r-1)!(t-r-1)!}{(t-1)!},$$

b) that $\mu = r/t$,
c) that

$$\sigma^2 = \frac{\mu(1-\mu)}{t+1} = \frac{r(t-r)}{t^2(t+1)}$$

d) that if t and $r$are integers, $f(x)$ may be written in terms of the binomial distribution:

$$f(x) = (t-1)\, C_{r-1}^{t-2} x^{r-1}(1-x)^{t-r-1}$$

4.15 Transform the beta distribution given in the Exercise 4.14 by

$$y = a + (b-a)\,x, \quad a \le y \le b$$

a) Find $f_y(y)$ and (b) Find μ_y.

4.16 A PDF of impact velocities is given by $\propto e^{-\propto v}$. Find the PDF for impact kinetic energies E, where $E = \frac{1}{2}mv^2$.

4.17 The tensile strength of a group of shock absorbers is normally distributed with a mean value of 1000 lb. and a standard deviation of 40 lb. The shock absorbers are proof tested at 950 lb.

a) What fraction will survive the proof test?
b) If it is decided to increase the strength of the shock absorbers (i.e. to increase the mean strength while leaving the standard deviation unchanged) so that 99% pass the test, what must the new value of the mean strength be?
c) If it is decided to improve quality control (i.e. to decrease the variance while leaving the mean strength unchanged) so that 99% pass the test, what must the new value of the standard deviation be?

4.18 An elastic bar is subjected to a force l. The resulting strain energy is given by

$$\varepsilon = cl^2$$

where c is $d/2AE$, with d the length of the bar, A the area, and E the modulus of elasticity. Suppose that the PDF of the force can be represented by standardized normal form $f_l(l)$. Find the PDF $f(\varepsilon)$ for the strain energy.

4.19 The life of a tool bit is normally distributed with
mean: $\bar{t}$ = 10 hours variance: σ^2 = 4 housr^2.
What is the L_{10} of the tool?
(L_{10} = time at which 10% of the tools have failed.)

4.20 Suppose that

$$f_{\mathbf{x}}(x) = \begin{Bmatrix} 0, & x < 1 \\ 1, & 1 < x < 2 \\ 0, & x > 2 \end{Bmatrix}$$

a) if $y = \ln(x)$, find the PDF for y. (b) if $z = \exp(x)$, find the PDF for z.

4.21 The total load on a building may often be represented as the sum of three contributions: the dead load **d,** from the weight of the structure; the live load **1,** from human beings, furniture, and other movable weights; and the wind load **w.** Suppose that the loads from each of the sources on a support column are represented as normal distributions with the following properties:

$$\begin{aligned} \mu_d &= 6.0\,\text{kips} & \sigma_d &= 0.4\,\text{kips} \\ \mu_1 &= 9.2\,\text{kips} & \sigma_1 &= 1.2\,\text{kips} \\ \mu_w &= 4.6\,\text{kips} & \sigma_w &= 1.1\,\text{kips} \end{aligned}$$

Determine the mean and standard deviation of the total load.

4.22 If the strength of a structural member is known with 90% confidence to a factor of 3, to what factor is it known with (a) 99% confidence? (b) with 50% confidence? Assume a lognormal distribution.

4.23 Verify Eqs. (4.70) through (4.71).

4.24 The time to fly via a commercial airliner from one airport to another, say from Charlotte, North Carolina, to Burlington, Vermont, is uniformly distributed. This time may range from 120 minutes to 160 minutes. What is the probability of being on time, i.e. 140 minutes or sooner?

4.25 Consider the following response time data measured in seconds:

1.48	1.46	1.49	1.42	1.35
1.34	1.42	1.70	1.56	1.58
1.59	1.59	1.61	1.25	1.31
1.66	1.58	1.43	1.80	1.32
1.55	1.60	1.29	1.51	1.48
1.61	1.67	1.36	1.50	1.47
1.52	1.37	1.66	1.44	1.29
1.80	1.55	1.46	1.62	1.48
1.64	1.55	1.65	1.54	1.53
1.46	1.57	1.65	1.59	1.47
1.38	1.66	1.59	1.46	1.61
1.56	1.38	1.57	1.48	1.39

1.62	1.49	1.26	1.53	1.43
1.30	1.58	1.43	1.33	1.39
1.56	1.48	1.53	1.59	1.40
1.27	1.30	1.72	1.48	1.66
1.37	1.68	1.77	1.62	1.33

Source: Data from Green and Bourne (1972).

Make a normal probability plot of the data. What is the mean and standard deviation? Does the data seem to follow a normal distribution? Why?

4.26 Fifty measurements of the ultimate tensile strength of wire are given in the accompanying table.

a) Using MINITAB plot the data on a normal probability plot.
b) Repeat (a) as a three-parameter lognormal plot
c) Which seems better? Why? Engineering reasons make you change your mind?

Ultimate tensile strength			
103,779	102,325	102,325	103,799
102,906	101,651	105,377	100,145
104,796	105,087	104,796	103,799
103,197	106,395	106,831	103,488
100,872	100,872	105,087	102,906
97,383	104,360	103,633	101,017
101,162	101,453	107,848	104,651
98,110	103,779	99,563	103,197
104,651	101,162	105,813	105,337
102,906	102,470	108,430	101,744
103,633	105,232	106,540	106,104
102,616	106,831	101,744	100,726
103,924		101598	

Source: Data from Haugen (1980).

4.27 The following are 16 measurements of circuit delay times in microseconds: 2.1, 0.8, 2.8, 2.5, 3.1, 2.7, 4.5, 5.0, 4.2, 2.6, 4.8, 1.6, 3.5, 1.9, 4.6, and 2.1.
Make a normal probability plot of the data. What is mean and standard deviation and correlation coefficient?

4.28 The following failure times (in days) have been recorded in a proof test of 20 units of a new product: 2.6, 3.2, 3.4, 3.9, 5.6, 7.1, 8.4, 8.8, 8.9, 9.5, 9.8, 11.3, 11.8, 11.9, 12.3, 12.7, 16.0, 21.9, 22.4, and 24.2.

a) Make a lognormal plot
b) Calculate the sample mean, variance, skewness, and kurtosis for the proof test data

4.29 The times to failure in hours on four compressors are 240, 420, 630, and 1080.

a) Make a lognormal probability plot.
b) Estimate the median time to failure.

4.30 Use Eqs. (4.94) and (4.95) to estimate the 90% and the 95% confidence intervals for the mean and for the variance obtained in Exercise 4.27.

4.31 The following times to failure (in days) result from a fatigue test of 10 flanges: 1.66, 83.36, 25.76, 24.36, 334.68, 29.62, 296.82, 13.92, 107.04, and 6.26.

a) Make a lognormal probability plot.

Estimate the factor to which the time to failure is known with 90% confidence.

5

Continuous Distributions – Part 2 Weibull and Extreme Value Distributions

The "One Horse Shay"
Now in building of chaises, I tell you what,
There is always *somewhere* a weakest spot, —
In hub, tire, felloe, in spring or thill,
In panel, or crossbar, or floor, or sill,
In screw, bolt, thoroughbrace, — lurking still,
Find it somewhere you must and will, —
Above or below, or within or without, —
And that's the reason, beyond a doubt,
A chaise *breaks down*, but doesn't *wear out*.
Source: Oliver Wendell Holmes, Sr, The Deacon's Masterpiece, 1858. Public Domain.

5.1 Introduction

The Weibull distribution is used in reliability analysis and reliability engineering to describe failure modes of "parts." These parts can be systems, subsystems, modules, down to the piece part level. While the Weibull distribution is not the only failure distribution available, it has proven to be the most useful in approximately 95% of the failure studies. Other extreme value distributions will be discussed later in this chapter for the particular instances where they represent the "physics of failure" better than the Weibull.

The "Weakest Link" Theory from a Physics-of-Failure Point of View

The "weakest link" theory was originally developed by Waloddi Weibull to describe the tensile fracture of brittle materials. Specifically, due to the randomly distributed material defects (nonhomogeneities, inclusions, precipitates, and greater than-grain-size voids) in a material per volume unit, the theory states that fatigue crack initiates where the most dangerous defect or the weakest link exists (Weibull 1951). Therefore, a statistical distribution of defects within specimens/components leads to scatter in the fatigue behavior of the material. When those defects become the fracture origin, the fatigue failure is triggered by the largest defect. Other necessary assumptions are: (i) the largest flaw or the weakest link of material provides the crack initiation site, (ii) the size of defects is small compared with the distance between them (no interaction), and (iii) failure is defined as the first failure of any element, i.e. a series system (Wormsen and Härkegård 2004; Zhu et al. 2017).

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

Waloddi Weibull was a Swedish engineer and scientist who delivered his hallmark paper on this subject in 1951 (Weibull 1951). He claimed that his distribution, or more specifically his family of distributions, applied to a wide range of problems. He illustrated this point with seven examples ranging from the yield strength of steel to the size of adult males born in the British Isles. He claimed that the (Weibull) function " ... may sometimes render good service." He did not claim that it *always* worked or even that it was always the best choice (Weibull 1951).

A few real examples that Weibull analysis can help you solve:

1) A project engineer reports three failures of a component in service during a three-month period. The Program Manager asks, "How many failures will we have in the next quarter, six months, and year?" What will it cost? What is the best corrective action to reduce the risk and losses?
2) To order spare parts and schedule maintenance labor, how many units will be returned to depot for overhaul for each failure mode month by month next year? The program manager wants to be 95% confident that he will have enough spare parts and labor available to support the overall program.
3) A state Air Resources Board requires an automobile fleet recall when any part in the emissions system exceeds a 4% failure rate during the warranty period. Based on the warranty data, which parts will exceed the 4% rate and on what date?
4) After an engineering change, how many units must be tested for how long, without any failures, to verify that the old failure mode is eliminated or significantly improved with 90% confidence?
5) An electric utility is plagued with outages from superheater tube failures. Based on the inspection data forecast, the life of the boiler is based on plugging failed tubes. The boiler is replaced when 10% of the tubes have been plugged due to failure. The cost of an unplanned failure for a component, subject to a wear-out failure mode, is 20 times the cost of a planned replacement. What is the optimal replacement interval?

Uses of Weibull and Extreme Value Distributions

- Weibull analysis provides a simple graphical solution (a “plot”). The process consists of plotting a curve and analyzing it (Figure 5.1). Figure 5.1 illustrates a Weibull plot generated by MINITAB®. Here, we will be using MINITAB for our probability plotting and reliability analysis and graphics. Other software packages also can generate a Weibull plot (Reliasoft's Weibull++, Supersmith(R) and JMP™, to name a few). In most Weibull plots, the horizontal scale is some measure of life, perhaps start/stop cycles, operating time, or cycles. The vertical scale is the probability of occurrence of the event (often represented as percent failed). In the case of the **Weibull**, the **slope** of the line (**called the Greek letter β**) is significant and may provide a clue to the physics of the failure in question.

  Much more to follow in Section 5.1 on how to generate and interpret a Weibull plot.

- Weibull analysis may be used even with inadequacies in the data, as will be indicated later in the section. For example, the technique works with small samples. Methods will be described for identifying mixtures of failures, classes or modes, problems with the origin being at other than zero time, investigations of alternative scales other than time, nonserialized parts and components where the time on the part cannot be clearly identified, and even the construction of a Weibull curve when there are no failures at all, only success data!
- In addition, when the failure data differs markedly from a straight line fit on a Weibull plot, it is not difficult to make graphic comparisons with other distributions (e.g. lognormal and other extreme value distributions) to determine which distribution best fits the data. Of course, if there is engineering evidence supporting another distribution, this should be considered as well.

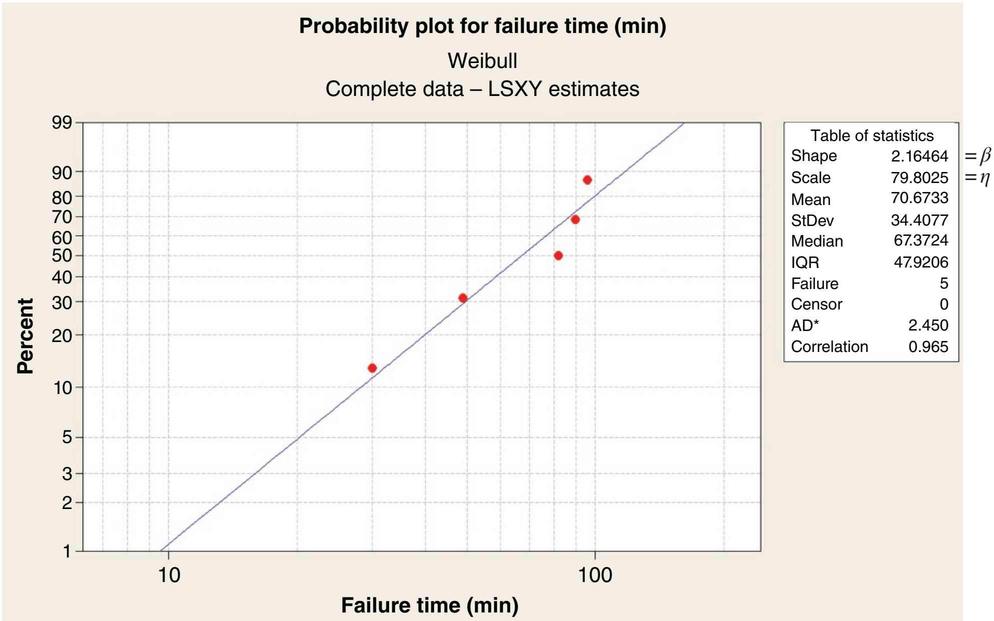


Figure 5.1 Typical Weibull plot.

Other Considerations

Age Parameters and Sample Sizes

Most applications of Weibull analysis are based on a single failure class or mode from a single part or component. An ideal application would consist of a sample of 20–30 failures. Except for material characterization laboratory tests, ideal data are rare; usually, the analysis is started with a few failures embedded in a large number of successful, also called "unfailed" or "censored" or "suspended" units.

The age of each part is usually required. The units of age depend on the part usage and the failure mode. For example, low and high cycle fatigue may produce cracks leading to rupture. The age units would be fatigue cycles. The age unit of an auto engine starter may be the number of engine starts. Jet engine turbine parts may fail as a function of the number of excursions from low temperature to high temperature and back to low temperature.

In most cases, the knowledge of the "*Physics-of-Failure*"[1] will provide the age scale. When the units of age are unknown, several age scales must be tried to determine the best fit.

Predeclared sample sizes at a (say) 90% confidence level can be calculated in the design phase of a product in order to better detect failure modes at the part, then module, subsystem before the system is tested. These predeclared test calculations use information on the historical failure modes that need to be designed out, in conjunction with the life of a system, or the time between a scheduled maintenance event.

1 *Physics of failure* tries to understand how physical, chemical, mechanical, thermal, or electrical stresses can degrade or cause the failure of an item.

Engineering Changes, Maintenance Plan Evaluation, and Risk Prediction

Weibull analysis is used to evaluate engineering changes as to their effect on the entire fleet of a product, modules, control systems, engines, and other systems.

Risk predictions and maintenance schedules and plans are also evaluated using Weibull analysis. In each case the baseline Weibull analysis and risk analysis are conducted without the engineering change or maintenance change or what is sometimes referred to as "no fixes assumed" risk. The study is then repeated with the estimated effect of the change in risk with the engineering change or maintenance change.

This can be done by modifying the Weibull distribution of the failure mode or modes. However, most problems and interactions of maintenance or engineering change go beyond the Weibull plot alone and involve integrating the Weibull distribution(s) into a Monte Carlo simulation (or other stochastic model) of the process. Thus, the difference between the before and after gives the effect of the changes that are being proposed to reduce risk or maintenance.

The risk parameters may be the predicted number of reliability failures, safety incidents, life cycle cost, depot loading, spare parts usage, hazard rate, or aircraft availability.

Weibulls with Cusps or Curves

After a Weibull plot is generated, it should be inspected to see (visually) how well the failure data fit the straight line. The scatter should be evenly distributed about the line. You will find and learn through examples that many "Goodness-of-Fit" (GOF) tests for the Weibull fit fail the "fat pencil test" where a fat pencil can be placed on a Weibull line and the eyeball can visually check that a fit is good or not, often disagreeing with the GOF test!!

However, sometimes, the failure points will not fall on a straight line *on* the Weibull plot, and modification of the initial Weibull plot will be required. The bad fit may relate to the physics of the failure or to the quality of the data.

There are at least two reasons why a bad fit may occur. The first (and easiest thing to check) is to see if the points fall on a gentle curve. It may be that the origin of the age scale is not located at zero, as required by Weibull analysis (see Figure 5.2). There may be physical reasons why this will be true.

For example, the first nearly 25 hours of operation of a system may be to check out all subsystems and controls at a lower temperature or pressure. When the product is delivered to the field the

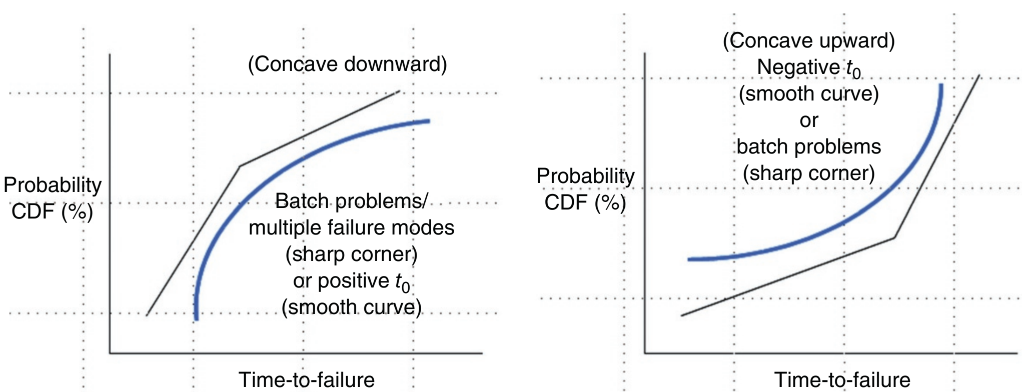


Figure 5.2 Weibull plot needing a third parameter (the location parameter) or investigating two or more failure modes.

customer treats the product as if it started at "0" time and uses it without restriction. That means the first ~25 hours were run more "gently" than the customer would be running the product in the field. So later, when field failures occur, a Weibull like that in Figure 5.2 will appear concave downward. The nearly 25-hour origin correction can then be calculated.

However, the origin correction may be either positive or negative (i.e. the curved Weibull could also be concave upward. A concave upward indicates that part life was "used up" before it was installed. A classical example of using up life before a part is installed is bearing corrosion; when a bearing is not properly desiccated in storage. A procedure for determining the origin correction will be illustrated in the section titled Shifting Weibull Procedure "Weibull Plots and Their Estimates of β and η."

Second, a mixture of failure modes – sometimes the plot of the failure points – will show cusps in sharp corners (sometimes referred to as a "dogleg bend"). This is an indication that there is more than one failure mode represented in the data (see Figure 5.3).

In this case it is necessary to conduct a laboratory failure analysis of each failure to determine if separate failure modes are present. If this is found to be the case, then separate Weibull plots are made for each set of data for each failure mode. If the laboratory analysis successfully categorizes the failures into separate "failure modes," the separate Weibull plots should show good fits. On each plot, the failure data points from the other failure mode(s) are treated as successful (also called "censored" or nonfailed) units.

System Weibulls

A Weibull plot is used for data from a SINGLE failure mode. As noted above, you can detect two or more failure modes often just by looking at the curves and bends of the plot. However, the analyst should always wind up with a Weibull plot of each individual failure mode. If you plotted all failures of a system, you would (probably) disguise batch problems and you would have no information on the individual failure modes. You need individual failure mode Weibulls when predicting (and ranking) the failure modes to be worked on first, second, etc.

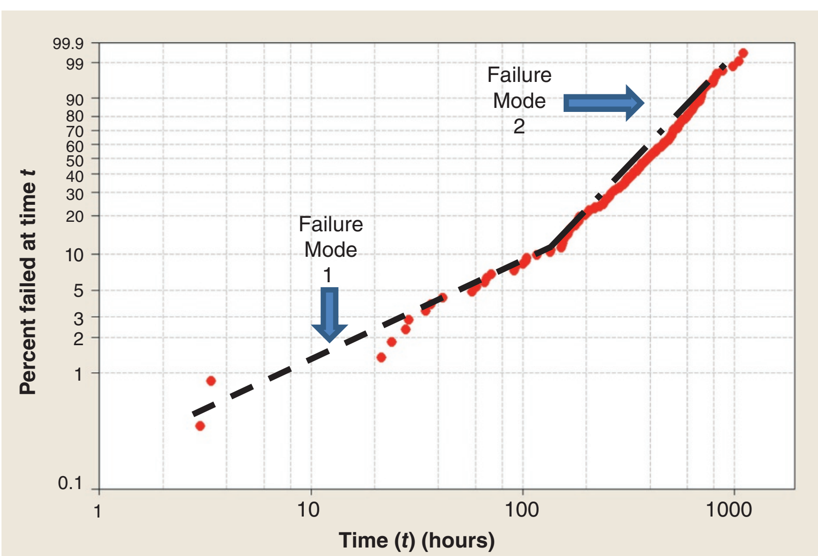


Figure 5.3 Mixture of failure modes.

No Failure Weibulls

Often, warranty data or field inspection will point to a part that "almost" failed. We will discuss the approach to this analysis in the section titled "Weibayes Analysis."

Small Sample Weibulls

No one wants a lot of failures, especially if a failure could become a safety incident. So, often you may have 1, 2, or 3 failures and have to do the analysis with those failures and the remaining population of unfailed units. As you can imagine from elementary statistics, the confidence bounds on the Weibull parameters β and η are very wide with so few failure points. The best advice here is to use the Weibull generated with the small number of failures and generate the reliability/safety analysis to predict the *expected* future incidents. You will find that the Weibull analysis technique is robust to small samples of failures. More about this when we go over risk analysis.

Summary

- Weibull analysis refers to the process of fitting a Weibull distribution to a set of (usually) time-oriented data and much like a normal (bell-shaped) fit to manufacturing thicknesses with a mean and standard deviation. A Weibull fit to time-oriented failure data has a slope (β) and scale parameter (η) that describes the time-to-failure distribution of the part in question.
- This fitted Weibull distribution can be used to answer RELIABILITY questions:
  - If the data is from one population of failures:
    - What is the 1/1000 probability of failure?
    - How many of the population will fail by time (t) in the future?
    - How many items and how long do I have to test each item to assure a level of reliability in a new design?
  - If the data is from two suppliers of fatigue sample populations:
    Are the supplier's distributions of part fatigue significantly different? Does the extrapolation to (say) 1/100 probability meet the requirement?
- As in the normal distribution case, the engineer can *extrapolate* the fitted line to make predictions outside the bounds of the data.

5.2 Statistics of the Weibull Distribution

The Weibull distribution is widely employed for reliability-related problems. The Weibull distribution's relationship to extreme value distributions is analogous to that between the lognormal and the normal distribution. The Weibull distribution, like the log normal, ranges $0 < x < \infty$, while extreme value distributions, like the normal distribution, have the range $-\infty < x < \infty$. Moreover, the distributions are related through a logarithmic transformation. We now concentrate on the Weibull distribution and then discuss the extreme value distributions in Section 5.3.

Weibull "Mathematics"

The usefulness of the Weibull distribution was described in Section 5.1. Now we answer the question of what does the Weibull statistical distribution look like mathematically that will allow us to utilize it in solving problems.

Fundamentally, the Weibull distribution depends on the "weakest link" theory. The analogy to a chain is often used to explain the weakest link theory. That is, every system, subsystem, and module has a part that will be first to fail during its lifetime (if the system is not retired first).

For example:

1) A V-8 automobile engine with eight pistons when run long enough will often see the failure of one piston or one spark plug, or one valve, ... that part will be the "weakest" piston, or spark plug or valve,... in the engine. The environment the engine was used in, in terms of stresses, is assumed to be approximately equal for each of the pistons, spark plugs, and valves; so, that first failure is the "weakest link" in the "CHAIN" that is the family of 8 pistons or 16 (or more) valves, or 8 spark plugs. The Weibull distribution will model all of these mechanical failures individually.
2) Suppose that you have a turbine disk in a modern commercial jet engine consisting of 68 blades. The disk is turning at 4,000–12,000 rpm during operation. All 68 blades are subjected to heat, pressure, and possibly foreign objects in the airstream. One of these blades (under normal operating conditions) will be the first blade to fail (unless the blades are removed at a predetermined time to prevent the first failure (and any others).

   Given that you may have 100s (or 1000s) of engines with these blades, you can model the failure distribution of each failure mode of the turbine blades with the Weibull distribution. Then, do a "risk analysis" to project how many future failures you could expect. Here, "risk analysis" simply means a prediction of how many future failures will occur due to the same failure mode that has been observed.
3) A human being has many body parts, much like a mechanical system. Depending on the stresses and strengths in the human system, one part of the system will be the first to "fail." Now, to extend this, if a new drug is being developed and given to (say) 20 patients in the first drug trial where each patient is very close to the same stage of the disease, the "weakest link" also applies, and often, the Weibull distribution can be used.

The Weibull two-parameter CDF (cumulative distribution function):

$$F(t) = \text{Prob}[\text{life} \leq t] = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{5.1}$$

where t is the cumulative time to failure, β is the slope of the Weibull distribution, η is the characteristic life (the time at which 63.2% of the population is predicted to fail), and e is the Naperian logarithmic base. The CDF, denoted $F(t)$, "sums up" or integrates the probabilities of all values less than t. And using the calculus, you can derive the PDF of the Weibull by *differentiating* the Weibull CDF with respect to t to obtain:

The Weibull PDF (probability density function):

$$f(t) = \left(\frac{\beta}{\eta}\right)\left(\frac{t}{\eta}\right)^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{5.2}$$

The Weibull PDF describes the shape of the distribution with "*slope*" β and "*characteristic life*" η.

Thinking of it in reverse, the PDF, denoted $f(t)$, is the mathematical function that is *integrated* in order to calculate the CDF probabilities. The PDF is referred to as the "density" function because it tells the user how "dense" the data is at any point t (frequency of occurrence per unit of t). See Figures 5.4 and 5.5.

The relationship between PDF and CDF is illustrated in Figure 5.6.

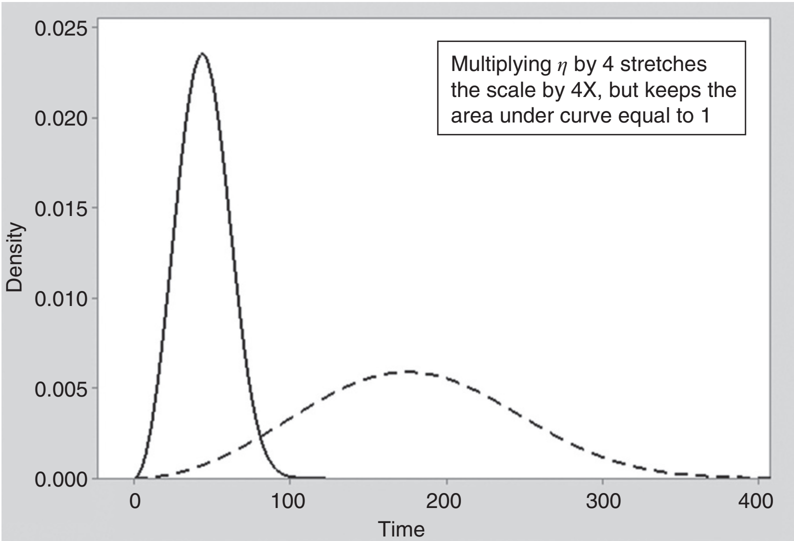


Figure 5.4 η scales the PDF.

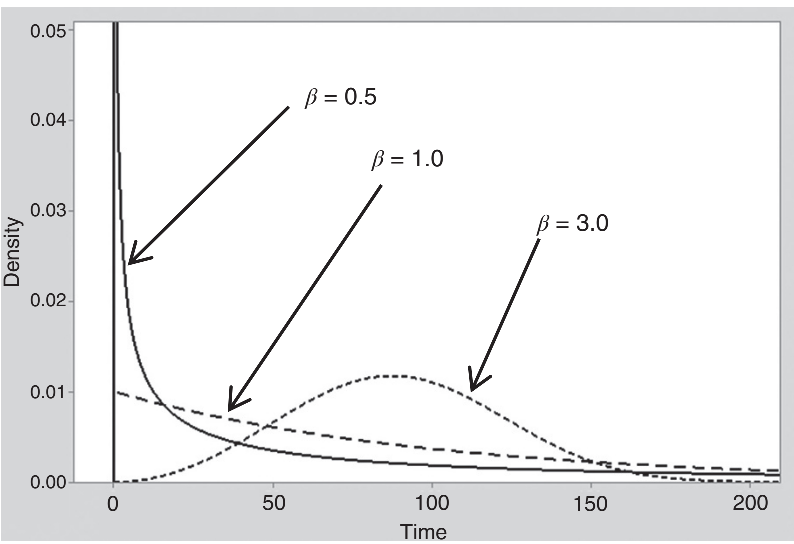


Figure 5.5 β determines the PDF shape.

The mean and the variance of the distribution are obtained from Eqs. (4.15) and (4.16), respectively. They are rather the complicated functions of the scale and shape parameters:

$$\mu = \eta\,\Gamma(1 + 1/\beta) \tag{5.3}$$

and

$$\sigma^2 = \eta^2\left[\Gamma(1 + 2/\beta) - \Gamma^2(1 + 1/\beta)\right] \tag{5.4}$$

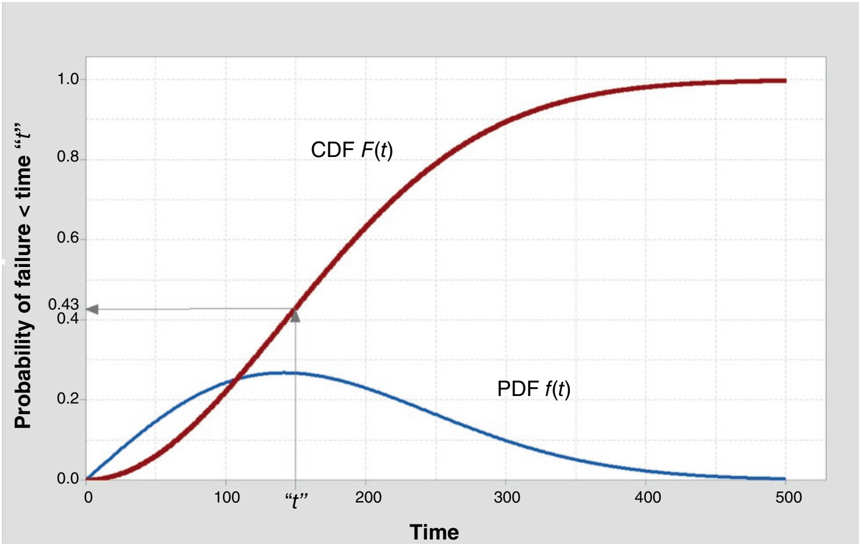


Figure 5.6 The relationship between the Weibull PDF and CDF.

In these expressions, the complete gamma function $\Gamma(\nu)$ defined by the integral

$$\Gamma(\nu) = \int_0^{\infty} \zeta^{\nu-1} e^{-\zeta} d\zeta \tag{5.5}$$

is used. Figure 5.7 shows the dependence of $1/\Gamma(\nu)$ for the values $0 < \nu < 1$, and when $\nu > 1$, can be obtained from the identity:

$$\Gamma(\nu) = (\nu - 1)\,\Gamma(\nu - 1) \tag{5.6}$$

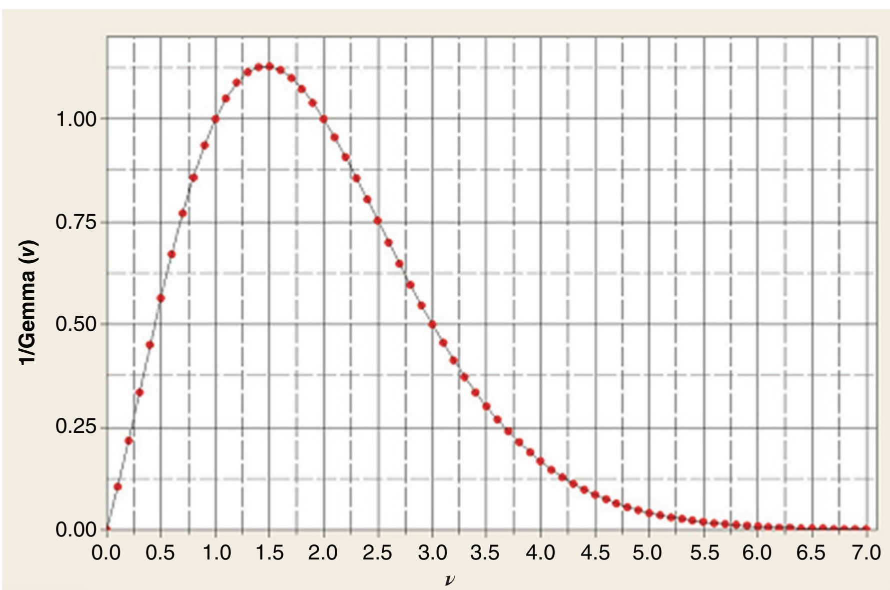


Figure 5.7 The gamma function.

For nonrepairable populations, the failure rate is defined as the (instantaneous) rate of failure for the survivors to time t during the next instant of time.

The Hazard rate is given by

$$h(t) = \frac{f(t)}{1 - F(t)} \tag{5.7}$$

For the Weibull distribution, this becomes

$$h(t) = \frac{f(t)}{1 - F(t)} = \frac{\frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta - 1} 1 - \mathrm{e}^{\left(-\left(\frac{\eta}{\eta}\right)^{\beta}\right)}}{1 - \left(1 - \mathrm{e}^{\left(-\left(\frac{\eta}{\eta}\right)^{\beta}\right)}\right)} = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta - 1} \tag{5.8}$$

η is defined as the age by which 63.2% of the units will fail.

This is true of all Weibulls since:

$$F(\eta) = 1 - \mathrm{e}^{\left(-\left(\frac{\eta}{\eta}\right)^{\beta}\right)} = 1 - \mathrm{e}^{\left(-(1)^{\beta}\right)} = 1 - \frac{1}{e} \cong 0.632 \tag{5.9}$$

For the details of how the Weibull distribution as a "weakest link" phenomena can be derived, see Supplement 1 – "Weibull derived from weakest link theory".

A special case of the Weibull distribution was introduced in Chapter 3, the "Exponential Distribution." Letting $\beta = 1$ in the Weibull PDF and CDF results in the single-parameter "*exponential distribution*":

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)} \tag{5.10}$$

and the PDF:

$$f(t) = \frac{1}{\eta} e^{-\left(\frac{t}{\eta}\right)} \tag{5.11}$$

Examples of the Weibull "family" where a Weibull distribution with different slopes can look like:

- $\beta = 1.0$: identical to the exponential distribution
- $\beta = 2.0$: often referred to as the Rayleigh distribution
- $\beta = 2.5$: approximates the lognormal distribution
- $\beta = 3.4$–3.6: approximates the normal distribution
- $\beta = 5.0$: approximates the peaked normal distribution.

The Weibull Probability Plot

The first use of the Weibull plot will be to determine the parameter (β), which is known as the slope or shape parameter. What is so important about knowing β? Knowing the β will tell you not only where you are on the "Bathtub" curve but also some information on possible failure mode as shown in Figure 5.8. This information can often be used in conjunction with the previous experience with failure modes of this type on previous models or products to help confirm the failure mode type.

The Weibull plot is also used to determine the onset of the failure. For example, it may be of interest to determine the time at which 1% (or probability 1/100) of the population will have failed.

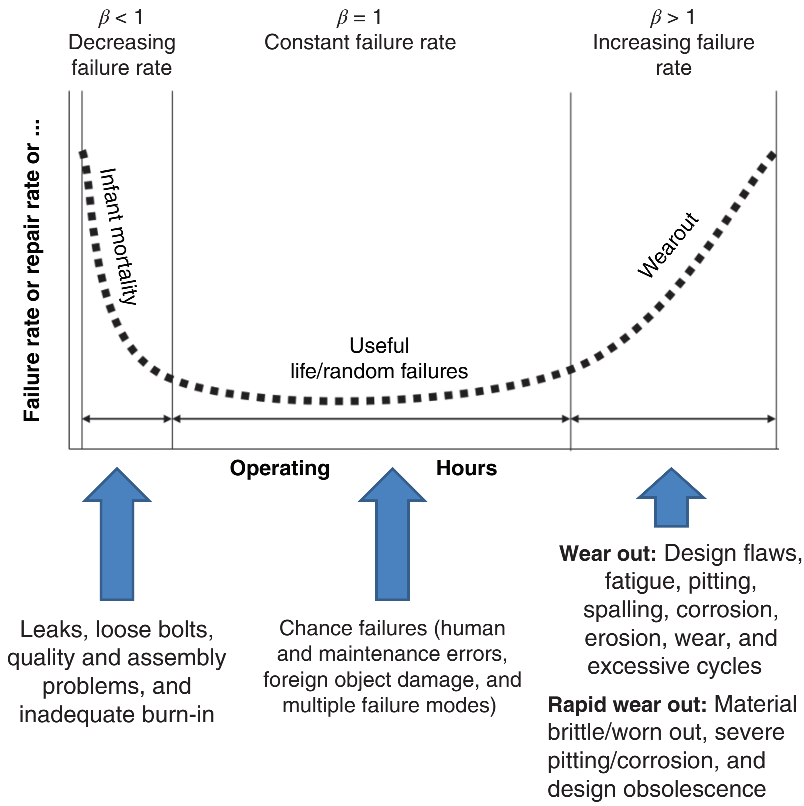


Figure 5.8 The bathtub curve and further interpretation of results of the analysis.

This is called the Bl life. Alternatively, it may be of interest in determining the time at which one-tenth of 1% (or probability 1/1000) of the population will have failed, which is called B.l life. These values can be read from the Weibull plot by inspection. Note: It is thought that "B" lives nomenclature had its origin in the bearing industry where the design point for a bearing started out at 10% (or B10 life).

We begin our statistical assessment by finding values of β and η that best fit our data. These are estimates of the population values of β and η. We use two methods:

1) Rank regression – uses linear regression of x on y
2) Maximum likelihood – purely mathematical (details to follow).

First, the "Weibull plot method" (rank regression) using Weibull paper to estimate β and η, where software programs use regression analysis (line fitting) to calculate the Weibull parameters β and η.

What makes the Weibull plot method work is a bit of algebraic manipulation of the Weibull CDF:

Starting with the CDF

$$F(t) = 1 - e^{-(t/\eta)^{\beta}} \tag{5.12}$$

$$1 - F(t) = e^{-(t/\eta)^{\beta}} \tag{5.13}$$

$$\ln(1 - F(t)) = -(t/\eta)^{\beta} \tag{5.14}$$

$$\ln\left(\frac{1}{1-F(t)}\right) = (t/\eta)^{\beta} \tag{5.15}$$

$$\underbrace{\ln\ \ln\left(\frac{1}{1-F(t)}\right)}_{Y} = \underbrace{\beta \ln t}_{mx} \underbrace{- \beta \ln \eta}_{+b} \tag{5.16}$$

That is, if the cumulative probability $F(t)$ is converted to "Y," and failure times are converted as "X," then β is the slope of the Weibull line, and once you know β, it is straightforward to solve for η, since the intercept ("b" above) = $-\beta$ ln η.

So, the Y-axis of the Weibull is a "double natural log" scale in probability, and the x-axis is a natural log scale in the time parameter.

A typical Weibull plot is illustrated in Figure 5.9. This plot is generated using **MINITAB**; however, the definitions apply to all Weibull plots with the same information.

Probability Plotting Points – Median Ranks

Failure probability is calculated by its rank, i.e. its place in the ascending order of the data. If 10 data points were available and sorted in ascending order, the rank of the first data would be 1 and that of the tenth data would be 10, given no "nonfailed"/suspended/censored datapoints. The y plotting positions for the Weibull distribution are based on the median ranks (MRs) of each of the (ordered) failure points.

MRs may be obtained by

$$\sum_{k=1}^{N} C_k^N (MR)^k (1-MR)^{N-k} = 0.5$$

and can be approximated using EXCEL by the Excel function "BETAINV(0.5,i,n-i+1)" as well as using the F distribution as discussed in Chapter 2 under "Binomial Confidence Bounds."

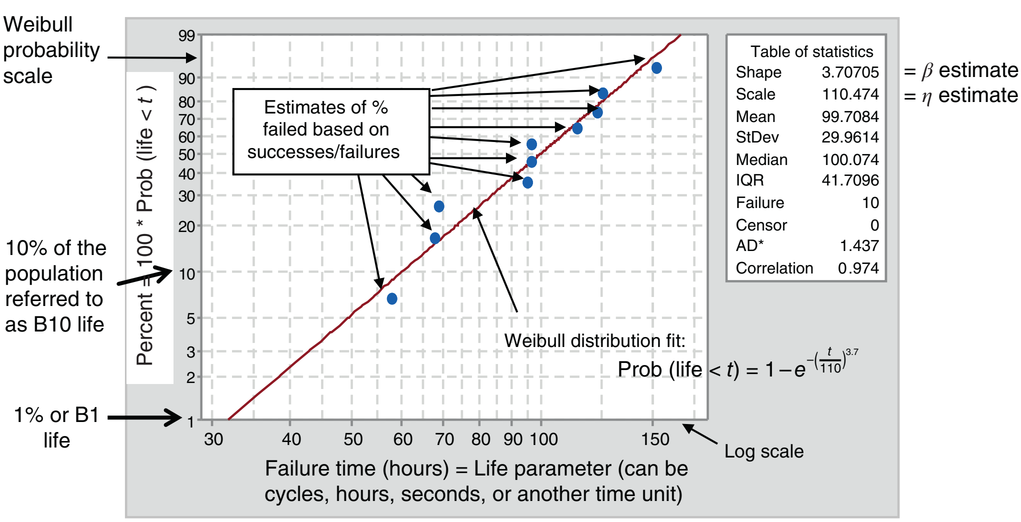


Figure 5.9 Typical Weibull plot with definitions of items on the plot.

However, the MR estimation formula due to Bernard is used by most statistical programs when plotting the Weibull distribution. Bernard MR formula:

$$F(t) = \frac{i - 0.3}{n + 0.4}$$

See Appendix D ("Rank Statistics") for a discussion of Mean Ranks and other MR formulae, with examples.

The "ranked regression" (or sometimes referred to as "LSXY" for least squares X on Y) estimation and subsequent probability plot will use MRs estimated by Bernard's formula and will be illustrated in the following sections.

NOTE: The Weibull probability scale is defined so that if data are from a Weibull distribution, they will follow an approximate straight line. Note that **only made-up** data will all lie **exactly** on the line; hence, this plot also illustrates the look of a "typical" Weibull plot. Variation about the fitted line is due to the effects of stress (temperature, pressure, part interaction, etc.) and material strength on the part, human, or process failure mode.

We can now say that the $\beta = 3.7$ in Figure 5.9 indicates a wear-out mode, and since we do not see any concave upward or downward in the plot as a whole, with the data scattered uniformly around the line, we have a reasonable Weibull estimate based on the 10 failures. Since this type of wear out is <4, in conversations with whoever may have provided the data could include a discussion of fatigue, pitting, spalling, corrosion, erosion, and normal wear excessive (thermal or pressure) cycles.

How to Do a "Weibull Analysis"

A Weibull analysis is to be used for the analysis of ONE failure mode. However, very often, the first failures that occur have not been segregated into failure modes, and you will see the data on a Weibull plot as a curved line or "dogleg bend" as mentioned in the Weibull introduction.

You may receive the failure data from a variety of sources:

- Laboratory failures
- Nonlaboratory failure such as failure of a product during design testing
- Field failure (warranty or product support engineering)
- You may have been investigating a failure mode or two and have discovered failure data from historical files of one sort or another.

So, when fitting a Weibull distribution to data, often you have incomplete data (particularly if it is warranty data or a field safety problem); therefore, you are only finding *estimates* of β and η. You may have most of the failure points, but not all; you may have most of the unfailed points, but not all. Therefore, your Weibull plot is an estimate of the failure mode based on a SAMPLE.

So, you are ready to fit a Weibull in order to make inferences about the population, including

- Parameter estimates
- Predictions of future events
- Decisions (maintenance plans and retrofits).

Failure time data, or life data, present unique challenges not encountered with dimensional data. Nonfailed units or units that fail by a different failure mode are "censored" or "suspended" units. These data cannot be ignored even though the suspensions are never plotted. Times on suspended units **must** be included in the analysis.

In short, *ALWAYS* include your suspended or unfailed data. If you use failure-only data, your Weibull will give risk values that are unrealistically high. If you want the most accurate answer, use ALL your data… *failure times AND unfailed times*!

How failure data is plotted (with and without unfailed units) in the case of ranked regression (LSXY) to produce a "Weibull plot" as described in Appendix D – Nonparametric Methods and Probability Plotting. Computer software (MINITAB, JMP, Weibull^{++}, etc.) uses the same approach for producing a Weibull plot (or any other probability plot for that matter).

Example 5.1 Weibull Analysis of Inlet Airseal Rivets

Let us start with a lab data example that includes suspensions – inlet airseal rivets tested to failure in order to replicate the field failures (Abernethy et al. 1983).

You have eight datapoints, but only five of these have failed (i.e. three suspensions or unfailed points):

- Failures at 30, 49, 82, 90, and 96 seconds.
- Unfailed units at 10 seconds (due to fixture failure), 45 seconds (failed due to a different failure mode), and 100 seconds (test terminated without failure).

As an illustration of what would happen if we did not use all the data, suppose that we only used the five failures, and ignored the three suspensions/unfailed units?

Figure 5.10b shows both the Weibull plots, the one we illustrated in Figure 5.10a, and the solid line of the "failure-only" Weibull.

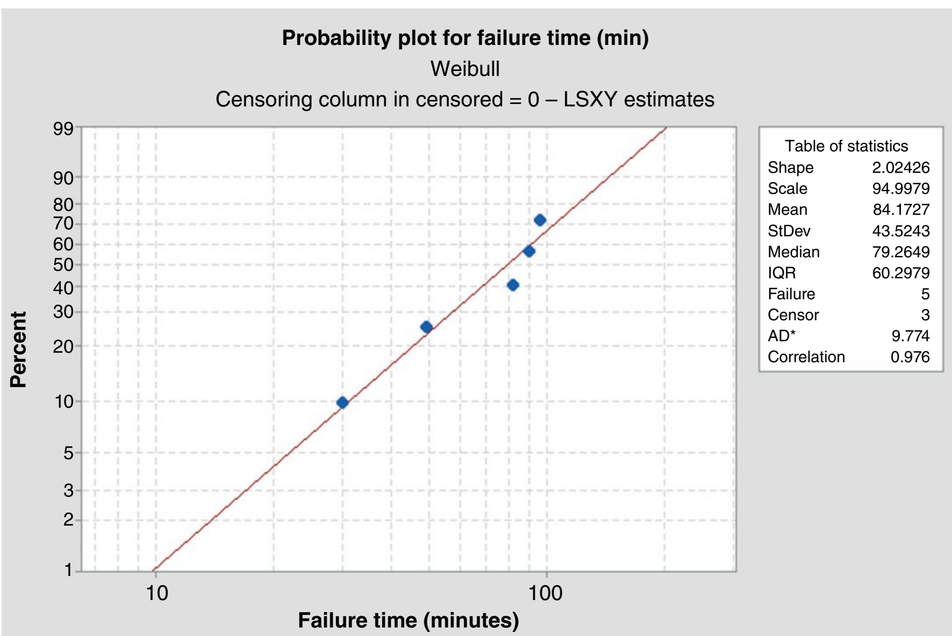


Figure 5.10a Using "least squares (LSXY)" best fit of Inlet Airseal rivet Lab failures.

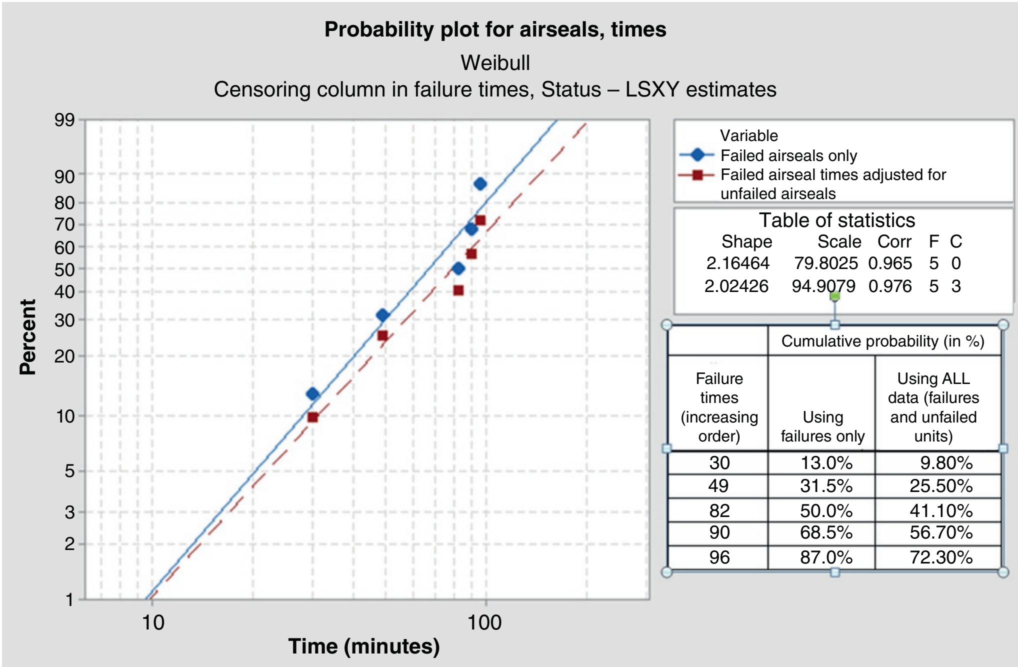


Figure 5.10b Inlet air seal Weibulls side by side showing why you should use ALL unfailed data. Putting this data into MINITAB and asking for two plots of the data on top of each other (one with failures only, the other with failures and suspended items).

Two things to notice:

1) The slopes are very close in value.
2) The failure-only Weibull produces higher probability of failure for each time. Hence, when predicting the future risk, the total number of failures over any future time will be overpredicted. With only eight points in a data set like this lab data, the difference may not be very significant; when there are thousands of unfailed units in a fleet, the results can be VERY significant, and unneeded fleet action would be the result. As will be discussed in the Risk Analysis section, the objective is to predict the expected number of future failures.

Example 5.2 Flashlight Bulb Failures

Based on lab testing of flash bulbs, the following failures were recorded (Table 5.1, Figure 5.11).

Weibull Plots and Their Estimates of β, η

The "job" of an LSXY (ranked regression or sometimes termed a least squares regression) Weibull plot is to provide a good, simple graphic for seeing if your data fit a Weibull distribution (plot as a

Table 5.1 Flashlight bulb failures

72	82	97	103	113
117	126	127	127	139
154	159	199	207	

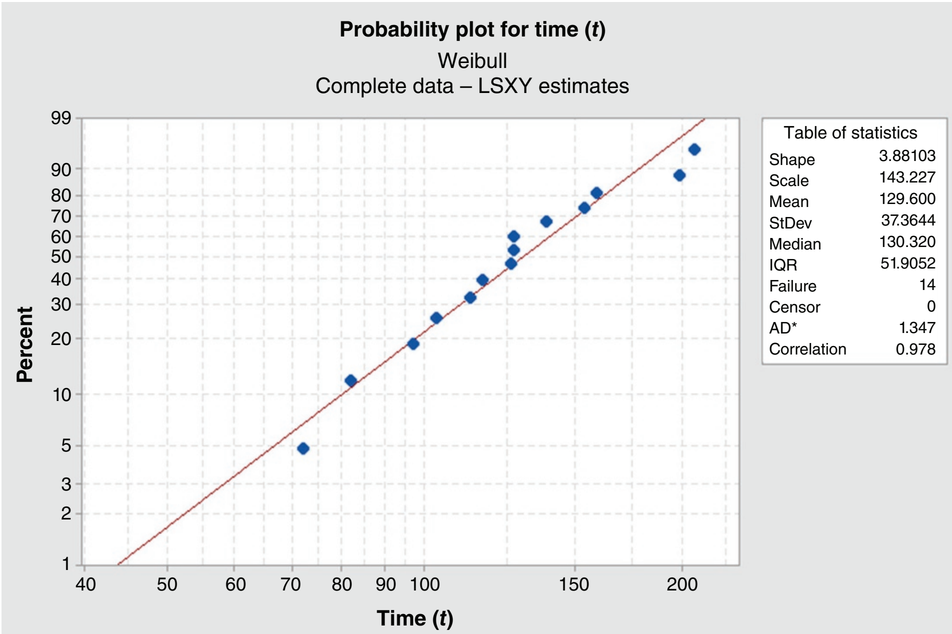


Figure 5.11 Flash bulb Weibull illustrates wear out β = 3.88 and characteristic life of 143 “flashes” before failure.

straight line on Weibull paper). The LSXY Weibull plot is used by your eyes plot to see if there are any anomalies in the data.

As mentioned in the Introduction, there are several anomalies that can appear in the first Weibull plot you produce with your data. We cover the main items and show you what they mean and, when applicable, how to fix the data.

1) The data has a gradual convex (or concave) bend on Weibull paper.

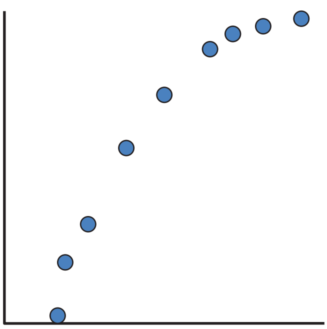


Figure 5.12a Positive t_0 is needed.

Solution: The data needs a t_0 correction (positive or negative) or a different distribution.

Graphically, you have two possibilities (Figures 5.12a and 5.12b).

The three-parameter Weibull adds a t_0 or starting point to the distribution. In all of our discussions to this point t_0 was assumed to be 0. Now, we use this Weibull fitting technique to explain the third parameter. First, the three-parameter Weibull has the following CDF:

$$F(t) = \text{Prob}[\text{life} \leq t] = 1 - e^{-\left(\frac{t-t_0}{\eta}\right)^{\beta}} \tag{5.17}$$

where β and η are the slope and characteristic life, and t_0 is the correction for the time axis (t) axis *not beginning at 0*.

2) Suppose that we have failure data that when plotted looks like Figure 5.13.

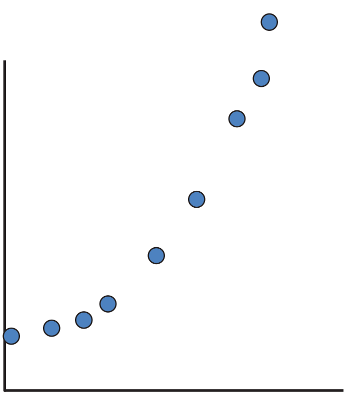


Figure 5.12b Negative t_0 is needed.

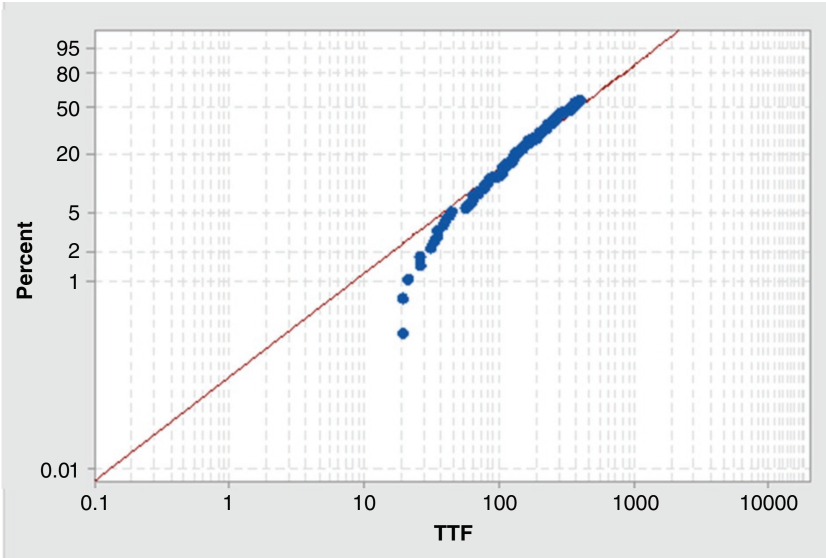


Figure 5.13 Raw field failure data illustrating a gradual curve.

The data can appear with a concave downward curve for several reasons:

- Time does not start at zero, early "burn in"/"run in" time not accounted for
- Early failures are impossible
- Early failure data not reported.

Before you use software that automatically replots the data with the optimal t_0, use your eyeball to estimate where the t_0 is as shown in Figure 5.14.

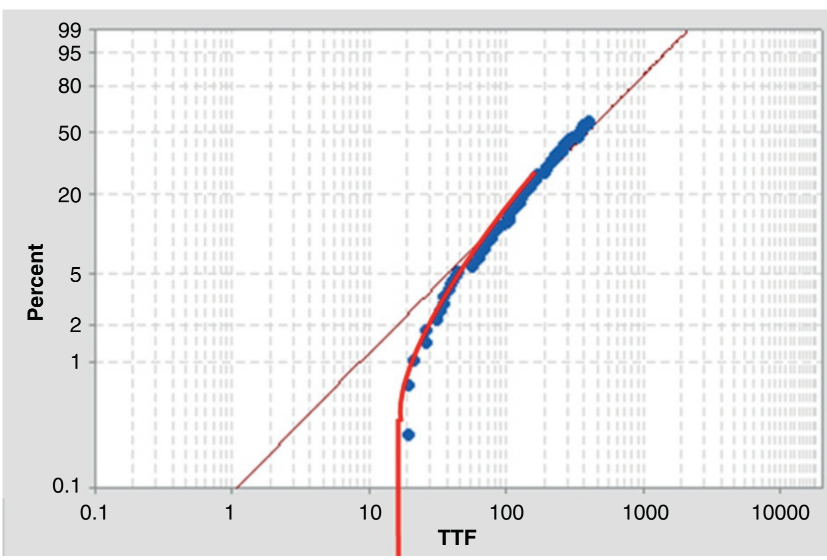


Figure 5.14 t_0 estimate is about 18 hours.

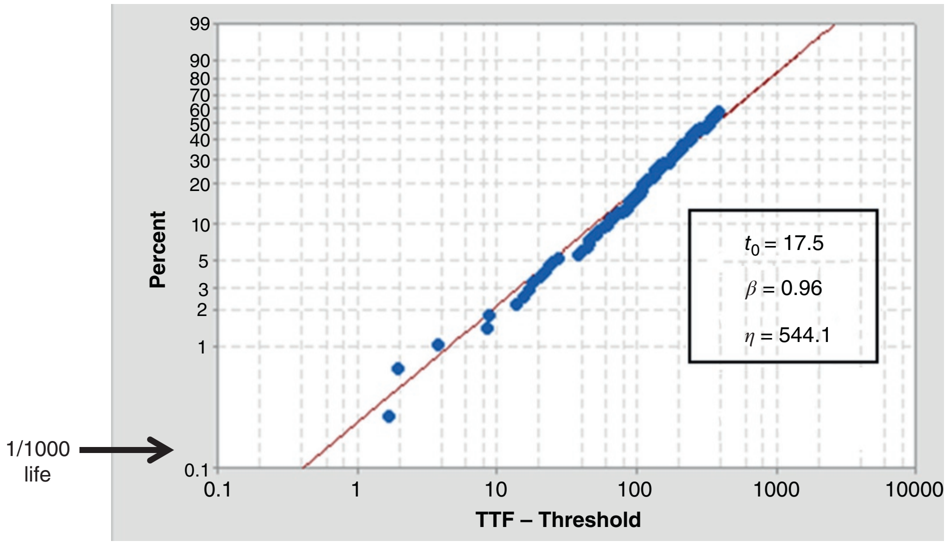


Figure 5.15 MINITAB-calculated t_0 agrees closely with the eyeball estimate.

Now, after inputting the data into MINITAB, you find Figure 5.15.

You must remember, however, that when using a Weibull with a $t_{0,}$ add back the t_0 to what you read off the three-parameter Weibull, as illustrated in Figure 5.16.

For example, see Figure 5.16.

Suppose that you have already determined you have curvature (not a “dogleg” bend), so be aware of the following three-parameter caveats:

- Three-parameter Weibulls occur, but not frequently in some industries or processes. In addition, positive t_0s occur more often than negative t_0s in the authors experience.
- There should be a physical explanation of why failures:
  - Cannot occur before – positive t_0 (e.g. bearing spalling, and part not run to full power for the first (say) 500 miles)
  - Or, age on the shelf before entering service – negative t_0 (while this does not occur that often, improperly desiccated bearings are an example of a phenomenon that gives a negative t_0)
- A significant increase in the correlation coefficient (r) should be observed in going from two- to three-parameter Weibull (using LSXY regression in **MINITAB**). If the correlation coefficient increases from 0.98 to 0.999, that is at least an order of magnitude increase, the look of the three-parameter Weibull should match that increase, i.e. the data should be noticeably straightened. If, on the other hand, you have curvature, but your three-parameter least-squares plot does not look very much, or any, better than the two-parameter, then you need to consider a different distribution for your data.

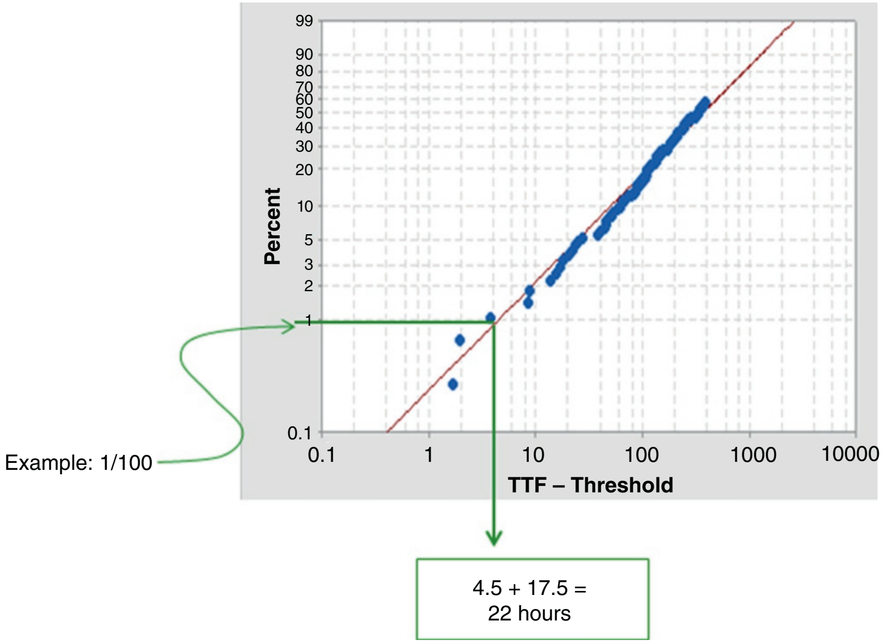


Figure 5.16 t_0 Example 2: Add back t_0 when calculating life.

The Three-Parameter Weibull Did Not Work, What Are My Choices?

First, you need to look at the parts if at all possible to make sure you have only one failure mode. If the data was obtained from a supplier or some other part of your organization, ask them for any details they have on the part failure mode to assure you that the failure mode was the same; after all, it was a smooth *curve* on a Weibull plot, not a straight line.

Given each part failed due to the same failure mode, and you still have curvature after you tried a three-parameter Weibull, you can use **MINITAB** "Distribution ID plot." Pay particular attention to the lognormal: two- and three-parameter fit and how the data looks. The lognormal is usually the best choice after a Weibull. After that you might try a Gamma distribution (although the Gamma is not a frequent solution).

See Figures 5.17a and 5.17b to see the progression from plotting some failure data on a Weibull plot that turns out to be lognormal.

The Data has a "Dogleg" Bend or Cusp When Plotted on Weibull Paper

Solution: Break the data apart into two (or more) failure modes (use the parts to tell you where the break should be).

The Weibull plot can look like either of the two examples, Figure 5.18a or 5.18b.

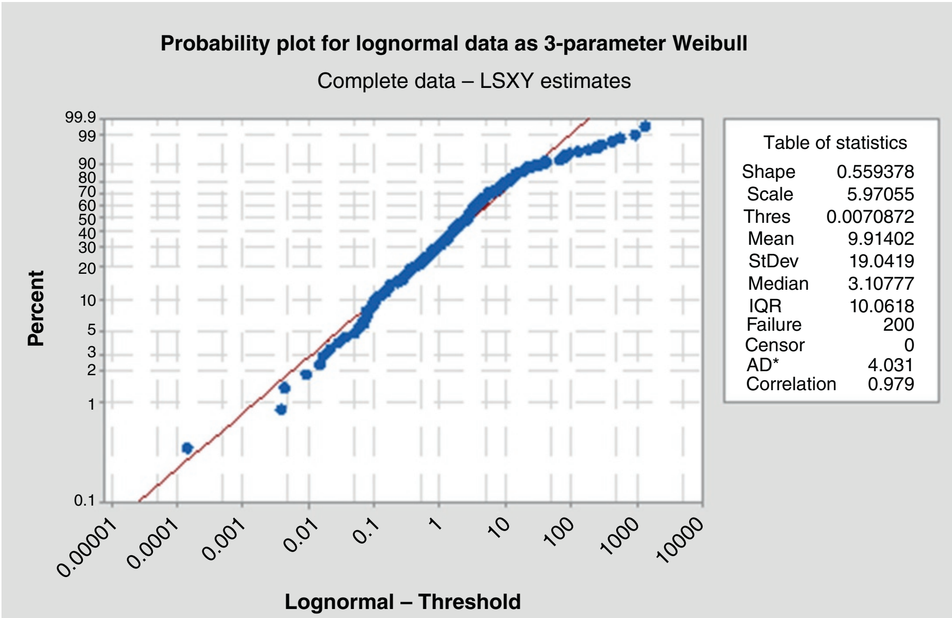


Figure 5.17a Known lognormal failure data plotted as a three-parameter Weibull (correlation = 0.979).

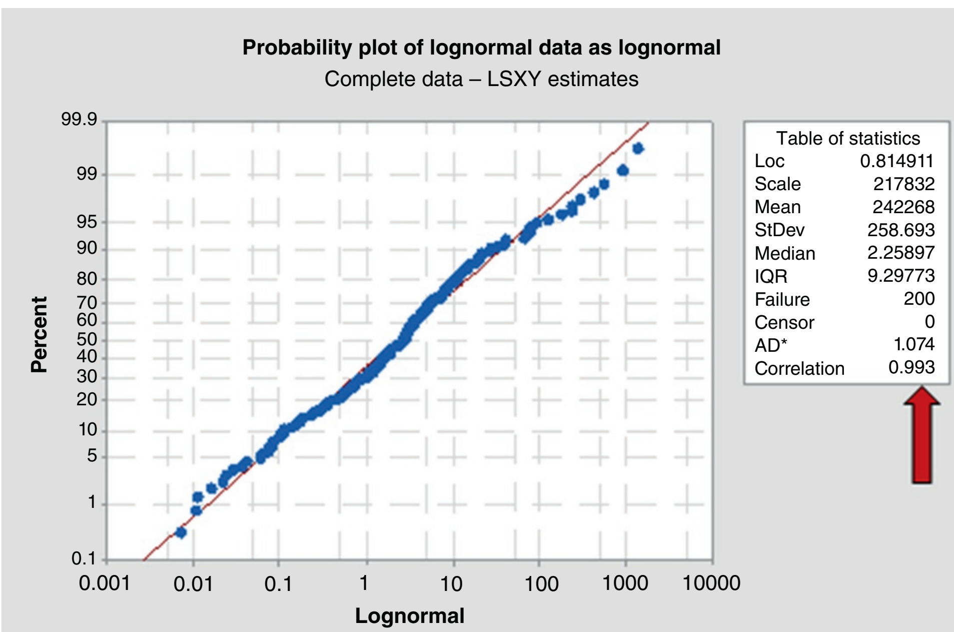


Figure 5.17b Known lognormal failure data plotted on lognormal plot (correlation = 0.993).

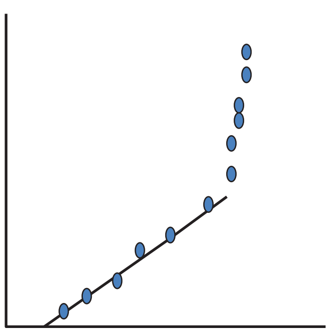


Figure 5.18a Early quality failure mode followed by later wear-out mode (this is the usual case).

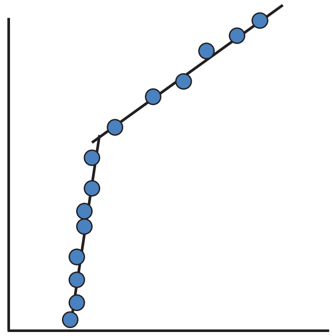


Figure 5.18b Wear-out mode followed by perpetual survivors or the wear-out mode may be a batch problem.

Good engineering investigation of the parts that failed is essential in either of the "dogleg" bend situations illustrated above.

An example, see Figure 5.19a.

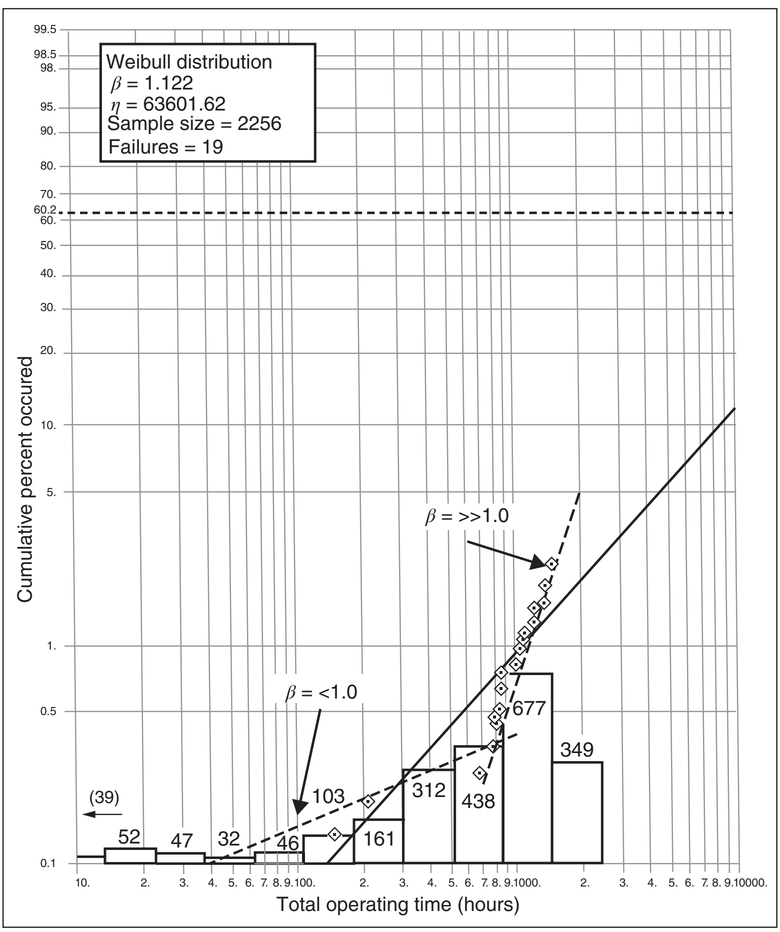


Figure 5.19a An infant mortality problem ($\beta < 1.0$) causing the compressor start bleed to fail. Then a wear-out mode ($\beta >> 1$) affecting the compressor start bleed after about 700
(1983). Public Domain.

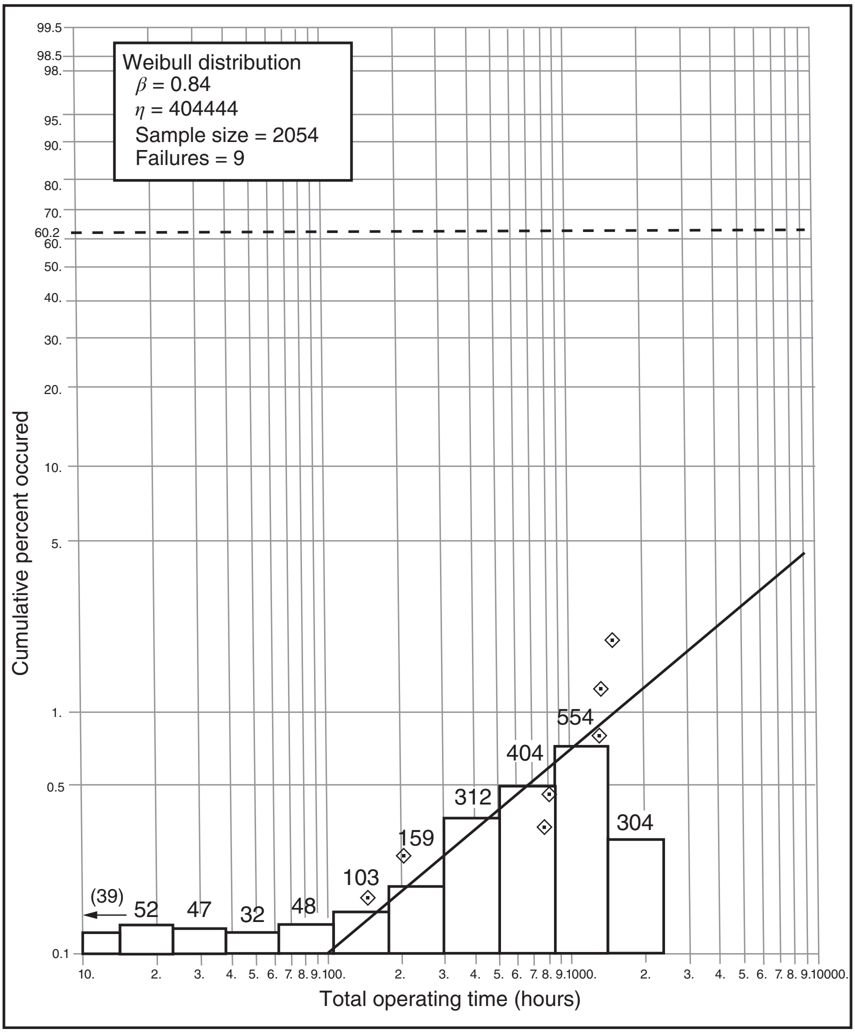


Figure 5.19b Infant mortality mode appears on non-Island base. *Source*: Based on Abernethy et al. (1983). Public Domain.

But wait, the only good engineering way to find out where the infant mortality problem stops so you can separate the two failure modes and do individual Weibulls is to **inspect each failure** and categorize by failure mode. After a thorough engineering investigation of the compressor start bleed is done by location (i.e. Air Force Base), it was discovered that only one base was responsible for the rapid wear-out portion – an AFB on an island $\beta = 5.2$ (see Figure 5.19c)! The rest of the failures followed an infant mortality failure mode $\beta = 0.84$ (see Figure 5.19b).

What was causing the difference? The salt air on the island base was causing corrosion to build up on the start bleed causing the start bleed to hang. The infant mortality mode was caused by

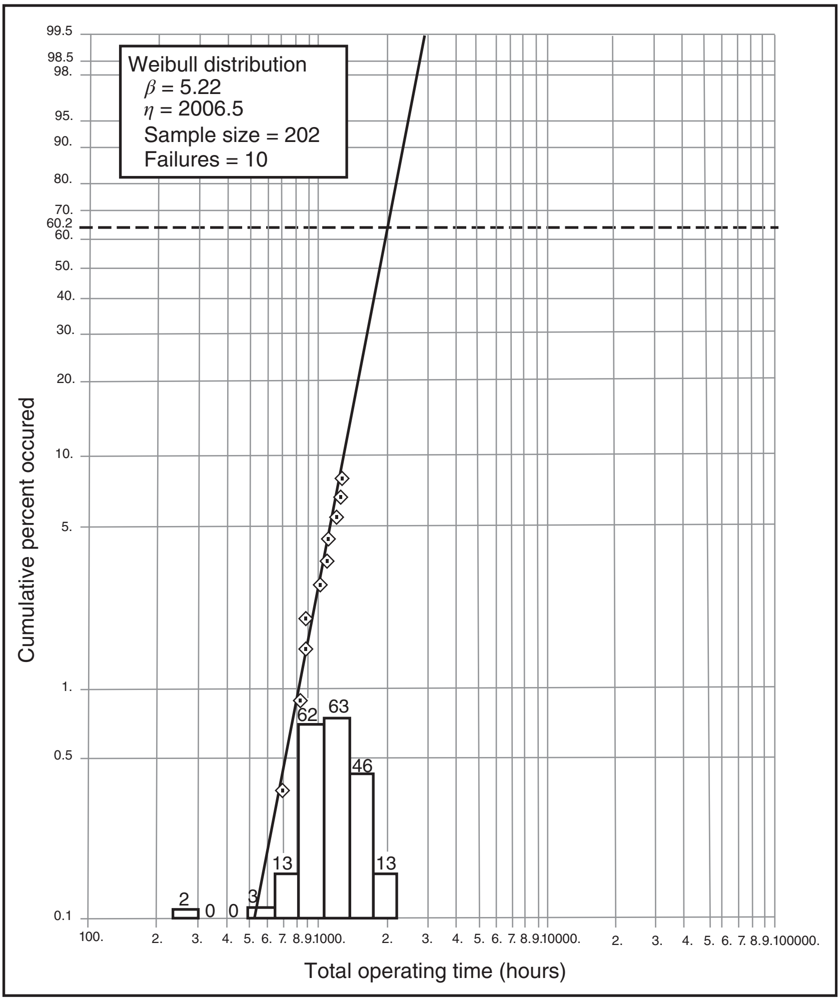


Figure 5.19c Rapid wear-out mode is in the rest of the fleet. *Source*: Based on Abernethy et al. (1983). Public Domain.

misassembly in production. Two different failure modes – wear-out(corrosion) and infant mortality(Misassembly); the good news is both were identified and fixed!

Steep Weibull Slopes (βs) May Hide Problems

It has been the author's personal experience that a failure Weibull very seldom has a $\beta > 12$. In fact, the author has only seen one with that high a β in 40+ years of working with field and lab data.

However, the Weibull distribution can fit many different failure phenomena. So, if you receive data that when first plotted on a Weibull plot gives an extremely high β, consider a three-parameter Weibull.

Example 5.3 (Table 5.2)

Table 5.2 Results of materials lab testing 26 specimens in a Pull test to failure.

22.007	21.970	21.864	21.731	21.841	22.086
22.032	21.987	22.070	22.255	21.995	
21.834	22.068	22.202	21.794	22.567	
22.280	22.422	22.147	22.130	22.236	
22.096	22.254	21.753	22.466	21.985	

The initial Weibull looked like Figures 5.20a and 5.20b.

Low-Time Failures and Close Serial numbers – Batch Problems

The two major sources of problems identifying a failure cause are Weibull data with low-time failures **only** and serial numbers that are close to each other (e.g. within 50 or 100 of each other). Sometimes, the low times can be after a rework at a depot, where the total time could disguise the problem, so Time Since Overhaul (TSO) as the time parameter would reveal the batch. Similarly, if low-time units have no failures, mid-time units have failures, and high-time units have no failures, a batch problem is strongly suggested. Something may have changed in the manufacturing process for a short period and then changed back.

If possible, find the records of the serial number of each part that failed. If not serialized, keep the manufacturing date or lot number. This can often allow you to track down a batch problem.

Figure 5.21 is an example of low-time part failures on main oil pumps. Since there were over 1000 engines in the field with these pumps, most of the pumps with many more hours than these three, what was going wrong? Upon examination of the failed parts, it was determined that they contained oversized parts; i.e. something had changed in the manufacturing process at the supplier. The oversized parts caused an interference with the gears in the pump which resulted in failure. Again, low-time failures provide a clue to a quality problem (e.g. production or assembly process change), especially true when there are many successful high-time units in the field.

Example 5.4 Main oil pump failures in a large fleet (taken from Abernethy et al. 1983, p. 36)
Quality? Assembly? Manufacturing design change?

(Note: Turns out to have been a manufacturing change by the supplier.)

Maximum-Likelihood Estimates of β and η

We have covered fitting data to a Weibull and producing a Weibull plot. Why do we need "Maximum-Likelihood Estimates (MLEs)"? First, we explain what MLEs are and then why we need them (hint: especially when we are projecting the risk due to a failure mode that is fit by a Ranked Regression Weibull).

The maximum-likelihood Weibull analysis method consists of finding the values β and η which maximize the "likelihood," of obtaining β and η (the greatest probability), given the observed data.

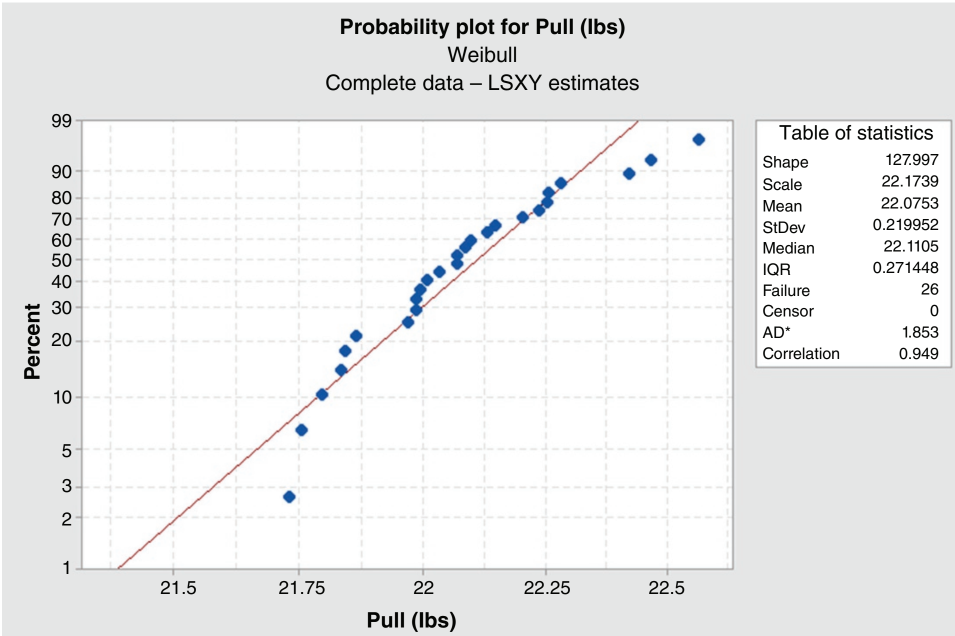


Figure 5.20a Weibull of Pull data shows curvature AND β is unrealistically high, solution. Try a three-parameter Weibull or a lognormal (think about the Pull phenomenon from an engineering phenomenon).

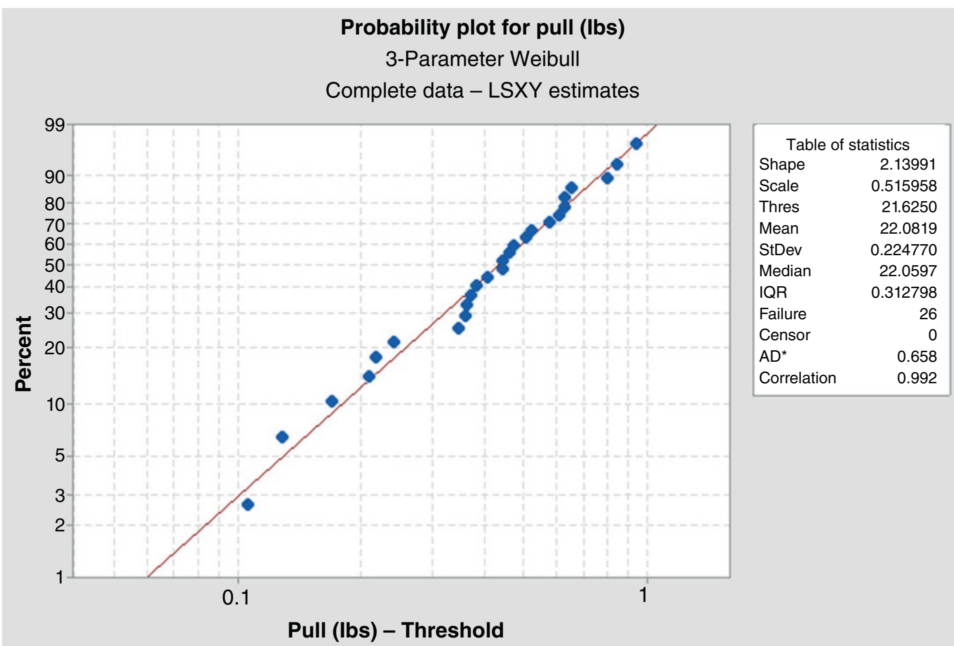


Figure 5.20b Three-parameter Weibull shows a t_0 = 21.625 lbs, indicating that failures will start after this t_0. Also, the β = 2.3 is more realistic. Note that the correlation coefficient is considerably better, which you would expect just by "eyeballing" the difference in the fit between Figures 5.18a and 5.18b.

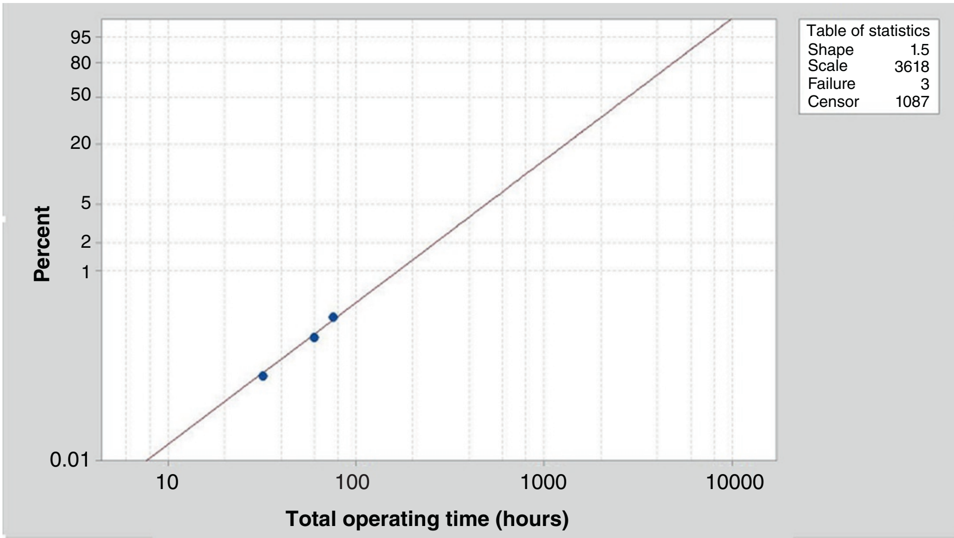


Figure 5.21 Main oil pump failures: three failures so early and none after indicate a batch problem. *Source*: Based on Abernethy et al. (1983).

The likelihood is expressed in Weibull probability density form. It is a function of the data and the parameters β and η. Maximum-likelihood finds the values of β and η which maximize this mathematical likelihood function.

Maximum-likelihood solution for samples with right-censored data and exact failure times:

$$\text{Likelihood Equation } L = \underbrace{f(x_1)\cdot f(x_2)\cdots f(x_r)}_{\substack{\text{One ``}f(x)\text{'' term for}\\ \text{each of the ``}r\text{'' failures}\\ f(x_i)\,=\,\text{PDF evaluated}\\ \text{at failure time } x_i}} \cdot \underbrace{[1-F(x_{r+1})]\cdot[1-F(x_{r+2})]\cdots[1-F(x_n)]}_{\substack{\text{One ``}1-f(x)\text{'' term for}\\ \text{each of the ``}n-r\text{'' suspensions}\\ F(x_i)\,=\,\text{CDF evaluated}\\ \text{at suspension time } x_i}} \tag{5.18}$$

For a given sample of failures and suspensions, L is a function only of the unknown values of β, η.

$$L = \prod_{i=1}^{r}\left(\frac{\beta}{\eta}\right)\left(\frac{x_i}{\eta}\right)^{\beta-1} e^{-\left(\frac{x_i}{\eta}\right)^{\beta}} \prod_{j=1}^{k} e^{-\left(\frac{x_j}{\eta}\right)^{\beta}} \tag{5.19}$$

where $\prod$ = product over all failures and $k = n - r$ (# suspensions).

We need to find the values of β, η that maximize L. Usually, we do that by finding β, η that satisfy $\dfrac{\partial \log L}{\partial \beta} = 0$ and $\dfrac{\partial \log L}{\partial \eta} = 0$ which reduces to:

$$\frac{\sum_{i=1}^{n} x_i^{\beta_{ML}} \ln(x_i)}{\sum_{i=1}^{n} x_i^{\beta_{ML}}} - \frac{1}{r}\sum_{i=1}^{r} \ln(x_i) - \frac{1}{\beta_{ML}} = 0, \text{solve this for } \beta_{\text{ML}} \tag{5.20}$$

then,

$$\eta_{\text{ML}} = \left[\frac{\sum_{i=1}^{n} x_i^{\beta_{\text{ML}}}}{r}\right]^{\frac{1}{\beta_{\text{ML}}}} \tag{5.21}$$

β_{ML}, η_{ML} are the maximum likelihood estimates of β, η.

Example 5.5 Calculating the maximum likelihood estimates, given the data in Table 5.3 (Figure 5.22).

Table 5.3 Field test results.

Cycles	Status
1500	Failure
1750	Suspension
2250	Failure
4000	Failure
4300	Failure
5000	Suspension
7000	Failure

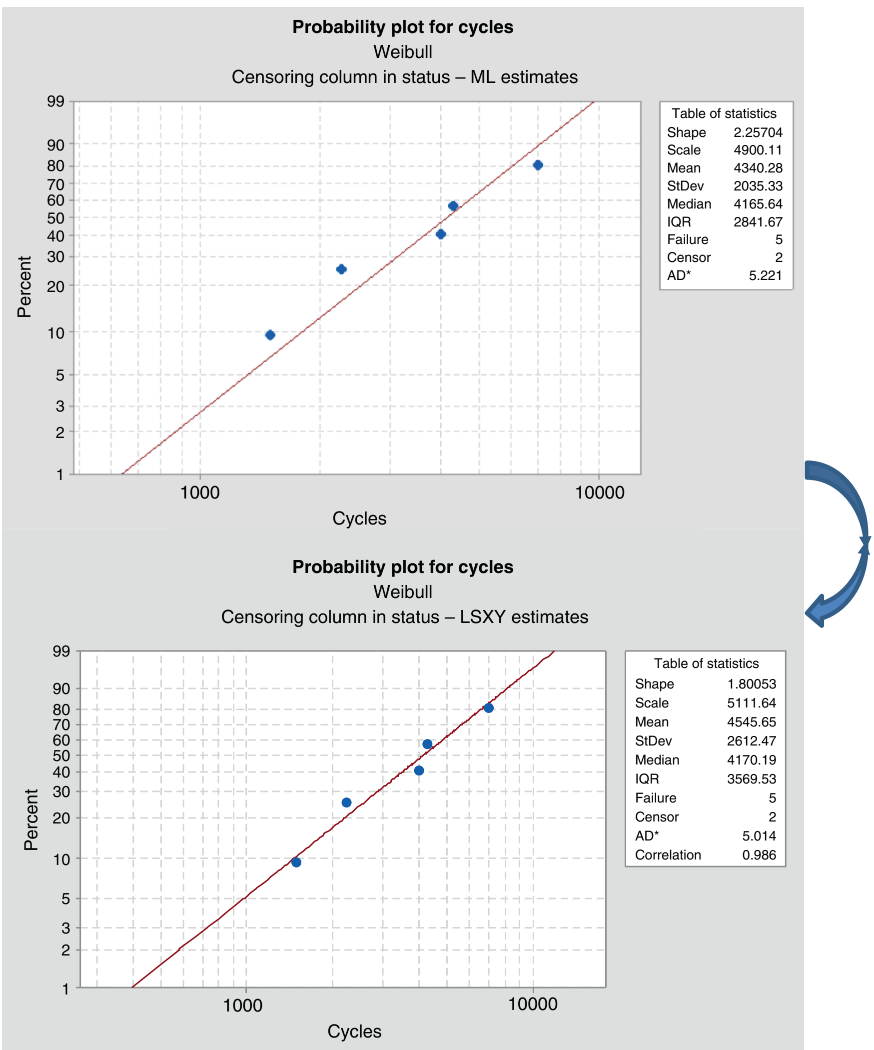


Figure 5.22 Using MINITAB to produce a Weibull plot of the data plot; since the β MLE and β LSXY are close, you probably do not

So, why use maximum likelihood estimates? When are they better, and when are ranked regression estimates better?

This comparison in Table 5.4 is based on the research published in the USAF Weibull Handbook by Abernethy et al. (1983).

While very obviously maximum-likelihood estimation is a purely mathematical technique, a Weibull plot is necessary. Hence, the MRs and plotting positions of the failures are the same as ranked regression, BUT the Weibull line is based on the MLE β & η. You can see this in the particular case given in Figure 5.22.

Weibayes Analysis

Often, a Weibull plot cannot be made because of lack of data:

1) There are few (1 or 2) or no failures.
2) The age of the units is unknown, and only the number of failures is known.
3) A test plan for a new design is needed (Chapter 6).

Especially for those instances where the customer support engineers have observed parts from the field (either directly or warranty claims) that show parts that were not performing according to design. None of the parts were "broken," and no safety incidents were observed due to these parts (yet). However, the customer support engineers in conjunction with the design engineers believe that a failure is "imminent."

So, no *failures* have been observed, but because of the seriousness of the potential failure, which is judged to be "imminent," an estimate of the problem seriousness must be done.

Weibayes analysis has been developed to solve problems such as this when Weibull analysis cannot be used. Weibayes is never preferred over Weibull analysis but is often required because of weaknesses in the data. Weibayes is defined as Weibull analysis with an assumed β parameter, where a failure is imminent. Since the assumptions requires judgment, this analysis is regarded as an informal Bayesian procedure.

Table 5.4 Comparison of maximum-likelihood and ranked regression (Weibull plot) methods.

Characteristics	Ranked regression (Weibull plot)	Maximum likelihood
1. Supporting graphics	**Yes**	Limited[a]
2. Applicable to censored data	All but interval-censored data	**Yes**
3. Bias	About equal	About equal
4. Precision	Worse	**Better**
5. Able to assess uncertainty in estimates	No	**Yes**
6. Bias, precision in predictions of future failures	Poor	**Much better**
7. Estimates of β, η with only one failure	No	Yes
8. Can detect batch problem	**Yes**	No

[a] Uses median ranks for the Weibull plot and MLE β, η estimates for fit.

Weibayes Background (You Do Not Necessarily Have Any Failure Times)

The assumptions in Weibayes are:

1) You know the Weibull β (or range in which the β occurs) for the failure mode.

   That knowledge comes from "a priori" information (aka previous experience) with a similar failure mode to the one you are now observing. For example, many companies have "Weibull" failure mode libraries, or at least extensive design files for previous designs, or at least warranty records that might include a similar failure mode in a previous product. Any of these sources will give some idea of the failure mechanism and therefore the ~β or range of βs. For example:

- $1 < \beta < 2.5$ covers most bearing failure modes
- $2.5 < \beta < 5.5$ covers most low cycle fatigue cracking modes
- $\beta = 1.0$ for random shock, unrelated to part age
- $\beta = 2.0$ for linearly increasing hazard rate
- If you have material specimen data, you can approximate the β using the data in Table 5.5.

2) You have at least a histogram of population times
3) You will assume that one failure is "imminent."

Given these assumptions, the Weibayes calculation of η, based on the maximum-likelihood formulation (Eq. (5.21)), is

$$\eta = \left(\frac{\sum_{i=1}^{n} t_i^{\beta}}{NF} \right)^{\frac{1}{\beta}} \tag{5.22}$$

where β is the Weibull slope, t_i is the individual time on each of n units, and NF is the number of failures.

Example 5.6 The design system-predicted 1/1000 life for the compressor disk is 1000 cycles. Does the field data substantiate it?

Five disks have accumulated 1500 cycles, and five have 2000 cycles without any failures. If most disk LCF failures have a β of 3.0, is this success data sufficient to increase the predicted design life?

Taken from Abernethy et al. (1983), p. 87.

Table 5.5 Design analysis of the typical to min life ratio provides the values to be multiplied by η to determine the mean, standard deviation, mode, and median of the Weibull distribution, for several values of β.

Beta	Mean	Median (B50)	1/10 (B10)	1/100 (B1)	1/1000 (B.1)	Mode	B50 to B.1 ratio	Std. dev.	Variance
0.5	2.00000	0.48045	0.01110	0.00010	0.00000	No mode	479972.60	4.47214	20.00000
1	1.00000	0.69315	0.10536	0.01005	0.00100	0.00000	692.80	1.00000	1.00000
1.5	0.90275	0.78322	0.22308	0.04657	0.01000	0.48075	78.30	0.61294	0.37569
2	0.88623	0.83255	0.32459	0.10025	0.03163	0.70711	26.32	0.46325	0.21460
2.5	0.88726	0.86363	0.40651	0.15881	0.06311	0.81519	13.68	0.37967	0.14415
3	0.89298	0.88500	0.47231	0.21580	0.10002	0.87358	8.85	0.32455	0.10533
3.5	0.89975	0.90058	0.52573	0.26865	0.13897	0.90834	6.48	0.28473	0.08107
4	0.90640	0.91244	0.56973	0.31662	0.17785	0.93060	5.13	0.25429	0.06466
4.5	0.91257	0.92178	0.60648	0.35978	0.21547	0.94568	4.28	0.23009	0.05294
5	0.91817	0.92932	0.63758	0.39851	0.25121	0.95635	3.70	0.21031	0.04423
5.5	0.92320	0.93553	0.66421	0.43327	0.28483	0.96417	3.28	0.19379	0.03756
6	0.92772	0.94074	0.68725	0.46455	0.31625	0.97007	2.97	0.17977	0.03232
6.5	0.93178	0.94517	0.70736	0.49277	0.34554	0.97463	2.74	0.16769	0.02812
7	0.93544	0.94899	0.72507	0.51832	0.37279	0.97822	2.55	0.15717	0.02470
7.5	0.93874	0.95231	0.74078	0.54153	0.39813	0.98110	2.39	0.14793	0.02188
8	0.94174	0.95522	0.75480	0.56269	0.42172	0.98345	2.27	0.13973	0.01952
8.5	0.94447	0.95780	0.76740	0.58205	0.44369	0.98538	2.16	0.13240	0.01753
9	0.94697	0.96009	0.77877	0.59982	0.46418	0.98700	2.07	0.12582	0.01583
9.5	0.94925	0.96215	0.78909	0.61617	0.48332	0.98836	1.99	0.11986	0.01437
10	0.95135	0.96401	0.79849	0.63127	0.50121	0.98952	1.92	0.11446	0.01310

It also gives the ratio of the B50 to B.1 lives, for several values of β. Sometimes, we are given a value of this ratio ("typical to min life ratio") and work backward to get an estimate of β. This table uses $\eta = 1$ in the calculations.

Table 5.6 Using compressor disk data to calculate if a B.1 of 1000 cycles has been demonstrated.

Test time (cycles)	Test time (^{3})
1500	3,375,000,000
1500	3,375,000,000
1500	3,375,000,000
1500	3,375,000,000
1500	3,375,000,000
2000	8,000,000,000
2000	8,000,000,000
2000	8,000,000,000
2000	8,000,000,000
2000	8,000,000,000
Sum=	56,875,000,000

Source: Based on Abernethy et al. (1983).

Solution: Using Eq. (5.22) and the test data in Table 5.6.

So,

$$\eta = \left(\frac{\sum_{i=1}^{n} \text{times}_i^{\beta}}{NF} \right)^{\frac{1}{\beta}}$$

$$= \left(\frac{56,875,000,000}{1} \right)^{\frac{1}{3}} = 3846 \text{ cycles}$$

Using $\beta = 3$, with $\eta = 3846$, and solving for the 1/1000 life (prob of failure = 0.001) = 385 cycles. So, you have *not* demonstrated a 1000 cycle B.1 life.

We use the Weibayes assumption when setting up reliability tests based on the Weibull discussed in Chapter 6.

Example 5.7 Fifteen jet engine compressor vane and case failures have been experienced in a large fleet of engines. A test plan was set up to substantiate a new design

Weibull analysis provides a β of 4.4 (see Figure 5.23) from field data. Three redesigned compressor cases have been tested in engines to 4000, 5800, and 6200 hours without failure. Is this enough testing to substantiate that the redesign is at least 2× better?

Using the MLE formula for calculating η, assuming the same β as the old design:

$$\eta = \left[\frac{(4000)^{4.4} + (5800)^{4.4} + (6200)^{4.4}}{1} \right]^{\frac{1}{4.4}} = 7166 \text{ hours}$$

Conclusion: The new design is ~2.5× better than the current design as shown in Figure 5.24.

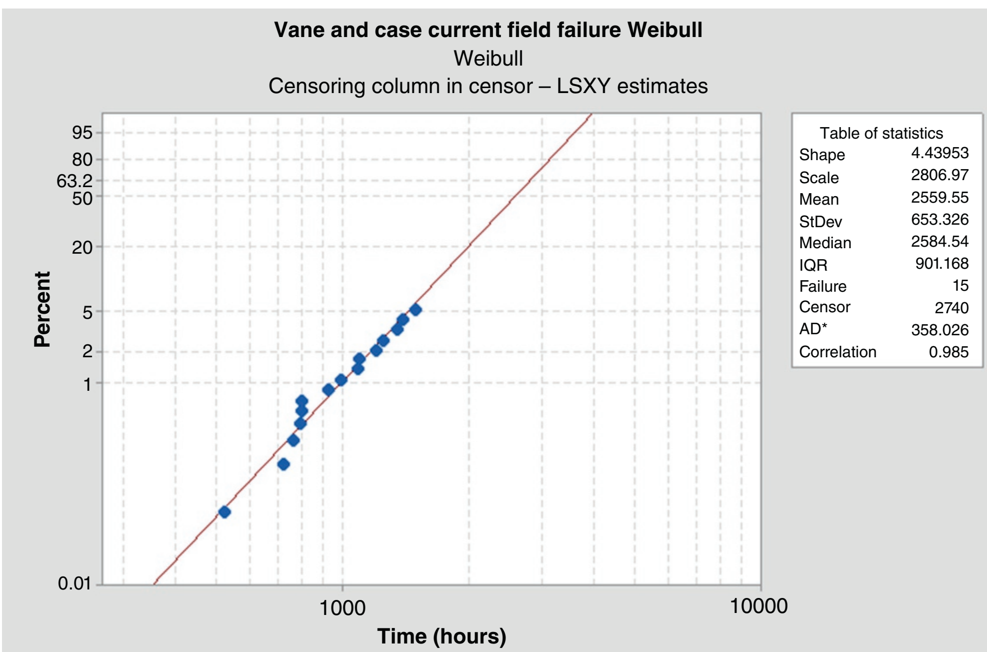


Figure 5.23 Vane and case Weibull β = 4.4.

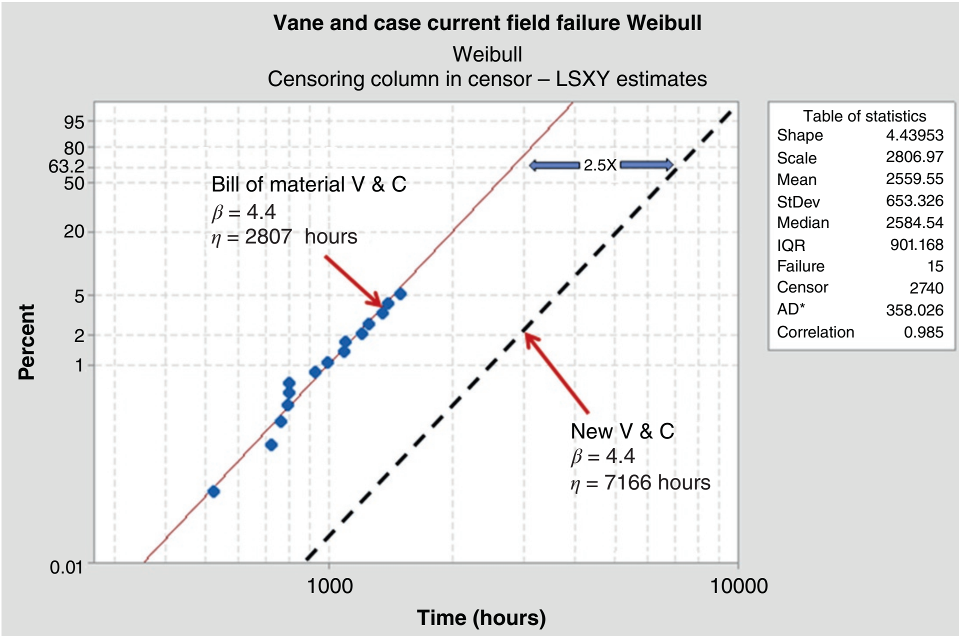


Figure 5.24 New design vane and case has demonstrated 2.5 × better life.

Weibull Analysis with Failures Only and Unknown Times on the Unfailed Population

Here you have the failure times from the field, but the part is not serialized, so you have no idea of the times on the unfailed parts. This happens in many products. Serializing parts and tracking their times is expensive for customers. Therefore, usually only safety issues with *known* part causes are serialized. BUT a new product can be used in a different way and create a failure mode that has not been seen before. So how do you construct a Weibull so you can make an estimate of future failures when this scenario happens?

Shifting Weibull Procedure

1) Plot the *failure data* on Weibull probability paper and estimate β and η.
2) Calculate the mean time to failure (MTTF):

$$\text{MTTF} = \frac{\sum_{i=1}^{\#\text{failures}} \text{failure age}_i}{\#\,\text{failures}} \tag{5.23}$$

3) Draw a vertical line on the Weibull plot of failures only at the MTTF.
4) Calculate the proportion failed in the population:

$$\text{Proportion failed} = \frac{\#\,\text{failures}}{\#\,\text{failures} + \#\,\text{suspensions}} \tag{5.24}$$

Then, $\%\text{failed point} = (1 - e^{-\text{Proportion failed})}) \times 100$. Draw a horizontal line from the % failed point.

5) At the intersection of the vertical and horizontal lines draw a line parallel to the "failure only" Weibull.

6) This line is an estimate of the Weibull of failures "corrected" for the suspensions.

Example 5.8 Five failures, no time on the other 4995 gears
Suppose that you have five gear failures with the following mileages: 3165, 3579, 4098, 5134, and 5402 miles in a population of 5000; however, the mileage on the unfailed units is unknown. Generate your best estimate of the gear population Weibull (Figure 5.25).

Two assumptions have been made in using this shifting technique:

1) You do not have a batch problem.
2) The unfailed times are distributed relatively uniformly around the failures, i.e. some before, some among, and some after the last failure.

Confidence Bounds and the Weibull Distribution

Confidence intervals are measurements of precision in estimating a parameter. A confidence interval around an unknown parameter is an interval of numbers derived from sample data that almost surely contains the parameter. The confidence level, usually 90% or higher, is the frequency with which the interval calculation method could be expected to contain the parameter if there were repeated applications of the method.

One easy way to look at confidence is confidence = 1-risk. So, if you have 90% bounds around a Weibull β, there is only a 10% risk the next samples will have a β outside those limits.

In terms of reliability and in particular the Weibull distribution, the confidence intervals give:

- A plausible range of values for a population parameter
  - (e.g. β, η, *Bx* life, $R(t)$, FailureRate(t)).
  - MINITAB can generate all of these confidence bounds and more.
- The precision of an estimate. (When sampling variability is high, the confidence interval will be wide to reflect the uncertainty of the observation.)

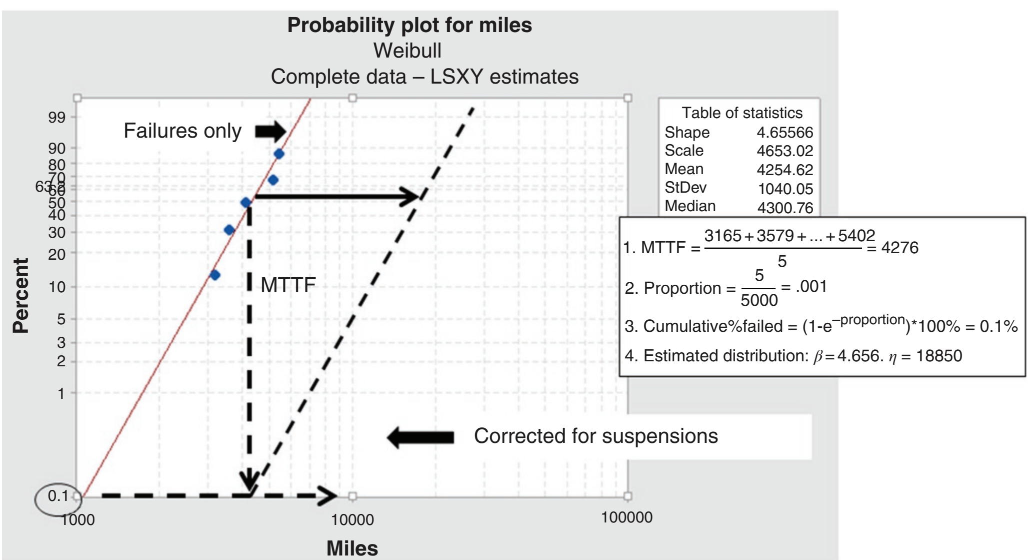


Figure 5.25 Shifting Weibull example.

However, confidence bounds are more useful in *comparing two data sets:*

1) New design vs old design
2) Different geographic sources
3) Different fleets or customers
4) Different product usage
5) Different production lots
6) Different vendors
7) Different alloys (e.g. material life comparison).

This is where we concentrate our attention. For comparing two data sets:
Methods:

1) 90% confidence bounds do not overlap at B10 life. This will be give you 90% confidence that they are different if the bounds do not overlap.
   - (MINITAB can be used here)
2) Maximum-likelihood (β, η) contours do not overlap.
   - (need Supersmith™ or ReliaSoft's Weibull++ ™ or JMP/SAS™ to produce these)

Example 5.9 Using Method 1: Comparing two Weibull distributions
Suppose that we have asked two possible suppliers for a particular component to test eight each of their production of the same component and test each of the eight to failure (Table 5.7).

- The Weibull analysis for each sample results in the following:
  - Weibull distribution for supplier A: β=2.90, η = 825.8 hours
  - Weibull distribution for supplier B: β=3.15, η = 2004 hours
- Should we conclude that there is a real (statistically significant) difference in the reliability performance of the two suppliers?

Using two-sided 80% CIs on B10 for each sample, declare a difference if their CIs do not overlap.

- For A: B10 = 380, 2S-80%CI = (235, 614)
- For B: B10 = 981, 2S-80%CI = (635, 1515)

Note: The confidence bounds can be read off the **MINITAB** plots; in this case you know the bounds do not overlap, but a graphical explanation is better for presentation (Figure 5.26).

Table 5.7 Hours to failure.

Supplier A	Supplier B
220	805
520	1200
550	1400
730	1600
780	1800
890	2200
1050	2500
1150	2800

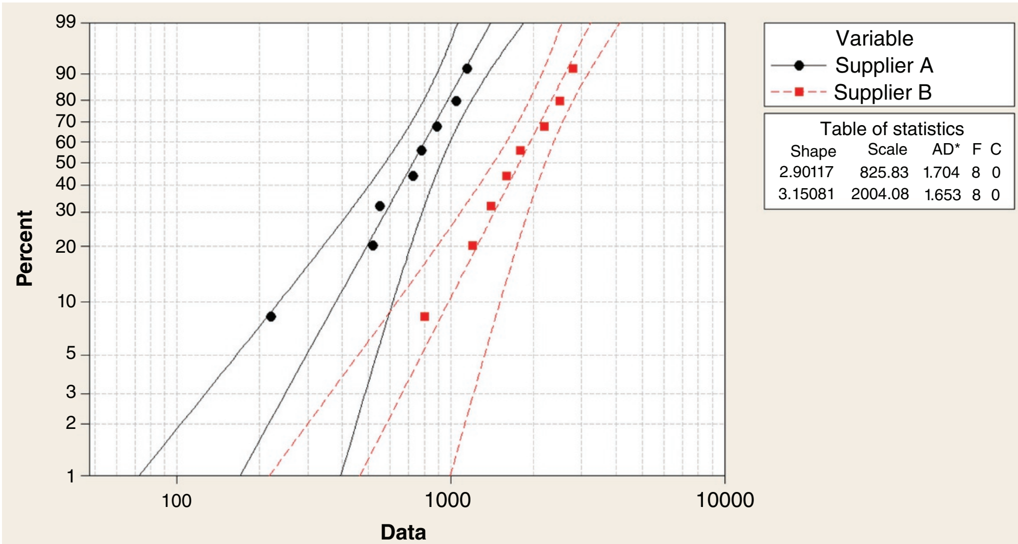


Figure 5.26 Weibull plot illustration of difference between two suppliers (90% confidence bounds on the median line).

Variable: Supplier A

Parameter estimates

Parameter	Estimate	Standard Error	90.0% Lower	Normal CI Upper
Shape	2.90117	0.849840	1.79192	4.69708
Scale	825.830	105.362	669.501	1018.66
Mean (MTTF)	736.396	96.9590	593.001	914.467
Standard deviation	275.798	67.5860	184.304	412.712
Median	727.822	104.061	575.294	920.789
First quartile (Q1)	537.507	109.636	384.305	751.781
Third quartile (Q3)	924.244	112.721	756.248	1129.56
Interquartile range (IQR)	386.737	95.8772	257.228	581.451

Variable: Supplier B

Parameter estimates

Parameter	Estimate	Standard Error	90.0% Lower	Normal CI Upper
Shape	3.15081	0.888449	1.98150	5.01016
Scale	2004.08	237.276	1649.45	2434.96
Mean (MTTF)	1793.63	221.197	1464.32	2196.99
Standard deviation	623.831	144.083	426.655	912.130
Median	1784.01	236.482	1434.51	2218.65
First quartile (Q1)	1349.54	252.015	992.628	1834.78
Third quartile (Q3)	2222.98	250.163	1847.34	2675.01
Interquartile range (IQR)	873.446	207.119	591.348	1290.12

Figure 5.27 An excerpted portion of the information on parameter confidence bounds from the analysis of the supplier A and B data.

Other confidence bounds (β, η, MTTF (mean time to failure),...) are readily available in the MINITAB analysis portion when a Weibull plot is produced (Figure 5.27).

Example 5.10 Life testing flashlight bulbs
Life testing was undertaken to examine the effect of the operating time and the number of on–off cycles on incandescent bulb life. Six volt flashlight bulbs were operated at 12.6 V in order to increase the failure rates. The wall-clock failure times, in minutes, for 26 bulbs operated continually and 27 bulbs operated on a 30-seconds on–30-seconds off cycle are given in Table 5.8. Use probability plotting to fit the two sets of data to Weibull distributions, and determine the effect of on–off cycling on the life of the bulb.

Using MINITAB with 90% confidence bounds on each Weibull line (Figure 5.28).

When the clock time is converted to operating time, steady-state times are not changed, but cyclic times are ½ . So, adjusting all cyclic times to operating times produces (Figure 5.29).

Thus, since the confidence bounds on each of the Weibull lines overlap at the 10% failure line, the two sets of data give indistinguishable results when cast in terms of operating time. Therefore, the effects of the on–off cycling on bulb lifetime are negligible.

Arbitrary Censored Data – Left-Censored, Right-Censored, and Interval Data

What do we do if we have inspection data? Inspection data or any data from field-scheduled visits could be "interval" data.

This data can either be left, right, or interval censored (Figure 5.30).

Table 5.8 Wall clock failure times in minutes.

Steady state		Cyclic	
72	125	161	258
82	126	177	262
87	127	186	266
97	127	186	271
103	128	196	272
111	139	208	280
113	140	219	284
117	148	224	292
117	754	224	300
118	159	232	317
121	177	247	332
121	199	243	342
124	207	243	355
			376

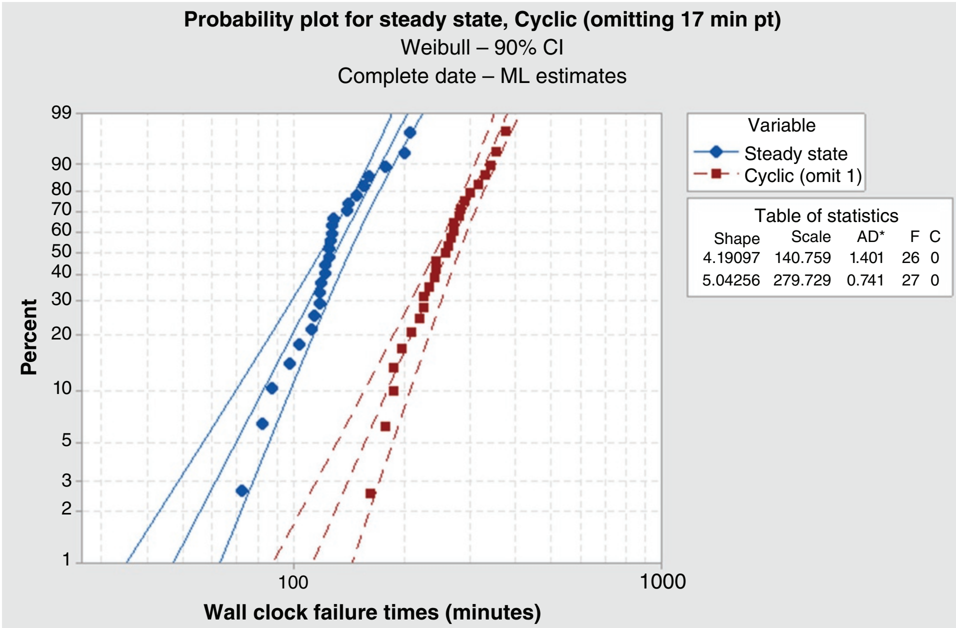


Figure 5.28 Weibull plot of steady state and cyclic testing of wall clocks.

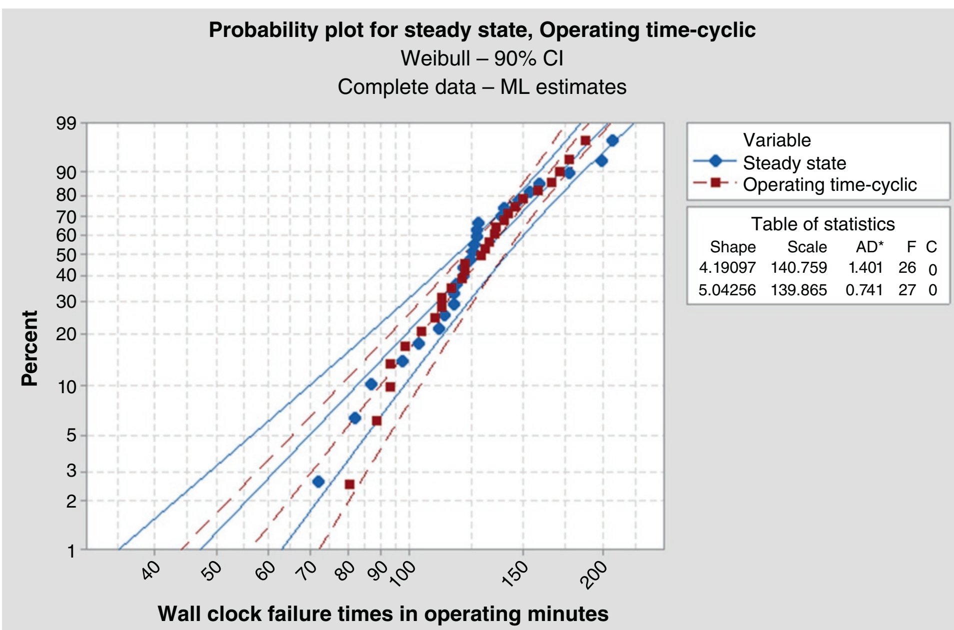


Figure 5.29 After adjusting the cyclic times to operating times, there is no significant difference.

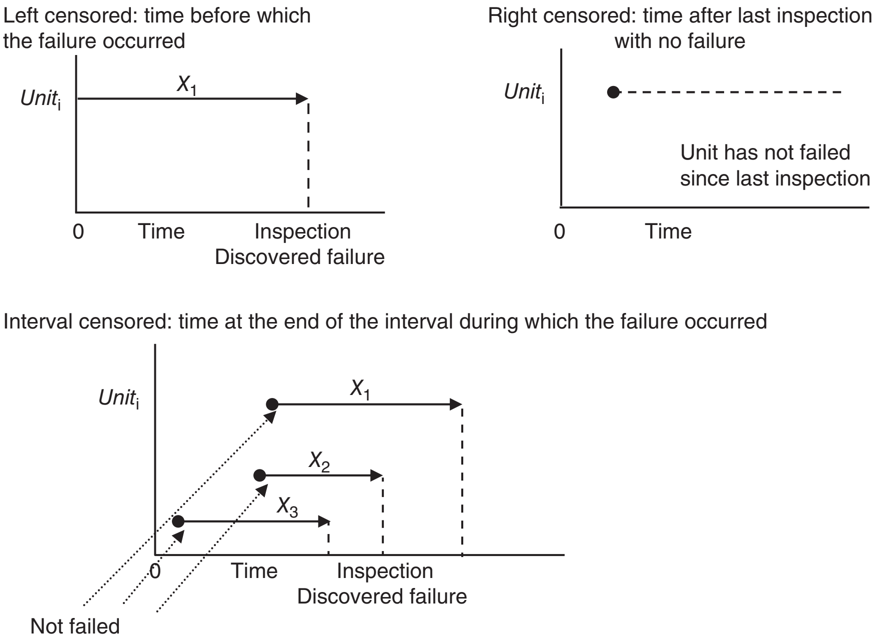


Figure 5.30 Graphic illustration of the left, right, and interval-censored data.

MINITAB uses a maximum-likelihood estimation technique for finding the Weibull distribution that has the highest probability of explaining the interval data.

Example 5.11 Given the following nine interval failure points in Table 5.9[2], generate a Weibull using MINITAB's "arbitrary censoring" (Figure 5.31).

Table 5.9 Interval data.

Start (h)	End (h)
*	6.12
6.12	19.92
19.92	29.64
29.64	35.4
35.4	39.72
39.72	45.24
45.24	52.32
52.32	63.48
63.48	*

Source: Data from Nelson (1982).

2 *Source*: Data from Nelson (1982), p. 415.

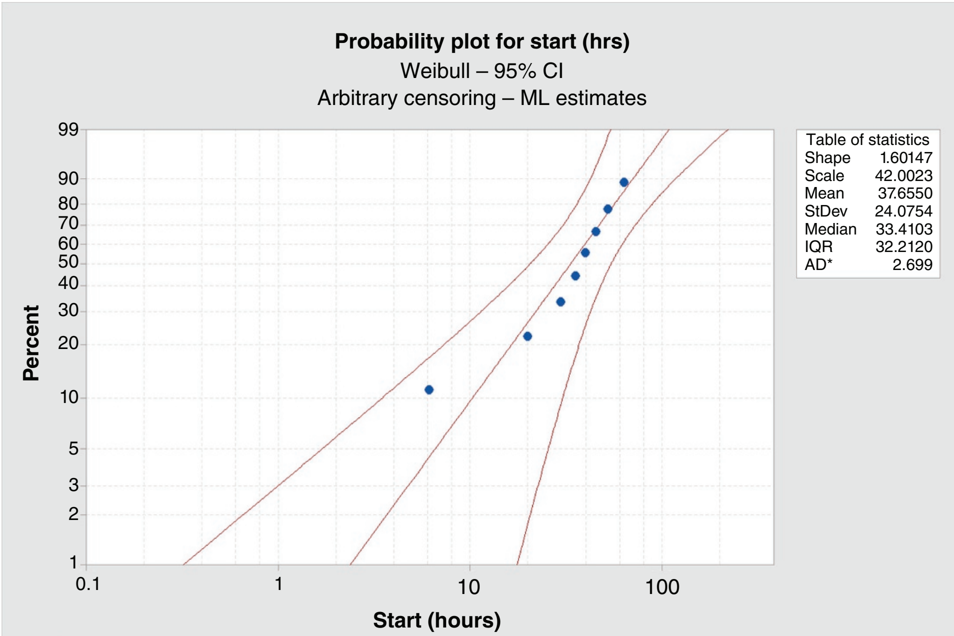


Figure 5.31 Slow wear-out failure mode indicated.

Example 5.12 Given the inspection data in Table 5.10, generate a Weibull (Figure 5.32).

Table 5.10 "Mixed" interval data.

	Discovered		Censor
Start	Failed	Freq	Type
*	1,000	5	Left
1,000	2,000	3	Interval
2,000	3,000	1	Interval
4,000	5,000	1	Interval
7,000	8,000	1	Interval
10,000	11,000	1	Interval
11,000	12,000	1	Interval
12,000	13,000	1	Interval
13,500	13,500	1	Exact
16,000	17,000	1	Interval

Note: The data on the Weibull plots illustrated for interval data are plotted using MRs, while the best fit line and confidence bounds on the best fit line are based on the MLE estimates of β and η. Hence, the "eyeball" fit does not always look good. A Weibull plot is necessary for explanation and presentation but can cause questions when MLE-based lines are on a plot of MR-placed points.

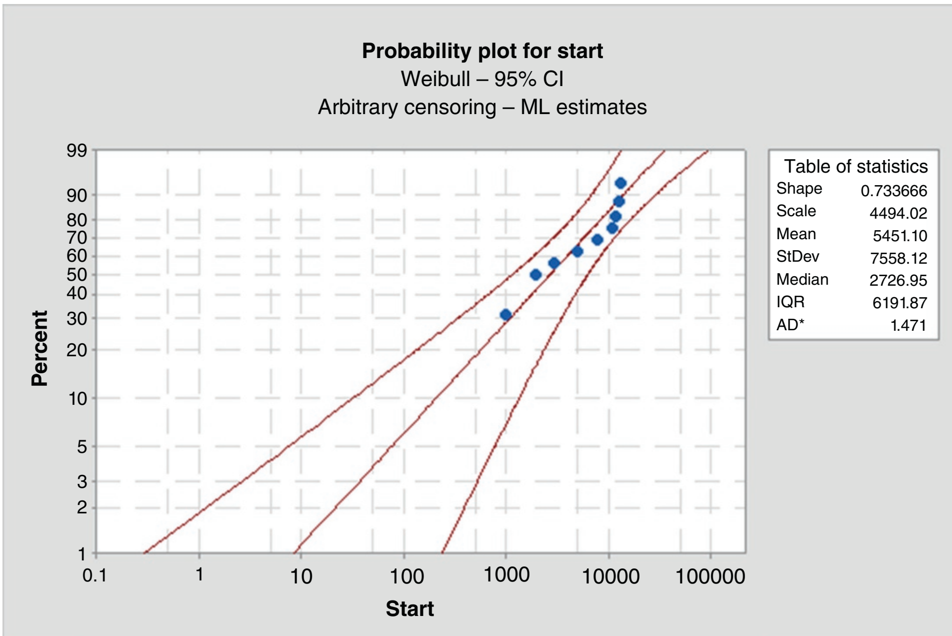


Figure 5.32 Infant mortality (quality or maintenance) failure mode indicated.

The Weibull Distribution in a System of Independent Failure Modes

Consider a system with a failure rate that results from the contributions of independent modes. Suppose that some modes are associated with failure rates that decrease with time, while the failure rates of others are either constant or increase with time. Weibull distributions are particularly useful for modeling such modes. If we write

$$\int_0^t \lambda(t')dt' = \left(\frac{t}{\eta_a}\right)^{\beta a} + \left(\frac{t}{\eta_b}\right)^{\beta b} + \left(\frac{t}{\eta_c}\right)^{\beta c} \tag{5.25}$$

and take $0 < \beta_a < 1$, $\beta_b = 1$, and $\beta_c > 1$, the three terms correspond, respectively, to contributions to the failure-rate contributions that decrease, remain flat, and increase with time. These are associated with early failures, random failures, and wear failures, respectively. Thus, the shape of the bathtub curve can be expressed as a superposition of Weibull failure rates. It is not valid to think of these individual terms as arising from Eqs. (3.57) through (3.63) unless each of them results from independent failure modes or the failures of different components. When they arise as the result of a single cause, the contributions from infant mortality, random, and aging effects are strongly interactive. In these cases, Eq. (5.25) may be a useful empirical representation of the failure rate curve so long as the individual terms are not identified uniquely with infant mortality, random, or aging failures. We consider the interactions that give rise to the bathtub curve in more detail in Chapter 8, where they are related to loading and capacity.

5.3 Extreme Value Distributions

Extreme value distributions or, more precisely, asymptotic extreme value distributions frequently rise in situations where the number of variables – flaws, acceleration, etc. – from which the data is gathered is very large. Both largest and smallest extreme value distributions are applied in reliability engineering.

There are a number of different types of extreme value distributions. We confine our attention here to the type I or Gumbel distributions, the CDF and PDF, and mean and variance for the largest extreme value distribution[3]:

The PDF of the largest extreme value distribution is

$$f(x) = \frac{1}{\theta} e^{-(x-\mu)/\theta} \exp\left[-e^{-(x-\mu)/\theta}\right] \qquad -\infty < x < \infty \tag{5.26}$$

The CDF of the largest extreme value distribution is

$$F(x) = \exp\left[-e^{-(x-\mu)/\theta}\right] \qquad -\infty < x < \infty \tag{5.27}$$

Continuing, the mean and variance are:

$$\text{Mean of the Largest Extreme Distribution} = \mu + \gamma\theta = \mu + 0.57722\theta \tag{5.28}$$

where γ is Euler's constant = 0.57722.

$$\text{Variance of the Largest Extreme Distribution} = \frac{1}{6}\pi^2\theta^2 \tag{5.29}$$

The PDF for the largest and smallest extreme distributions are plotted in Figure 5.33. Note that they have long tails on the right and left, respectively.

Similar to the normal and lognormal distribution, a reduced variant can be defined, which simplifies the CDF. If we let $w = (x - \mu)/\theta$, then the CDF becomes

$$F_w(w) = \mathrm{e}^{-e^{-w}} \tag{5.30}$$

This explains why type I extreme value distributions are frequently referred to as "double exponential" distributions.

The largest extreme value distribution often works well in combining loads on a system when it is the maximum load that determines whether the system will fail. Suppose that $x_1, x_2, x_3,..., x_N$ are the magnitudes of the individual loads, and let y denote the maximum of these loads. To determine the probability that Y will not exceed some specified value y, we may write

$$P\{Y \le y\} = P\{x_1 \le y \cap x_2 \le y \cap x_3 \le y \cap \cdots \cap x_N \le y\}$$

If the magnitudes of the successive loads are independent of one another, this expression simplifies to

$$P\{Y \le y\} = P\{x_1 \le y\}P\{x_2 \le y\}P\{x_3 \le y\} \cdots P\{x_N \le y\}$$

3 Largest extreme value mathematics (Gumbel 1958).

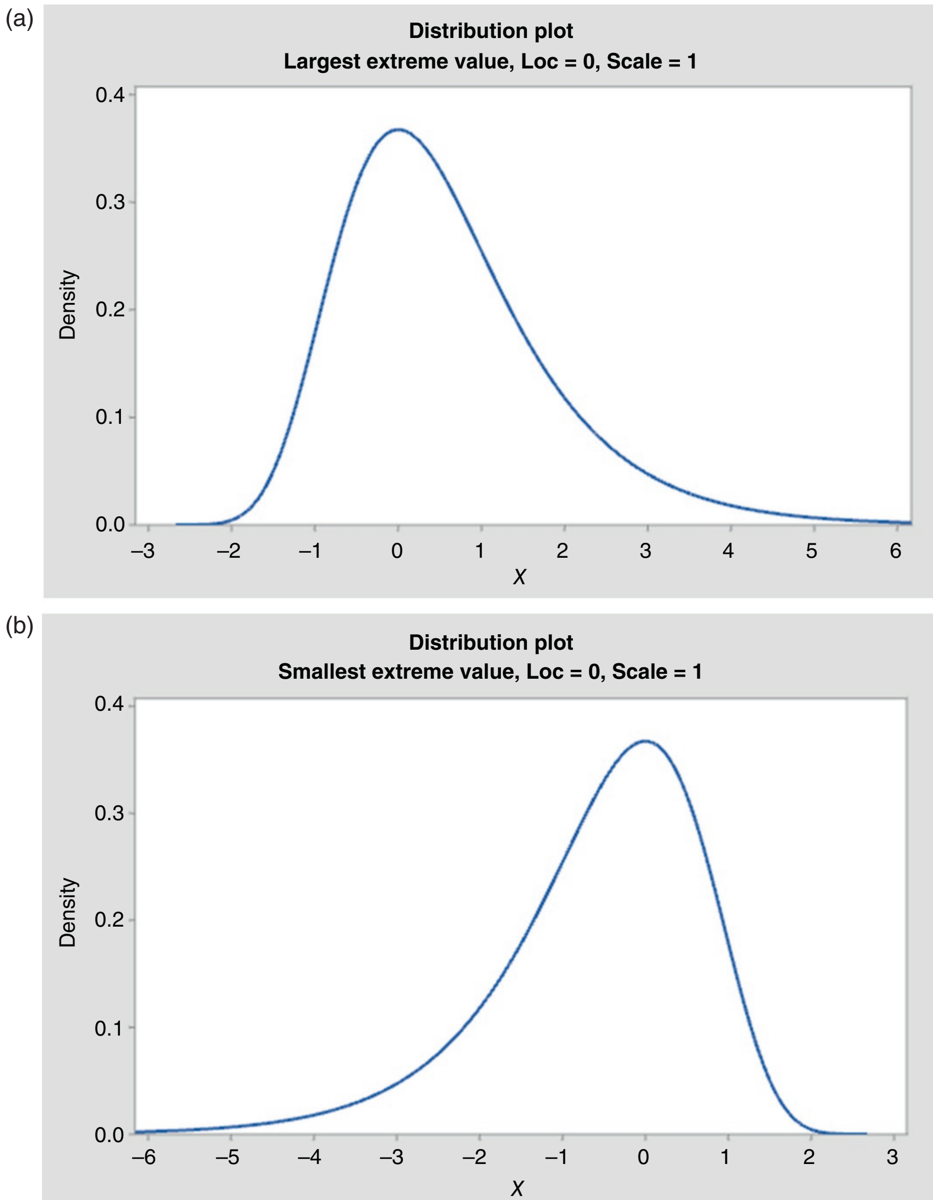


Figure 5.33 Extreme value probability density functions (E.J. Gumbel op. cit.). (a) Largest extreme value PDF. (b) Smallest extreme value PDF.

We also note that each of these probabilities is a CDF. Thus, if the loads are identically distributed, we may rewrite this equation as

$$F_Y(y) = [F_x(y)]^N \tag{5.31}$$

Now, assume that the CDF for each loading is the largest extreme value distribution. We then have

$$F_Y(y) = \left\{ \exp\left[-e^{-(y-\mu)/\theta} \right] \right\}^N = \exp\left[-Ne^{-(y-\mu)/\theta} \right] \tag{5.32}$$

The CDF for y can be written as a single extreme value distribution:

$$F_Y(y) = \exp\left[-e^{-(y-\mu')/\theta}\right] \tag{5.33}$$

where the displacement parameter has been increased to a value of

$$u' = u + \theta \ln(N) \tag{5.34}$$

and θ remains unchanged.

See Appendix D – Nonparametric Methods and Probability Plotting – Extreme value distribution (smallest and largest) for details of how extreme value distribution probability plots are generated.

We are often interested in extreme values of a parameter (maximum strength, maximum impinging force, maximum change in a stock price, and maximum pit depth due to corrosion) because they are the values that determine whether a system will potentially fail: for example wind strengths impinging on a building – it must be designed to sustain the maximum wind with smallest damage within the bounds of the finances available to build it; maximum wave height for designing offshore platforms, breakwaters, and dikes; pollution emissions for a factory to ensure that, at its maximum, it will fall below the legal limit; determining the strength of a chain, since it is equal to the strength of its weakest link; and modeling the extremes of meteorological events since these cause the greatest impact.

Example 5.13 Modeling pit depths in steel tanks

The maximum pit depth values (in mm) of steel tanks exposed to cyclic dry/wet conditions were measured after 4, 6, and 12 years of service to determine the corrosion life of the tanks before they failed (data from Kowaka et al. 1995)[4]. See Table 5.11 (Figure 5.34).

Using this plot the probability of having a pit depth > 2.65 mm is ~0.01 (or 1/100) (Figure 5.35).

A summary of results is in Table 5.12.

Table 5.11 Maximum pit depths (mm) of steel tanks.

4 Years	0.3	0.7	0.7	0.7	0.7	0.7	0.7	0.8	0.8	0.8
	0.8	0.8	0.9	0.9	0.9	0.9	1	1	1	1
	1.1	1.1	1.1	1.1	1.1	1.2	1.2	1.2	1.2	1.3
	1.3	1.3	1.3	1.3	1.4	1.4	1.4	1.4	1.4	1.5
	1.5	1.6	1.6	1.6	1.6	1.6	2	2.1	2.3	2.5
6 Years	1	1.1	1.1	1.2	1.2	1.2	1.3	1.3	1.3	1.3
	1.4	1.4	1.5	1.5	1.5	1.6	1.7	1.7	1.9	1.9
	1.9	2	2.3	2.3	2.7					
12 Years	0.8	0.8	0.8	1	1	1	1	1.1	1.4	1.5
	1.5	1.6	1.8	1.9	2.1	2.1	2.2	2.3	2.4	
	3.1	3.2	3.3	3.8	3.8	3.9	4.4	5	5	

Source: Data from Kowaka et al. (1995).

4 Kowaka et al. (1995). Creative commons.

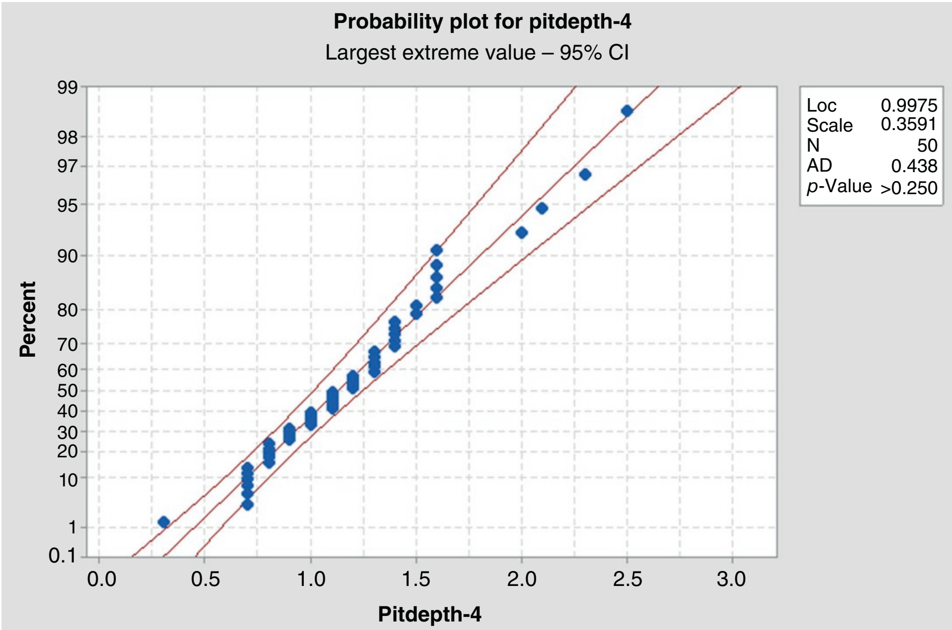


Figure 5.34 Using the 4-year data, generating a largest extreme value plot in **MINITAB**.

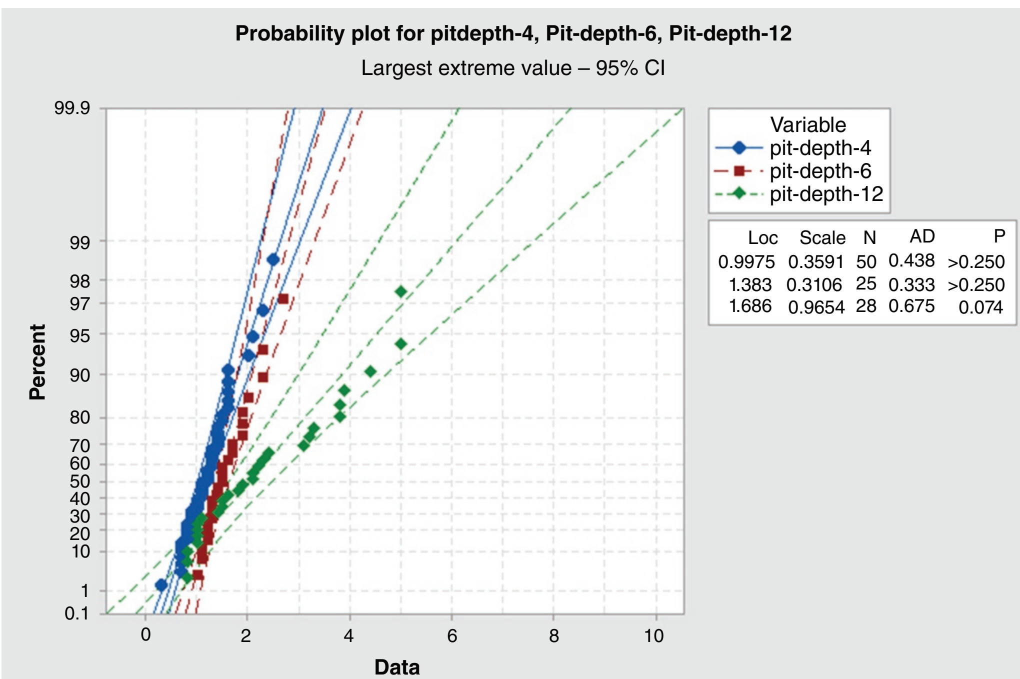


Figure 5.35 Comparing 4-, 6-, and 12-year data together to see the changes in maximum predicted pit depth.

Table 5.12 Summary of expected and upper 95% bound of pit depths vs years.

	Probability = 0.001 of a pit depth	
	Expected (mm)	Upper 95% bound (mm)
After 4 years	3.5	4
After 6 years	3.5	4.3
After 12 years	8.4	10.6

With this information, the materials engineers can calculate the probability of a leak and/or failure of the storage tanks.

Example 5.14 Modeling extreme earthquake magnitudes worldwide 1900–2014
Data is from USGS database of deaths caused directly by earthquakes magnitude 6.8 and higher from 1900 to 2014 earthquake (deaths from factors such as mudslides took deaths over 1000).

Using the largest extreme value distribution, see Figure 5.36.

Interestingly enough, if you use the data of *all recorded Tsunami-causing earthquakes* (227 BC to 2013 AD), a Weibull distribution fits best. This was after trying the largest extreme value distribution first (see Figure 5.37).

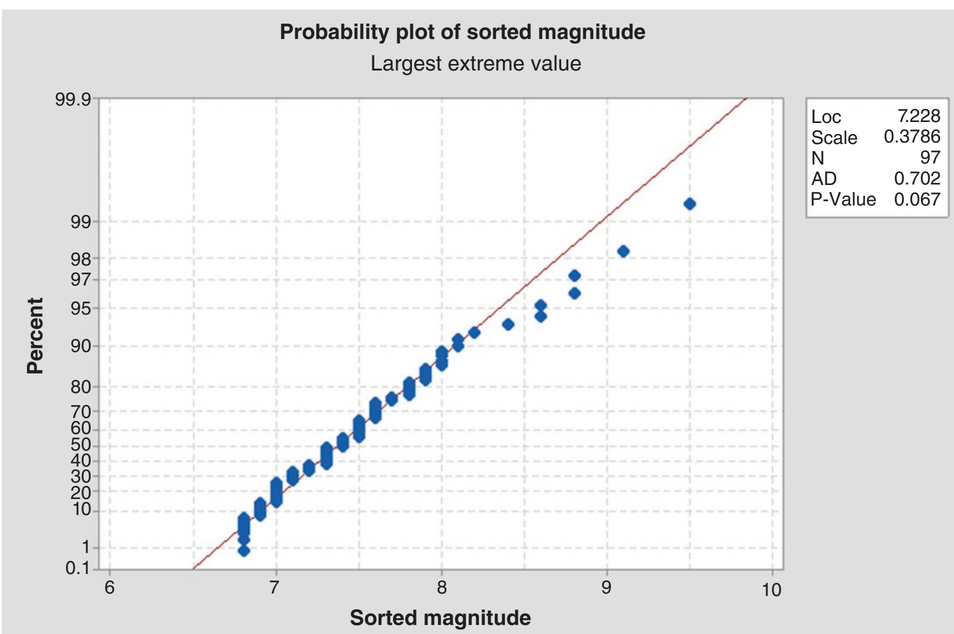


Figure 5.36 Magnitude >6.8 earthquakes since 1900 show probability = 0.008 of earthquake as large as 9.5.

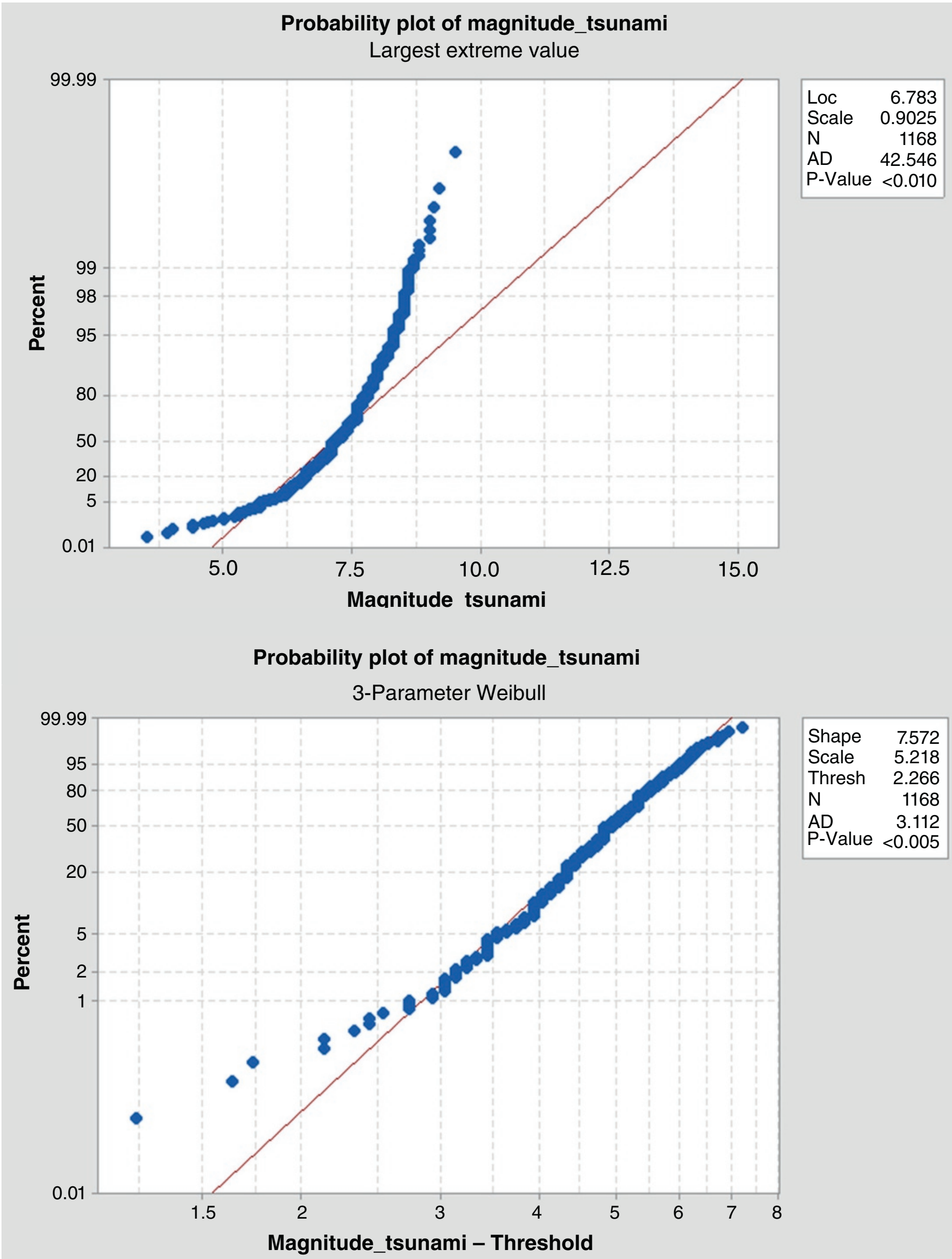


Figure 5.37 Obviously, the largest extreme value *does not fit* the data well. Using a three-parameter Weibull, one would expect less than 1 in 10,000 to surpass magnitude 7.5. The lower tail (from magnitude 3 on down) could be due to not having all the data; quite possible for magnitudes <3. So, this is a case of the largest extreme value distribution not fitting the data as well as the three-parameter Weibull. The lesson learned: try to fit with the distribution that "might" be best and then go back to the Weibull (or use the "Distribution ID" in Appendix D).

The largest extreme value distribution models a Gumbel distribution for the largest extreme. The Smallest extreme distribution, for a variable that has an exponential family lower tail, is given by the complementary smallest extreme value distribution.

The extreme value distributions are asymptotic results, meaning that the probability distribution of the maximum of a set of independent values drawn from some distribution approaches the extreme value distributions only as sample size (n) approaches infinity.

The smallest extreme value distribution is sometimes used as an alternative to the Weibull in describing strength distributions and related phenomena (particularly when the Weibull does not seem to fit the data). The CDF and PDF for the corresponding smallest extreme value distribution are[5]

The PDF of the smallest extreme value distribution is

$$f(x) = \frac{1}{\theta} e^{(x-\mu)/\theta} \exp\left[-e^{(x-\mu)/\theta}\right] \qquad -\infty < x < \infty \tag{5.35}$$

The CDF of the smallest extreme value distribution is

$$F(x) = 1 - \exp\left[-e^{(x-\mu)/\theta}\right] \qquad -\infty < x < \infty \tag{5.36}$$

Continuing, the mean and variance are:

$$\text{Mean of the Smallest Extreme Distribution} = \mu - \gamma\theta = \mu - 0.57722\theta \tag{5.37}$$

where γ is Euler's constant = 0.57722.

$$\text{Variance of the Smallest Extreme Distribution} = \frac{1}{6}\pi^2\theta^2 \tag{5.38}$$

The smallest extreme value PDF is plotted in Figure 5.33b.

It is noteworthy that the smallest extreme value distribution is closely related to the Weibull distribution, and as a result, it is often used for similar distributions such as representing distributions of times to failure. If we let

$$x = \ln(y) \tag{5.39}$$

then the foregoing equations in x for the smallest extreme value distribution reduce to a Weibull distribution in y; the Weibull parameters are given in terms of those for the extreme value distribution by

$$\eta = e^{\mu} \tag{5.40}$$

and

$$\beta = 1/\theta \tag{5.41}$$

Thus, the Weibull distribution has the same relationship to the smallest extreme value distribution as the lognormal has to the normal: In both cases they are related by $x = \ln(y)$, and in the first, the domain of the random variable is $-\infty < x < \infty$, while in the second it is $0 < y < \infty$.

5 Smallest Extreme Value Mathematics (Gumbel 1958).

Table 5.13 Annual minimum temperature by year at Ft Collins, CO, 1895–2019.

Year	Annual min temp	Year	Annual min temp	Year	Annual min temp	Year	Annual min temp	Year	Annual min temp
1895	−28	1920	−12	1945	−21	1970	−9	1995	−10
1896	−11	1921	−12	1946	−13	1971	−20	1996	−18
1897	−26	1922	−27	1947	−17	1972	−18	1997	−10
1898	−22	1923	−21	1948	−32	1973	−5	1998	−13
1899	−38	1924	−30	1949	−28	1974	−11	1999	5
1900	−23	1925	−15	1950	−19	1975	−7	2000	0
1901	−31	1926	−18	1951	−41	1976	−8	2001	−3
1902	−31	1927	−16	1952	−14	1977	−9	2002	−6
1903	−28	1928	−16	1953	−10	1978	−16	2003	−3
1904	−7	1929	−22	1954	−17	1979	−15	2004	−8
1905	−27	1930	−38	1955	−19	1980	−14	2005	−10
1906	−25	1931	−3	1956	−23	1981	−14	2006	−11
1907	−5	1932	−30	1957	−13	1982	−17	2007	−8
1908	−15	1933	−31	1958	−12	1983	−16	2008	−11
1909	−19	1934	−2	1959	−25	1984	−28	2009	−15
1910	−21	1935	−25	1960	−20	1985	−15	2010	−10
1911	−18	1936	−31	1961	−22	1986	−6	2011	−13
1912	−16	1937	−26	1962	−32	1987	−8	2012	−1
1913	−30	1938	−11	1963	−25	1988	−8	2013	−8
1914	−18	1939	−10	1964	−15	1989	−22	2014	−16
1915	−14	1940	−21	1965	−10	1990	−24	2015	−3
1916	−24	1941	−14	1966	−14	1991	−2	2016	−9
1917	−18	1942	−30	1967	−9	1992	−2	2017	−16
1918	−21	1943	−31	1968	−10	1993	−7	2018	−3
1919	−35	1944	−13	1969	−4	1994	−6	2019	−9

Source: Data from Western Regional Climate Center of the Desert Research Institute.

Example 5.15 In a study of the minimum annual temperature at Ft Collins, CO, to help in determining electrical output requirements for local power stations, the following data were obtained (see Table 5.13).

(data from Western Regional Climate Center of the Desert Research Institute, https://wrcc.dri.edu/)

Plotting this data as a smallest extreme value distribution gave Figure 5.38. Over this 125-year period the minimum temperature was −41 °F. Looking at the "break" in the data at ~−30 °F and extrapolating the fit to follow the trend downward temperature data "tail" suggests that the probability of −50 °F is <1/1000. One can postulate many reasons for the dogleg bend in this data, one of which is failure to report colder temps than −30 deg F because of limited instrumentation.

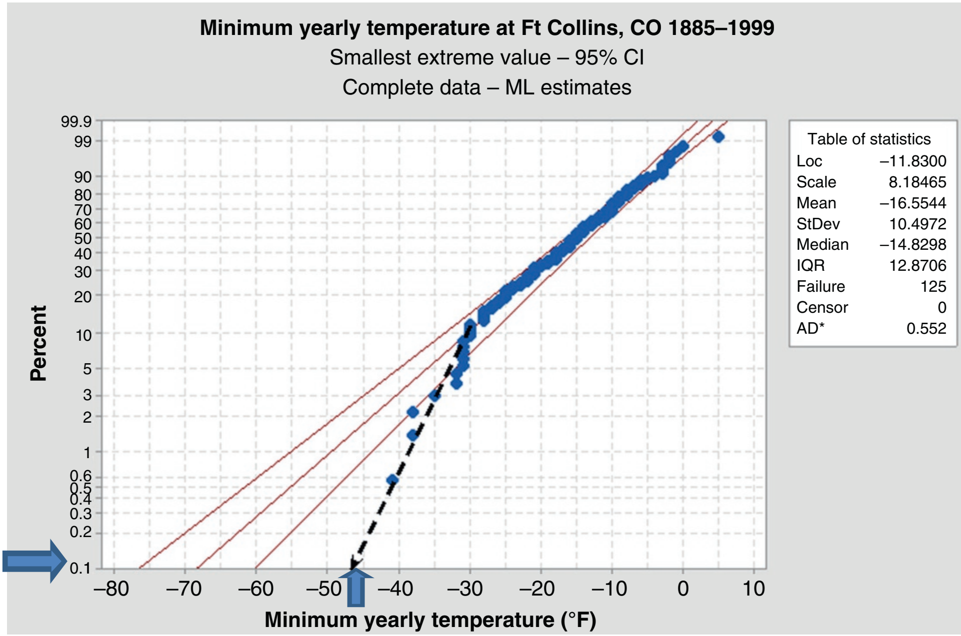


Figure 5.38 Extreme value plot of minimum yearly temperature data.

5.4 Introduction to Risk Analysis

One of the major uses of Weibull analysis is to predict the number of occurrences of a failure mode as a function of time. This projection is important because it gives the management a clear view of the potential magnitude of a problem. In addition, if this prediction is made for different failure modes, the management is able to set the priority for the solution of each problem.

In this section, the use of the Weibull and largest/smallest extreme value probability distribution functions in predicting the occurrences of a failure mode is explained.

The additional input needed for risk analysis will be covered, and several examples are presented to explain further the techniques involved. It should be emphasized that the forecast analysis is only as good as the failure data. The data should be examined closely to ensure that they are from a single failure mode and will fit a Weibull distribution or extreme value distribution.

A risk analysis calculates the number of incidents projected to occur over some future period.

The observed failures and the population of units that have not failed are used to obtain the failure distribution, as discussed in Sections 5.1–5.3. The following additional input is needed for forecasting: (i) usage rate per unit per month (or year, day, etc.) and (ii) introduction rate of new units (if they are subject to this same failure mode).

With this information, a risk analysis can be produced. The techniques used to produce the risk analysis can vary from simple calculations to those involving Monte Carlo simulation. Monte Carlo simulation is required when complications arise in the risk analysis. These will be explained further in Chapter 11.

Risk Analysis "Mathematics"

Calculating risk is a simple application of conditional probability:

Let X = random variable, representing the number of failures observed in some risk period, in **n** engines (X is a discrete random variable, taking on values 0, Assuming **no** replacement of failed parts with similar parts with the same life distribution F:

$$X = \sum_{i=1}^{n} X_i \text{ where } X_i = \begin{cases} 1 \text{ if engine } i \text{ fails during risk period} \\ 0 \text{ if it does not} \end{cases} \tag{5.42}$$

Now, by definition, risk = $E(X)$ and

$$\begin{aligned}
E(X) &= \sum_{1}^{n} E(X_i) \\
&= \sum_{1}^{n} \{1 \cdot P(X_i = 1) + 0 \cdot P(X_i = 0)\} \\
&= \sum_{1}^{n} P(X_i = 1) \\
&= \sum_{1}^{n} P(\text{engine } i \text{ fails in next } \Delta_i \text{ cycles, given it has reached age } c_i) \\
&\quad \text{which, by the definition of Conditional Probability,} \\
&= \sum_{1}^{n} P(\text{engine } i \text{ fails in next } \Delta_i \text{ cycles}) \cap P(\text{engine } i \text{ has reached age } c_i)/P(\text{engine } i \text{ has reached age } c_i) \\
&= \sum_{1}^{n} \frac{F(c_i + \Delta_i) - F(c_i)}{1 - F(c_i)}
\end{aligned} \tag{5.43}$$

where $F(t)$ is the CDF of the failure distribution, e.g. $F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}}$ for the Weibull.

Example 5.16 Risk analysis using Weibull distributions, no remedial action

A simple risk analysis, using the following input:

A Weibull failure mode whose $\beta = 3.0$ and $\eta = 10{,}000$ hours,

A population of 50 units, 10 each with times 1000, 2000, 3000, 4000, and 5000 hours.

Three failures have occurred to date.

25 hours/month are placed on each unit

What is the risk after 6 months?

Setting this up in EXCEL yields Table 5.14.

Table 5.14 Simple risk analysis in EXCEL.

No. engines	Time = Now	F (now time)	F(t + 150)	(F(t + 150) – F(t))/(1 – F(t))	Expected failures now	Expected failures in 6 months	Expected cumulative failure in 6 months
10	1000	0.0009995	0.0015197	0.000521	0.009995	0.005207	0.015202
10	2000	0.00796809	0.0098892	0.001936	0.079681	0.019365	0.099046
10	3000	0.02663876	0.0307725	0.004247	0.266388	0.042468	0.308856
10	4000	0.061995	0.0689789	0.007446	0.619950	0.074455	0.694405
10	5000	0.1175031	0.127673	0.011524	1.175031	0.115240	1.290271
				Sum=	2.151044	0.256735	2.407780

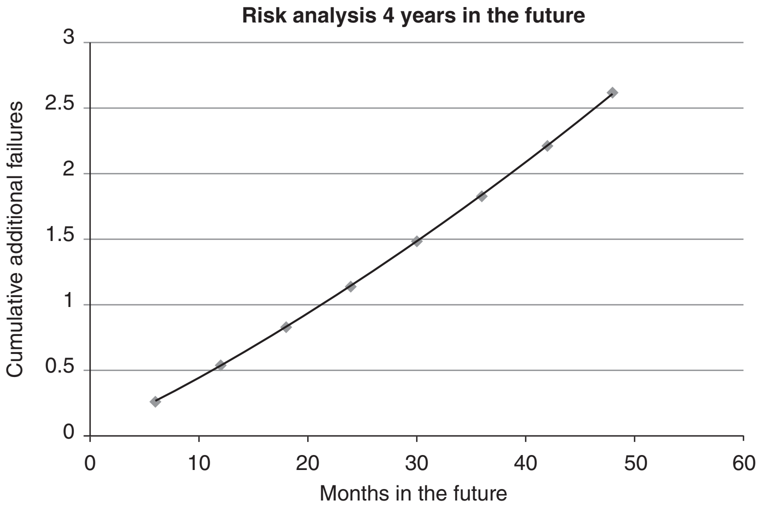


Figure 5.39 Risk analysis 4 years in the future. Risk projection is based on the given Weibull and assumes that no fixes are introduced into the fleet. In looking at this risk plot, the program or project manager would probably choose 18 months to have a fix in the operating fleet. Why? The expected number of failure is less than 1 up to approximately 18 months.

You had three failures to date; based on the calculation, the risk analysis predicted that you should have had 2.15 failures to date and an additional 0.26 failures in the next 6 months. If you redid this risk for 12, 18, 24, 30, 36, 42, and 48 months, you would have Figure 5.39.

Now, suppose that the project manager asked for a 6-month projection ONLY.

Based on Table 5.14, the expected number of additional failure is 0.26.

The project manager looks at that number and asks, " Well, is that 0 or 1 failure?"

A better way to explain the expected risk when it is <1.0 is to convert that expected risk to the probability of 1 or more future failures. This can be accomplished using a Thorndike chart [developed by Frances Thorndike at Bell Labs in 1926 (Thorndike 1926)]. See Chapter 2 – Poisson Distribution – for more details.

The risk analysis predicted 0.26 additional failures after 6 month of fleet activity. However, the chance of having one or more failure in that 6-month period = 0.23 or approximately 1 chance in 4. In cases like this, the Thorndike chart (Figure 5.40) is a "visual" that goes over well in presenting the results to the management.

Example 5.17 Weibull risk analysis example with fleet inspections[6]
Bearing cage fracture times of 230, 334, 423, 990, 1009, and 1510 hours were observed. The population of bearings within which the failures occurred is shown in Figure 5.41.

6 Abernethy et al. (1983).

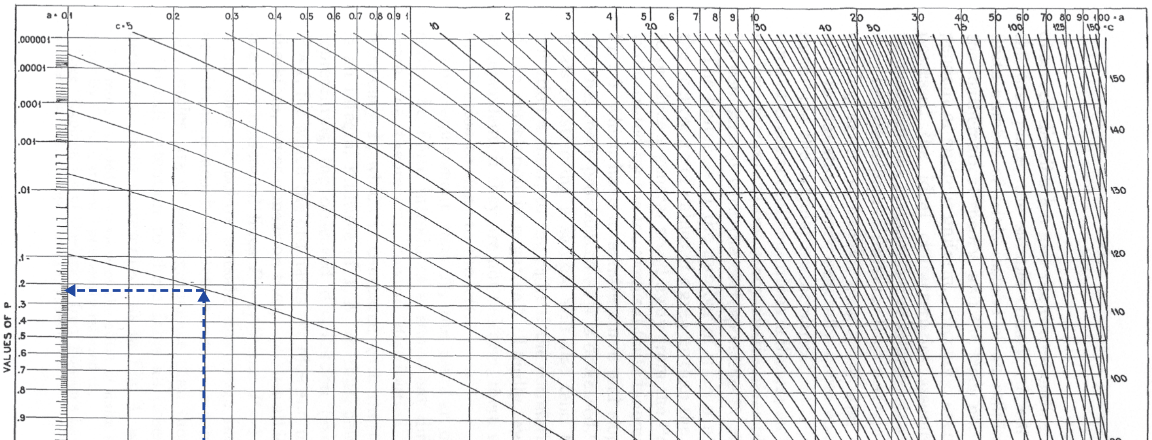


Fig. 5—Probability curves showing Poisson's exponential summation

Figure 5.40 Thorndike chart (see Chapter 2) explanation of risk analysis results for customer presentation. *Source*: Thorndike (1926). Reused with permission of Nokia Corporation and AT&T Archives.

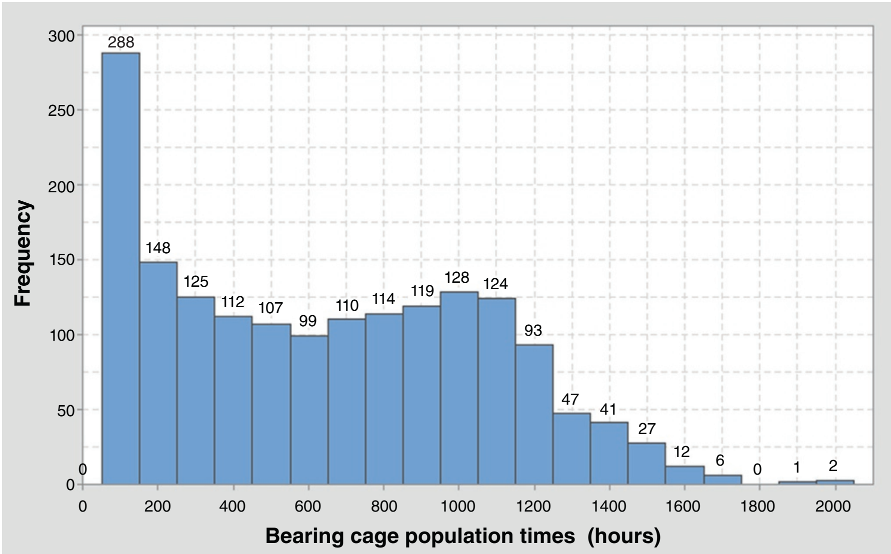


Figure 5.41 Histogram of bearing cage population. Sample size = 1703, including six failures.

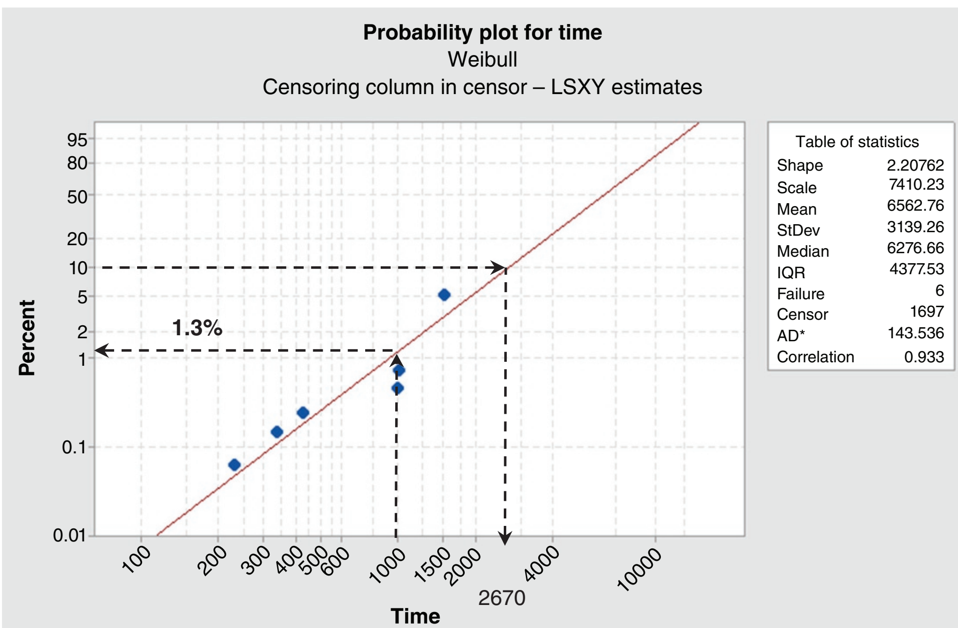


Figure 5.42 Weibull plot of bearing cage fracture.

a) A Weibull plot using the six failures and the histogram of the population by assuming the time of each histogram bar is at the midpoint was completed.
b) The Weibull plot will show that the B10 life (time at which 10% of the population will have failed) is approximately 2670 hours (see Figure 5.42).

Table 5.15 Tabular form of bearing cage population histogram.

Time	Censor	Freq
100	0	288
200	0	147
230	1	1
300	0	124
334	1	1
400	0	111
423	1	1
500	0	107
600	0	99
700	0	110
800	0	114
900	0	119
990	1	1
1000	0	126
1009	1	1
1100	0	124
1200	0	93
1300	0	47
1400	0	41
1500	0	26
1510	1	1
1600	0	12
1700	0	6
1800	0	0
1900	0	1
2000	0	2

This is much less than the B10 design life of 8000 hours, so a redesign was undertaken.

Additionally, the management wanted to know how many failures would be observed before this redesign entered the field, based on inspecting the bearings at various intervals.

The histogram represents the times on the entire population. The center of each histogram bar along with its count of bearing cages is put in the table. Note that each histogram bar is ± 50 around the center value of the bar. The number of failures are subtracted from the freq (e.g. failure at 230 hours is in the 200 ± 50 bar, so the original 148 is reduced to 147, and the failure point at 230 is added below). Note that the censor is changed to "1" for 230 to indicate a failure at that time. This same process is followed for the other five failures. Thus, the population of suspensions/ unfailed units is 1697, and the number of failures is 6 for a total population of 1703.

Table 5.15 can then be copied into **MINITAB**, and a Weibull plot of the failure mode is produced (Figure 5.42).

Risk questions and solutions:

1) How many failures could be expected by the time units had reached 1000 hours?
   Solution: Assuming failed units are not replaced, go into the Weibull x-axis at 1000 hours up to the Weibull fit line and across to the Y-axis… and find that ~1.3% of the population is expected to fail by 1000 hours. So, after all 1703 of the population have gone through 1000 hours, $0.013 \times 1703 = 22$ bearings would be expected to have failed.
2) How many failures could be expected when 4000 hours had been accumulated on each bearing if we instituted a 1000-hour inspection? A 2000-hour inspection?
   Solution: From the above, the probability of a bearing failure by 1000 hours is 0.013.
   Therefore, assuming that a 1000-hour inspection makes a bearing "good as new" in terms of cage fracture, there is a total expectation of failure for each bearing by 4000 hours of $0.013 + 0.013 + 0.013 + 0.013 = 0.052$. For 1703 bearings who have an inspection every 1000 hours and run to 4000 hours that would mean $0.052 \times 1703 = 89$ failed bearings.
   For a 2000-hour inspection, the probability by 2000 hours is 0.06. Therefore, by 4000 hours with an inspection every 2000 hours, every bearing would have the expectation of $0.058 + 0.058 = 0.116$ of failing. So, the number of failures in the bearing population with a 2000-hour inspection is $0.116 \times 1703 = 198$.
   Going one step further, suppose that *no* inspections were made and the bearings were retired at 4000 hours. The probability of failure at 4000 hours is 0.25. So, by not inspecting but retiring the bearings at 4000 hours, the expected number of bearing failures is $0.24 \times 1703 = 409$.

These answers would give the project management sufficient information to make a decision on inspecting and at what interval or possibly not doing inspections. Of course, the customer impact has to be considered in these decisions.

Bibliography

Abernethy, R.B. (2006). *The New Weibull Handbook*, Chapters 1–3, 5e.

Abernethy, R.B., Breneman, J.E., Medlin, C.H., and Reinman, G.L. (1983). *USAF Weibull Analysis Handbook*, AFWAL-TR-83-2079. Ohio: Air Force Systems Command, USAF, Wright-Patterson AFB.

Ang, A.H.-S. and Tang, W.H. (1985). *Probability Concepts in Engineering Planning and Design-Decision, Risk & Reliability*, vol. **2**. New York: Wiley.

Gumbel, E. (1958). *Statistics of Extremes*. New York: Columbia University Press.

Johnson, L.G. (1965). *The Statistical Treatment of Fatigue Experiments*. Amsterdam, The Netherlands: Elsevier Publishing Co.

Kalbfleisch, J.D. and Prentice, R. (1980). *The Statistical Analysis of Failure Time Data*. Wiley.

Kowaka, M., Tsuge, H., Akashi, M. et al. (1995). Introduction to life prediction of industrial plant materials (application of the extreme value method for corrosion analysis). *Materials Science and Engineering Technology* **26(10)**: 519–572, fmi-A100.

Lapin, L.L. (1998). *Probability and Statistics for Modern Engineering*. Belmont, CA: Brooks/Cole.

Lee, E. (1992). *Statistical Methods for Survival Data Analysis*, 2e. Wiley.

Lieblen, J. and Zelen, M. (1956). Statistical investigation of the fatigue life of deep-grooved ball bearings. *Journal of Research of the National Bureau of Standards* **57** (5): 273.

Mendenhall, W. and Hader, R.J. (1958). Estimation of parameters of mixed exponential distribution failure times from censored life test data. *Biometrika* **63**: 449–464.

Montgomery, D.C. and Runger, G.C. (2018). *Applied Statistics and Probability for Engineers*. New York: Wiley.

Nelson, W. (1982). *Applied Life Data Analysis*. Wiley.

Olkin, I., Gieser, Z.J., and Derman, G. (2018). *Probability Models and Applications*. New York: Macmillan Co.

Pieruschka, E. (1963). *Principles of Reliability*. Englewood Cliffs, NJ: Prentice-Hall.

Pike, M.C. (1966). A method of survival analysis of a certain class of experiments in carcinogenesis. *Biometrics* **22**: 142–161.

Pochampally, K.K. and Gupta, S.M. (2016). *Reliability Analysis with MINITAB*. CRC Press.

Quinn, J.B. and Quinn, G.D. (2010). A practical and systematic review of Weibull statistics for reporting strengths of dental materials. *Dental Materials* **26**: 135–147.

Reiss, R.D. and Thomas, M. (2001). *Statistical Analysis of Extreme Values*, 2e. Birkhauser.

Paik, S., Shak, S., Tang, G. et al. (2004). A multigene assay to predict recurrence of tamoxifen-treated, node-negative breast cancer. *The New England Journal of Medicine* **351** (27): 2817–2826.

Thorndike, F. (1926). Applications of Poisson's probability summation. *Bell System Technical Journal* **5**: 604–625.

Vivek, B.L., Hendricks, R.C., and Zaretsky, E.V. (2013). Probabilistic Analysis for Comparing Fatigue Data Based on Johnson-Weibull Parameters. NASA/TP—2013-217633.

Weibull, W. (1939a). *A Statistical Theory of the Strength of Materials*. Ingeniörsvetenskapsakademiens Handlingar, Nr 151. Stockholm: Generalstabens Litografiska Anstalts Förlag.

Weibull, W. (1939b). *The Phenomenon of Rupture in Solids*. Ingeniörs Vetenskaps Akademien-Handlingar, Nr 153. Stockholm: Generalstabens Litografiska Anstalts Förlag.

Weibull, W. (1951). A statistical distribution function of wide applicability. *Transactions of the ASME, Journal of Applied Mechanics* **18** (3): 293–297.

Wingo, D.R. (1973). Solution of the three-parameter Weibull equations by constrained modified Quasilinearization (progressively censored samples). *IEEE Transactions on Reliability* **R-22**: 96–100.

Wormsen, A. and Härkegård, G. (2004). A statistical investigation of fatigue behaviour according to Weibull's Weakest Link Theory. Proceedings of the 15th European Conference of Fatigue-2004.

U.S. Dept of the Interior (n.d.). USGS database of Earthquakes. Datalink: https://www.usgs.gov/programs/earthquake-hazards/science/earthquake-data

U.S. Dept of the Interior (n.d.). Western Regional Climate Center, (https://wrcc.dri.edu) associated with National Centers for Environmental Information (NCEI), State Climate Offices, Regional Climate Centers (RCCs), USDI Climate Science Centers (CSCs), and NOAA Regional Integrated Sciences and Assessments (RISA)21.

Zhu, S.-P., Foletti, S., and Beretta, S. (2017). Evaluation of size effect in low cycle fatigue for Q&T rotor steel. 3rd International Symposium on Fatigue Design and Material Defects, FDMD 2017, 19–22 September 2017, Lecco, Italy.

Exercises

5.1 An engine bearing has a Weibull failure mode of $\beta = 2.0$ and $\eta = 1000$ hours.
a) What is the probability of failure in the first 500 hours?
b) What is the probability of failure in the second 500 hours?

5.2 Fatigue specimens were put on test. They were *all* tested to failure, and the failure times were 150, 85, 250, 240, 135, 200, 240, 150, 200, and 190 hours.
a) Construct a Weibull plot and determine its slope β and characteristic life η.
b) If you were quoting the B10 life, what would the value be?

5.3 There were live failures of a part in service. The information on these parts is

Serial number comm	Time (hours)	F/S
831	9	F
832	6	F
833	14.6	S
834	1.1	F
835	20	F
836	7	S
837	65	F
838	8	S

F, failure; S, suspension.

a) Construct a Weibull with suspensions included and determine its slope, β and characteristic life, η
b) What is the failure mode?
c) Are there other clues which may lead to an answer to the problem?

5.4 The following set of failure points will result in curved Weibull: 90, 130, 65, 220, 275, 370, 525, and 1200 hours. Plot on Weibull paper, or use your favorite software.
a) Is this Weibull good as is? Why not?
b) What value is needed to straighten the Weibull? Now, "Eyeball" a curve through the data and read an approximate to where it intersects the bottom scale. Is your “Eyeball close” to what the software calculated for t_0?
c) Is the t_0 found in "b" to be added or subtracted from the failure values?

5.5 *Source*: Data from Lieblen and Zelen (1956).
a) Generate a Weibull plot. Is the fit to the data good?
b) Does the Weibull β seem to justify “fatigue” ?
(Note: Through experience, bearings have Weibull βs from ~1.2 to ~2.8, depending on the application.)

Ball bearing endurance life (× 10^6 revolutions)	Censor
17.88	F
28.82	F
33	F
41.52	F
42.12	F
45.6	F
48.48	F
51.84	F
51.96	F
54.12	F
55.56	F
67.8	F
68.64	F
68.64	F
68.88	S
84.12	F
93.12	F
98.64	F
105.12	F
105.84	F
125.04	F
127.82	F
173.4	S

5.6 *Source*: Data from The Weibull Distribution, ReliaWiki.

19 "Widgets" were put on test, but due to production needs, some were withdrawn from the test before the last one failed; hence, those withdrawn had not failed and are "suspensions."

a) Generate a least squares Weibull plot, noting the β and η.
b) Generate a maximum-likelihood Weibull plot, also noting the β_{MLE} and η_{MLE}.
c) Compare the two Weibulls. What conclusions can you draw?

Data point	State (F/S)	Time to failure
1	F	2
2	S	3
3	F	5
4	S	7
5	F	11
6	S	13

Data point	State (F/S)	Time to failure
7	S	17
8	S	19
9	F	23
10	F	29
11	S	31
12	F	37
13	S	41
14	F	43
15	S	47
16	S	53
17	F	59
18	S	61
19	S	67

5.7 (*Source*: Data from Nelson (1982), p. 317) 70 diesel engine fans accumulated 344,440 hours in service and 12 of them failed. A table of their life data is shown next (+ denotes nonfailed units or suspensions, using Dr. Nelson's nomenclature). Evaluate the parameters with their two-sided 95% confidence bounds, using MLE for the two-parameter Weibull distribution.

Status	Failure time (h)	Status	Failure time (h)	Status	Failure time (h)	Status	Failure time (h)	Status	Failure time (h)
F	450	S	2030	S	4150	S	5000	S	8100
S	460	F	2070	S	4150	S	5000	S	8200
F	1150	F	2070	S	4150	S	6100	S	8500
F	1150	F	2080	S	4150	F	6100	S	8500
S	1560	S	2200	S	4300	S	6100	S	8500
F	1600	S	3000	S	4300	S	6100	S	8750
S	1660	S	3000	S	4300	S	6300	F	8750
S	1850	S	3000	S	4300	S	6450	S	8750
S	1850	S	3000	F	4600	S	6450	S	9400
S	1850	F	3100	S	4850	S	6700	S	9900
S	1850	S	3200	S	4850	S	7450	S	10100
S	1850	F	3450	S	4850	S	7800	S	10100
S	2030	S	3750	S	4850	S	7800	S	10100
S	2030	S	3750	S	5000	S	8100	S	11500

5.8 (*Source*: Data from Quinn and Quinn 2010)

Dental Porcelain 1 and Porcelain 2 are being stress tested.

Porcelain 1 and Porcelain 2 both had cross sections of 3 mm × 4 mm, and both were tested in 1/4-point, 4-point flexure. The Porcelain 2 test specimens were shorter than the Porcelain 1 test specimens, however, and were tested using shorter spans. Porcelain 2 was tested with a 20-mm outer span and 10-mm inner span.

The longer Porcelain 1 test specimens were tested with the same fixture design but with a 40-mm outer span and 20-mm inner span. The test results are in the table to the right. Each result is stress at fracture in MPa.

a) Do a side-by-side Weibull analysis of the Porcelain 1 and Porcelain 2 data, without confidence bands.
b) What are your conclusions looking at the Weibull plots?
c) Now repeat the side-by-side Weibulls but add 90% confidence bands, what are your conclusions now?

Porcelain 1	**Porcelain 2**
75	90.5
76	95
77.5	102
78	104
79	105.5
82	106
82.5	107
83	107.5
83.5	110
83.7	111
84	112
85	112.5
85.5	114
86	114.5
87	115
88	115
88.3	116
88.5	118
89.5	119
89.7	119.5
90	119.5
90.2	119.5
91	120
92	120.5
93	123

5.9 Coil failure consists of failures of *twin* coils in motors. If a motor has a failure, the coil data consists of the failure time of one coil followed by an equal running time for the other coil as a suspension.
a) Produce a ranked regression Weibull.
b) What is the slope of the Weibull line?
c) What type of failure mode is indicated?

Times	F/S	Times	F/S
1175	F	1665	F
1175	S	1665	S
1521	F	1713	F
1521	S	1713	S
1569	F	1761	F
1569	S	1761	S
1617	F	1881	F
1617	S	1881	S
1665	F	1953	F
1665	S	1953	S

5.10 Looking at the Weibull plot from Problem 5.9, the lowest set of coils was determined to be an outlier. Redo the Weibull analysis and then determine if any further analysis should be done.

5.11 The data below, from Pike (1966), give the times from insult with the carcinogen DMBA to mortality from vaginal cancer in rats. Two groups were distinguished by a pretreatment regime. (The times are in days);
Group 1:
143, 164, 188, 188, 190, 192, 206, 209, 213, 216, 220, 227, 230, 234, 246, 265, 304, 216+, 244 +
Group 2:
142, 156, 163, 198, 205, 232, 232, 233, 233, 233, 233, 239, 240, 261, 280, 280, 296, 296, 323. 204+, 344 +
+Censored
Compare the result of the treatment on Group 1 to the treatment on Group 2. (Use 90% confidence and MLE estimation for your Weibulls.)

5.12 Leukemia remission data, *Source*: Data from Paik et al. (2004):

Group 1	Censor 1	Group 2	Censor 2
6	F	1	F
6	F	1	F
6	F	2	F
7	F	2	F

(*Continued*)

Group 1	Censor 1	Group 2	Censor 2
10	F	3	F
13	F	4	F
16	F	4	F
22	F	5	F
23	F	5	F
6	S	8	F
9	S	8	F
10	S	8	F
11	S	8	F
17	S	11	F
19	S	11	F
20	S	12	F
25	S	12	F
32	S	15	F
32	S	17	F
35	S	22	F
35	S	23	F

Analyze whether there is a significant difference between Group 1 and Group 2 treatments.

5.13 Ten failures are noted in the field out of a population of 2000. The 10 failures times are: 51, 79, 116, 164, 197, 230, 232, 327, 414, and 451 hours. Generate a Weibull distribution that best represents the total population.

5.14 The remission times of 42 patients (21 given an experimental chemo, and 21 given a placebo) in a randomized clinical trial[7]. Analyze this data assuming that a Weibull distribution fits both the distributions. Is there a significant difference between the chemo group and the placebo group? (In this data, 0 = censored, 1 = failure)

Remission times for chemo patients			
Chemo	**Censor 1**	**Placebo**	**Censor 2**
6	1	1	1
6	1	1	1
6	1	2	1
7	1	2	1
10	1	3	1
13	1	4	1

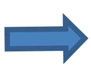
7 *Source*: Data from Lee (1992).

Remission times for chemo patients			
Chemo	**Censor 1**	**Placebo**	**Censor 2**
16	1	4	1
22	1	5	1
23	1	5	1
6	0	8	1
9	0	8	1
10	0	8	1
11	0	8	1
17	0	11	1
19	0	11	1
20	0	12	1
25	0	12	1
32	0	15	1
32	0	17	1
34	0	22	1
35	0	23	1

5.15 A component has the following failures: 30, 49, 82, 90, and 96 hours and suspensions at 10, 45, and100 hours.

a) Generate an MLE Weibull of this data
b) 10 units have entered the field in the past two months with times: What is the expected number of units predicted over the next 5 months?

Unit	Hours
1	25
2	33
3	40
4	45
5	50
6	60
7	64
8	75
9	80
10	99



5.16 Using Eqs. (4.15) and (4.16) to verify that (a) the mean of the Weibull is Eq. (5.3) and (b) the variance of the Weibull is Eq. (5.4).

$$\text{Hint: Use } \Gamma(a) = \int_0^\infty x^{a-1} e^{-x} dx$$

5.17 What fractions of items tested are expected to last more than 1 MTTF if the distribution of times to failure is

a) exponential,
b) normal,
c) lognormal with $\omega = 2$,
d) Weibull with $\beta = 2$.

5.18 The reliability for the Rayleigh distribution (a Weibull distribution with $\beta = 2$) is

$$R(t) = e^{-(t/\eta)^2}.$$

Find the MTTF in terms of η.

5.19 A failure PDF for an appliance is assumed to be a Weibull distribution with $\beta = 4.622$ and $\eta = 5.44$ years. What is the design life at:

a) a reliability of 90%,
b) a reliability of 99%.

5.20 A designer assumes a 90% probability that a new piece of machinery will fail at some time between 2 years and 10 years.

a) Fit a Weibull distribution to this belief.
b) What is the MTTF?

5.21 The life of a rocker arm is assumed to be 4 million cycles. This is known to a factor of 2 with 0.90 probability. If the reliability is to be 0.95, how many cycles should the design life be? (assume lognormal distributed).

5.22 Two components have the same MTTF; the first has a constant failure rate λ_0, and the second follows a Rayleigh distribution (a Weibull distribution with $\beta = 2$), for which

$$\int_0^t \lambda(t')\,dt' = \left(\frac{t}{\eta}\right)^2$$

a) Find η in terms of λ_0.
b) If for each component the design-life reliability must be 0.9, how much longer (in percentage) is the design life of the second (Rayleigh) component?

5.23 Consider the two components in Exercise 5.22.

a) For what design-life reliability are the design lives of the two components equal?
b) On the same graph, plot reliability versus time for the two components.

5.24 The two-parameter Weibull distribution with $\beta = 2$ is known as the Rayleigh distribution. For a nonredundant system made of N components, each described by the same Rayleigh distribution, find the system MTTF in terms of N and the component η.

5.25 Suppose that the reliability of a single unit is given by a Weibull distribution with $\beta = 2$. Use Eq. (3.103) to show that a standby system consisting of two such units has a reliability of

$$R_s(t) = e^{-(t/\eta)^2} + \sqrt{2\pi}(t/\eta)\mathrm{erf}\left(\sqrt{1/2}t/\eta\right)e^{-\frac{1}{2}(t/\eta)^2}$$

where the error function is defined by

$$\mathrm{erf}(y) = \frac{1}{\sqrt{\pi}}\int_0^y e^{-x^2}dx.$$

5.26 Suppose that two identical units are placed in active parallel. Each has a Weibull distribution with known η and $\beta > 1$.
a) Determine the system reliability.
b) Find a rare-event approximation for a.

5.27 Suppose that the units in Exercise 5.26 each have a Weibull distribution with $\beta = 2$. By how much is the MTTF increased by putting them in parallel?

5.28 The B10 life (sometimes called L10) of a bearing is the life of the bearing at which 10% failures may be expected. A new bearing design follows a Weibull distribution with $\beta = 2$, and an L10 of one year. (a) What fraction of the bearings would you expect to fail in six months? (b) If you had to guarantee no more than 1% failures, to what length of time would you limit the design life?

5.29 One-inch-long ceramic fibers are known to have a strength given by a Weibull distribution with a scale parameter of 8 lb and a shape parameter of 7.0. Assume the weakest link theory.
a) What will the scale and shape parameters be for fibers that are 2-in. long?
b) If 1.0% of the 1-in. fiber breaks under the stress of a particular application, what fraction of the 2-in. fibers would you expect to break under the same stress?

5.30 The distribution of detectable flaw sizes in tubing is given by

$$F(x) = 1 - e^{-x/\eta}, \quad 0 \le x \le \infty$$

with $\eta = 1/17$ cm. There are an average of three detectable flaws per centimeter of tubing.
a) What fraction of the flaws will have a size larger than 0.8 cm?
b) What is the probability of finding a flaw larger than 0.8 cm in a 100-m length of tubing?
c) In 1000 m of tubing?

5.31 Suppose that a system contains 12 of the bearings from Exercise 5.28 and the system fails with the failure of the first bearing failure. Estimate the system L_{10}.

5.32 The following failure time data were collected: 5.2, 6.8, 11.2, 16.8, 17.8, 19.6, 23.4, 25.4, 32.0, and 44.8 minutes. Make a probability plot and estimate β and η. Does it appear to be exponential?

5.33 The Mechanical Design Chief has just stopped at your desk and asked: "What would be the Weibull slope of a material that had a B50 to B.1 ratio of ~6.5?" What would you tell him?

5.34 Electronic module failures have occurred in the field:

1,100	13,489	33,180	50,545	98,674
6,697	16,818	35,367	60,280	101,702
8,238	23,885	39,703	67,084	102,829
9,766	24,323	49,412	70,740	158,880
10,455	27,987	49,729	76,039	206,640

What type of failure mode is this? And what is the MTTF?

5.35 Grouped suspension MLE example
Source: Data from Wingo (1973).

Wingo uses the following times to failure: 37, 55, 64, 72, 74, 87, 88, 89, 91, 92, 94, 95, 97, 98, 100, 101, 102, 102, 105, 105, 107, 113, 117, 120, 120, 120, 122, 124, 126, 130, 135, 138, and 182.

In addition, the following suspensions are used: 4 at 70, 5 at 80, 4 at 99, 3 at 121, and 1 at 150.

What can you say about this data?

5.36 Suppose that we want to model a left-censored, right-censored, interval, and complete data set, consisting of 274 units under test of which 185 units fail. The following table contains the data.

Data pt	Number in state (freq)	Last inspection	End time	(SorF)
1	2	5	5	F
2	23	5	5	S
3	28	0	7	F
4	4	10	10	F
5	7	15	15	F
6	8	20	20	F
7	29	20	20	S
8	32	0	22	F
9	6	25	25	F
10	4	27	30	F
11	8	30	35	F
12	5	30	40	F
13	9	27	45	F
14	7	25	50	F
15	5	20	55	F
16	3	15	60	F
17	6	10	65	F
18	3	5	70	F
19	37	100	100	S
20	48	0	102	F

a) Produce a Weibull plot of this data.
b) What type of data do you suppose this is?
c) Where on the bathtub curve is this failure mode? And why?

5.37 Microcircuits undergo accelerated life testing. The analysis is to be carried out using Weibull analysis for ungrouped data.
a) The first test series on six prototype microcircuits results in the following times to failure (in hours): 1.6, 2.6, 5.7, 9.3, 16.2, and 39.6. Fit a Weibull distribution to this data.
b) The second test series of six prototype microcircuits results in the following times to failure (in hours): 2.5, 2.8, 3.5, 5.7, 10.3, and 23.5. Fit a Weibull distribution to this data.
c) Plot both sets of data on the same plot, use MLE and ask for 90% confidence bounds. Are the two sets of data significantly different? If the data sets are not significantly different, plot them as one data set and compare to dual plots.

5.38 Twenty units of a catalytic converter are tested to failure without censoring. The times to failure (in days) are the following:

2.6	3.2	3.4	3.9	5.6
7.1	6.4	6.8	6.9	9.5
9.8	11.3	11.8	11.9	12.7
12.3	16.0	21.9	22.4	24.2

Determine whether the failure mode is increasing or decreasing or staying constant (i.e. exponential).

5.39 The data that follow are obtained for the time to failure of 128 appliance motors
a) Do a distribution ID plot of the interval data.
b) Make a Weibull probability plot and a normal probability plot of the grouped data. Extend the cumulative probability axis to start at 0.1 on both probability plots. What is the predicted 0.1 life on each plot? See something strange?

Hours	# Failures	Hours	# Failures
0–10	4	50–60	31
10–20	8	60–70	22
20–30	11	70–80	10
30–40	16	80–90	2
40–50	23	90–100	1

5.40 A wear test is run on 20 specimens, and the following failure times in hours are obtained: 81, 91, 95+ , 97, 100+ , 106, 109, 110+, 112, 114+, 117+, 120, 126, 128, 130, 132+, 139, 144, 154, and 163. (Note: + indicates a censored value.)

Do a Weibull plot and a three-parameter Weibull plot. Which seems better? Use your eyeball, look at the correlation/AD values, and pay attention to the values of β.

5.41 Of a group of 180 transformers, 20 of them fail within the first 4000 hours of operation. The times to failure in hours are as follows:[8]

10	1046	2096	3200
314	1570	2110	3360
730	1870	2177	3444
740	2020	2306	3508
990	2040	2690	3770

a) Produce a Weibull probability plot of the data.
b) Estimate how many transformers will fail between 4000 and 8000 hours. Needs a negative t_0.

5.42 Fifteen components undergo a 100-hour life test. Failures occur at 31.4, 45.9, 50.2, 56.4, 70.7, 73.2, 86.6, and 96.3 hours. From the previous experience the data is expected to obey a lognormal distribution. Make a probability plot using MINITAB and indicate the lognormal parameters, including MTTF. How can you tell this is a good fit-to-the-failure data?

5.43 The test started in Exercise 5.42 is run to completion. The remaining samples fail at 100.6, 117.9, 124.8, 146.7, 159.5, 205.2, and 232.5 hours. Redo the analysis and compare the lognormal parameters and the MTTF to the values obtained in Exercise 5.42.

5.44 Repeat Exercise 5.43 but fit the data to a two-parameter Weibull distribution.

5.45 Data for the failure times of 318 radio transmitter receivers are given in the following table.[9]

Time interval (h)	Failures	Time interval (h)	Failures
0–50	41	300–350	18
50–100	44	350–400	16
100–150	50	400–450	15
150–200	48	450–500	11
200–250	28	500–550	7
250–300	29	550–600	11

At 600 hours, 51 of the receiver–transmitters remained in operation. Use the arbitrary censoring option in MINITAB and assume a Weibull failure distribution.

(Note: Wayne Nelson used the midpoint of the interval to generate a Weibull of this data. You might do that to compare it to the arbitrary censoring output.)

8 *Source*: Data from Nelson (1982).
9 *Source*: Data from Mendenhall and Hader (1958).

5.46 The following uncensored grouped data were collected on the failure time of feedwater pumps, in units of 6 hours:

Interval	Number of failures
$0 < t < 6$	5
$6 < t < 12$	19
$12 < t < 18$	61
$18 < t < 24$	27
$24 < t < 30$	20
$30 < t < 36$	17

Produce a Weibull probability plot as well as a plot of reliability (called a survival plot in MINITAB) and hazard (failure) rate plot. Use MINITAB with arbitrary censoring.

5.47 The annual snowfall from 1900 to 2019:

Year	Annual snowfall	Year	Annual snowfall	Year	Annual snowfall	Year	Annual snowfall	Year	Annual snowfall	Year	Annual snowfall
1900	29.2	1920	31.7	1940	33.5	1960	47	1980	37.3	2000	56
1901	25.7	1921	37.7	1941	61.5	1961	53.9	1981	17.3	2001	44.1
1902	48.4	1922	66.3	1942	56.3	1962	42.2	1982	67.8	2002	72.1
1903	10.5	1923	48.8	1943	60.6	1963	44.7	1983	83.9	2003	29.1
1904	27.6	1924	21.2	1944	65.6	1964	48.9	1984	47.6	2004	54.6
1905	38.8	1925	45	1945	8.5	1965	26	1985	73.5	2005	26.9
1906	75.1	1926	38.8	1946	68.4	1966	34.8	1986	67.3	2006	56.5
1907	21.8	1927	36.9	1947	63.2	1967	55.5	1987	89.5	2007	38.1
1908	64.5	1928	45.8	1948	61.8	1968	32.3	1988	59.3	2008	39.1
1909	25.3	1929	32.6	1949	25.7	1969	54.3	1989	77.2	2009	88.7
1910	38.9	1930	31.3	1950	33.7	1970	54.3	1990	41.8	2010	23.7
1911	55.2	1931	31.7	1951	44.1	1971	53.8	1991	50.3	2011	49.9
1912	38	1932	35.8	1952	48.6	1972	45.3	1992	63.5	2012	79.2
1913	49.5	1933	15.4	1953	22.9	1973	57.3	1993	61.6	2013	49.9
1914	27.5	1934	11.7	1954	49.9	1974	44.4	1994	41.5	2014	42
1915	23.6	1935	25.1	1955	62.2	1975	61.6	1995	54.1	2015	72.8
1916	87.3	1936	43.6	1956	57.3	1976	26.3	1996	58.4	2016	36.1
1917	51.6	1937	41	1957	32.3	1977	63.6	1997	55.3	2017	35.3
1918	30.2	1938	38.8	1958	66.6	1978	75.2	1998	40	2018	48.6
1919	65.7	1939	35.7	1959	42.6	1979	114.1	1999	39.4	2019	48

a) Find the best distributional fit for this data.
b) What is the projected amounts of snowfall with probability 0.01 and probability 0.99?

5.48 The following numbers of bends to failure were recorded for 20 paper clips: 11, 29, 15, 20, 19, 11, 12, 9, 9, 8, 13, 20, 11, 22, 20, 9, 25, 19, 11, and 10.

a) Make a distribution ID plot in MINITAB and identify the best fit distribution.
b) Fit the data with the distribution chosen.
c) Briefly discuss your results.

5.49 Consider the following multiply censored data[10] for the field windings for 16 generators. The times to failure and removal times (in months) are 31.7, 39.2, 57.5, 65.0+, 65.8, 70.0, 75.0+, 75.0+, 87.5+, 86.3+, 94.2+, 101.7+, 105.8, 109.2+, 110.0, and 130.0+. Make a probability plot of the data. What type of phenomenon are we seeing for field windings failures? (NOTE: + indicated a censored value in Nelson's book.)

5.50 A producer of consumer products offers a three-year double-your-money back guarantee over a limited marketing area and collects the failure data tabulated below.

a) Fit the data to a Weibull distribution and estimate the parameters.
b) Fit the data to a lognormal distribution and estimate the parameters.
c) Does the Weibull or the lognormal distribution yield the better fit?
d) What % of population will fail by 24 months? 36 months?

Quarter sold:	W92	S92	S92	F92	W93	S93	S93	F93	W94	S94	S94	F94
Number sold:	842	972	1061	1293	939	1014	1036	1185	979	1125	1205	1300
Number failed:												
W92	18											
S92	42	22										
S92	33	42	21									
F92	32	39	45	26								
W93	32	37	43	54	19							
S93	27	35	38	51	38	22						
S93	34	31	42	50	39	43	20					
F93	42	35	37	46	34	39	43	23				
W94	27	32	35	46	37	39	40	50	19			
S94	26	26	29	40	32	36	38	48	44	26		
S94	21	31	36	43	33	37	41	42	41	44	28	
F94	25	27	31	41	29	33	35	45	35	46	49	24

5.51 The following multiply-censored times-to-failure (in hours) have been obtained from a battery-powered motor used in inexpensive consumer products: 22, 37, 41, 43, 56, 57+, 58, 61, 62+, 63+, 64, 64, 65+, 69, 69, 69+, 70, 76+, 78, 87, 88+, 89, 94, 100, and 119 (Note + indicates right-censored data).

a) Fit the data to a Weibull distribution and estimate the parameters.
b) Plot the reliability (survival) and hazard plot for this data.

10 From Nelson (1982).

5.52 A nonreplacement test with type I censoring is run for 50 hours on 30 microprocessors. Five failures occur at 12, 19, 28, 39, and 47 hours. Estimate the value of the constant failure rate.

5.53 Ten units are on test. The units are not replaced when they fail (nonreplacement).
One unit fails at $t_1 = 685$ hours, and a second unit fails at $t_2 = 1690$ hours.
The test is ended at $t = 2500$ hours with no additional failures.
a) What is the total accumulated test time?
b) What is the MTTF?

Supplement 1: Weibull Derived from Weakest Link Theory

A wide-spread use of the Weibull distribution is in describing the weakest link phenomena. This may be illustrated by considering a proverbial chain, where the strengths of the N link are described by the random variables $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \ldots \mathbf{x}_N$. The strength of the chain is then also a random variable, say y, which takes on the value of the weakest link. Thus,

$$P\{\mathbf{y} > y\} = P\{\mathbf{x}_1 > y \cap \mathbf{x}_2 > y \cap \mathbf{x}_3 > y \cap \cdots \cap \mathbf{x}_N > y\} \tag{5S1.1}$$

If the link strengths are independent,

$$P\{\mathbf{y} > y\} = P\{\mathbf{x}_1 > y\}\, P\{\mathbf{x}_2 > y\}\, P\{\mathbf{x}_3 > y\} \cdots P\{\mathbf{x}_N > y\} \tag{5S1.2}$$

If all of the links are governed by identical strength distributions, express the probabilities on the right in terms of a single CDF, $F_{\mathbf{x}}(x)$:

$$P\{\mathbf{x}_l > y\} = 1 - P\{\mathbf{x}_l \le y\} = 1 - F_{\mathbf{x}}(y) \tag{5S1.3}$$

Likewise, since the CDF for y may be written as $F_{\mathbf{y}}(y) = 1 - P\{\mathbf{y} > y\}$, Eq. (5S1.2) becomes

$$F_{\mathbf{y}}(y) = 1 - [1 - F_{\mathbf{x}}(y)]^N \tag{5S1.4}$$

Now, suppose that the link strengths are governed by a Weibull distribution,

$$F_{\mathbf{x}}(x) = 1 - \exp\left[-(x/\eta)^\beta\right] \tag{5S1.5}$$

then combining these two equations, we have

$$F_{\mathbf{y}}(y) = 1 - \left[e^{-(y/\eta)^\beta}\right]^N = 1 - e^{-N(y/\eta)^\beta} \tag{5S1.6}$$

Thus, the chain strength may also be expressed as a Weibull distribution

$$F_{\mathbf{y}}(y) = 1 - \exp\left[-(y/\eta')^\beta\right] \tag{5S1.7}$$

with the same shape parameter, and a scale parameter of

$$\eta' = N^{-1/\beta}\, \eta \tag{5S1.8}$$

Even in situations where the underlying distribution is not explicitly known, but the failure mechanism arises from many competing flaws, the Weibull distribution often provides a good empirical fit to the data.

Example 5S1.1 A chain is made of links whose strengths are Weibull distributed with $\beta = 5$ and $\eta = 1000$ lbs. (a) What is the mean strength of one link? (b) What is the mean strength of a chain of 100 links? (c) At what load is there a 5% probability that the 100 link chain will fail?

Solution:

a) Using Eq. (5.3): $\mu_{\mathrm{x}} = \eta\Gamma(1 + 1/\beta) = 1000\ \Gamma(1.20) = 1000 \cdot 0.918 = 918$ lbs.
b) From Eq. (5S1.8): $\eta' = 100^{-1/5} \cdot 1000 = 398$ lbs. Thus, $\mu_{\mathrm{y}} = 398\ \Gamma(1.20) = 398 \cdot 0.918 = 365$ lbs.
c) $0.05 = 1 - \exp[-(y/\eta')^{\beta}]$ or $y = \theta'[\ln(1/0.95)]^{1/5} = 398 \cdot 0.552 = 220$ lbs.

6

Reliability Testing

> "Reliability cannot be achieved by adhering to detailed specifications. Reliability cannot be achieved by formula and analysis. Some of these may help to some extent, but there is only one road to reliability.
> Build it, test it, and fix the things that go wrong. Repeat the process until the desired reliability is achieved. It is a feedback process and there is no other way …"
>
> *Source*: David Packard, the late cofounder of Hewlett-Packard Company, November 1982, in *Quality Magazine*

6.1 Introduction

Reliability tests employ a number of the statistical tools introduced in previous chapters. Here, we examine more closely how the gathering of data and its analysis is used for reliability prediction and verification through the various stages of design, manufacturing, and operation. In reality, the statistical methods that may be employed are often severely restricted by the costs of performing tests with significant sample sizes and by restrictions on the time available to complete tests.

Reliability testing is constrained by cost, since often the achievement of a statistical sample which is large enough to obtain reasonable confidence intervals may be prohibitively expensive, particularly if each one of the products tested to failure is expensive. Accordingly, as much information as possible must be gleaned from small statistical samples or in some cases from even a single failure. The use of failure mode analysis to isolate and eliminate the mechanism leading to failure may result in design enhancement long before sufficient data is gathered to perform formal statistical studies.

Testing is also constrained by the time available before a decision must be made in order to proceed to the next phase of the product development cycle. Frequently, one cannot wait the life of the product for it to fail. On specified dates, designs must be frozen, manufacturing commenced, and the product delivered. Even where larger sample sizes are available for testing, the severe constraints on testing time lead to the prevalence of censoring and acceleration. In censoring, a reliability test is terminated before all of the units have failed. In acceleration, the stress cycle frequency or stress intensity is increased to obtain the needed failure data over a shorter time period.

These cost and time restrictions force careful consideration of the purpose for which the data is being obtained, the timing as to when the results must be available, and the required precision. These considerations frequently lead to the employment of different methods of data analysis at different points in the product cycle. One must carefully consider what reliability characteristics

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website:

are important for determining the adequacy of the product. For example, time to failure may be measured in at least three ways:

1) operating time
2) number of on–off cycles
3) calendar time.

If the first two are of primary interest, the test time can be shortened by applying compressed time accelerations, whereas if the last is of concern, then intensified stress testing must be used. These techniques are discussed in detail in Section 6.5.

The third constraint on testing is the customer requirements. Initial requirements are set by the customer, then preliminary design begins, and initial testing starts. At this point, the customer will often change his requirements (e.g. larger electrical load requiring a larger transformer of generator and a larger weapon load requiring a larger engine because the vehicle has to meet the speed and range requirements).

Figure 6.1 is a synopsis of the testing that will be presented along with a pictorial reminder of the cost, time, and customer requirement challenges.

During the conceptual and detailed design stages, before the first prototype is built, reliability data plays a crucial role. Reliability objectives and the determination of the associated component reliability requirements enter the earliest conceptual design and system definition. The parts count method, treated in Chapter 3, and similar techniques may be used to estimate reliability from the known failure rate characteristics of standard components. Comparisons to similar existing systems and a good deal of judgment also must be used during the course of the detailed design phase.

Tests may be performed by suppliers early in the design phase on critical components even before system prototypes are built. Thus, aircraft, automotive, and other engines undergo extensive

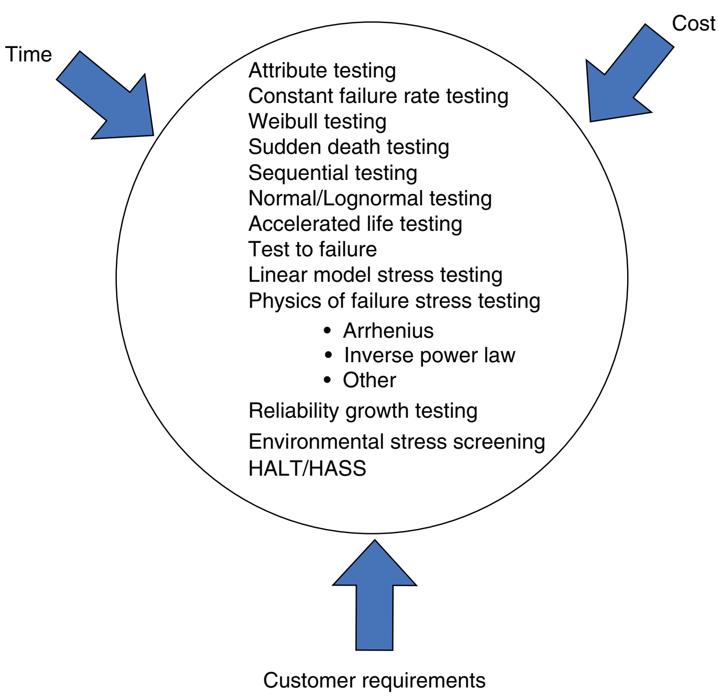


Figure 6.1 The reliability testing "balloon" and its overall challenges.

reliability testing before incorporation into a vehicle. On a smaller scale, one might decide which of a number of electric motor suppliers to utilize in the design of a small appliance by running reliability tests on the motors. Depending on the design requirement and the impact of failure, such tests may range from quite simple binomial tests, in which one or more of the motors is run continuously for the anticipated life of the machine, to more exhaustive statistical analysis of life-testing procedure.

Completion of the first product prototypes allows operating data to be gained, which in turn may be used to enhance reliability. At this stage, the test–fix–test–fix cycle is commonly applied to improve design reliability before more formal measures of reliability are applied. As more prototypes become available, environmental stress testing may also be employed in conjunction with failure mode analysis to refine the design for enhanced reliability. These reliability enhancement procedures are discussed in Section 6.5. It should be noted that some of these enhancement procedures can be used throughout the design–development–production–field operation cycles.

As the design is finalized, more extensive use of the life-testing procedures discussed in Sections 6.2–6.5 may be required for design verification. During the manufacturing phase, qualification and acceptance testing become important to ensure that the delivered product meets the reliability standards to which it was designed. Through aggressive quality improvement, defects in the manufacturing process must be eliminated to insure that manufacturing variability does not give rise to unacceptable numbers of infant-mortality failures. Finally, the collection of reliability data throughout the operational life of a system is an important task, not only for the correction of defects that may become apparent only with extensive field service but also for the setting and optimization of maintenance schedules, parts replacement, and warranty policies.

Data is likely to be collected under widely differing circumstances ranging from carefully controlled laboratory experiments to data resulting from field failures. Both have their uses. Laboratory data are likely to provide more information per sample unit, both in the precise time to failure and in the mechanism by which the failures occur. Conversely, the sample size for field data is likely to be much larger, allowing more precise statistical estimates to be made. Equally important, laboratory testing may not adequately represent the environmental condition of the field, even though attempts are made to do so. The exposures to dirt, temperature, humidity, and other environmental loading encountered in practice may be difficult to predict and simulate in the laboratory. Similarly, the care in operation and quality of maintenance provided by consumers and field crews is unlikely to match that performed by laboratory personnel.

Collecting data in many instances has its own challenges. If a product is sold in the commercial arena, warranty returns (if warranties are given) may be the only data available. Products sold to the military or other government agencies where safety and reliability are of utmost importance will have more complete failure and nonfailure data. If a product or system is owned by a leasing firm (e.g. commercial aircraft), the data is often only available after the lease has run out (3–5 years)!

6.2 Attribute Testing (Binomial Testing)

A unit either meets or fails to meet a test requirement. When there are no failures in n tests, we say there is a *success run of length n*. For example, a set of 27 bearings does not exhibit brinnelling[1] under a specified loading condition; a sample of 10 metal strips may each meet a tensile and elongation requirement; or a sample of 100 firings of an upper stage rocket engine at simulated deep

1 *Brinelling* is the permanent indentation of a hard surface. True *brinelling* indicates that the load on the bearing is greater than the elastic limit of the ring or bearing material.

space conditions was successful. In these examples we would say that we have a success run of 27, 10, and 100, respectively. The purpose of a success run test is usually to demonstrate compliance to a requirement or to demonstrate some degree of reliability. The term q*ualification testing* is also found in this context, and such testing is often used to "qualify" materials, electromechanical components and subassemblies, or entire products.

A very common measure of reliability when using success runs is to state the "lower confidence bound", $-R_0$, on the unknown reliability. Using this technique one may claim that $R > R_0$ with a degree of confidence, say C. R_0 is derived from a probability argument about the occurrence of no failures in n tests.

In the present discussion there is no consideration for the underlying distribution of failure times, and so the method is referred to as nonparametric.

The Classical Success Run

Suppose that a series of n tests is performed without failure. The test conditions remain constant from test to test, and the n tests are independent. With a given confidence level, say C, what reliability is demonstrated by a success run of length n?

We know from our discussion of the binomial distribution (Chapter 2) that the binomial describes pass/fail phenomenon; hence, in general, for n trials, the probability of s successes is

$$P(\text{success}) = C_s^n p^s q^{n-s}$$

or, in Reliability terms; let R(reliability) = probability of success p, and Q(unreliability) = $(1 - R)$ = probability of failure q

$$\text{Then}, P(\text{success}) = C_s^n R^s (1-R)^{n-s}$$

If there are s successes in n Bernoulli trials, the point estimates of R and Q are:

$$Q = (1-R) = \frac{n-s}{n} \text{ and } R = \frac{s}{n}$$

From Eq. (2.63) we can find the lower one-sided confidence interval $100(1-\alpha)\%$ (CL) for the Reliability R where $r = n - s$ failures in a sample of size n:

$$\sum_{k=0}^{r} C_k^n (1-R_L)^k (R_L)^{n-k} = \alpha = 1 - CL \tag{6.1}$$

where CL is the confidence level, r is the number of failures among n tests, and R_L is the lower bound confidence level on reliability. Note that if no failures occurred during the test, Eq. (6.1) becomes

$$1 - CL = R^n \tag{6.2}$$

Zero-Failure Attribute Tests

We can now use Eq. (6.2) to solve the following examples:

Example 6.1 What reliability can be demonstrated with 90% confidence if your device is pass/fail and you test it 100 times successfully?

Using $1 - CL = R^n$
with $n = 100$ and $CL = 0.90$,
$1 - 0.90 = R^{100}$
$R = (0.1)^{\frac{1}{100}} = 0.977$

So, you can be 90% confident that your reliability is AT LEAST 0.977.

Example 6.2 How many tests do you need to run on a pass/fail device to assure 0.99 reliability with 90% confidence?

Using $1 - CL = R^n$
with $R = 0.99$ and $CL = 0.90$,
$1 - 0.90 = 0.99^n$
$0.1 = 0.99^n$
$\ln(0.1) = n^* \ln(0.99)$
$$n = \frac{\ln(0.1)}{\ln(0.99)} = 230 \text{ (note : always round up)}$$

Example 6.3 An engineer just ran 50 compressor start tests with no failures, he needs to pass the customer's requirement of 80% confidence of 0.90 reliability. Has he done that?

Using $1 - CL = R^n$
with $n = 50$ and $CL = 0.80$,
$1 - 0.80 = R^{50}$
$0.2 = R^{50}$
$R = (0.2)^{\frac{1}{50}} = 0.968$

Since $0.968 > 0.90$, the engineer has met the customer requirements.

Often, a table of representative values can quickly answer a zero-failure test question and can give you trade-offs if needed. See Table 6.1.

Non-Zero-Failure Attribute Tests

Often, zero-failure attribute testing is not possible. So, when tests are complete, the question becomes: What reliability has been demonstrated at a given confidence level?

From Eqs. 2.76 and 2.79 we can find the *two-sided* confidence interval $100(1 - \alpha)\%$ for the Reliability R, where $r = n - s$ failures in a sample of size n:

1) for the lower *two-sided* Confidence limit (CL) on R (R_L) solve the equation:

$$\sum_{k=0}^{r} C_k^n (1 - R_L)^k (R_L)^{n-k} = \frac{\alpha}{2} = \frac{1 - CL}{2} \tag{6.3}$$

2) for the upper *two-sided* Confidence limit (CL) for R (R_U), solve the equation:

$$\sum_{k=r}^{n} C_k^n (1 - R_U)^k (R_U)^{n-k} = \frac{\alpha}{2} = \frac{1 - CL}{2} \tag{6.4}$$

Table 6.1 Number of tests without failure to demonstrate various reliability/confidence levels.

		Confidence level					
		90	95	97.5	99	99.5	99.9
Reliability	0.99999	230,258	299,572	368,887	460,515	529,830	690,773
	0.9999	23,025	29,956	36,887	46,050	52,981	69,075
	0.999	2302	2995	3688	4603	5296	6905
	0.998	1151	1497	1843	2301	2647	3451
	0.997	767	998	1228	1533	1764	2300
	0.996	575	748	921	1149	1322	1724
	0.995	460	598	736	919	1058	1379
	0.994	383	498	613	766	881	1148
	0.993	328	427	526	656	755	984
	0.992	287	373	460	574	660	861
	0.991	255	332	409	510	587	765
	0.99	230	299	368	459	528	688
	0.98	114	149	183	228	263	342
	0.97	76	99	122	152	174	227
	0.96	57	74	91	113	130	170
	0.95	45	59	72	90	104	135
	0.94	38	49	60	75	86	112
	0.93	32	42	51	64	74	96
	0.92	28	36	45	56	64	83
	0.91	25	32	40	49	57	74
	0.9	22	29	36	44	51	66
	0.8	11	14	17	21	24	31
	0.7	7	9	11	13	15	20
	0.6	5	6	8	10	11	14
	0.5	4	5	6	7	8	10

Using Eqs. 2.76 and 2.79 we can also find the *one-sided* confidence intervals for Reliability R

3) for the lower *one-sided* Confidence limit (CL) for R:

$$\sum_{k=0}^{r} C_k^n (1-R_L)^k (R_L)^{n-k} = \alpha = 1 - CL \tag{6.5}$$

4) for the upper *one-sided* Confidence limit (CL) for R:

$$\sum_{k=r}^{n} C_k^n (1-R_U)^k (R_U)^{n-k} = \alpha = 1 - CL \tag{6.6}$$

These equations can be used in EXCEL's SOLVER to find R_L and R_U; however, that becomes a tedious exercise.

Instead, based on Kapur and Lamberson (1977), these equations can be transformed into ones based on the F distribution.

In each of the following equations and F-distribution look-up is required. The F-distribution is of the form:

$$F_{\alpha,\nu_1,\nu_2}$$

where

ν_1 = numerator degrees of freedom and
ν_2 = denomintor degrees of freedom

While the F-distribution is used in elementary statistics to compare two population variances, it is also used to transform Binomial and Beta distribution equations to make them more tractable.

Using EXCEL's function F.inv($1-\alpha$, ν_1, ν_2) saves us time from looking up and interpolating in a printed F-table.

Using the F-distribution transformation described above, we can now use Eqs. (6.7) and (6.8) to calculate the two-sided confidence bounds for reliability and Eqs. (6.9) and (6.10) to calculate the lower one-sided and upper one-sided confidence bounds on reliability

1) for the lower *two-sided* Confidence limit (CL) R_L:

$$R_L = \frac{1}{1 + \frac{n-s+1}{s} F_{1-\alpha/2;\,2(n-s)+2;\,2s}} \tag{6.7}$$

2) for the upper *two-sided* Confidence limit (CL) R_U:

$$R_U = \frac{1}{1 + \frac{n-s}{s+1} F_{\alpha/2;\,2(n-s);\,2s+2}} \tag{6.8}$$

3) for the lower *one-sided* Confidence limit (CL) R_L:

$$R_L = \frac{1}{1 + \frac{n-s+1}{s} F_{1-\alpha;\,2(n-s)+2;\,2s}} \tag{6.9}$$

4) for the upper *one-sided* Confidence limit (CL) R_U:

$$R_U = \frac{1}{1 + \frac{n-s}{s+1} F_{\alpha;\,2(n-s);\,2s+2}} \tag{6.10}$$

Example 6.4 After information on 500 augmentor (sometimes referred to afterburners) lights on a fighter aircraft, it was noted that there had been 14 failures to light on the first attempt. The customer asked what the 90% lower confidence bound was for this data.

Using Eq. (6.9):

Here $n = 500$, $s = 486$, $1 - \alpha = 0.90$

$$R_L = \frac{1}{1 + \frac{n-s+1}{s} F_{1-\alpha;\,2(n-s)+2;\,2(s)}}$$

$$= \frac{1}{1 + \frac{500-486+1}{486} F_{0.90;\,2(500-486)+2;\,2(486)}}$$

Using EXCEL's F.inv function: "F.inv(0.9,2∗(500-4860=2,2∗486)=1.35

$$= \frac{1}{1 + \frac{15}{486}(1.35)} = 0.96$$

So, you can be 90% confident that the augmentor will light *at least* 96 times in 100 attempts.

6.3 Constant Failure Rate Estimates

In this section, we examine in more detail the testing procedures for determining the MTTF when the data are exponentially distributed. This is justified both because the exponential distribution (i.e. the constant failure rate model) is the most widely applied in reliability engineering, and because it provides insight into the problems of parameter estimation that are indicative of those encountered with other distributions.

We must, of course, determine whether the constant failure rate model is applicable to the test at hand. At least four approaches to this problem may be taken. The exponential distribution may be assumed, based on the experience with the equipment of similar design. It may be identified using one of the standard statistical goodness-of-fit criteria or by probability plotting and examining the results visually for the required straight-line behavior. Finally, it may be argued from the failure mode whether the failures are random, as opposed to early or aging failures. If defective products or aging effects are identified as causing some of the failures, the data must be censored appropriately.

The exponential distribution has only a single parameter to be estimated, the failure rate λ. Rather than estimate the failure rate directly, most sampling schemes are cast in terms of the MTTF, denoted by MTTF $\equiv \mu = 1/\lambda$. For uncensored data, the value of μ may be estimated from

$$\hat{\mu} = \frac{1}{N}\sum_{i=1}^{N} t_i \tag{6.11}$$

Moreover, when *N*, the number of test specimens, is sufficiently large, the central limit theorem, which was discussed in Chapter 4, may be used to estimate a confidence interval. In particular, the 69% confidence interval is given by $\hat{\mu} \pm \sigma/\sqrt{N}$, where σ^2 is the variance of the distribution. Since for the exponential distribution $\sigma = \mu$, we may estimate the 69% confidence interval from $\hat{\mu} \pm \hat{\mu}/\sqrt{N}$.

Censoring on the Right

It is clear from the foregoing expressions that for a precise estimate a large sampling size is required. Using many test specimens is expensive, but, more important, a very long time is required to complete the test. As *N* becomes large, the last failure is likely to occur only after several MTTFs have elapsed. Moreover, the analysis of the failures that occur after long periods of time is problematic for two reasons. First, a design life is normally less than the MTTF, and secondly, it is often not possible to hold up the final design, production, or operation while tests are carried out over many design lives. Equally important, many of the last failures are likely to be caused by other failure modes. Thus, they must be removed from the data by censoring if a true picture of the random failures is to be gained.

Type I and type II censoring from the right are attractive alternatives to uncensored sampling. By limiting the period of the test while increasing the number of units tested, we can eliminate most of the aging failures and estimate more precisely the time-independent failure rate. Within this framework, four different test plans may be used. With the assumption that the test is begun with N test units, these plans may be distinguished as follows:

- If the test is terminated at some specified time, say t^*, then *type I censoring* is said to take place.
- If the test is terminated immediately after a particular number of failures, say n, then *type II censoring* is said to take place.

With either type I or type II censoring, we may run the test in either of two ways. In the nonreplacement method, each unit is removed from the test at the time of failure. In the replacement method, each unit is immediately repaired or replaced following failure so that there are always N units operating until the test is terminated.

The choice between type I and type II censoring involves the following trade-off:

Type I censoring is more convenient because the duration of the test t^* can be specified when the test is planned. The time t_n of the nth failure, at which a test with type II censoring is terminated, however, cannot be predicted with precision at the time the test is planned, for t_n is a random variable. Conversely, the precision of the measurement of the MTTF for the exponential distribution is a stronger function of the number of failures rather than of the test time. Therefore, it is often considered advisable to wait until some specified number of failures have occurred before concluding the test.

A number of factors also come into play in determining whether nonreplacement or replacement tests are to be used. In laboratory tests, the cost of the test units compared with the cost of the apparatus required to perform the test may be the most significant factor. Consider two extreme examples. First, if jet engines are being tested, nonreplacement is the likely choice. When a specified number of engines are available, more will fail within a given length of time if they are all started at the same time than if some of them are held in reserve to replace those that fail. The same is true of any other expensive piece of equipment that is to be tested as a whole.

Conversely, suppose that we are testing fuel injectors for large internal-combustion engines. The supply of fuel injectors may be much larger than the number of engines upon which to test them. Therefore, it would make sense to keep all the engines running for the entire length of the test by immediately replacing each fuel injector following failure, provided that the replacement can be carried out swiftly and at minimum cost. Minimizing cost is an important provision, for generally the personnel costs are larger with replacement tests; in nonreplacement tests, personnel or instrumentation is required only to record the failure times. In replacement tests, personnel and equipment must be available for carrying out the repairs or replacements within a short period of time.

The situation is likely to be quite different when the data are to be accumulated from actual field experience with breakdowns. Here, in the normal course of events, equipment is likely to be repaired or replaced over a time span that is short compared to the MTTF. Conversely, records may indicate only the number of breakdowns, not when they occurred. The number of breakdowns might be inferred, for example from spare parts orders or from numbers of service calls. In these circumstances, replacement testing describes the situation. Moreover, unlike nonreplacement testing, the MTTF estimation does not require that the times of failures be recorded.

One last class of test remains to be mentioned. Sometimes referred to as percentage survival, it is a simple count of the fraction (or percentage) of failed units. From the properties of the exponential distribution, we infer the MTTF. This test procedure requires no surveillance, for failed equipment does not need to be replaced or times of failure recorded. Not surprisingly, the estimate obtained is less precise. The method is normally not recommended, unless failures are not apparent at the time they take place and can only be determined by destructive testing or other invasive techniques following the conclusion of the test.

MTTF Estimates

Except for the percentage survival technique, the same estimator may be shown to be valid for all the test procedures described (Bazovsky 1961):

$$\hat{\mu} = \frac{T}{n} \tag{6.12}$$

T = total operational time of all test units,
n = number of failures.

For each class of test, however, the total operating time T is calculated differently.

Consider first the nonreplacement testing with type I censoring (i.e. the test is terminated at some predetermined time t^*). If $t_1, t_2, \ldots, t_n$ are the times of the n failures, the total operational time T for the N units tested is

$$T = \sum_{i=1}^{n} t_i + (N - n)t^* \tag{6.13}$$

since $N - n$ units operate for the full-time t^*.

Example 6.5 A 30-day nonreplacement test is carried out on 20 rate gyroscopes. During this period of time, 9 units fail; examination of the failed units indicates that none of the failures is due to defective manufacture or to wear mechanisms. The failure times (in days) are 27.4, 13.5, 10.5, 20.0, 23.6, 29.1, 27.7, 5.1, and 14.4. Estimate the MTTF.

Solution: From Eq. (6.13), with $N = 20$ and $n = 9$.

$$T = \sum_{i=1}^{9} t_l + (20 - 9) \times 30$$
$$= 171.3 + 11 \times 30 = 501.3$$
$$\hat{\mu} = \frac{T}{n} = \frac{501.3}{9} = 55.7\ \text{days}$$

For type II censoring, the test is stopped at t_n, the time of the nth failure. Thus, if there is no replacement of test units, the total operating time is calculated from

$$T = \sum_{i=1}^{n} t_i + (N - n)t_n \tag{6.14}$$

since the nonfailed $(N - n)$ units are taken out of service at the time of the nth failure. Note that in the event that some of the units, say k of them, are removed from the test because they fail from another mechanism, such as aging, then T is still calculated by Eq. (6.13) or (6.14). Now, however, the estimate is obtained by dividing only by the number $n - k$ of random failures:

$$\hat{\mu} = \frac{T}{n-k} \tag{6.15}$$

Example 6.6 The engineer in charge of the test in the preceding problem decides to continue to test until 10 of the 20 rate gyroscopes have failed. The tenth failure occurs at 41.2 days, at which time the test is terminated. Estimate the MTTF.

Solution: From Eq. (6.14), with $N = 20$ and $n = 10$,

$$T = \sum_{i=1}^{10} t_n + (20 - 10)41.2$$

$$T = (171.3 + 41.2) + 10 \times 41.2 = 624.5$$

$$\hat{\mu} = \frac{T}{n} = \frac{624.5}{10} = 62.4 \text{ days}$$

In replacement testing, all N units are operated for the entire length of the test. Thus, for type I censoring, we have $T = Nt^*$, where t^* is the specified test time. Hence,

$$\hat{\mu} = \frac{Nt^*}{n} \tag{6.16}$$

For type II censoring, we have $T = Nt_n$, where t_n is the time at which the nth unit fails. Thus, $T = Nt_n$ or

$$\hat{\mu} = \frac{Nt_n}{n} \tag{6.17}$$

Example 6.7 A chemical plant has 24 process control circuits. During 5000 hour of plant operation, the circuits experience 14 failures. After each failure, the unit is immediately replaced. What is the MTTF for the control circuits?

Solution: From Eq. (6.16)

$$T = Nt^* = 24 \times 5000 = 120,000$$

$$\hat{\mu} = \frac{T}{n} = \frac{120,000}{14} = 8571 \text{ hours}$$

Example 6.8 Six units of a new high-precision pressure monitor are placed on an industrial furnace. After each failure, the monitor is immediately replaced. However, the eighth failure occurs after only 840 hours of service. It is decided that the high-temperature environment is too severe for the instruments to function reliably, and the furnace is shut down to replace the pressure monitors with a more reliable, and expensive, design. Assuming that the failures are random, estimate the MTTF of the monitors.

Solution: From Eq. (6.17)

$$T = Nt_8 = 6 \times 840 = 5040 \text{ hours}$$

$$\hat{\mu} = \frac{T}{n} = \frac{5040}{8} = 630 \text{ hours}$$

As alluded to earlier, the MTTF may also be estimated from the percentage survival method. We begin by first estimating the reliability at the end of the test, time t_0 as $R(t_0) = 1 - n/N$. With an exponential distribution, however, the reliability is given by

$$R(t_0) = \exp(-t_0/\mu) \tag{6.18}$$

Thus, combining these equations, we estimate MTTF from

$$\mu = \frac{t_0}{\ln[1/(1-n/N)]} \tag{6.19}$$

Example 6.9 A National Guard unit is supplied with 20,000 rounds of ammunition for a new model rifle. After 5 years, 18,200 rounds remain unused. From these, 200 rounds are chosen randomly and test fired. Twelve of them misfire. Assuming that the misfires are random failures of the ammunition caused by storage conditions, estimate the MTTF.

Solution: In Eq. (6.19), take $n = 12$, $N = 200$, and $t_0 = 5$ years. We have

$$\hat{\mu} = \frac{5}{\ln\{1/[1-12/200]\}} = 81 \text{ years}$$

Confidence Intervals

We next consider the precision of the MTTF estimates made with Eq. (6.12). The confidence limits for the both replacement and nonreplacement tests may be expressed in terms of $\hat{\mu}$ and the number of failures using the χ^2 distribution. We consider type II censoring first.

Let $U_{\alpha/2,n}$ and $L_{\alpha/2,n}$ be the upper and lower limits for the $100 \times (1-\alpha)\%$ confidence interval for *type II censoring*.

In order to use the χ^2 table, let $L_{\alpha/2,2n} = \dfrac{2T}{\chi^2_{\alpha/2,2n}}$ and $U_{\alpha/2,2n} = \dfrac{2T}{\chi^2_{1-\frac{\alpha}{2},2n}}$, so $(1-\alpha) \times 100\%$ confidence bounds on an MTTF are:

$$\frac{2T}{\chi^2_{\alpha/2,2n}} \leq \text{MTTF} \leq \frac{2T}{\chi^2_{1-\frac{\alpha}{2},2n}}$$

The two-sided confidence interval states that if the test is stopped after the nth failure, there is a $1-\alpha$ probability that the true value of MTTF lies between

$$P\left[\frac{2\text{T}}{\chi^2_{\alpha/2,2n}} \leq \text{MTTF} \leq \frac{2T}{\chi^2_{1-\frac{\alpha}{2},2n}}\right] = 1-\alpha \tag{6.20}$$

Example 6.10 What is the 90% confidence interval for the rate gyroscopes tested in Example 6.6 taking the failure at 41.2 days into account?

Solution: For a 90% confidence interval, we have $100(1-\alpha) = 90$ or $\alpha = 0.1$ and $\alpha/2 = 0.05$. For $n =$ 10 failures, we find from Eq. (6.20) that

$$\frac{2(624.5)}{\chi^2_{(0.1/2),2(10)}} \leq \text{MTTF} \leq \frac{2(624.5)}{\chi^2_{(1-(0.1/2)),2(10)}}$$

then, from the χ^2 table at the end of the chapter:

$$\frac{1249}{30.14} \leq \text{MTTF} \leq \frac{1249}{10.12}$$

$41.4 \leq \text{MTTF} \leq 123.4$ with 90% confidence.

With slight modifications the results of Eq. (6.20) may also be applied to type I censoring, where the test is ended at some time t^*. Using the properties of the χ^2 distribution, it may be shown that the upper confidence limit and $\hat{\mu}$ remain the same. The lower confidence limit, in general, decreases. The two-sided $(1-\alpha)$ 100% confidence interval for Type I censoring is

$$\frac{2T}{\chi^2_{\frac{\alpha}{2},2(n+1)}} \le \text{MTTF} \le \frac{2T}{\chi^2_{1-\frac{\alpha}{2},2n}} \tag{6.21}$$

Again, the confidence limits are applicable to both the nonreplacement and replacement testing.

Example 6.11 During the first year of operation, a demineralizer suffers seven shutdowns. Estimate the MTBF and the 95% confidence interval.

Solution: From Eq. (6.12)

$$\hat{\mu} = \text{MTBF} = \frac{T}{n} = \frac{12\text{ months}}{7} = 1.71\text{ months}$$

For a 95% confidence interval, $\alpha = 0.05$ and $\alpha/2 = 0.025$. Using Eq. (6.21),

$$\frac{2T}{\chi^2_{0.025,2(7+1)}} \le \text{MTTF} \le \frac{2T}{\chi^2_{1-0.025,2(7)}} = \frac{2(12)}{27.49} \le \text{MTTF} \le \frac{2(12)}{5.01}$$

so, 0.87 months ≤ MTTF ≤ 4.79 months with 95% confidence.

Example 6.12 A computer specification calls for an MTBF of at least 100 hours with 90% confidence. If a prototype fails for the first time at 210 hours, can these test data be used to demonstrate that the specification has been met?

Solution: $\hat{\mu} = T/n = 210/1 = 210\text{ hour}$. For the 90% one-sided confidence interval, $\alpha/2 = 0.1$. From Eq. (6.21),

$$\frac{2T}{\chi^2_{0.1,2(1)}} \le \text{MTTF}$$

or

$$\frac{2(210)}{4.605} = 90.3\text{ hours}$$

The test is inadequate, since the specified value of 100 hours. is less than the lower (i.e. outside) confidence.

A word is in order concerning the percentage survival test discussed earlier. It is a form of binomial sampling, with the ratio n/N being the estimate of the failure probability of failure. Consequently, the method discussed in Chapter 2 can be used to estimate the confidence interval of the failure probability, and from this the confidence interval on the MTTF can be estimated. The uncertainty is greater than that obtained from testing in which the actual failure times are recorded.

Example 6.13 Estimate the 90% confidence interval for the National Guard ammunition problem, Example 6.9.

Solution: Since, in 5 years, 12 of 200 rounds fail, the 5-year failure probability may be calculated from Eqs. (2.1a) and (2.1b) to be

$$\hat{p} = \frac{n}{N} = \frac{12}{200} = 0.06$$

since $N\hat{p} > 5$, we can use the Normal approximation to calculate the confidence interval on a proportion:

If $\hat{p}$ is the proportion of failures in a random sample of size n, and $\hat{q} = 1 - \hat{p}$, an approximate $(1-\alpha)100\%$ confidence interval for the binomial parameter p is given by

$$\hat{p} - z_{\frac{\alpha}{2}}\sqrt{\frac{\hat{p}\hat{q}}{n}} < p < \hat{p} + z_{\frac{\alpha}{2}}\sqrt{\frac{\hat{p}\hat{q}}{n}}$$

where $z_{\frac{\alpha}{2}}$ is the z-value leaving an area of $\alpha/2$ to the right.

Hence,

$$0.06 - 1.645\sqrt{\frac{(0.06)(0.94)}{200}} < p < 0.06 + 1.645\sqrt{\frac{(0.06)(0.94)}{200}}$$
$$0.06 - 0.028 < p < 0.06 + 0.028 \text{ or } 0.032 < p < 0.088$$

(see, e.g. Montgomery and Runger 2011).

For a constant failure rate, we have

$$p = 1 - e^{-t/\mu} \text{ or } \mu = -t/\ln(1-p)$$

Therefore, with $t = 25$ years,

$$\frac{-25}{\ln(1-0.088)} < \mu < \frac{-25}{\ln(1-0.032)}$$
$$271 \text{ years} < \mu < 769 \text{ years}$$

with 90% confidence.

6.4 Weibull Substantiation and Reliability Testing

In Chapter 5, we used the Weibull distribution to analyze failure data. We now use the Weibull distribution as the underlying distribution to establish statistical requirements for substantiation and reliability testing.

Substantiation testing demonstrates that a redesigned part, subsystem, or system has eliminated or significantly improved the life of a known failure mode. In substantiation testing, the Weibull β and η are known.

Reliability testing demonstrates that a reliability requirement has been met. Further, in reliability testing, in this chapter, it is assumed that the Weibull slope (β) is known. This is true in most instances because most businesses that make parts, modules, subsystems, or systems have been in business for some length of time and have failure mode experience from previous parts or systems that were produced. They have kept track of that experience (sometimes in a "Weibull Library") and can use that previous experience to then use those Weibull failure analyses to indicate an experiential β and adjust the characteristic life based on engineering principles and experience. However, if the failure mode is known to be Weibull (say from literature searches), but the actual value of a historical Weibull is unavailable, you can bracket the Weibull β based on engineering or metallurgical evidence. For example, a part cracked beyond limits in the field, the crack is deemed to be an LCF (low cycle fatigue)-caused crack. Typical LCF βs range from 2 to 4. So, using the range of 2–4 will give you the conservative amount of reliability testing needed to meet the reliability goal.

If you have *absolutely no guess* at the Weibull β, but do know that the failure mode follows a Weibull distribution, you can consult test plans published by Fertig and Mann (1980).

Both substantiation testing and reliability testing require a test plan. A test plan gives the required number of units and the amount of time to be accumulated on each to either substantiate a fix or meet a reliability goal. It also gives a success criterion, where the test is passed if the success criterion is met. In a zero-failure test plan, the success criterion is no failure: the test is passed if every unit runs the prescribed amount of time, and no unit fails while on test.

Test plans can also be generated with a one-failure success criterion, zero- or one-failure criterion, a two-failure success criterion, etc. But all of these plans require more testing than the zero-failure plan.

A measure of statistical confidence is usually built into statistically designed test plans, guaranteeing that if the failure mode in question has not been fixed or the reliability requirement has not been achieved, there is a low probability that the test will be passed. For example, the zero-failure test plans in this chapter guarantee with 90% confidence that the test will be failed if the required goal has not been achieved. Thus, a part or system will have at most a 10% chance of being accepted as satisfactory when in fact it is not.

Zero-Failure Test Plans for Substantiation Testing

A ball and roller bearing system has a Weibull failure mode, unbalance, with $\beta = 2$, and $\eta = 500$ hours. The system is redesigned, and three redesigned systems are available for testing. How many hours should each system be tested to demonstrate that this mode of unbalances has been eliminated or significantly improved?

The Weibull plot in Figure 6.2 illustrates the time-to-unbalance distribution.

Table 6.2 is used to answer this type of question. It is entered with the value of β and the number of units to be tested. The corresponding table entry is multiplied by the characteristic life to be demonstrated to find the test time required of each unit.

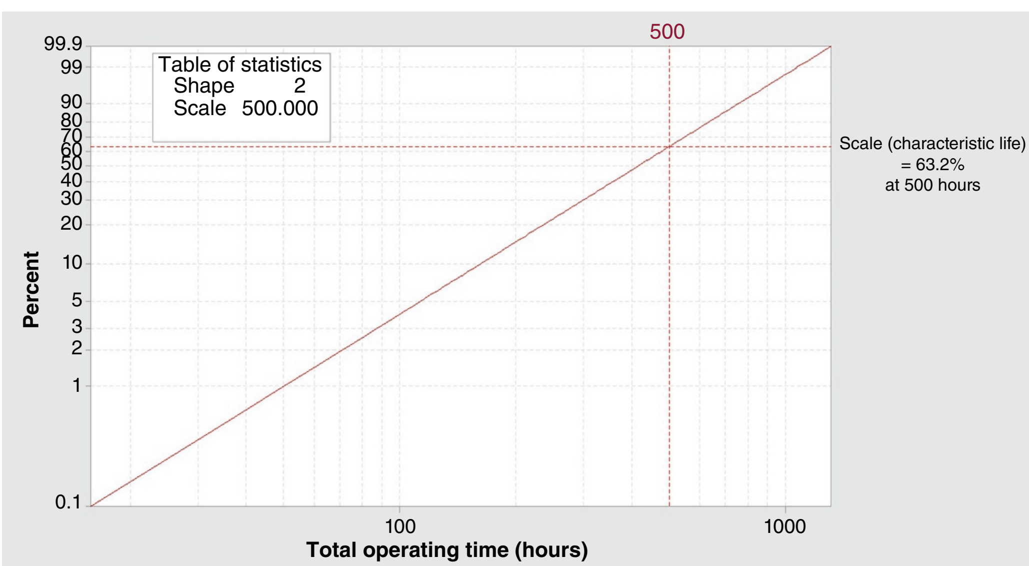


Figure 6.2 Ball and roller bearing unbalance distribution.

Table 6.2 Substantiation testing: characteristic life multipliers for zero-failure test at **90% confidence.**

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
N	**Infant mortality**	**Random**	**Early wear out**					**Old age rapid wear out**		
2	1.3255	1.1513	1.0985	1.0730	1.0580	1.0481	1.0411	1.0358	1.0318	1.0286
3	0.5891	0.7675	0.8383	0.8761	0.8996	0.9156	0.9272	0.9360	0.9429	0.9485
4	0.3314	0.5756	0.6920	0.7587	0.8018	0.8319	0.8540	0.8710	0.8845	0.8954
5	0.2121	0.4605	0.5963	0.6786	0.7333	0.7722	0.8013	0.8238	0.8417	0.8563
6	0.1473	0.3838	0.5281	0.6195	0.6818	0.7267	0.7606	0.7871	0.8083	0.8257
7	0.1082	0.3289	0.4765	0.5735	0.6410	0.6903	0.7278	0.7573	0.7811	0.8006
8	0.0828	0.2878	0.4359	0.5365	0.6076	0.6603	0.7006	0.7325	0.7582	0.7795
9	0.0655	0.2558	0.4030	0.5058	0.5797	0.6348	0.6774	0.7112	0.7386	0.7614
10	0.0530	0.2303	0.3757	0.4799	0.5558	0.6129	0.6573	0.6927	0.7216	0.7455
11	0.0438	0.2093	0.3525	0.4575	0.5350	0.5938	0.6397	0.6764	0.7064	0.7314
12	0.0368	0.1919	0.3327	0.4380	0.5167	0.5768	0.6240	0.6618	0.6929	0.7188
13	0.0314	0.1771	0.3154	0.4209	0.5004	0.5616	0.6098	0.6487	0.6807	0.7074
14	0.0271	0.1645	0.3002	0.4055	0.4858	0.5479	0.5971	0.6368	0.6696	0.6970
15	0.0236	0.1535	0.2867	0.3918	0.4726	0.5354	0.5854	0.6259	0.6594	0.6874
16	0.0207	0.1439	0.2746	0.3794	0.4605	0.5240	0.5747	0.6159	0.6500	0.6786
17	0.0183	0.1354	0.2637	0.3680	0.4495	0.5136	0.5649	0.6067	0.6413	0.6704
18	0.0164	0.1279	0.2539	0.3577	0.4393	0.5039	0.5557	0.5980	0.6332	0.6628
19	0.0147	0.1212	0.2449	0.3481	0.4299	0.4949	0.5472	0.5900	0.6256	0.6557
20	0.0133	0.1151	0.2367	0.3393	0.4212	0.4865	0.5392	0.5825	0.6185	0.6490
21	0.0120	0.1096	0.2291	0.3311	0.4130	0.4786	0.5318	0.5754	0.6119	0.6427
22	0.0110	0.1047	0.2221	0.3235	0.4054	0.4713	0.5247	0.5688	0.6056	0.6367
23	0.0100	0.1001	0.2156	0.3164	0.3983	0.4643	0.5181	0.5625	0.5996	0.6311
24	0.0092	0.0959	0.2096	0.3097	0.3916	0.4578	0.5119	0.5565	0.5940	0.6258
25	0.0085	0.0921	0.2039	0.3035	0.3852	0.4516	0.5059	0.5509	0.5886	0.6207
26	0.0078	0.0886	0.1987	0.2976	0.3792	0.4457	0.5003	0.5455	0.5835	0.6158
27	0.0073	0.0853	0.1937	0.2920	0.3735	0.4402	0.4949	0.5404	0.5786	0.6112
28	0.0068	0.0822	0.1891	0.2868	0.3681	0.4349	0.4898	0.5355	0.5740	0.6068
29	0.0063	0.0794	0.1847	0.2818	0.3630	0.4298	0.4849	0.5308	0.5695	0.6025
30	0.0059	0.0768	0.1806	0.2770	0.3581	0.4250	0.4802	0.5263	0.5653	0.5984
40	0.0033	0.0576	0.1491	0.2399	0.3192	0.3861	0.4423	0.4898	0.5302	0.5650
50	0.0021	0.0461	0.1285	0.2146	0.2919	0.3584	0.4150	0.4632	0.5046	0.5403

In the ball and roller bearing example, Table 6.2 is entered with $\beta = 2$, and a sample size of three. The corresponding table entry is 0.876. The characteristic life to be demonstrated is 500 hours. The number of hours that each system should be tested is 0.876×500 hours = 438 hours.

Thus, the zero-failure test plan to substantiate the ball and roller bearing system fix is to test three systems for 438 hours each. If all three systems are in balance at the end of the test, then the unbalance mode was either eliminated or significantly improved (with 90% confidence).

Table 6.2 may be recalculated at any confidence level by employing the following relationship:

$$\begin{aligned}
&(1-\text{Confidence}) = R^N, \quad \text{where } R = e^{-(t/\eta)^\beta} \\
&\text{Let } k = t/\eta, \text{ then} \\
&(1-\text{Confidence}) = \left(e^{-(k)^\beta}\right)^N \\
&\ln(1-\text{Confidence}) = N\left[-(k)^\beta\right] = -N(k)^\beta \\
&\text{So, } k = [(-1/N)\ln(1-\text{Confidence})]^{(1/\beta)}
\end{aligned} \tag{6.22}$$

Statistically, Eq. (6.22) is based on the null hypothesis that the new design is no better than the old. Given that the null hypothesis is true, the probability of passing the test is set equal to one minus the confidence level.

Thus, the zero-failure test plan to substantiate the ball and roller bearing system is to test three ball and roller bearing systems for 438 hours each **without failure** to show you have significantly improved the unbalance mode (with 90% confidence in this case).

We will cover the further problem when the Boss would ask "How significantly has it been improved" in the section titled "Reexpression of a Reliability Goal to Determine η."

Likewise, Eq. (6.22) can be also be rearranged:

$$N = \left(-\left(\frac{\eta}{t}\right)^\beta\right)^* \ln(1-\text{Confidence}) \tag{6.23}$$

which will allow the k value (η/t) to be calculated at any confidence level. Table 6.3 gives the result for k values at a confidence level of 90%.

Supplements 1 and 2 contain Tables 6.2 and 6.3 for 80%, 90%, 95%, and 99% confidence since these are the most commonly used confidence levels.

Weibull Zero-Failure Test Plans for Reliability Testing

We now turn our attention to zero-failure test plans for demonstrating a reliability goal when the underlying failure distribution is Weibull with known slope parameter β.

For our example we set up a reliability test for a turbine engine combustor's reliability goal of 99% reliability at 1800 cycles under service-like conditions. In this case, success was defined as a combustor having no circumferential cracks longer than 20 inches (out of a possible 53 inches). The number of cycles required to reach a 20-inch crack was known to follow a Weibull distribution with $\beta = 3$. How many combustors must be tested, and how many cycles must each accumulate, to demonstrate this goal with a high level of confidence?

First, the reliability goal is reexpressed as a characteristic life goal, and then the test plan is designed.

Table 6.3 Substantiation testing table for zero-failure test at **90% confidence.**

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
t/η	**infant mortality**	**Random**	**Early wear out**			**Old age rapid wear out**				
0.01	24	231	2303	23,026	230,259	---	---	---	---	---
0.02	17	116	815	5757	40,705	---	---	---	---	---
0.03	14	77	444	2559	14,772	85,281	492,370		---	---
0.04	12	58	288	1440	7,196	35,978	179,890	899,448	---	---
0.05	11	47	206	922	4,119	18,421	82,380	368,414	---	---
0.06	10	39	157	640	2,612	10,661	43,520	177,669	725,330	---
0.07	9	33	125	470	1,777	6,714	25,374	95,902	362,473	---
0.08	9	29	102	360	1,273	4,498	15,901	56,216	198,752	---
0.09	8	26	86	285	948	3,159	10,529	35,096	116,984	---
0.10	8	24	73	231	729	2,303	7,282	23,026	72,815	---
0.12	7	20	56	160	462	1,333	3,847	11,105	32,056	---
0.14	7	17	44	118	314	840	2,243	5,994	16,020	---
0.16	6	15	36	90	225	563	1,406	3,514	8,784	21,960
0.18	6	13	31	72	168	395	931	2,194	5,170	12,186
0.20	6	12	26	58	129	288	644	1,440	3,218	7,196
0.22	5	11	23	48	102	217	462	983	2,096	4,468
0.24	5	10	20	40	82	167	340	695	1,417	2,892
0.26	5	9	18	35	67	132	257	504	989	1,938
0.28	5	9	16	30	56	105	199	375	708	1,338
0.30	5	8	15	26	47	86	156	285	520	948
0.32	5	8	13	23	40	71	125	220	389	687
0.34	4	7	12	20	35	59	101	173	296	507
0.36	4	7	11	18	30	50	83	138	229	381
0.38	4	7	10	16	26	42	69	111	180	291
0.40	4	6	10	15	23	36	57	90	143	225
0.42	4	6	9	14	21	32	48	74	115	177
0.44	4	6	8	12	18	28	41	62	93	140
0.46	4	6	8	11	17	24	35	52	76	112
0.48	4	5	7	10	15	21	31	44	63	91
0.50	4	5	7	10	14	19	27	37	53	74
0.55	4	5	6	8	11	14	19	26	34	46
0.60	3	4	5	7	9	11	14	18	23	30
0.65	3	4	5	6	7	9	11	13	16	20
0.70	3	4	4	5	6	7	9	10	12	14
0.75	3	4	4	5	5	6	7	8	9	10
0.80	3	3	4	4	5	5	6	6	7	8
0.85	3	3	3	4	4	4	5	5	5	6
0.90	3	3	3	3	3	4	4	4	4	4
0.95	3	3	3	3	3	3	3	3	3	3
1.00	3	3	3	3	3	3	3	3	3	3

Reexpression of a Reliability Goal to Determine η

Reliability requirements generally assume one of the following forms (β is known in all forms):

Form 1: The requirement is stated as a reliability. The reliability of the unit is required to be at least X hours or cycles (or whatever the time unit is being used).

Form 2: The requirement is stated as a B life. The B10 life (or B1 life, or B.1 life, etc.) is required to be at least X hours or cycles. By definition, the unit has a 10% chance of failing before reaching its B10 life, a 1% chance of failing before reaching its B1 life, a 0.1% chance of failing before reaching its B1 life, etc.

Form 3: The requirement is stated as an MTTF. Using the known β, convert the MTTF into an equivalent η using

$$\eta = \frac{\text{MTTF}}{\Gamma\left(1 + \frac{1}{\beta}\right)} \tag{6.24}$$

Reliability requirements in any of these three forms are transformed into an equivalent characteristic life requirement. Given that the time-to-failure distribution is Weibull, with a known β, reliability at time t is a function of η. The equation for Weibull reliability,

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{6.25}$$

and solving for η:

$$\eta = \frac{t}{(-\ln R(t))^{\frac{1}{\beta}}} \tag{6.26}$$

Example 6.14 A turbine engine combustor reliability goal is a B1(1/100 probability) life of 1800 cycles or longer under service-like conditions. Success is defined as a combustor having no circumferential cracks longer than 20 inches (out of a possible 53 inches). The number of cycles required to reach a 20-inch crack was known to follow a Weibull distribution with $\beta = 3.0$. How many combustors must be tested, and how many cycles must each accumulate, to demonstrate this goal with 90% confidence?

Equation (6.26) can be used to express either Form 1 or 2 above into equivalent values of η. If the requirement is, for example that the reliability of the turbine engine combustor must be at least 0.99 at 1800 cycles ($\beta = 3$), then substituting $t = 1800$ and $R(t) = 0.99$ into Eq. (6.4) gives

$$\eta = \frac{t}{(-\ln R(t))^{\frac{1}{\beta}}} = \frac{1800}{(-\ln 0.99)^{\frac{1}{3}}} = 8341 \tag{6.27}$$

The 0.99 reliability requirement is equivalent to the requirement that η be at least 8340.9 cycles (see Figure 6.3). This is derived from “not more than 1% failures occur before 1800 cycles.”

Figure 6.4 illustrates an example based on a B10 life requirement.

Designing the Test Plan

Once the minimum characteristic life (η) requirement has been calculated, Tables 6.2 and 6.3 can be used to design the zero-failure test plan. In the combustor reliability example, the 99% reliability goal at 1800 cycles was reexpressed as an 8341-cycle characteristic life goal. Ten combustors were available for this reliability demonstration test. To find the test cycles required of each combustor,

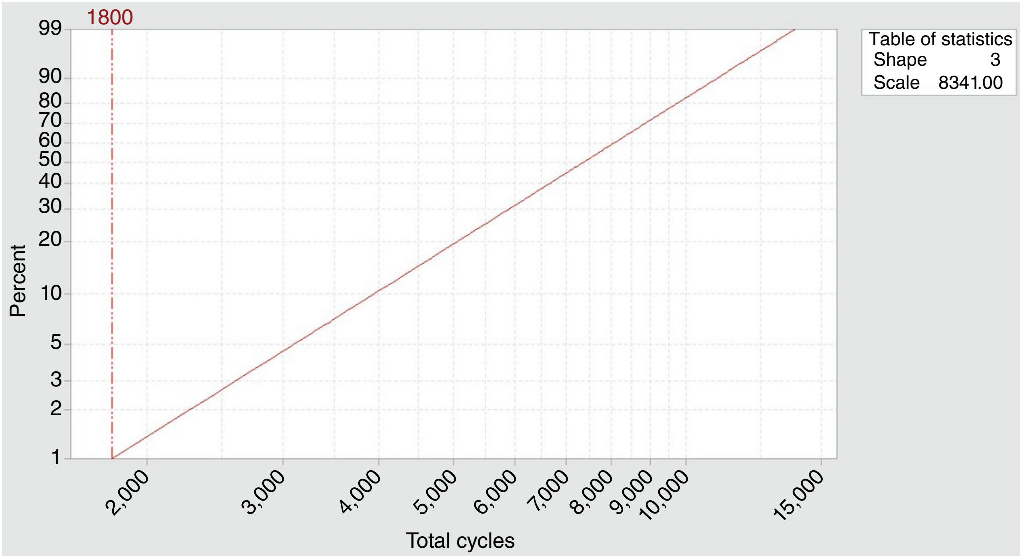


Figure 6.3 99% Reliability at 1800 cycles or B1 life of 1800 are equivalent when β = 3.

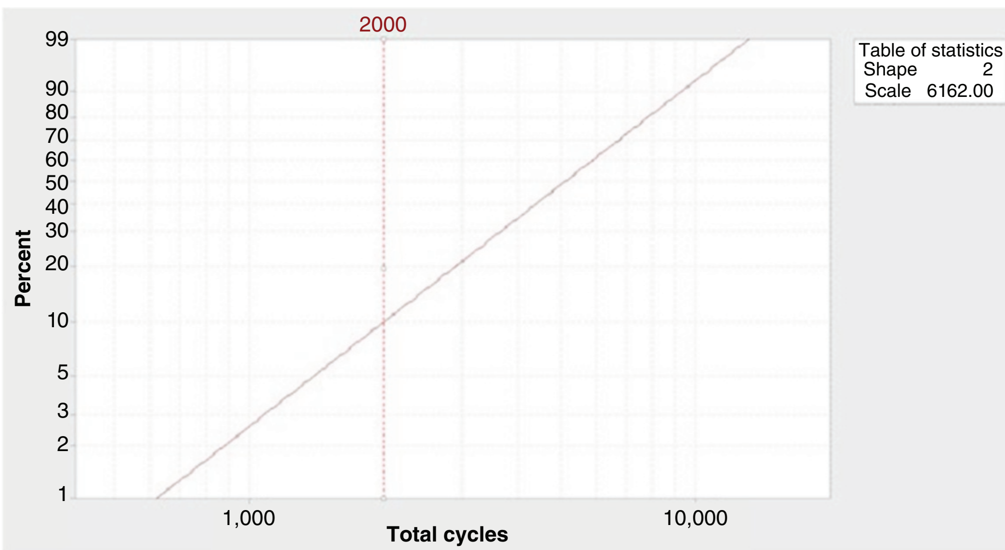


Figure 6.4 90% Reliability at 2000 cycles or B10 life of 2000 cycles with β = 2 are equivalent to η = 6162.

enter Table 6.2 with $\beta = 3.0$ and a sample size of 10. The corresponding table entry is 0.613. Multiply the table entry by the characteristic life requirement to find the test time required of each unit. In the combustor example, multiplying the Table 6.2 entry of 0.613 by the characteristic life requirement of 8341 cycles gives a test time of 0.613×8341 cycles = 5113.0 cycles. Thus, the 90% confidence zero-failure test plan to demonstrate 99% reliability at 1800 cycles requires testing 10 combustors for 5113 cycles each. If no combustor develops a circumferential crack longer than 20 inches, then the test is passed.

How many combustors are required if each can accumulate 7500 test cycles? To answer this, enter Table 6.3 with the assumed value of β, the Weibull slope parameter, and the ratio of the test time to the calculated characteristic life requirement. In the combustor example, $\beta = 3.0$, and the ratio of the test time to the calculated characteristic life requirement is

$$\frac{7500 \text{ test cycles per combustor}}{8341 \text{ cycles}} = 0.9 \tag{6.28}$$

The corresponding entry in Table 6.3 is 4. The resulting test plan requires testing four combustors for 7500 cycles each. If no combustor develops a circumferential crack longer than 20 inches, then the test is passed.

Test Units with Censored Times (due to Julius Wang, Fiat-Chrysler)

$$R(t_d) = \exp\left[\frac{\ln(1-C)}{\sum_{i=1}^{m}\left(\frac{T_i}{t_d}\right)^{\beta} + \sum_{j=1}^{n}\left(\frac{T_j}{t_d}\right)^{\beta}}\right] \tag{6.29}$$

where

$R(t)$ = reliability at time "t_d"
t_d = design life or life at a reliability to be demonstrated
N = total sample size, $=n + m$
T_i = total test time of each part where T_i represents the specific censored time of each of the m censored parts
T_j = total test time of each part where T_j represents the specific uncensored time of the individual part, and n is the total number of uncensored part times
β = Weibull shape or slope parameter
C = statistical confidence level specified as probability (e.g. 90% confidence is represented 0.90).

This equation suggests that each part can be stopped at different times. The usefulness of this equation is for trading off on number of parts and test times when certain parts are no longer available during the testing. This may be due to the fact that certain testing fixtures are broken, and those parts may be required for other purposes and be pulled out of testing. Note that the basic test plan is not modified.

Example 6.15 The plan is to test each of the budgeted parts without failure to demonstrate 95% reliability at 1000 hours (design life in lab testing) at 90% statistical confidence level. The Weibull slope is assumed to be 3.0. The budget will allow 14 parts to be tested.

First, using the equation for reliability for a Weibull failure mode:

$$R = e^{-(t/\eta)^{\beta}}$$

So, in this case, $0.95 = e^{-(1000/\eta)^3}$, or $\eta = 2691$ hours (see Figure 6.5).

Using the 0 failure table for 90% confidence (Table 6Sup1.2), entering at the budgeted number of parts = 14, the characteristic multiplier is 0.548.

Then, $0.548 \times 2691 = 1475$ hours on each of the 14 parts.

Right in the middle of the testing, two parts were stopped at 450 hours due to a broken test stand connector. At this time, another department requires these two parts for other use, so you lose these

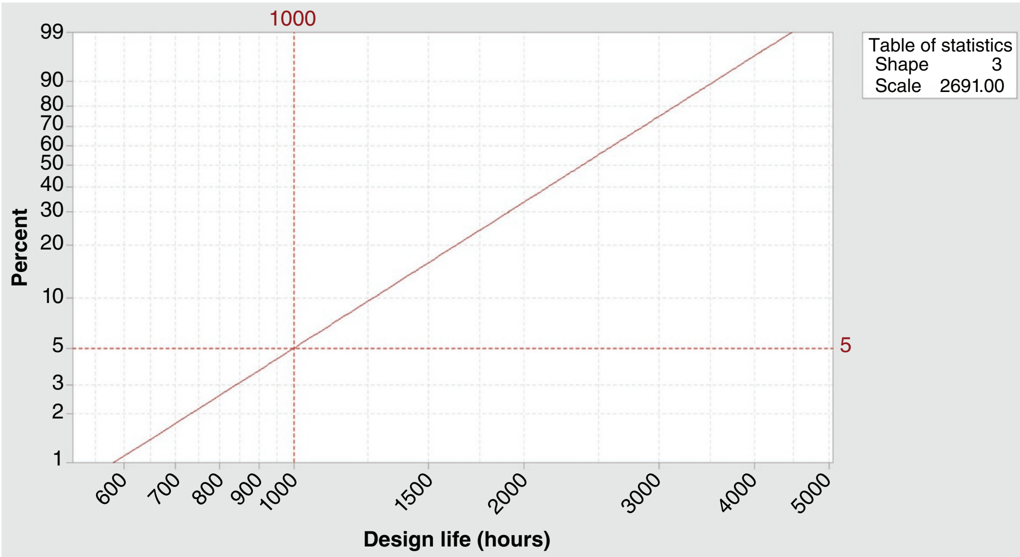


Figure 6.5 Demonstrated design life of 0.95 implies that η = 2691 hours.

two parts! How long should the other 12 parts be tested to maintain the reliability demonstration requirement?

In this case, substituting in Eq. (6.29)

$$R(t_d) = 0.95 = \exp\left[\frac{\ln(1-0.90)}{2\left(\frac{450}{1000}\right)^3 + 12\left(\frac{T}{1000}\right)^3}\right] \tag{6.30}$$

Solving, $T = 1550$ hours. Hence, the remaining 12 parts will each be tested to 1550 hours, rather than 1475 hours as originally planned.

This technique can be generally applied for each suspension/censored time (i.e. not all censored parts need have the same time).

Total Test Time

Under **Designing Test Plans** two reliability test plans were constructed to demonstrate a characteristic life of 8340.9 cycles, with 90% confidence.

So, now let us discuss the next steps that would be taken to complete the combustor testing and reliability demonstration.

Ten combustors for a modern-day fighter engine would be too expensive to manufacture. In addition, the combustor testing cost of running even one combustor for 5113 cycles on a rig duplicating a typical 2 hour mission would take 400+ days to run. So, testing 10 combustors is unrealistic, and testing 4 combustors is probably unrealistic as well. So what is the answer???

The answer is accelerated life testing. By putting four combustors on test in the same test rig and running an *accelerated* mission profile, you could run the equivalent of $0.832*8341 = 5774$ cycles in 8–10 days of continuous running.!!

More about this in the section titled "Accelerated Life Testing".

Why Not Simply Test to Failure?

Recall the ball and roller bearing unbalance test from the earlier discussion. It was determined that three ball and roller bearings could be tested for 438 hours each, and if none of the ball/roller bearings were unbalanced after that time, you could be 90% confident that your new design had a life greater than 500 hours.

Why not test all three to failure?

1) Testing each part of the three ball/roller bearings to failure (unbalance) would take much longer on the average. Suppose that the redesigned parts had twice the characteristic life; then, each of the redesigned parts would run two times as long, costing two times as much for the test time.
2) Also, when constructing your three *failure* Weibull with a lower 90% confidence bound on the Weibull line, you have only a ~20% chance of a 500-hour life at 0.9 reliability.
3) Finally, what will happen if your "test to failure" does not prove that your new design is significantly better than 500 hours? Redesign? Or maybe test three more of the new design?

To assess your chances of passing a zero-failure test ahead of time, let us analyze what the trade-offs are.

Example 6.16 So, to find the probability of successfully completing a zero-failure test for field-bearing failure mode $\beta = 2.0$, $\eta = 1200$ hours where the units TRUE characteristics life is 2400 hours is

$$r = \frac{\text{True } \eta}{\eta \text{ Demonstrated}} = \frac{2400}{1200} = 2 \tag{6.31}$$

In Table 6.4, at a $\beta = 2$ and $r = 2$, read that 0.562. or the probability of passing the zero-failure test is ~0.56.

You can also read this off of Figure 6.6 (well maybe not to two decimal places).

Table 6.4 and the curves were generated using the following equation:

$$\text{Probability of Passing} = R^N = \left(e^{-\left(\frac{k}{r}\right)^{\beta}}\right)^N \tag{6.32}$$

where

$t = k\eta_{\text{Goal}}$ = test time per unit
k = Table 6.2 coefficient
r = Ratio of $\eta_{\text{New}}/\eta_{\text{Goal}}$
N = Number of units tested

6.5 How to Reduce Test Time

Leonard G. Johnson (General Motors Research) in his book *The Statistical Treatment of Fatigue Experiments* suggested three ways to reduce test time.

Run (Simultaneously) More Test Samples Than You Intend to Fail

Suppose that you have funding for testing 20 samples, put them all on test at the same time and stop after 10 have failed (saving test time on the remaining 10). This allows you to produce a 10-point Weibull with 10 right censored (unfailed) points.

Table 6.4 Probability of passing zero-failure test.

(*k*/*r*)	β = 0.5	β = 1.0	β = 1.5	β = 2.0	β = 2.5	β = 3	β = 3.5	β = 4.0	β = 4.5	β = 5
1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
1.1	0.111	0.123	0.136	0.149	0.163	0.177	0.192	0.207	0.223	0.239
1.2	0.122	0.147	0.173	0.202	0.232	0.264	0.296	0.329	0.363	0.396
1.3	0.133	0.170	0.212	0.256	0.303	0.351	0.399	0.447	0.493	0.538
1.4	0.143	0.193	0.249	0.309	0.371	0.432	0.492	0.549	0.603	0.652
1.5	0.153	0.215	0.286	0.359	0.434	0.505	0.573	0.635	0.690	0.738
1.6	0.162	0.237	0.321	0.407	0.491	0.570	0.641	0.704	0.757	0.803
1.7	0.171	0.258	0.354	0.451	0.543	0.626	0.698	0.759	0.809	0.850
1.8	0.180	0.278	0.385	0.491	0.589	0.674	0.745	0.803	0.849	0.885
1.9	0.188	0.298	0.415	0.528	0.630	0.715	0.784	0.838	0.880	0.911
2	0.196	0.316	0.443	0.562	0.666	0.750	0.816	0.866	0.903	0.931
2.1	0.204	0.334	0.469	0.593	0.697	0.780	0.842	0.888	0.922	0.945
2.2	0.212	0.351	0.494	0.621	0.726	0.806	0.864	0.906	0.936	0.956
2.3	0.219	0.367	0.517	0.647	0.751	0.828	0.883	0.921	0.947	0.965
2.4	0.226	0.383	0.538	0.670	0.773	0.847	0.898	0.933	0.956	0.971
2.5	0.233	0.398	0.558	0.692	0.792	0.863	0.911	0.943	0.963	0.977
2.6	0.240	0.412	0.577	0.711	0.810	0.877	0.922	0.951	0.969	0.981
2.7	0.246	0.426	0.595	0.729	0.825	0.890	0.931	0.958	0.974	0.984
2.8	0.253	0.439	0.612	0.746	0.839	0.900	0.939	0.963	0.978	0.987
2.9	0.259	0.452	0.627	0.760	0.851	0.910	0.946	0.968	0.981	0.989
3	0.265	0.464	0.642	0.774	0.863	0.918	0.952	0.972	0.984	0.991
3.1	0.270	0.476	0.656	0.787	0.873	0.926	0.957	0.975	0.986	0.992
3.2	0.276	0.487	0.669	0.799	0.882	0.932	0.961	0.978	0.988	0.993
3.3	0.282	0.498	0.681	0.809	0.890	0.938	0.965	0.981	0.989	0.994
3.4	0.287	0.508	0.693	0.819	0.898	0.943	0.969	0.983	0.991	0.995
3.5	0.292	0.518	0.704	0.829	0.904	0.948	0.972	0.985	0.992	0.996
3.6	0.297	0.527	0.714	0.837	0.911	0.952	0.974	0.986	0.993	0.996
3.7	0.302	0.537	0.724	0.845	0.916	0.956	0.977	0.988	0.994	0.997
3.8	0.307	0.546	0.733	0.853	0.921	0.959	0.979	0.989	0.994	0.997
3.9	0.312	0.554	0.742	0.860	0.926	0.962	0.981	0.990	0.995	0.997
4	0.316	0.562	0.750	0.866	0.931	0.965	0.982	0.991	0.996	0.998
4.1	0.321	0.570	0.758	0.872	0.935	0.967	0.984	0.992	0.996	0.998
4.2	0.325	0.578	0.765	0.878	0.938	0.969	0.985	0.993	0.996	0.998
4.3	0.329	0.585	0.772	0.883	0.942	0.971	0.986	0.993	0.997	0.998
4.4	0.334	0.593	0.779	0.888	0.945	0.973	0.987	0.994	0.997	0.999
4.5	0.338	0.599	0.786	0.893	0.948	0.975	0.988	0.994	0.997	0.999
4.6	0.342	0.606	0.792	0.897	0.951	0.977	0.989	0.995	0.998	0.999
4.7	0.346	0.613	0.798	0.901	0.953	0.978	0.990	0.995	0.998	0.999
4.8	0.350	0.619	0.803	0.905	0.955	0.979	0.991	0.996	0.998	0.999
4.9	0.353	0.625	0.809	0.909	0.958	0.981	0.991	0.996	0.998	0.999
5	0.357	0.631	0.814	0.912	0.960	0.982	0.992	0.996	0.998	0.999

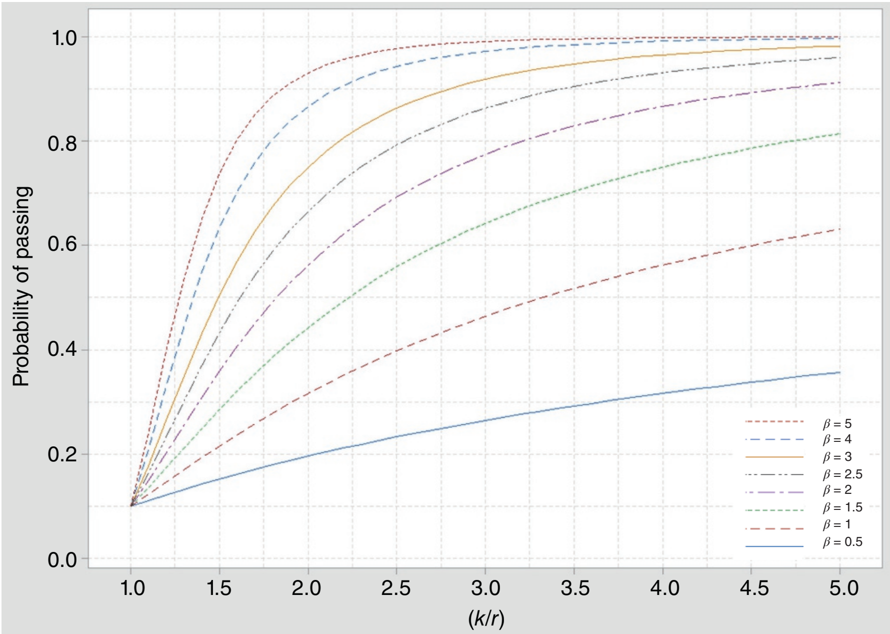


Figure 6.6 Probability of passing a zero-failure test.

For a $\beta = 1$, the median time required for failing 10 out of 20 is 24% of the median time required to fail 10 out of 10.

For a $\beta = 3$, the median time required for failing 10 out of 20 is 62% of the median time required to fail 10 out of 10.

Sudden Death Testing

In sudden death testing, the total sample to be tested (from a recommended as few as nine units to more than 15 units, depending on the cost) is divided into groups of three or more, all groups being of equal size. All units in each group are (preferably) tested simultaneously. When the first unit in a group fails, the group has failed (weakest link), and testing is stopped on the remaining units in the group. Hence, the name "sudden death" testing. Sudden death testing has reduced bearing test times by 60–75%; saving experimental test time, and just as important, has saved calendar time. In short, if the cost of test to failure and the cost of a unit to put on test are reasonable, "sudden death" testing can be a good alternative.

Suppose that you have 40 bearings and divide them into 5 groups of 8 bearings each.

The median rank of the first failure in each group of 8 is as we saw in Chapter 5 on the Weibull distribution, where

$$\text{Median Rank} = \frac{i - 0.3}{N + 0.4}$$

so, for the 1st failure in 8, $\text{MR}_1 = \dfrac{1 - 0.3}{8 + 0.4} = 0.083.$

Therefore, the failure time each of the first failures in the 5 groups will be on the Sudden death 8.3% line. From this we can extrapolate to the Weibull for the entire population of 40 bearings (the remaining bearings in each group are censored at the time of the first failure in the group).

Example 6.17 Suppose that the first failure of 8 in each of the six groups failed at 711, 456, 1341, 1214, 1137, and 619 hours.

A Weibull plot can be produced with the 6 failures and 42 censored times (Figure 6.7).

The MINITAB data input would look like Table 6.5.

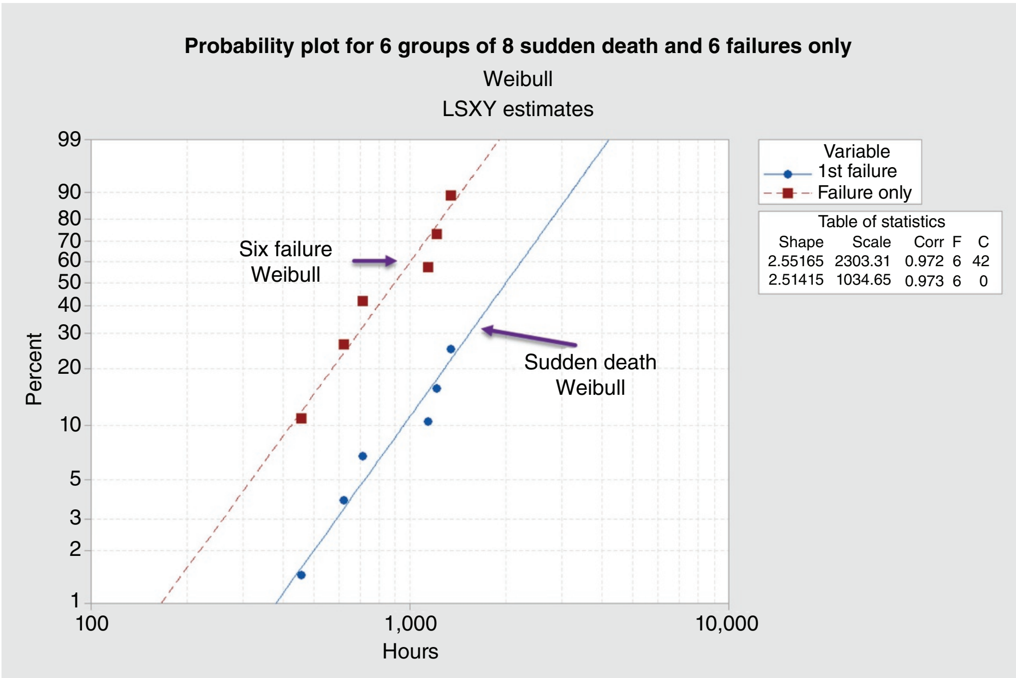


Figure 6.7 Sudden death 6 failure Weibull has approximately the same slope as the Weibull of 6 failures with 42 suspensions.

Table 6.5 Combined 6 failures with 42 censored times.

	1st Failure	Freq	Censor
Grp1	711	1	1
Grp2	456	1	1
Grp3	1341	1	1
Grp4	1214	1	1
Grp5	1137	1	1
Grp6	619	1	1
	711	7	0
	456	7	0
	1341	7	0
	1214	7	0
	1137	7	0
	619	7	0

Here, Censor = 1 indicates failed time, and Censor = 0 indicates a censored time. Freq indicates the number of points at the time.

You could also solve this problem starting with the 6 point Weibull and "shifting" it based on the of the population:

Where characteristic life of 6 failures (η_6) = 1034 hours.

Then,

$$\left(\frac{1}{8}\right) = 1 - \exp\left[-\left(\frac{1034}{\widetilde{\eta}_{SD}}\right)\right]^{2.5} \Rightarrow \widetilde{\eta}_{SD} = 2315 \text{ hours, which is almost the same as actual } \eta_{SD}$$

Example 6.18 (data type analysis based on ideas from Abernethy 2006).

A company tests 16 bearings to failure out of every batch of 100,000 bearings. To compare the efficiency of sudden death testing relative to testing all 16 to failure, the 16 bearings were divided into 4 sets of 4 each. Each set of 4 was tested until the first failure occurred, but then the remaining three were all tested to failure as well. This same procedure was followed for the other three sets of 4 bearings. At the end, they had results of a sudden death test AND results of having tested all bearings in order to compare the results. The data are in Table 6.6.

Analyzing this as a sudden death test, the first failure in each set, along with that failure time 3X as a censored time, will produce a Weibull (Figure 6.8).

Analyzing the complete 16 failure data produces this Weibull (Figure 6.9).

Conclusion: In this case, sudden death testing produced a slightly smaller B10 life. However, the difference in potential test time savings is significant:

Sudden death: 608,389 total test cycles.

Testing all to failure test time = 1,407,407 cycles.

A test time saving of ~800,000 cycles.

Sudden death testing is not ALWAYS this good; in this case it was. A small number of bearings tested overall and hence in each set gives a wider confidence bound. So, the more items overall, and hence in each group will result in smaller confidence interval and the closer the sudden death testing will be (and still save considerable test time). However, for expensive test articles, and hence smaller numbers of articles available (~15 or fewer), sudden death testing is not an optimal choice.

Sequential Testing

Sequential testing is a method of experimental testing (and statistical analysis) whose characteristic feature is that the number of observations required by the procedure is *not determined in advance of the experiment*. Essentially, this approach lets one design a large-scale experiment in successive

Table 6.6 Sudden death vs "total life test."

Set 1	Set 2	Set 3	Set 4
18,993	107,470	97,783	114,862
52,196	105,354	93,105	69,910
73,178	88,331	180,174	97,604
27,520	182,614	25,562	72,751

16 bearings tested to failure as 4 groups of 4 where we can analyze the differences and advantages of one approach to the other.

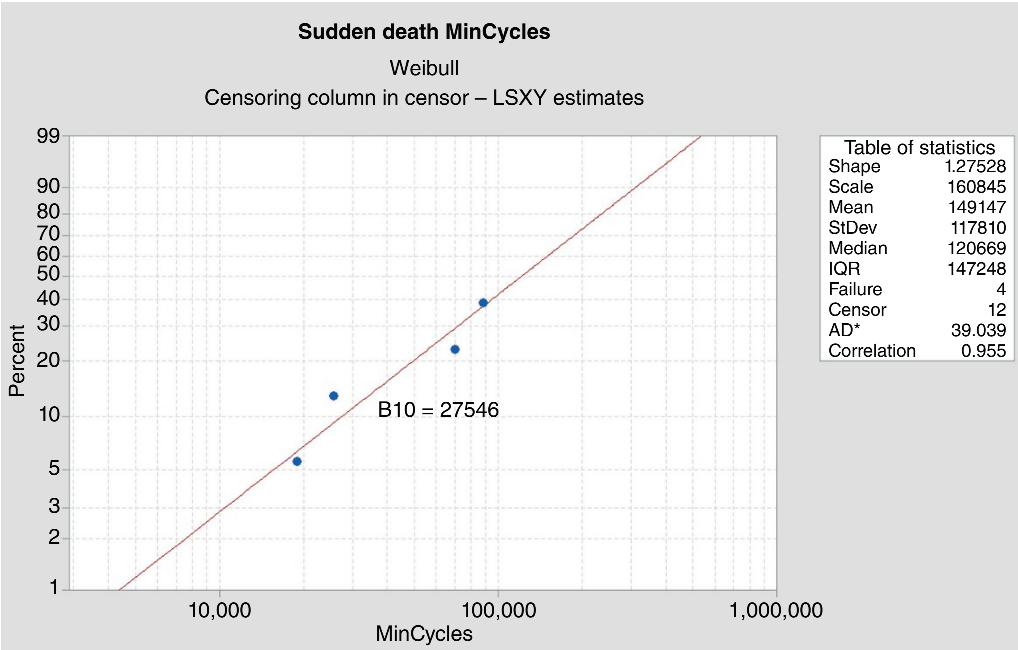


Figure 6.8 Analyzing the data as sudden death testing gives B10 life of 27,546 cycles.

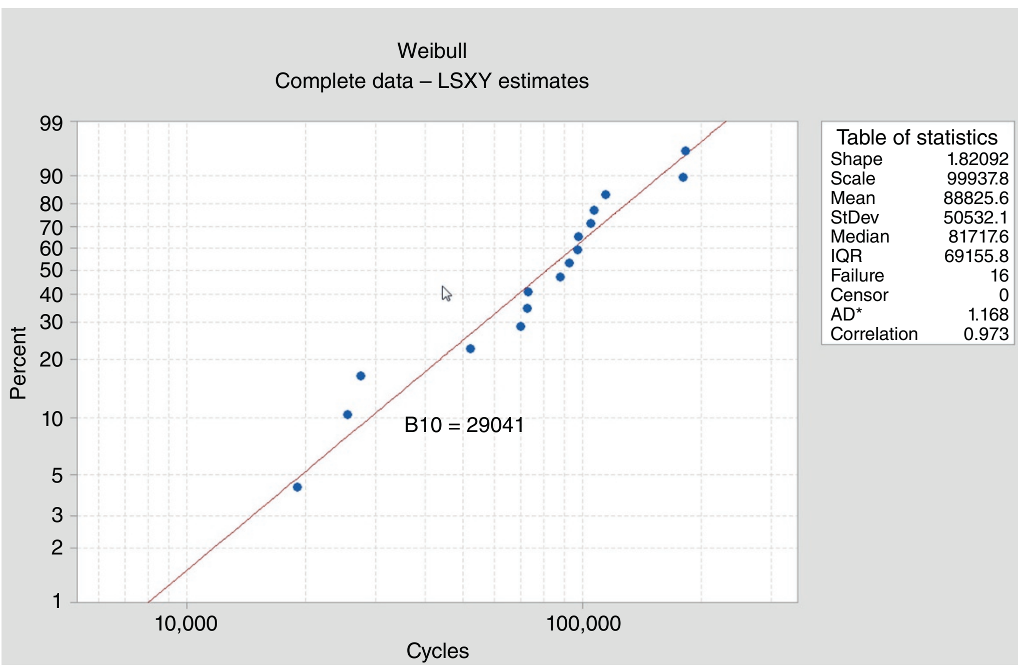


Figure 6.9 Testing all 16 bearings to failure gives B10 life of 29,041cycles.

stages, where the next stage depends on what occurred in the previous stage. Specifically, the decision to terminate or continue the experiment depends, at each stage, on the results of the observations previously made. A merit of the sequential method, as applied to reliability testing, is that test procedures can be constructed which require, on the average, a substantially smaller number of observations than equally reliable test procedures based on a predetermined number of observations.

The *sequential probability ratio test* (SPRT) was devised by Wald in 1943 mainly for the purpose of testing statistical hypotheses. A comparison of this particular sequential test procedure with any other (sequential or nonsequential) was shown by Wald to give the greatest possible saving in the average number of observations, when used for testing a simple hypothesis against a single alternative. The sequential probability ratio test frequently results in a saving of about 50% in the number of observations over the most efficient test procedure based on a fixed number of observations.

L.G. Johnson took Wald's idea and developed the methodology for sequential testing. The purpose of sequential testing is to establish in the shortest possible test time and at a minimum cost whether reliability is equal to or better than a specified minimum.

The method produces one of three decisions at any point of the sequence of tests:

- Accept the hypothesis that the higher (MTBF) has been demonstrated (terminate test)
- Reject the hypothesis that the higher (MTBF) has been demonstrated (terminate test)
- Continue testing.

Figure 6.10 is the graphic used to illustrate what decisions have to be made as a product is tested, until the product either is "accepted" as having demonstrated higher reliability than the product it was replacing or "rejected" as not having shown a desired reliability.

Key parameters to define for sequential reliability test:

- Minimum acceptable reliability (m_1)
  - Mean time between failure = m_1
    (minimum reliability requirement)
- Upper reliability value (m_0)
  - Mean time between failure = m_0
    (value based on producer input, the estimated reliability)

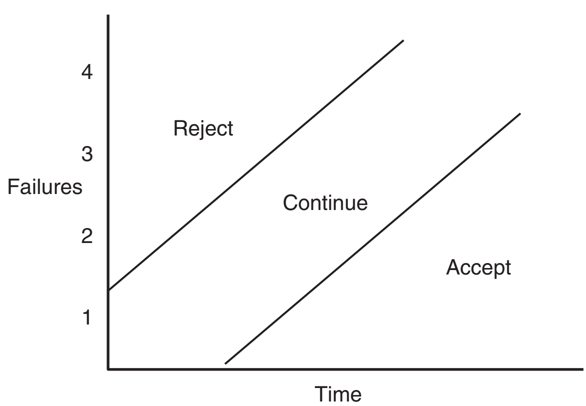


Figure 6.10 Graphical outline of a sequential test (open ended).

Threshold probabilities

- Consumer risk (β)
  - Probability of accepting as good when bad (worse than m_1)
    (probability of rejecting as bad when bad $= 1-\beta$)
- Producer risk (α)
  - Probability of rejecting as bad when good (better than m_0)
    (probability of accepting good $= 1-\alpha$)

Accepted risks are defined by the threshold probability ratios:

$$A = \frac{1-\beta}{\alpha} = \frac{\text{Probability of correctly rejecting}}{\text{Probability of rejecting when should have accepted}} \tag{6.33}$$

$$B = \frac{\beta}{1-\alpha} = \frac{\text{Probability of accepting when should have rejected}}{\text{Probability of correctly accepting}} \tag{6.34}$$

The Poisson distribution is used to calculate the likelihood of a number of failures within a specific time period as follows:

$P_1 =$ probability of r failures given m_1
$P_0 =$ probability of r failures given m_0

$$\text{Calculating } P(r) = \text{probability of } r \text{ failures given } m = \left(\frac{t}{m}\right)^r \frac{e^{-t/m}}{r!} \tag{6.35}$$

where

$t =$ test time
$m =$ mean time between failure (MTBF)
$r =$ number of failures

The Sequential Probability Ratio Test (SPRT) determines the status during testing:

$$\text{Rule 1}: \frac{P_1}{P_0} < B \quad \text{ACCEPT} \tag{6.36}$$

$$\text{Rule 2}: \frac{P_1}{P_0} > A \quad \text{REJECT} \tag{6.37}$$

$$\text{Rule 3}: B < \frac{P_1}{P_0} < A \quad \text{CONTINUE TESTING} \tag{6.38}$$

Minimum test time equations:

In order to produce a graph similar to that illustrated in Figure 6.10, the following equations need to be solved (easily put into EXCEL™):

$$\text{For Accept}: \quad T_{\min} = \frac{\text{Ln}(B) + r\text{Ln}\left(\frac{m_1}{m_0}\right)}{(m_1 - m_0)/(m_1 m_0)} \tag{6.39}$$

$$\text{For Reject}: \quad T_{\min} = \frac{\text{Ln}(A) + r\text{Ln}\left(\frac{m_1}{m_0}\right)}{(m_1 - m_0)/(m_1 m_0)} \tag{6.40}$$

Table 6.7 Calculating plot points for a sequential testing plot.

A	B	C	D	E	F
1					
2					
3					
4		$\alpha =$	0.1	$m_1 =$	100
5		$\beta =$	0.1	$m_0 =$	200
6					
7			$A =$	9.000	
8			$B =$	0.111	
9					
10			T_{min}		
11		r	Accept	Reject	
12		0	439.4	−439.4	
13		1	578.1	−300.8	
14		2	716.7	−162.2	
15		3	855.3	−23.6	
16		4	994.0	115.1	
17		5	1132.6	253.7	
18		10	1825.7	946.8	

Example 6.19 Suppose that we have the following input to a sequential test:

- Consumer risk = $\beta = 0.1$ or 10% chance that bad part is accepted
- Producer risk = $\alpha = 0.1$ or 10% chance that good part is rejected
- Minimum MTBF required = $m_1 = 100$ hours
- Upper MTBF value assumed to be $2m_1 = m_0 = 200$ hours

Then, $A = \frac{1-\beta}{\alpha} = \frac{1-0.1}{0.1} = 9.0$ and $B = \frac{\beta}{1-\alpha} = \frac{0.1}{0.9} = 0.111$

And calculating Table 6.7 (using EXCEL), where the cells C12 and D12 are, for example:

```
Cell D12=(LN($E$8)+$C12*LN($F$4/$F$5))/(($F$4-$F$5)/($F$5*$F$4))
Cell E12=(LN($E$7)+$C12*LN($F$4/$F$5))/(($F$4-$F$5)/($F$5*$F$4))
```

Plotting this as a sequential testing plot (Figure 6.11).

To illustrate a test case, using the same ground rules as in Example 6.9.

Example 6.20 Input to the test:

- Consumer risk = $\beta = 0.1$ or 10% chance that bad part is accepted
- Producer risk = $\alpha = 0.1$ or 10% chance that good part is
- Minimum MTBF required = $m_1 = 100$ hours
- Upper MTBF value assumed to be $2m_1 = m_0 = 200$ hours

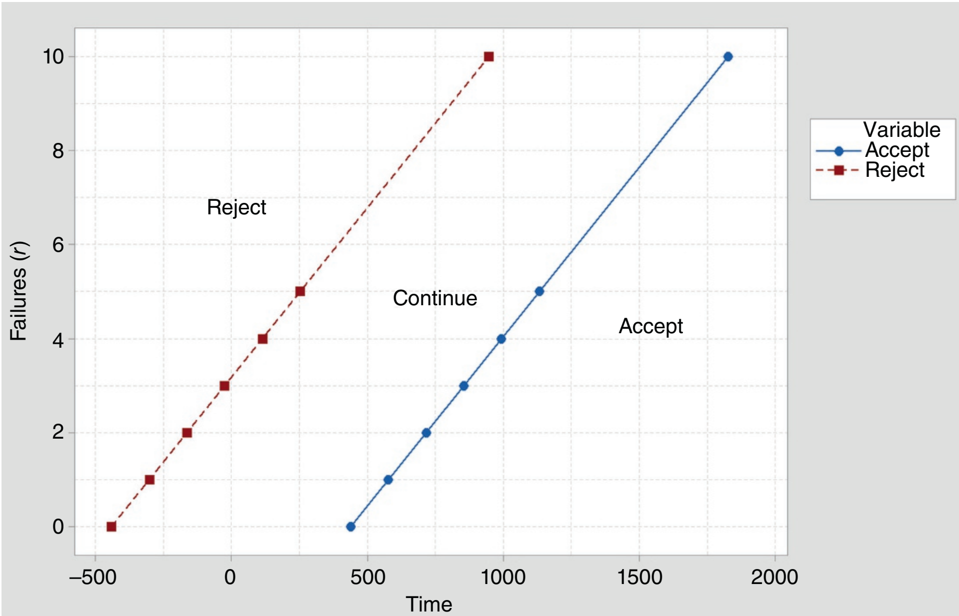


Figure 6.11 Example 6.9. Sequential test plan.

$$A = \frac{1-\beta}{\alpha} = \frac{1-0.1}{0.1} = 9.0 \quad \text{and} \quad B = \frac{\beta}{1-\alpha} = \frac{0.1}{0.9} = 0.111$$

First test results: No failures for first 50 hours (Figure 6.12).
Calculating the P_1/P_0 ratio gives the same result:

$$P_1(0) = \left[\frac{t}{m_1}\right]^r \frac{e^{-t/m_1}}{r!} = \left[\frac{50}{100}\right]^0 \frac{e^{-50/100}}{0!} = 0.61$$

$$P_0(0) = \left[\frac{t}{m_0}\right]^r \frac{e^{-t/m_0}}{r!} = \left[\frac{50}{200}\right]^0 \frac{e^{-50/200}}{0!} = 0.78$$

Then,

$$\frac{P_1}{P_0} = 0.78 \quad \text{CONTINUE TEST} \quad (\text{Rule 3})$$

Second test result: First failure occurs at 210 hours (Figure 6.13).
Again, using the P_1/P_0 ratio gives the same result:

$$P_1(1) = \left[\frac{t}{m_1}\right]^r \frac{e^{-t/m_1}}{r!} = \left[\frac{210}{100}\right]^1 \frac{e^{-210/100}}{1!} = 0.26$$

$$P_0(1) = \left[\frac{t}{m_0}\right]^r \frac{e^{-t/m_0}}{r!} = \left[\frac{210}{200}\right]^1 \frac{e^{-210/200}}{1!} = 0.37$$

Then,

$$\frac{P_1}{P_0} = 0.70 \quad \text{CONTINUE TEST} \ (\text{Rule 3})$$

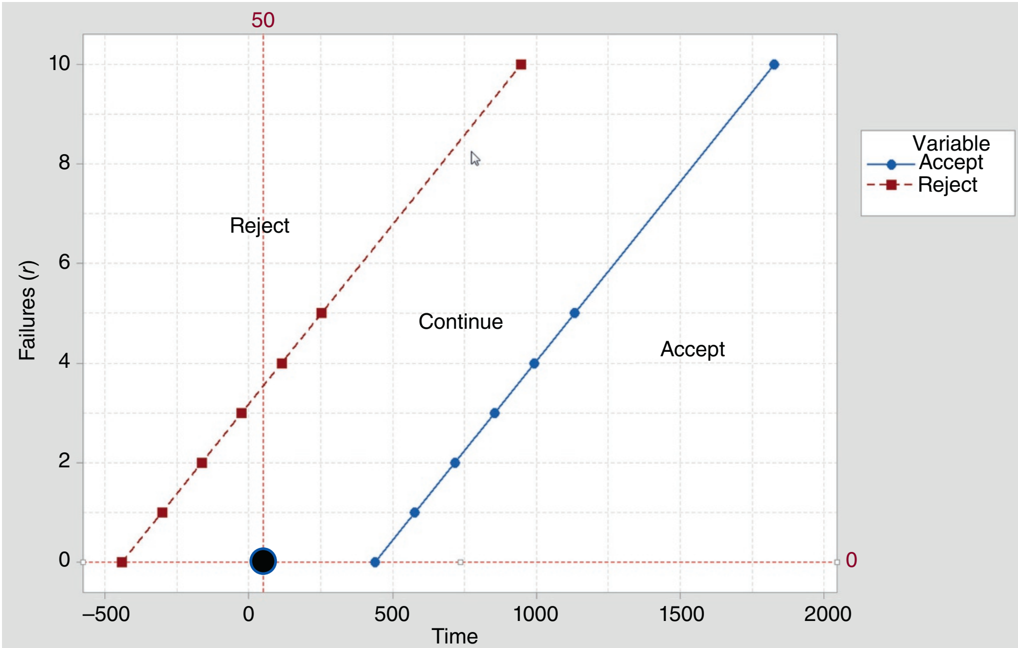


Figure 6.12 Plotting 0 failures at 50 hours shows "continue test."

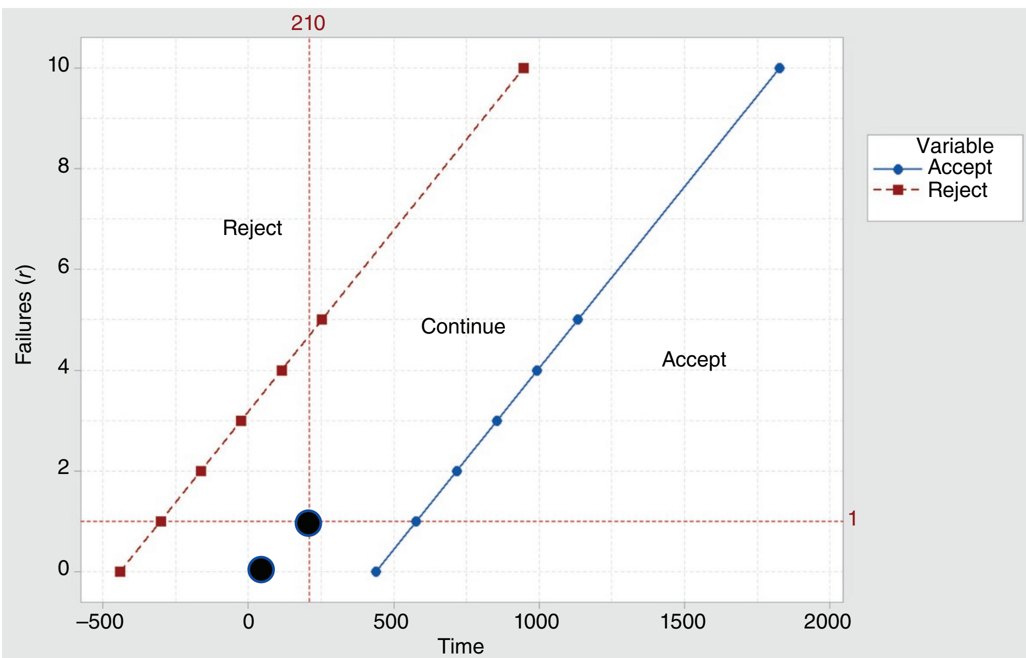


Figure 6.13 Plotting 1 failure at 210 hours shows "continue test."

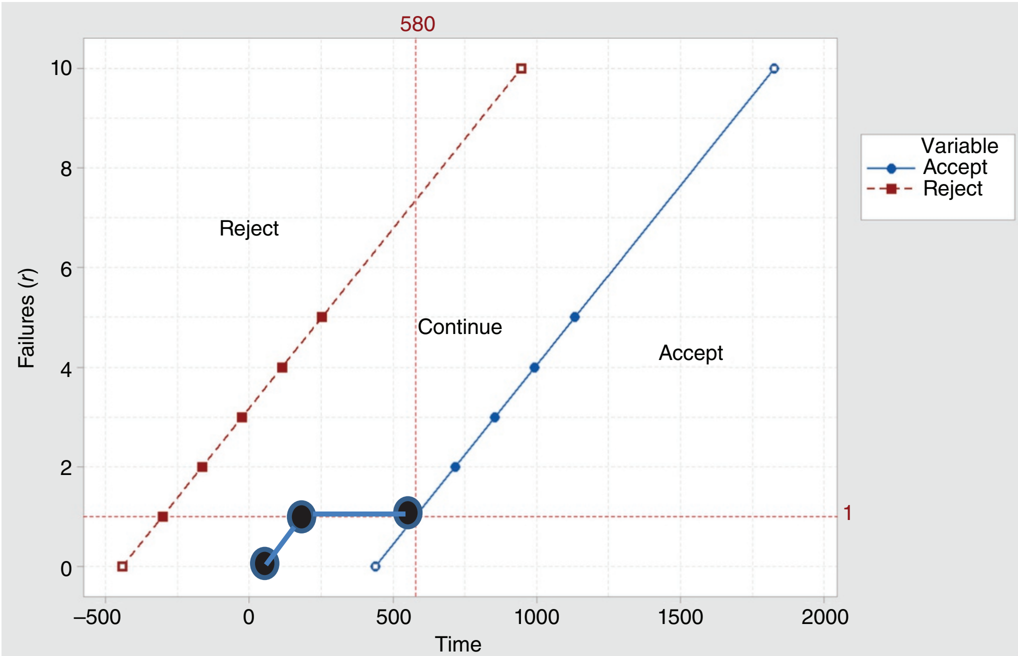


Figure 6.14 Plotting 1 failure at 580 hours shows "ACCEPT."

Third test result: First failure occurs at 210 hours, and no failure for another 370 hours (Figure 6.14).

Again, using the P_1/P_0 ratio gives the same result:

$$P_1(1) = \left[\frac{t}{m_1}\right]^r \frac{e^{-t/m_1}}{r!} = \left[\frac{580}{100}\right]^1 \frac{e^{-580/100}}{1!} = 0.02$$

$$P_0(1) = \left[\frac{t}{m_0}\right]^r \frac{e^{-t/m_0}}{r!} = \left[\frac{580}{200}\right]^1 \frac{e^{-580/200}}{1!} = 0.16$$

Then,

$$\frac{P_1}{P_0} = 0.11 \text{ ACCEPT (Rule 1) Terminate Test}$$

The graphic in Figure 6.14 is recommended for explaining the fact that it took only 580 hours of testing to show you had two times the current MTBF.

Example 6.21 Input to the test:

- Consumer risk $= \beta = 0.1$ or 10% chance that bad part is accepted
- Producer risk $= \alpha = 0.1$ or 10% chance that good part is rejected
- Minimum MTBF required $= m_1 = 100$ hours
- Upper MTBF value assumed to be $10m_1 = m_0 = 1000$ hours

$$A = \frac{1-\beta}{\alpha} = \frac{1-0.1}{0.1} = 9.0 \quad \text{and} \quad B = \frac{\beta}{1-\alpha} = \frac{0.1}{0.9} = 0.111$$

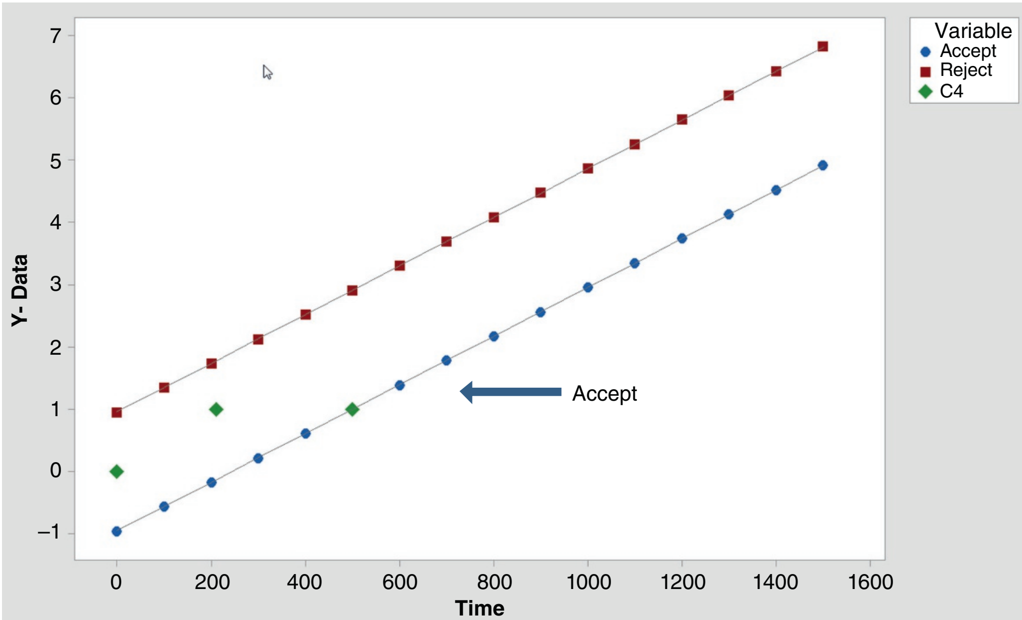


Figure 6.15 Plotting all failures and final conclusion: ACCEPT H_0.

Sequence:

1) No failure for first 50 hours $P_1/P_0 = 0.64$ ⟹ Continue Test
2) First failure occurs at 210 hours $P_1/P_0 = 1.52$ ⟹ Continue Test
3) No failures for 290 additional hours $P_1/P_0 = 0.11$ ⟹ ACCEPT H_0 Upper MTBF = 1000 hours (Figure 6.15)

Impact of choices of α, β, and m_0

- Smaller consumer (b) or producer (a) risk values result in longer tests
  - $a = 0.10$, $b = 0.10 \Rightarrow A = 0.9/0.1 = 9.00$, $B = 0.1/0.9 = 0.111$
  - $a = 0.10$, $b = 0.05 \Rightarrow A = 0.95/0.1 = 9.50$, $B = 0.05/0.9 = 0.056$
  - $a = 0.01$, $b = 0.01 \Rightarrow A = 0.99/0.01 = 99.0$, $B = 0.01/0.99 = 0.010$
- Increasing the upper MTBF value, m_0, decreases test time.
  - A greater m_0 value increases likelihood that test will reject when true and MTBF is worse than m_0 but better than m_1
  - Risk of rejecting equipment better than m_0 based on a.

6.6 Normal and Lognormal Reliability Testing

As mentioned in Chapter 4, while the Weibull distribution can fit approximately 95% (author's experience over 45 years of reliability analysis) of failure data well, the normal and lognormal will sometimes fit failure data better than a Weibull (note that the normal distribution is "bell shaped," and a Weibull with $\beta = 3.4$ will be approximately normal); hence, a normal distribution can sometimes fit a wear-out mode as long as the time scale is significantly large. The lognormal, of course, has a log time scale and hence can fit any failure mode that fits the "proportional effect theory" as discussed in Chapter 4.

We now discuss life test plans for the normal and lognormal distributions. These test plans are developed to assure a certain mean life (and hence any other quantile) when the life test is stopped at a time t and when the observed failures does not exceed a prescribed number "c."

Some of the background statistical theory for this section is explained in the paper by Gupta (1962).

Recall from Chapter 4 the lognormal as a two-parameter distribution:

$$\text{PDF}: \quad f_y(y) = \frac{1}{\omega y\sqrt{2\pi}} e^{-\left[\frac{1}{2\omega^2}\left\{\ln\left(\frac{y}{y_0}\right)\right\}^2\right]} \tag{6.41}$$

substituting $\omega = \sigma_x$ and $y_0 = e^{\mu_x}$

$$f(y;\mu_x,\sigma_x) = \frac{1}{\sigma_x y\sqrt{2\pi}} e^{--\left[\frac{1}{\sigma_x^2}\{\ln y - \ln y_0\}^2\right]} \tag{6.42}$$

also from Chapter 4:

$$\text{Mean of the lognormal} = e^{\mu_x + \frac{\sigma_x^2}{2}} \tag{6.43}$$

$$\text{Variance of the lognormal} = e^{2\mu_x + \sigma_x^2}\left(e^{\sigma_x^2} - 1\right) \tag{6.44}$$

$$\text{Mode of the lognormal} = e^{\mu_x - \sigma_x^2} \tag{6.45}$$

Mathematically, given a confidence level $P\,(0 < P < 100)$ as a fraction, a time t to test each item, a value μ_0 (the mean or median life, or a quantile point, e.g. 0.1, 0.2, 0.01, ...) which is the time we are interested in "proving" in the tests (where $\mu \geq \mu_0$), and an *acceptable number* of failures for the test (r), we want to find the smallest number of tests n so if the observed number of failures does not exceed r, we can say with confidence level P that $\mu \geq \mu_0$.

The required n is the smallest positive integer which satisfies the inequality:

$$\sum_{i=0}^{r} C_i^n p^i (1-p)^{n-i} \leq 1 - P \tag{6.46}$$

where $p = \int_{-\infty}^{z} \frac{e^{-x^2/2}}{\sqrt{2\pi}} dx$ is the probability of failure in time if the true parameter is μ_0 and $z = \frac{t-\mu_0}{\sigma}$ or $\left[z = \frac{\ln\, t - \mu_0}{\sigma} \text{ if using the lognormal}\right]$.

The following approximation formula can be used to find n:

$$n \simeq \left[\frac{0.5\chi^2_{2r+2,P}}{\Phi\left(\frac{t-\mu_0}{\sigma}\right)}\right] \tag{6.47}$$

where

$\chi^2_{2r+2,P}$ is the Chi-squared value with $2r + 2$ degrees of freedom and probability P.

$\Phi\left(\frac{t-\mu_0}{\sigma}\right)$ is the Normal (or Lognormal) distribution z-table value for $t - \mu_0/\sigma$ (or $(\ln t - \ln \mu_0)/\sigma$).

Example 6.22 Assume that the life distribution is lognormal with $\sigma = 2.0$, suppose you want to establish that your part/module/subsystem has a median life of 5000 hours. You want to find the trade-off between testing and the number of samples for $r = 0$, 1, or 2 failures at a 90% confidence level.

Using $t = 500$, 1000, 2000, and 3000 hours for each series of tests, how many parts should be tested to establish a 5000-hour median life?

Using Eq. (6.47)

$$n \simeq \left[\frac{0.5\chi^2_{2r+2,P}}{\Phi\left(\frac{t-\mu_0}{\sigma}\right)}\right]$$

First calculate for $t = 2000$ hours, $r = 0$ using Chi-square table in Supplement 5.

0.5*Chisq(0.90,2*0+2) = 0.5*Chisq(0.90,2) = 0.5*4.605 = 2.302

Calculating the z-value with median life $\mu_0 = \ln(5000)$ and $t = \ln(2000)$ with assumed $\sigma = 2$.

$$Z\left(\frac{\ln(2000) - \ln(5000)}{2}\right) = Z(-0.4581)$$

Using the normal table in Appendix C this translates to a probability of 0.3234.

$n \sim (2.302/0.3234) = 7$ (round up to a whole number).

So, you have to test 7 units to 2000 hours, each with $r = 0$ (i.e. NO failures), and you can then be 90% confident that your median life is 5000 hours or more (Figure 6.16).

While the more accurate way to calculate the above entails using some mathematics beyond the scope of this book, Figures 6.17a, 6.17b, 6.17c, and 6.17d gives the tests required to give the minimum sample size n to be tested for a time t in order to assert with probability P (0.80, 0.90, 0.95, 0.99) that $\mu \geq \mu_0$. The parameters μ and σ, where σ is assumed to be known, characterize the underlying normal(log normal) distribution of lifetimes. For the above confidence statement, the number of failures in time t should be $\leq r$.

Mathematically, for a given P and r, Figures 6.17a, 6.17b, 6.17c, and 6.17d gives the smallest positive integer n for which

$$\sum_{i=0}^{r} {}_nC_i\, p^i (1-p)^{n-i} \leq 1 - P \tag{6.48}$$

$$\text{where } p = \Phi\left(\frac{t-\mu_0}{\sigma}\right) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{(x-\mu_0)^2}{2\sigma^2}} dx \tag{6.49}$$

Example 6.23 Choosing a sample size using Figure 6.17c

Given that $r = 0$ or 1, $P = 0.95$, the life distribution is assumed to be lognormal with $\sigma = 2$. Suppose that we want to establish that the median life

$$e^{\mu} \geq e^{\mu_0} = 1000 \text{ hours}$$

The program manager wants to see the trade-off between test time t and the number of units tested to determine the lowest total cost to the program, picking test times: 450 hours, 1000 hours, and 2225 hours

Using EXCEL with Eq (6.47), you can do a trade study in terms of testing hours:

500 hours:

Conf Level =	0.9	Medain =	5000		
test time(t) =	500	Std Dev =	2		
r	DF(v)	$(X^2(CL, 2c+2))$	Chisq value/2	Z_p = (ln(t)-ln(Median))/sigma	n
Formula ➡	2c+2	= (CHISQ.INV($B$1,B_))	C_/2	NORM.DIST(LN($B$2), LN($D$1),2,TRUE)	‘ = Round(D_/E_),0)
0	2	4.605170186	2.302585093	0.124805951	18
1	4	7.77944034	3.88972017	0.124805951	31
2	6	10.64464068	5.322320338	0.124805951	43

1000 hours:

Conf Level =	0.9	Medain =	5000		
test time(t) =	1000	Std Dev =	2		
r	DF(v)	$(X^2(CL, 2c+2))$	Chisq value/2	Z_p = (ln(t)-ln(Median))/sigma	n
Formula ➡	2c+2	= (CHISQ.INV($B$1,B_))	C_/2	NORM.DIST(LN($B$2), LN($D$1),2,TRUE)	‘ = Round(D_/E_),0)
0	2	4.605170186	2.302585093	0.210490939	11
1	4	7.77944034	3.88972017	0.210490939	18
2	6	10.64464068	5.322320338	0.210490939	25

2000 hours:

Conf Level =	0.9	Medain =	5000		
test time(t) =	1000	Std Dev =	2		
r	DF(v)	$(X^2(CL, 2c+2))$	Chisq value/2	Z_p = (ln(t)-ln(Median))/sigma	n
Formula ➡	2c+2	= (CHISQ.INV($B$1,B_))	C_/2	NORM.DIST(LN($B$2), LN($D$1),2,TRUE)	‘ = Round(D_/E_),0)
0	2	4.605170186	2.302585093	0.323424004	7
1	4	7.77944034	3.88972017	0.323424004	12
2	6	10.64464068	5.322320338	0.323424004	16

3000 hours:

Conf Level =	0.9	Medain =	5000		
test time(t) =	1000	Std Dev =	2		
r	DF(v)	$(X^2(CL, 2c+2))$	Chisq value/2	Z_p = (ln(t)-ln(Median))/sigma	n
Formula ➡	2c+2	= (CHISQ.INV($B$1,B_))	C_/2	NORM.DIST(LN($B$2), LN($D$1),2,TRUE)	‘ = Round(D_/E_),0)
0	2	4.605170186	2.302585093	0.399202138	6
1	4	7.77944034	3.88972017	0.399202138	10
2	6	10.64464068	5.322320338	0.399202138	13

Figure 6.16 EXCEL calculation tables for Example 6.22; 90% confidence.

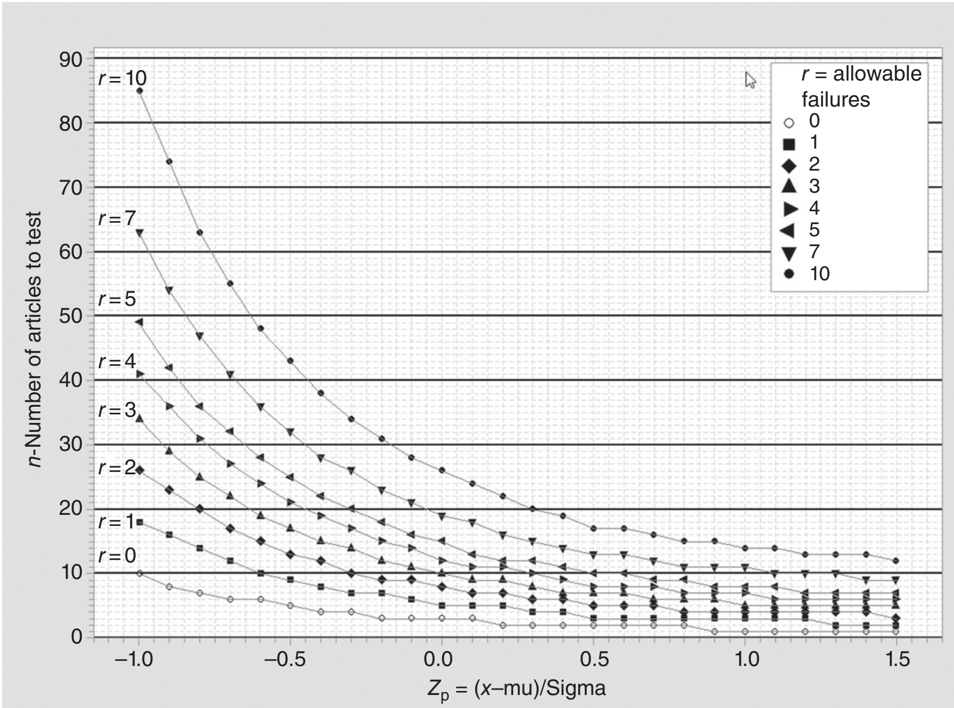


Figure 6.17a The minimum sample size to be tested for a time t in order to assert with probability $P = 0.80$ that $\mu > \mu_0$.

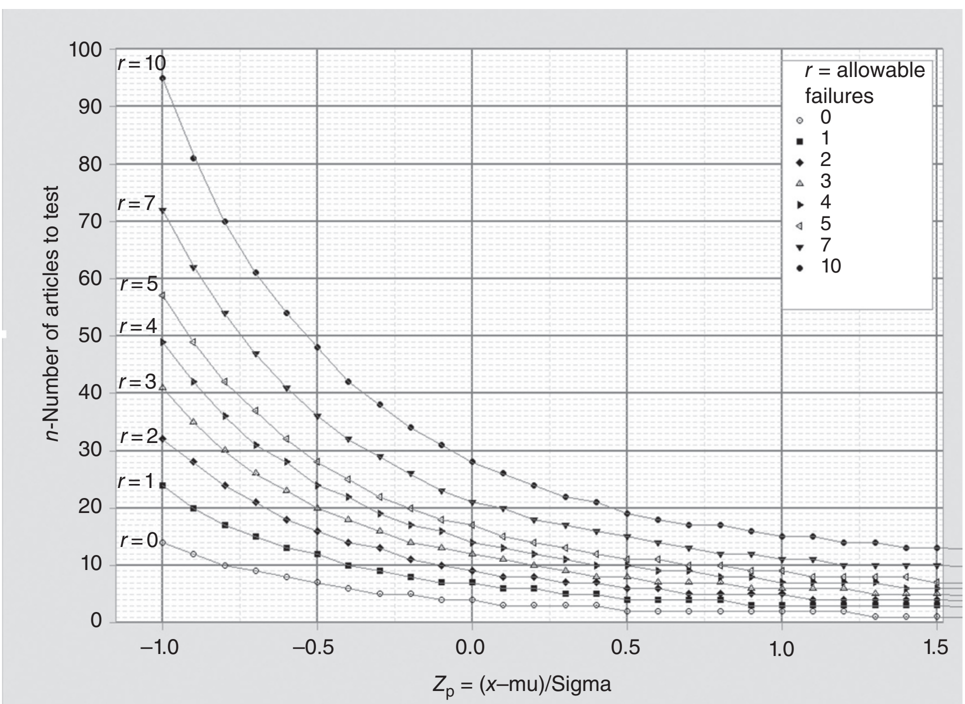


Figure 6.17b The minimum sample size to be tested for a time t in order to assert with probability $P = 0.90$ that $\mu > \mu_0$.

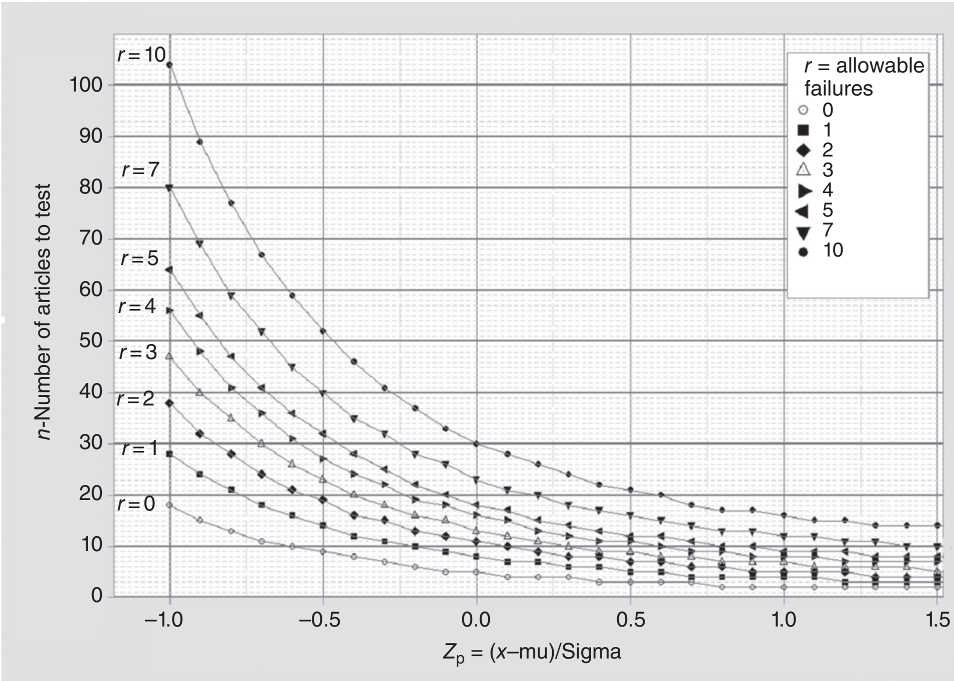


Figure 6.17c The minimum sample size to be tested for a time t in order to assert with probability $P = 0.95$ that $\mu > \mu_0$.

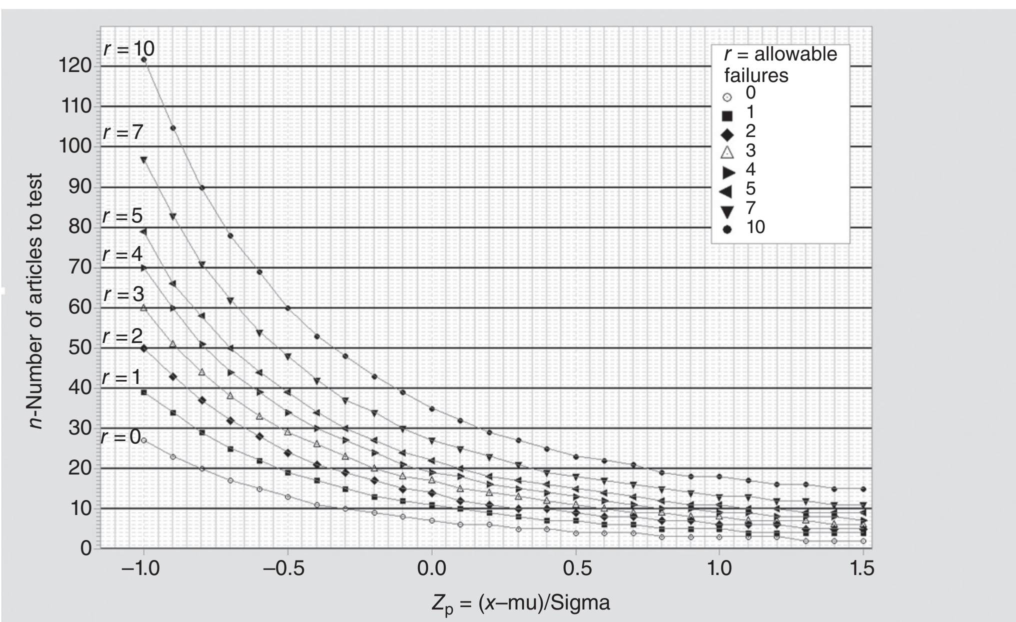


Figure 6.17d The minimum sample size to be tested for a time t in order to assert with probability $P = 0.99$ that $\mu > \mu_0$.

Table 6.8 Example 6.23. Summary results.

For P = 0.95, σ = 2	
Test time	**Units on test**
450 h	
$r = 0$	8
$r = 1$	12
1000 h	
$r = 0$	5
$r = 1$	8
2225 h	
$r = 0$	3
$r = 1$	6

$$\text{For hours} = 450, z = \frac{\ln(450/1000)}{2} = -0.4$$
$$\text{For hours} = 1000, z = \frac{\ln(1000/1000)}{2} = 0.0$$
$$\text{For hours} = 2225, z = \frac{\ln(2225/1000)}{2} = 0.4$$

Looking in Figure 1.16c, under $z = -0.4$, $n = 8$ for $r = 0$, or $n = 12$ for $r = 1$; for $z = 0$, $n = 5$ for $r = 0$, or $n = 8$ for $r = 1$; and for $z = 0.4$, $n = 3$ for $r = 0$, or $n = 6$ for $r = 1$.

Summarizing in Table 6.8 to the right, the finance person for the program can now decide (based on the cost of test hours and the cost of units) which test plan is best.

Example 6.24 Choosing a sample size using Figure 6.16a–d when you want to prove a lower quantile (not the median)

Assuming a lognormal distribution with $\sigma = 2.0$, we want to establish that the 1/10 life is at least equal to 1000 hours with 90% confidence. Let $r = 0$ and let the test time = 13,000 hours.

We have to replace z in Figure 6.16b with

$$z = \frac{\ln(t/\xi_{.01})}{\sigma} + \Phi^{-1}(p) = \frac{\ln(13000/1000)}{2} + \Phi^{-1}(0.1) = 1.28 - 1.28 = 0$$

Reading Figure 6.17b at $r = 0$, $Z = 0.0$, $n = 4$.

Testing 4 units to 13,000 hours equivalent each without failure and you can be 90% confident that your 1/10 life is 1000 hours.

One last note in using Figures 6.17a, 6.17b, 6.17c, and 6.17d. Unless you have an EXTREMELY expensive experiment, always use more than one experiment, even if the r and Z_p "allow" one experiment. From a real life engineering point of view, the variation in the experimental or production item is not being tested with one experiment. Bottom line: Always use two or more experiments *unless budget is very limited, or one experiment is extremely expensive.*

You will note in the Weibull testing section that we did not include the possibility of $n = 1$, exactly for the reason above.

6.7 Accelerated Life Testing

Inadequate time to complete life testing is an ubiquitous problem in making reliability estimates. The censoring from the right discussed in the preceding sections is a solution only if data from a sufficiently short time span is needed, or if that data can be confidently extrapolated to longer times. Fortunately, a number of acceleration methods may be used to counter the difficulties in performing life testing with time deadlines. Although none are without shortcomings, these procedures nevertheless contribute substantially to the timeliness with which reliability data are obtained. Accelerated tests can be divided roughly into two categories: compressed-time tests and advanced-stress tests.

Compressed-Time Testing

Unless the product is one that is expected to operate continuously, such as a wrist watch and an electric utility transformer, one can condense the component's lifetime by running it continuously to failure. Hence, many engines, motors, and other mechanical and electrical devices can be tested for durability in a small fraction of the calendar design life. Likewise, on–off cycles for many products can be accumulated over a condensed period of time compared to the calendar design life. An example of this is any wearout mode in a jet engine (low cycle fatigue, stress corrosion, bearing failure modes, etc.).

Reliability tests are frequently performed in which appliance doors are opened and closed, consumer electronics is turned on and off, or pumps or motors are started and stopped to reach a design life target over a relatively short period of time. These are referred to as compressed-time tests, for the product is used more steadily or frequently in the test than in normal use, but the loads and environmental stresses are maintained at the level expected in normal use.

Precaution must be exercised in amassing data from compressed-time tests. In field use, the appliance door may only be cycled (opened and closed) several times per day. But a compressed-time test can easily be performed in which the open–close cycle is performed a few times per minute. If the cycle is accelerated too much, however, the conditions of operation may change, increasing stress levels and thus artificially increasing failure rates. If the latch is worked several times per second, for example the heat of friction may not have time to dissipate. This, in turn, would cause the latch to overheat, increasing the failure rate and perhaps activating failure mechanisms that would not plague ordinary operation. Conversely, tests in which engines, motors, or other systems, which normally operate for intermittent periods of time, are operated continually until failure occurs will not pick up the cyclical failure modes caused by starting and stopping. To detect these, a separate cycling test is required, or the continuous operation must be interrupted by intervals long enough for ambient temperatures to be achieved. Compressed-time tests under the field conditions that a product will face may be more difficult to achieve. Nevertheless, some acceleration is possible. The field life of automobiles may be compressed by leasing them as taxicabs, and that of home kitchen appliances by testing them in restaurants. Differences, of course, will remain, but the data may be adequate for the design verification or other use for which it is needed.

Example 6.25 Accelerated Mission testing

A Case Study: A Fighter aircraft jet engine Compressed-Time Test (Sammons 1981).

During the development phases of a typical military jet engine, the statistical base is small, and there are uncertainties as to how the engine will be used in service. When engine production begins, a statistical database also begins to flesh out. As squadrons become operational, usage evolves and

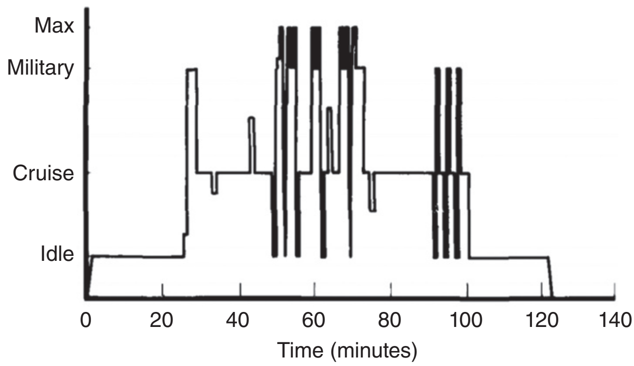


Figure 6.18a Average sorties provided by current data.

failure modes begin to rear their ugly heads. Maintenance and interface characteristics join the mix, with improvement in tooling and manuals. The overhaul cycle brings in new failure modes of worn parts interactions with newer parts. Lower failure rate problems now start to occur.

Each of the above phases of an engine's life drives specific types of durability and reliability problems:

- Early in the development phase – High cycle fatigue and stress rupture failure modes (low characteristic lives, Weibull βs from 1 to 5 – mission oriented caused failure modes).
- Engines approaching the first depot visit – Low cycle fatigue and variable geometry wear in some engines, Weibull βs between 2 and 4.
- Steady-state usage – Low cycle fatigue, wear problems, and statistically "remote" problems, some maintenance caused (Weibull βs >1 and some characteristic lives 2–5× the depot visit time).

The ingredients of a good accelerated mission test depend on the details of how the engines have been operating up to that point. For example:

- what failure modes have occurred in the field?
- how has the hardware looked when an engine came into depot for refurbishment?
- what feedback do we have from the base maintenance shops and from pilots?

A typical average sortie for a fighter engine in terms of power lever is illustrated in Figure 6.18a along with the corresponding AMT cycle in Figure 6.18b.

You can readily see that the "nonactive" times in the average sortie have been shrunk to give 30 seconds before and after each incursion from idle to military or above power to produce the AMT cycle. In this particular illustration, the acceleration factor is 4 : 1.

Since low cycle fatigue is driven by the idle to intermediate and above cycles, in 30 minutes of a test engine you can simulate 8 cycles, in 24 hours you can simulate 192 cycles, and you can simulate an 8000-cycle turbine disk life in ~42 days, as opposed to 8 calendar years for an engine in the field to accumulate 8000 cycles.

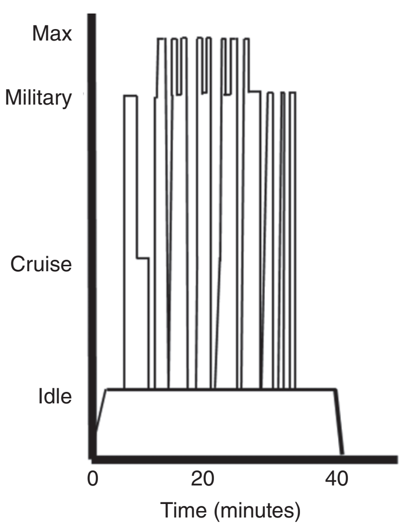


Figure 6.18b Accelerated mission test derived from Figure 6.17.

Another use of compressed-time testing is correlating test times in lab that reproduce a failure mode in the field. The following is an example.

Example 6.26 Turbopump Failures Excerpted from the book by Abernethy et al. (1983), pp 70ff.

Thirty eight turbopump failures occurred in service on jet engines. See Figure 6.19. Failure analysis indicated low lubricity of the hydraulic fluid as the cause of the failures. An accelerated bench test was designed using *extremely* low lubricity fluid. Two more turbopumps failed in a much shorter time, 95 and 155 hours, respectively. See Figure 6.20. The almost identical slopes of 2.7 in the lab versus 2.6 in field confirmed the capability of the bench test to duplicate the failure mode observed in service. This is an excellent check on the validity of an accelerated test. In addition, engineering compared the failed parts from the bench test to the failed parts from the field to assure that the failure mode was duplicated from an engineering standpoint.

(Lesson learned: The accelerated failure mode in the lab should physically look like the field failure mode. There is always a concern that an accelerated test will produce the wrong failure mode.)

The ratio of the Bill of Material (BoM) field failures to the BoM bench lab test failures is

$$\text{Test Acceleration Rate} = \frac{\eta_{\text{Field}}}{\eta_{\text{Lab}}} = \frac{2255}{143} = 15.8$$

The turbo pump was redesigned to fix the problem, and two units were tested in the lab to 500 hours without failure under the same accelerated conditions. Is the redesign successful? What service experience should be expected? Using the equation for MLE η (Eq. (5.14)) and the slope from the Weibull in Figure 6.19, the Weibayes characteristic life is

$$\eta = \left[\frac{(500)^{2.59} + (500)^{2.59}}{1}\right]^{1/2.59} = 653.4 \tag{6.50}$$

This Weibayes line is plotted in Figure 6.20. The new design Weibayes field Weibull has $\eta =$ 15.8∗653.5~10,326 hours, also plotted in Figure 6.20.

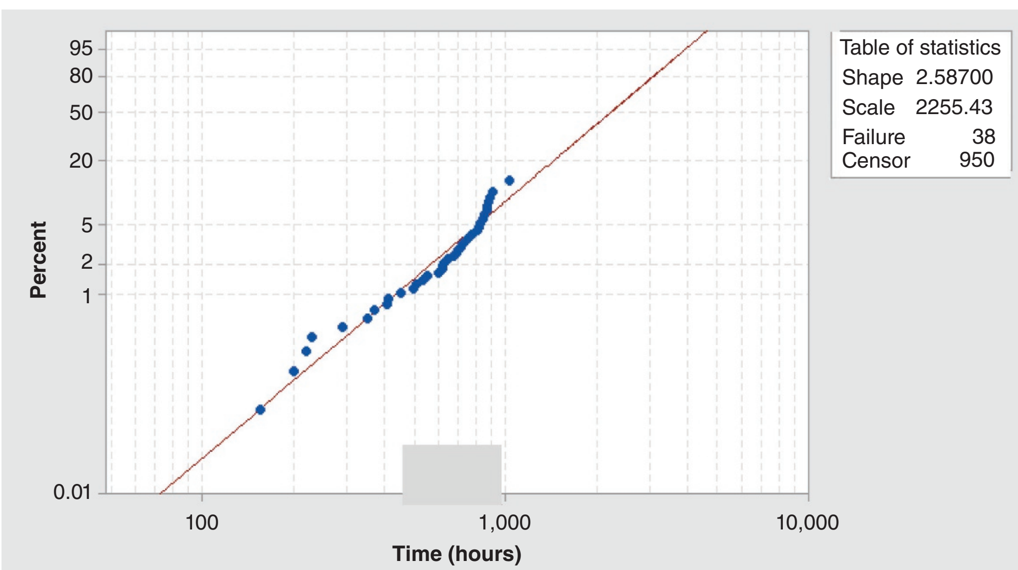


Figure 6.19 38 Turbopump failures in the field. *Source*: Based on Abernethy et al. (1983).

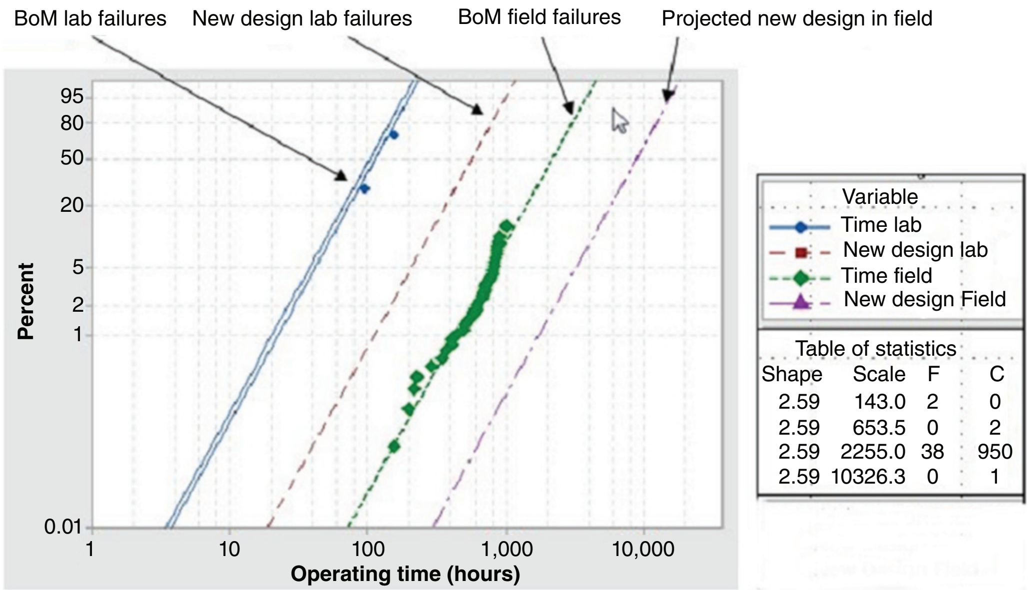


Figure 6.20 Comparison of Bill of Material (BoM)-accelerated test in lab to field failures and new design-accelerated test in lab compared to project new design in the field. *Source*: Based on Abernethy et al. (1983).

Advanced-Stress Testing – Linear and Acceleration Models

Systems that are normally in continuous operation or in which failures are caused by deterioration occurring, even though a unit is inactive, present some of the most difficult problems in accelerated testing. Failure mechanisms cannot be accelerated using the foregoing time compression techniques. Advanced-stress testing, however, may be employed to accelerate failures, since as increased loads or harsher environments are applied to a device, an increased failure rate may be observed. If a decrease in reliability can be quantitatively related to an increase in stress level, the life tests can be performed at high stress levels, and the reliability at normal levels inferred.

Both random failures and aging effects may be the subject of advanced-stress tests. In the electronics industry, components are tested at elevated temperatures to increase the incidence of random failure. In the nuclear industry, pressure vessel steels are exposed to extreme levels of neutron irradiation to increase the rate of embrittlement. Similarly, placing equipment under a high-stress level for a short period of time in a proof test may be considered accelerated testing to reveal the early failures from defective manufacture.

Accelerated test conditions are usually testing units at higher (lower) temperatures, vibratory levels, higher (lower) humidity, salt/no salt environments, pressure variations, wattages, voltages, cycle rates, amplitudes, loads, and (at a lower or higher level) of any other variable that a unit may see in customer use.

General outline for accelerated-stress testing:

- Understand the stress-life relationship
  - Understand the possible failure mechanism(s)
  - Pick at least three levels of "stressor" that will not immediately fail the product but will enable you to extrapolate to "use" stress

- Extrapolate to reliability of interest at the stress levels
  - Use background knowledge to pick the true failure distribution
  - Need to ensure unrealistic failure modes not introduced

Linear Model Stress Testing

The most elementary form of advance-stress test is to estimate the MTTF. Suppose that the MTTF is obtained at the number of different elevated-stress levels. The MTTF is then plotted versus some function of the stress level. Knowledge of either the stress effects or trial and error may be used to choose the function that will result in a linear graph. A curve is fitted to the data, and the MTTF is estimated at the stress level that the device is expected to experience during normal operation. This process is illustrated in the following example:

Example 6.27 Accelerated life tests are run on four sets of 12 flashlight bulbs, and the failure times in minutes are tabulated in Table 6.9. We want to estimate the MTTF at each voltage and extrapolate the results to the normal operating voltage of 6.0 V.

Fitting each of the distributions to an exponential distribution in Figure 6.21,

Plotting mean(MTTF) vs voltage on log–log scale and fitting the data (Figure 6.22).

But the foregoing has a serious drawback: it presumes an exponential distribution to calculate the MTTF. Therefore, one has no indication whether the shape, as well as the time scale of the distribution, is changing. Since changes in distribution shape are usually indications that a new failure mechanism is being activated by the higher stress levels, there is a danger that the simple exponential estimate will be inappropriately extrapolated.

We should analyze the data more in order to find the distribution that fits this type of data best. We can then apply this to advanced-stress data as follows. As stress is increased above that encountered at normal operating levels, failures should occur at earlier times, and therefore, the CDF for

Table 6.9 Light bulb failure times in minutes.

Failure #	9.4 V	12.6 V	14.3 V	16 V
1	63 (outlier)	87	9	7
2	3542	111	13	9
3	3782	117	23	9
4	4172	118	25	9
5	4412	121	28	9
6	4647	121	30	9
7	5610	124	32	10
8	5670	125	34	11
9	5902	128	37	12
10	6159	140	37	12
11	6202	148	39	13
12	6764	177	41	14

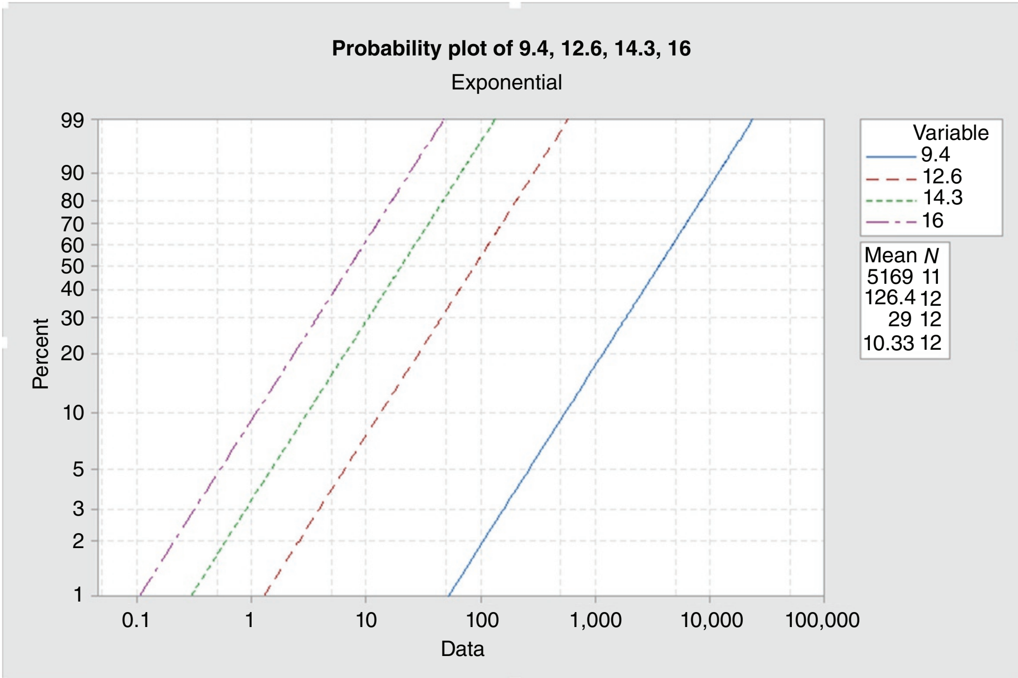


Figure 6.21 Each voltage set of data fit to an exponential (after deleting outlier in 9.4-V data).

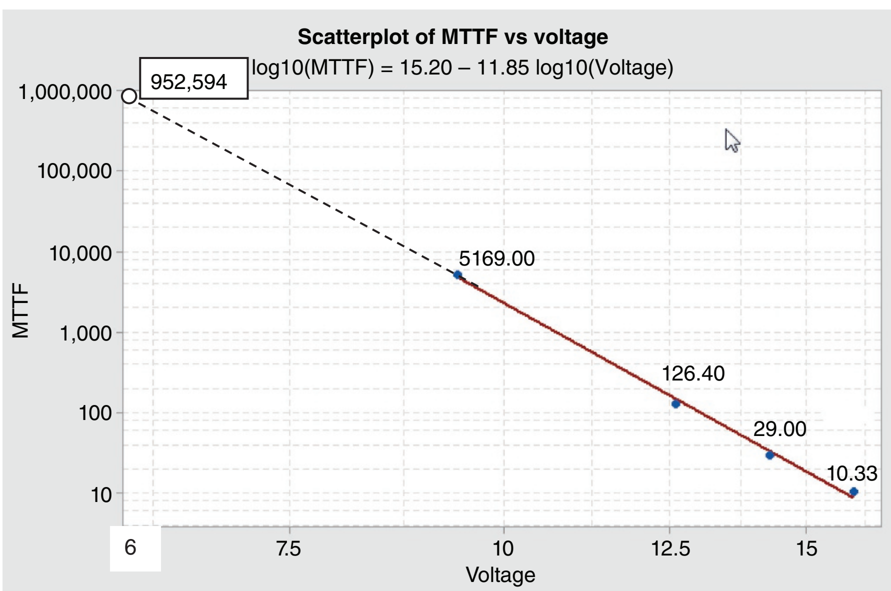


Figure 6.22 The log–log fit to the data predicts an MTTF of 952,594 hours at 6 V.

failure should rise more rapidly. Let $F_a(t)$ be the failure CDF under accelerated-stress conditions, and $F(t)$ be that obtained under ordinary operating conditions. Then, we would expect that at any time, $F_a(t) > F(t)$. True acceleration is said to take place if $F_a(t)$ and $F(t)$ are the same distribution and differ only by a scale factor in time. We then have

$$F_a(t) = F(\kappa t) \tag{6.51}$$

where $\kappa > 1$ is referred to as the *acceleration factor*.

The Weibull and lognormal distributions are particularly well suited for the analysis of advanced-stress tests, for in each case there is a scale parameter that is inversely proportional to the acceleration factor and a shape parameter that should be unaffected by acceleration. Thus, if the shape parameter remains relatively constant, some assurance is provided that no new failure mode has appeared.

The CDF for the Weibull distribution is given by Eq. (5.10). Thus, at an advanced stress it will be given by

$$F_a(t) = 1 - e^{-(t/\eta')^\beta} \tag{6.52}$$

where to satisfy Eq. (6.51), the scale parameter must be given by

$$\eta' = \eta/\kappa \tag{6.53}$$

A special case of the Weibull distribution, of course, is the exponential distribution, where $\beta = 1$, is also used for accelerated testing. Likewise, the CDF for the lognormal distribution is given by Eq. (4.69). At corresponding advanced stress, the distribution will be

$$F_a(t) = \Phi\left[\frac{1}{\omega}\ln\left(\frac{t}{t_0'}\right)\right] \tag{6.54}$$

where to satisfy Eq. (6.51), we must have

$$t'_0 = \frac{t_0}{\kappa} \tag{6.55}$$

The procedure for applying advanced-stress testing to determine the life of a device requires a good deal of care. One must be satisfied that the shape parameter is not changing before making a statistical estimate of the scale parameter. This is often difficult, for at any one stress level the number of failures is not likely to be large enough to determine the shape parameter within a narrow confidence interval, and moreover the estimates of these parameters will vary randomly from one stress level to the next. Thus, one must rely on other means to establish the shape parameter. Historical evidence from larger databases may be used, or more advanced maximum-likelihood methods may be used to combine the data under the assumption that there is a common shape parameter (a method usually used by software packages). Finally, additional data may be acquired at one or more of the stress levels to establish the parameter within a narrower bound. Some of these considerations are best illustrated by carrying through the analysis on a set of laboratory data. For this purpose, we return to the light bulb data used in Example 6.27.

Example 6.28 Make Weibull plots of the accelerated-life test data in Table 6.9. In addition to the 1 point that was an outlier in the 9.4-V data, the two early failures in the 14.3-V data are suspensions. Estimate the shape parameter and determine the acceleration factor as a function of voltage.

Solution: See Figure 6.23.

Once again, we can simply analyze the data as if it were linear (Figure 6.24).

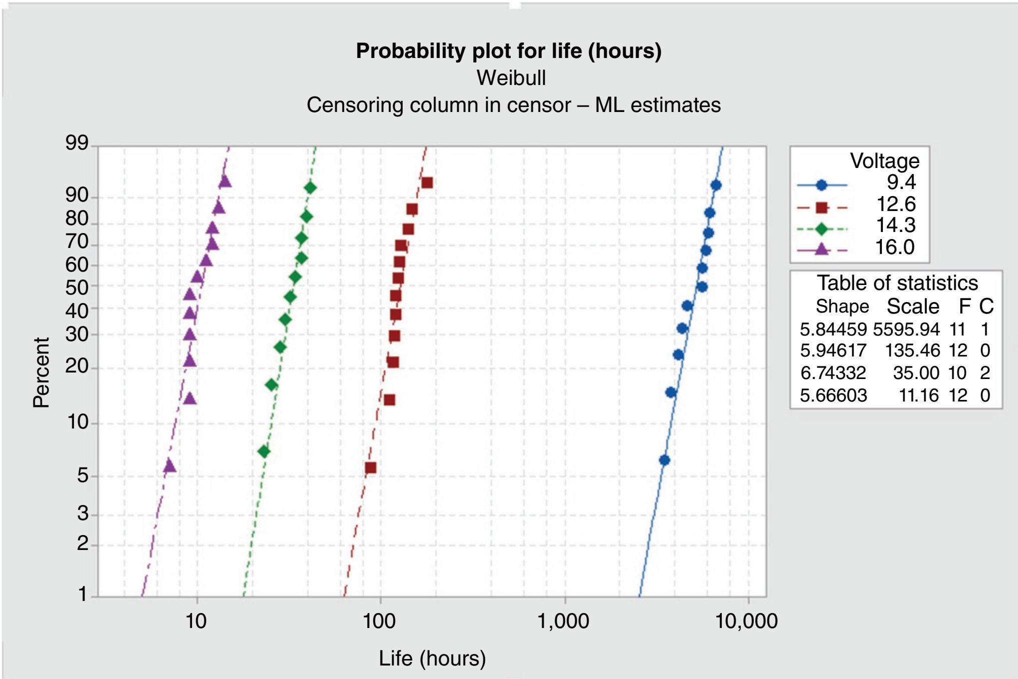


Figure 6.23 Analyzing the data in Table 6.9 using the Weibull distribution.

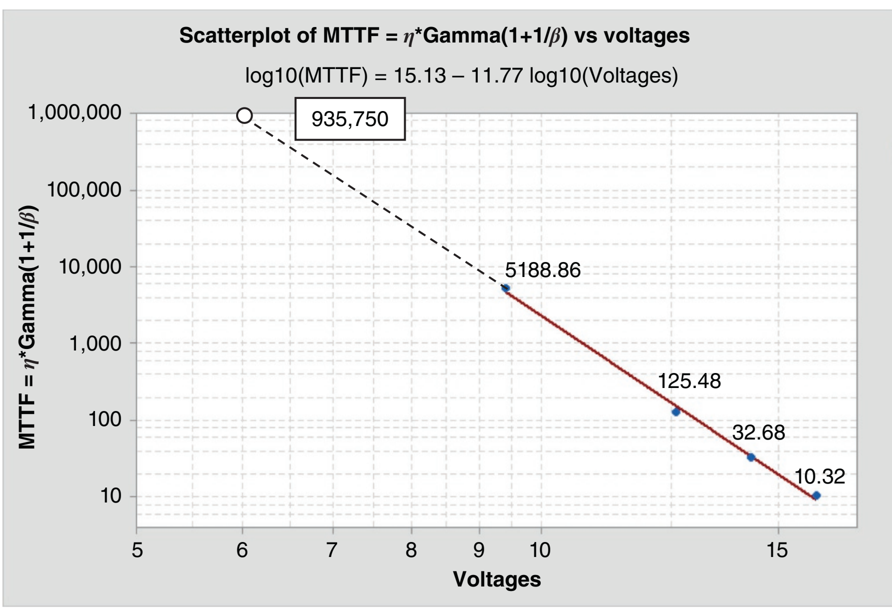


Figure 6.24 The MTTF at 6 V varied only a bit, but the fit of the data was better presented using a Weibull distribution.

Other distributions, such as the normal and extreme value, may also be used in advanced-stress testing. In these cases, however, the analysis is more complex since both distribution parameters change if Eq. (6.51) remains valid. For example, in the normal distribution, we have $\mu' = \mu/\kappa$ and $\sigma' = \sigma/\kappa$. Thus, lines drawn on probability plots at different stress levels will no longer be parallel with the time scaling. The normal distribution is more useful in modeling phenomena in which stress levels have additive instead of multiplicative effects on the times to failure, since μ is a displacement rather than a scale parameter, and thus in such situations only μ and not σ will be effected. A similar behavior is observed if the extreme value distribution is employed.

Advanced-Stress Testing – Acceleration Models

Physical acceleration means that operating a unit at high stress (i.e. higher temperature or humidity or voltage) should produce the same failures that would occur at a *use stress*, except that they happen much quicker.

A failure may be due to mechanical fatigue, corrosion, chemical reaction, or any number of physical phenomena. The failure modes may be known failure modes from earlier similar products or from finite element studies or lab tests that reveal the possibility of a particular failure mode.

In all of these modes, an *acceleration factor* (*AF*) is a constant multiplier between two stress levels. Engineering and previous customer experience must be used to identify the usage "stressors."

For example, if temperature (and indeed most chemical reactions) is determined to be the variable that most affects a unit's life, the *Arrhenius model* is typically used, n_1 units will be tested to failure at "Mean use temp $+\Delta temp_1$," n_2 units at "Mean use temp $+\Delta temp_2$", and so on for three or more levels of increasing temperature. Or, in like manner for chemical reactions.

The *inverse power model* is used for nonthermal accelerated stresses. For example, solid rocket engine thrust chambers may be tested at nominal pressures +5%, +10%, +20%, up to the highest pressure allowed by the design. In general, the inverse power model is used for many common mechanical failure modes and cycling.

We concentrate on these two models since they are used most frequently. A number of additional models exist, and references will be provided to these for your further use. Realize that the Weibull (exponential) or lognormal distribution can be used within these two "physics of failure" models.

The Arrhenius Model

The Arrhenius Model is:

$$R(T) = Ae^{-\frac{E_A}{KT}} \tag{6.56}$$

where

$R(T)$ = speed of the reaction at Temperature T
T = temperature in degrees Kelvin (°K = 273.15 + °C) or temperature in degrees Rankin (°R = 459.67 + °F)
A = a non-thermal constant factor
E_A = Activation energy in electron volts
K = Boltzman's constant ($8.61733326 \times 10^{-5}$ eV/K)

The Arrhenius life-stress model assumes that life is proportional to the inverse reaction rate of the process.

Then the Arrhenius life-stress model can be written:

$$L(S) = Ce^{\frac{E_A}{KT}} \tag{6.57}$$

where

L = a measure of life (e.g. mean life, Median life, B.1 life, characteristic life)
S = the stress level at temperature in degrees Kelvin or Rankin
C = a model parameter
E_A = Activation energy in electron volts
K = Boltzman's constant ($8.61733326 \times 10^{-5}$ eV/K)

We can now write the life at use temperature:

$$L_{\text{Use}}(S) = Ce^{\frac{E_A}{KT_{\text{Use}}}} \tag{6.58}$$

and Life at Accelerated temperature

$$L_{\text{Accel}}(S) = Ce^{\frac{E_A}{KT_{\text{Accel}}}} \tag{6.59}$$

Then the ratio of use life to accelerated life is:

$$\frac{L_{\text{Use}}(S)}{L_{\text{Accel}}(S)} = e^{\frac{E_A}{K}\left(\frac{1}{T_{\text{Use}}} - \frac{1}{T_{\text{Accel}}}\right)} \tag{6.60}$$

Since failure rate is directly proportional to rate of process failure: Eq. (6.58) becomes,

$$\lambda = \text{D}e^{-\frac{E_A}{KT}} \tag{6.61}$$

where D is a constant

As above, the Use temperature failure rate is:

$$\lambda_{\text{Use}} = \text{D}e^{-\frac{E_A}{KT_{\text{Use}}}} \tag{6.62}$$

And the Accelerated temperature failure rate is:

$$\lambda_{\text{Accel}} = \text{D}e^{-\frac{E_A}{KT_{\text{Accel}}}} \tag{6.63}$$

Dividing Eq. (6.62) by (6.63):

$$\lambda_{\text{Use}} = \lambda_{\text{Accel}} e^{-\frac{E_A}{K}\left(\frac{1}{T_{\text{Use}}} - \frac{1}{T_{\text{Accel}}}\right)} \tag{6.64}$$

The Acceleration Factor, A_F is:

$$A_F = \left(\frac{L_{\text{Use}}(S)}{L_{\text{Accel}}(S)}\right) = \frac{\lambda_{\text{Accel}}}{\lambda_{\text{Use}}} = e^{\frac{E_A}{K}\left(\frac{1}{T_{\text{Use}}} - \frac{1}{T_{\text{Accel}}}\right)} \tag{6.65}$$

For the Weibull distribution, the Arrhenius–Weibull model can be derived:

First, recall from Chapter 5 the pdf of the two-parameter Weibull distribution:

$$f(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{6.66}$$

letting $\eta = L(S) = Ce^{\frac{E_A}{KT}}$ and substituting in Eq. (6.66):

$$f(t,S) = \frac{\beta}{Ce^{\frac{E_A}{KT}}}\left(\frac{t}{Ce^{\frac{E_A}{KT}}}\right)^{\beta-1} e^{-\left(\frac{t}{Ce^{\frac{E_A}{KT}}}\right)^{\beta}} \tag{6.67}$$

substituting any of the temperatures for T will produce the pdf for that stressor, keeping the Weibull parameters constant.

E_A is usually determined experimentally by observing the times to failure of different batches of components at different temperatures. Also, many electronic component manufacturers have listed their component E_As. Most semiconductor devices have an E_A very close to 1.

Example 6.29 Class-H insulation life[2]

We have hours to failure of 40 motorettes with a Class-H insulation run at 190, 220, 240, and 260 °C (Table 6.10). The purpose is to estimate the median life and 95% confidence bounds at 180 °C (453.15 °K).

The insulation stressor is the temperature, and previous experience suggests that a lognormal life distribution is appropriate.

Using MINITAB with these assumptions:

1) Generate individual lognormal plots of hours to failure for each temperature.
2) Generate a fitted Arrhenius plot of hours to failure using all data.
3) Generate a fitted relation plot across all data from which we can read the 95% confidence bound at 180 °C (Figures 6.25, 6.26, 6.27, 6.28, and 6.29).

Note that the lower the temperature, the more spread the failure distribution (same lognormal location parameter for each temperature level).

Table 6.10 Motorette data.

°C	190	220	240	260
°K	463.15	493.15	513.15	533.15
	7,228	1764	1175	600
	7,228	2436	1175	744
	7,228	2436	1521	744
	8,448	2436	1569	744
	9,167	2436	1617	912
	9,167	2436	1665	1128
	9,167	3108	1665	1320
	9,167	3108	1713	1464
	10,511	3108	1761	1608
	10,511	3108	1953	1896

2 *Source*: Based on Nelson (1990), p. 115.

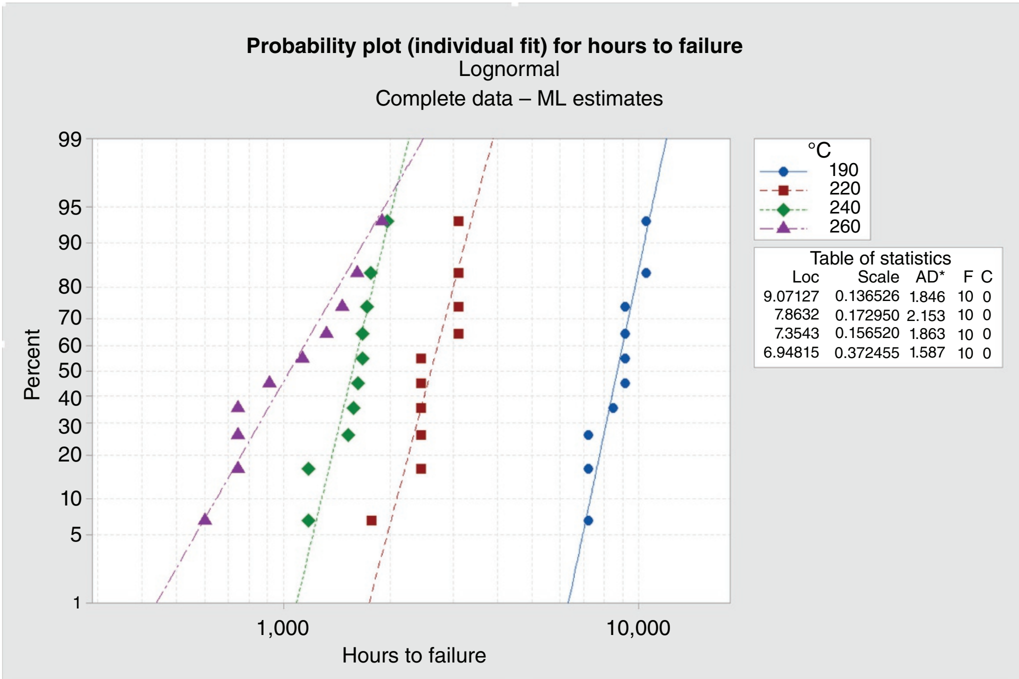


Figure 6.25 Individual log normal plots of each temperature's hours to failure. *Source*: Based on Nelson (1990).

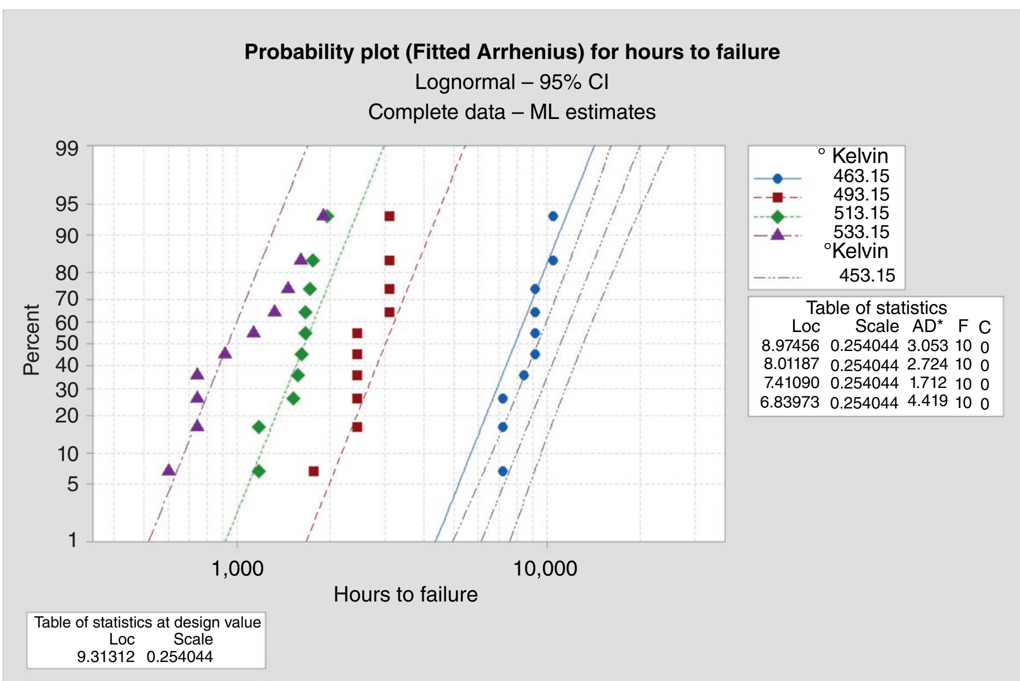


Figure 6.26 Comparison of accelerated testing at high temperatures to use temperature. *Source*: Based on Nelson (1990).

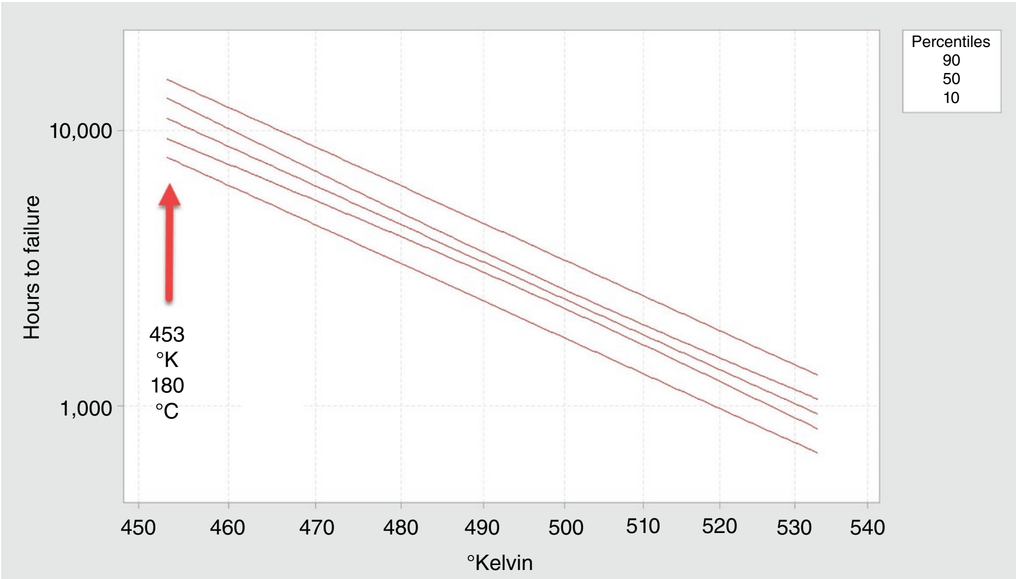


Figure 6.27 Curve fit of accelerated data 10, 50, and 90 percentiles projected to the use temperature 453.15 ° K (180 °C). *Source*: Based on Nelson (1990).

Percentiles = 50

Deg Kelvin	Hours to Failure	95% CI Lower Bound	95% CI Upper Bound
453.15	11082.5	9356.89	13126.3
457.361	9599.23	8206.77	11228.0
461.571	8328.18	7206.50	9624.46
465.782	7237.15	6334.96	8267.81
469.992	6299.05	5574.13	7118.25
474.203	5491.14	4908.61	6142.81
478.413	4794.22	4325.19	5314.11
482.624	4192.08	3812.59	4609.36
486.834	3671.03	3361.14	4009.50
491.045	3219.45	2962.66	3498.49
495.255	2827.48	2610.31	3062.71
499.466	2486.74	2298.46	2690.45
503.676	2190.12	2022.56	2371.57
507.887	1931.52	1778.80	2097.36
512.097	1705.75	1563.90	1860.48
516.308	1508.37	1374.89	1654.82
520.518	1335.58	1208.98	1475.43
524.729	1184.09	1063.56	1318.28
528.939	1051.12	936.230	1180.10
533.15	934.238	824.781	1058.22

Figure 6.28 Screen grab of 50 percentiles with confidence bound by temperature. The median design life is 11,082 hours, with 95% confidence bounds (9357, 13126). *Source*: Based on Nelson (1990).

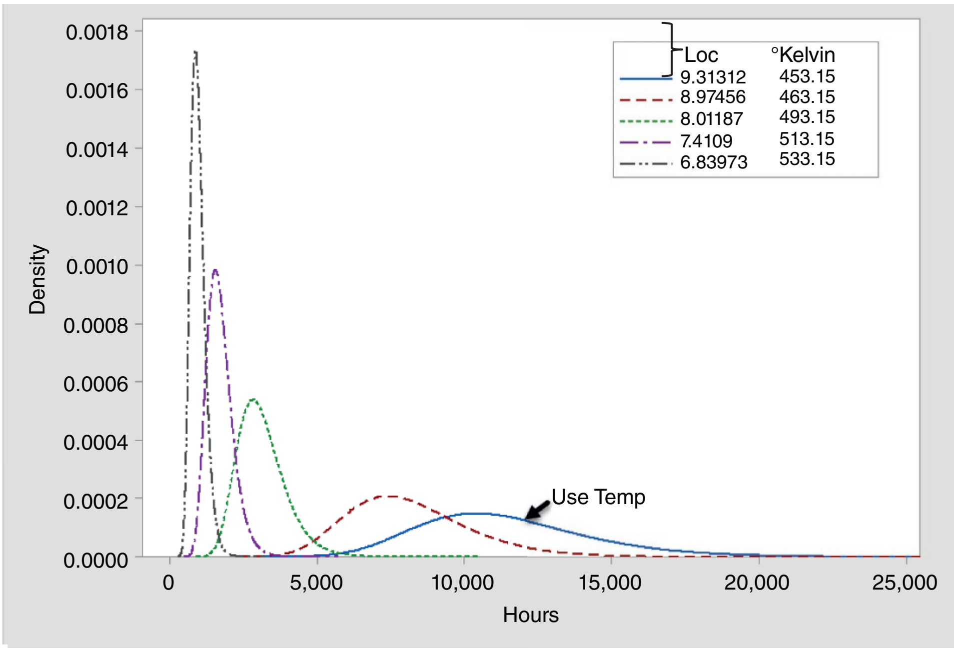


Figure 6.29 Arrhenius-lognormal PDFs of temperature levels. *Source*: Based on Nelson (1990).

The Inverse Power Law Model

When the life of a system has a *nonthermal* stressor, the *inverse power law* is used to model the life = *f*(Stress), given by:

$$L(S) = \frac{1}{KS^n} \tag{6.68}$$

where

L represents life (e.g. mean life, characteristic life, BX life)
S is the stress level
K and n are the two model parameters to be determined.

The inverse power law is a straight line when plotted on a log–log paper. The equation of the line based on Eq. (6.68) is given by:

$$\ln(L) = -\ln(K) - n\ln(S) \tag{6.69}$$

We can find the values of n and K by fitting the data to this straight line. The characteristic life at any accelerated stress S_A, is

$$\eta_A = \frac{1}{K(S_A)^n} \tag{6.70}$$

Likewise, the characteristic life at the use stress S_U, is

$$\eta_U = \frac{1}{K(S_U)^n} \tag{6.71}$$

The Acceleration Factor (AF) is defined as

$$AF = \frac{\eta_U}{\eta_A} = \frac{\dfrac{1}{K(S_U)^n}}{\dfrac{1}{K(S_A)^n}} = \frac{K(S_A)^n}{K(S_U)^n} = \left(\frac{S_A}{S_U}\right)^n \tag{6.72}$$

Example 6.30 Life data from an accelerated test on roller bearings: 40 roller bearing were tested, 10 at each of four loads. Data is in Table 6.11[3]. (The 0.012 data point at 1.09 load is an outlier or more likely a mistype.)

The model assumed here is Weibull life with an inverse power relationship.

We will generate Weibull plots for each load and accelerated testing plot for estimating the 10% life (reliability = 1-0.1 = 0.9 or 90% reliability) at a load of 0.75. 10% life is the usual bearing design point (Figures 6.30, 6.31, and 6.32).

Table 6.11 ALT results for 40 roller bearings.

Load					**Life (10^6 revolutions)**					
0.87	**1.67**	**2.2**	**2.51**	**3**	**3.9**	**4.7**	**7.53**	**14.7**	**27.8**	**37.4**
0.99	0.8	1	1.37	2.25	2.95	3.7	6.07	6.65	7.05	7.37
1.09	0.012*	0.18	0.2	0.24	0.26	0.32	0.32	0.42	0.44	0.88
1.18	0.073	0.098	0.117	0.135	0.175	0.262	0.27	0.35	0.386	0.456
Outlier										

Source: Nelson (1990).

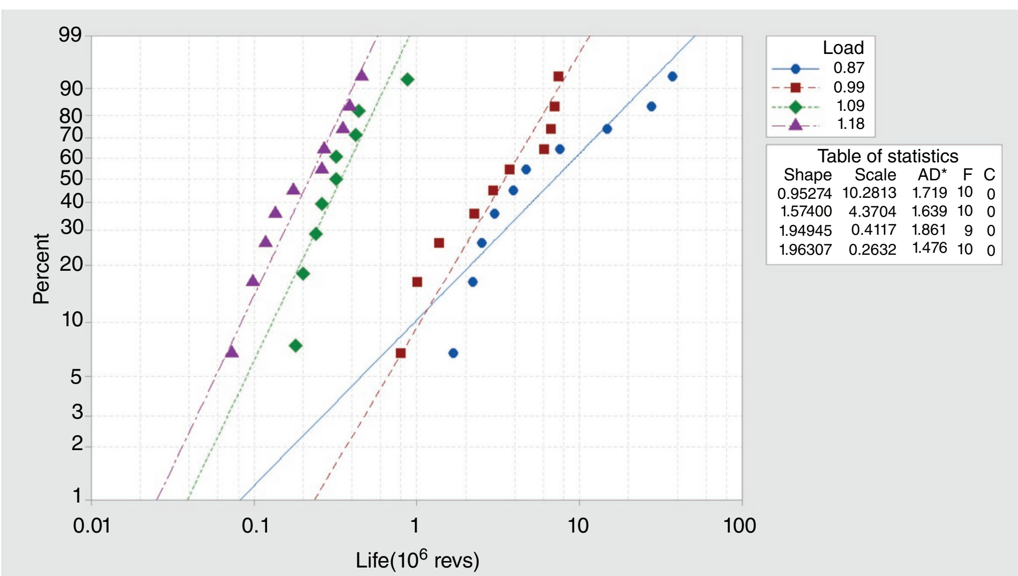
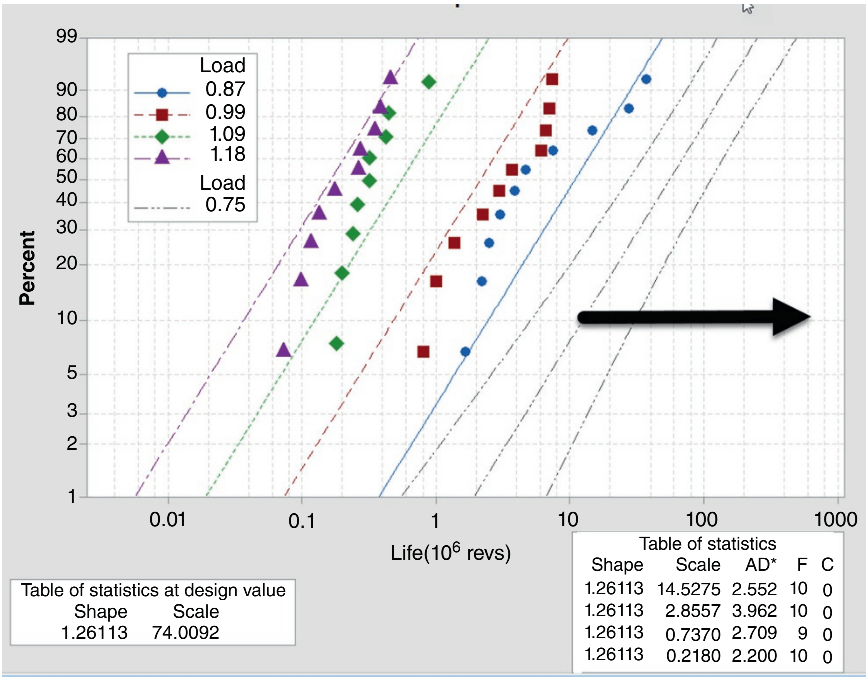


Figure 6.30 Individual fits for life by load. Note that the characteristic life goes down as each load setting goes up.

3 Nelson (1990), p. 157.



see Figure 6.32 for Lower 95% bound at reliability = 0.9

Figure 6.31 Accelerated testing extrapolating to 0.75 load.

Load = 0.75

Percent	Life (10^6 revs)	Lower Bound	Upper Bound
1	1.92815	0.553557	6.71611
2	3.35414	1.07690	10.4469
3	4.64483	1.58867	13.5801
4	5.85884	2.09349	16.3966
5	7.02174	2.59370	19.0095
6	8.14771	3.09076	21.4786
7	9.24572	3.58569	23.8402
8	10.3220	4.07924	26.1183
9	11.3809	4.57202	28.3299
10	12.4260	5.06450	30.4877
20	22.5296	10.0434	50.5388
30	32.6788	15.2723	69.9243
40	43.4475	20.9353	90.1673
50	55.3440	27.2509	112.398
60	69.0527	34.5475	138.021
70	85.7452	43.4080	169.375
80	107.936	55.0915	211.469
90	143.384	73.4566	279.879
91	148.562	76.1063	289.998
92	154.296	79.0303	301.240
93	160.729	82.2989	313.903
94	168.074	86.0145	328.419
95	176.654	90.3339	345.458
96	187.009	95.5170	366.139
97	200.144	102.044	392.550
98	218.285	110.977	429.353
99	248.427	125.614	491.313

Figure 6.32 Lower 95% bound at reliability =0.9 at 5.06×10^6 rev.

Example 6.31 An electric motor was run in life test at four speeds at a constant load.

The results are in Table 6.12. Using the IPL model, What is the model for stress versus life? What is the acceleration factor?[4]

Solution: See Table 6.12 and Figure 6.33.

Table 6.12 Test data.

RPM	Time to fail (h)
3200	150
2800	790
2400	2410
2000	7340

Source: Data from Nelson (1990), p.115.

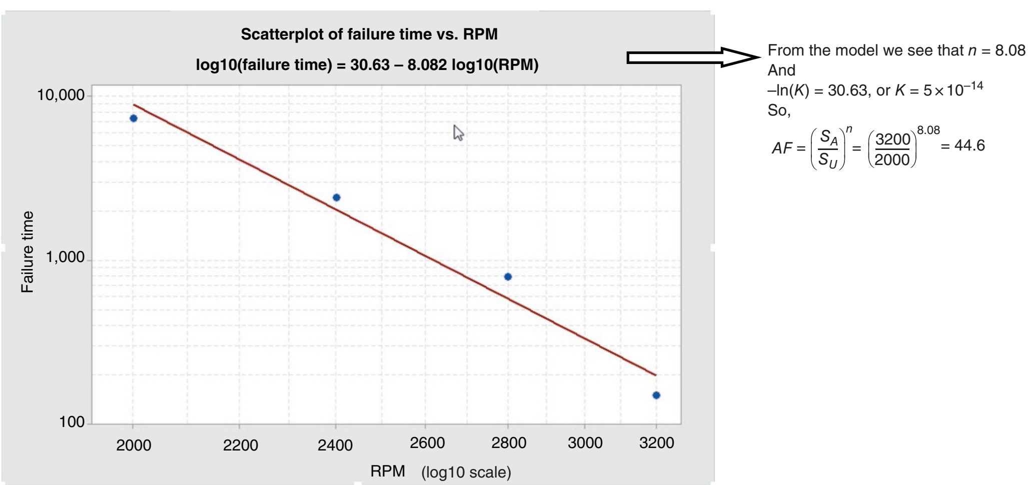


Figure 6.33 Fitting the electric motor data to model in Eq. (6.69).

Example 6.32 15 units were tested at each of 36 and 20 V. Testing at 20 V was terminated after the fourth failure. Assuming an inverse power relationship, determine the B10 life of a unit like this at 5 V,

Solution: Using the data in Table 6.13 at right.[5]

The first plot illustrates a Weibull of the failures at 20 and 36 V (Figures 6.34, 6.35, 6.36, and 6.37).

The acceleration factor here is

4 *Source*: Data from Accelerated Life Testing Presentation, Jim McLinn.
5 Taken from Kececioglu and Jacks (1984), with permission.

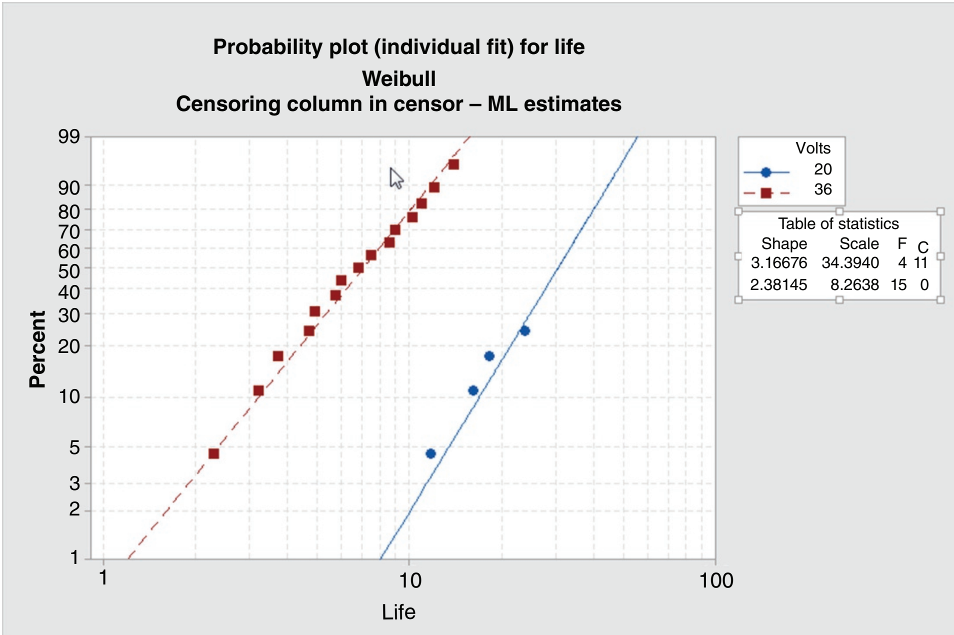


Figure 6.34 The Weibull distribution explains the failures.

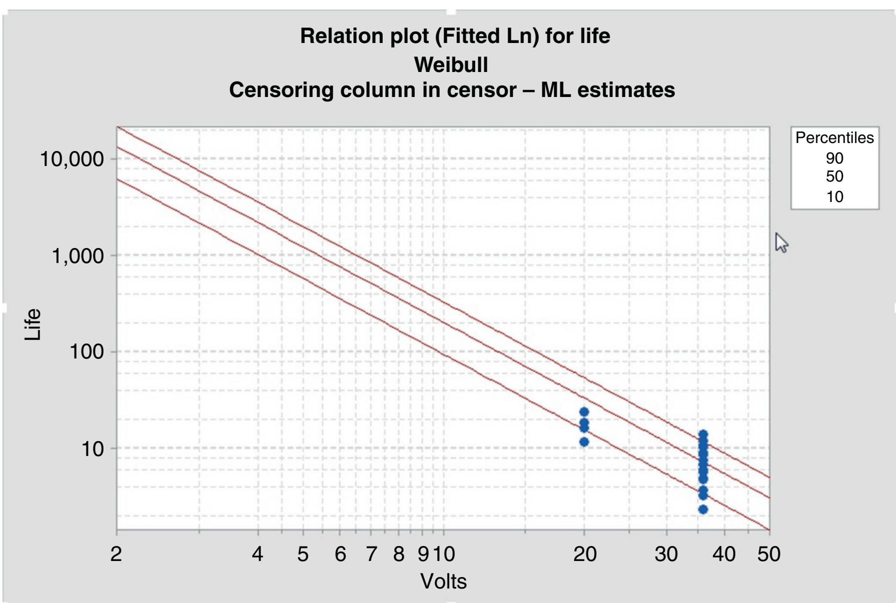


Figure 6.35 The extrapolation to the use voltage (5 V).

Percentiles = 10

Volts	Life
2.5	3465.89
5	570.681
7.5	198.665
10	93.9662
12.5	52.5734
15	32.7114
17.5	21.9014
20	15.4721
22.5	11.3875
25	8.65654
27.5	6.75493
30	5.38614
32.5	4.37331
35	3.60620
37.5	3.01351
40	2.54758

Figure 6.36 Lives at 0.9 reliability at discrete voltages, e.g. the 0.9 reliability (B10 life) at 5 V is 570.7 cycles.

$$AF = \frac{\eta_A}{\eta_U} = \frac{1417}{8.3} = 171$$

Other Acceleration Models

If you see that the Weibull or lognormal distributions at the different stress levels are very different, and hence, the life vs stress plot is nonlinear, you may need one of these models. For more details on each, see either Reliasoft (2007) or Kececioglu (1993) for details.

The following descriptions will give you some insight into the possible situations where the models may be useful.

1) The *temperature–humidity relationship model* is a variation of the Eyring model for predicting life at use conditions when temperature and humidity are both stressors.

$$L(S_1, S_2) = Ae^{\left(\frac{B}{S_1} + \frac{C}{S_2}\right)} \tag{6.73}$$

for two stressors, where

S_1 is temperature in absolute units as above
S_2 is relative humidity (decimal or percentage)
A and B are model parameters to be calculated
C is the activation energy for humidity

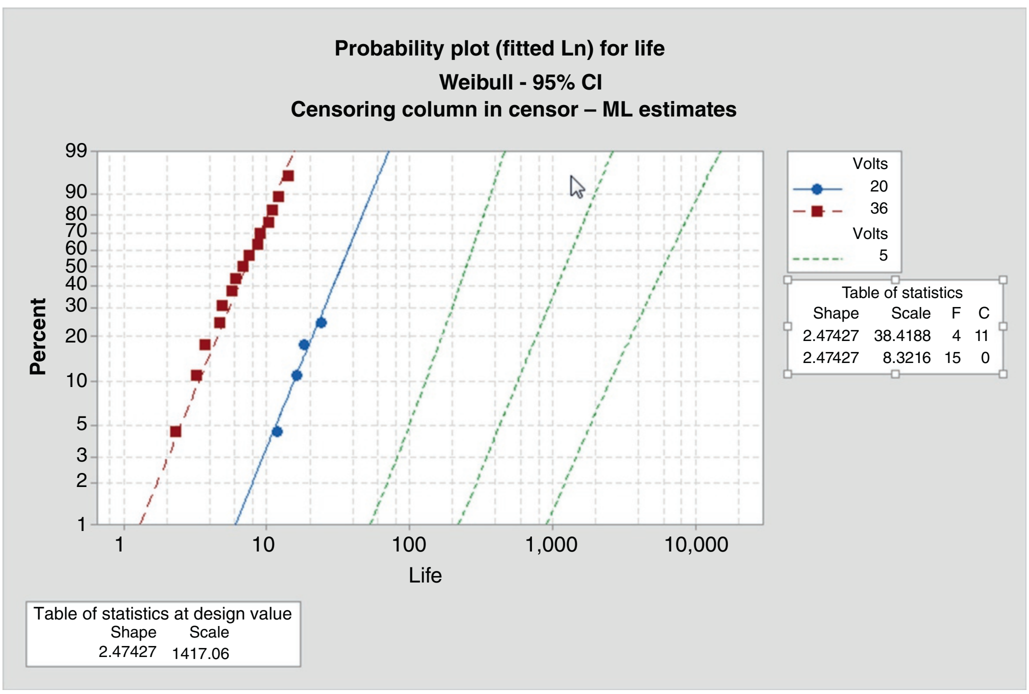


Figure 6.37 The details of the two combined accelerated Weibull β and the 5 V use Weibull with 95% confidence bands.

Table 6.13 Accelerated life at 20 and 36 V to predict life at 5 V.

36 V	20 V
2.3	11.7
3.2	16.2
3.7	18.3
4.7	23.8
4.9	Test stopped
5.7	After fourth failure 10 censored at 23.8 h
6	
6.8	
7.5	
8.6	
9	
10.2	
10.9	
12	
14	

Source: Data from Kececioglu and Jacks (1984).

2) The *Arrhenius–IPL combined model* can be used when a thermal AND a nonthermal stress are stressors:

$$L(S_1, S_2) = \frac{C}{S_2^n e^{-\frac{B}{S_1}}} \tag{6.74}$$

where

S_1 is the temperature in absolute units as above
S_2 is the non-therma1 stress (e.g. voltage, bends, vibration level)
B and C are to be calculated

3) The Eyring model

The *Eyring model* (sometimes called the *Eyring–Polyani model*) may be used for modeling the failure of chemical systems due to temperature; in addition, it is also used when humidity is a stressor. The Eyring model can be extended to consider the effects of two stressors – one thermal and one nonthermal.

The model is

$$L(S) = \frac{1}{S} e^{-\left(A - \frac{B}{S}\right)} \tag{6.75}$$

for one stressor, where

L represents a life measure
S represents a temperature in absolute units – deg Kelvin (°K = 273.15 + °C) or deg Rankine (°R = 459.67 + °F)

A and B are model parameters to be calculated

and

$$L(S_1, S_2) = \frac{1}{S_1} e^{\left(A + \frac{B}{S_1} + CS_2 + D\frac{S_2}{S_1}\right)} \tag{6.76}$$

for two stressors, where

S is the temperature in absolute units as above
S_2 is non-thermal (e.g. voltage)
A, B, C, and D are model parameters to be calculated

6.8 Reliability-Enhancement Procedures

Reliability studies during design and development are extremely valuable, for they are available at a time when design modifications or other corrections can be made at much less expense than later in the product life cycle. With the building of the first prototypes hands-on operational experience is gained. And as the limitations and shortcomings of the analytical models used for design optimization are revealed, reliability is enhanced through experimentally based efforts to eliminate failure modes. The number of prototype models is not likely to be large enough to apply standard statistical techniques to evaluate the reliability, failure rate, or related quantities as a function of time. Even if a sample of sufficient size could be obtained, life testing would not in general be appropriate before the design is finalized. If one ran life tests on the initial design, the results would likely underestimate the reliability of the improved model that finally emerged from the prototype testing phase.

The two techniques discussed in this section are often employed as an integral part of the design process, with the failures being analyzed and the design improved during the course of the testing procedure. In contrast, the life-testing methods discussed in Sections 6.3 and 6.4 may be used to improve the next model of the product, change the recommended operation procedures, revise the warrantee life, or for any number of other purposes. They are not appropriate, however, while changes are being made to the design.

Reliability Growth Modeling and Testing

Newly constructed prototypes tend to fail frequently. Then, as the causes of the failures are diagnosed and actions taken to correct the design deficiencies, the failures become less frequent. This behavior is pervasive over a variety of products and has given rise to the concept of *reliability growth*. A formal definition of *reliability growth*: the positive improvement in a reliability parameter over a period of time due to changes in product design or the manufacturing process.

Reliability growth is the result of an iterative design process:

1) Detection of failure sources.
2) Feedback of problems identified.
3) Redesign effort based on problems identified.
4) Fabrication of hardware.
5) Verification of redesign effect.

Sometimes referred to "Test, Analyze, Fix" or TAF.

(Note: the following is excerpted from MIL-HDBK-189C 2011.)

Timing of fixes during a development program is of utmost importance, especially if an accurate idea of reliability growth is to be reported. To reach the goal reliability, the development testing program will usually consist of several major test phases. Within each test phase, the fixes can be incorporated in any one of the three ways:

1) *Test–Fix–Test*

   In a pure test–fix–test program, when a failure is observed, testing stops until a corrective action is implemented on the system under test. When the testing resumes, it is with a system that has incrementally better reliability. The graph of reliability for this testing strategy is a series of small increasing steps, with each step stretching out longer to represent a longer time between failures; hence, the graph can be approximated by a smooth curve. In most cases, this is impractical because of the cost of test time, particularly for large systems (e.g. aircraft and rocket engines, aircraft, and the like). But for smaller subsystems or modules, this can be done.
2) *Test–Find–Test*

   During a test–find–test program, the system is tested to determine failure modes. However, unlike the test–fix–test program, fixes are not incorporated into the system during the test. Rather, the fixes are all inserted into the system at the end of the test phase and before the next testing period. Since a large number of fixes will generally be incorporated into the system at the same time, there is usually a significant jump in system reliability at the end of the test phase. The fixes incorporated into the system between test phases are called "delayed" fixes.
3) *Combination of Test–Fix–Test and Test–Find–Test*

   The test program most commonly used in development testing employs a combination of the previous two types of fix insertions. That is, some fixes are incorporated into the system during the test, while other fixes are delayed until the end of the test phase. Consequently, the system reliability will generally be seen as a smooth process during the test phase and then jump due to the insertion of the delayed fixes (Figure 6.38).

Row 1 shows Phase 1 as having all fixes delayed until the end of the testing phase.

Row 2 shows Phase 1 as having some fixes inserted during test and some delayed.

Row 3 shows Phase 1 as having all fixes inserted during test, with none delayed.

Column 1 shows Phase 2 as having all fixes delayed until the end of the testing phase.

Column 2 shows Phase 2 as having some fixes inserted during test and some delayed.

Column 3 shows Phase 2 as having all fixes inserted during test, with none delayed.

Figure 6.38a and i represent the two extremes in possible growth test patterns.

How to model the reliability growth phenomenon?

Suppose that we define the following:

T = total operation time accumulated on the prototype
$N(T)$ = number of failures from the beginning of operation through time T.

Duane (1964) observed that if $N(T/T)$ is plotted versus T on log–log paper, the result tends to be a straight line. From such empirical relationships, referred to as a Duane plots, we may make rough estimates of the growth of the time between failures and therefore also extrapolate a measure of how much reliability is likely to be gained from further cycles of test and fix.

Since Duane plots are straight lines, we may write

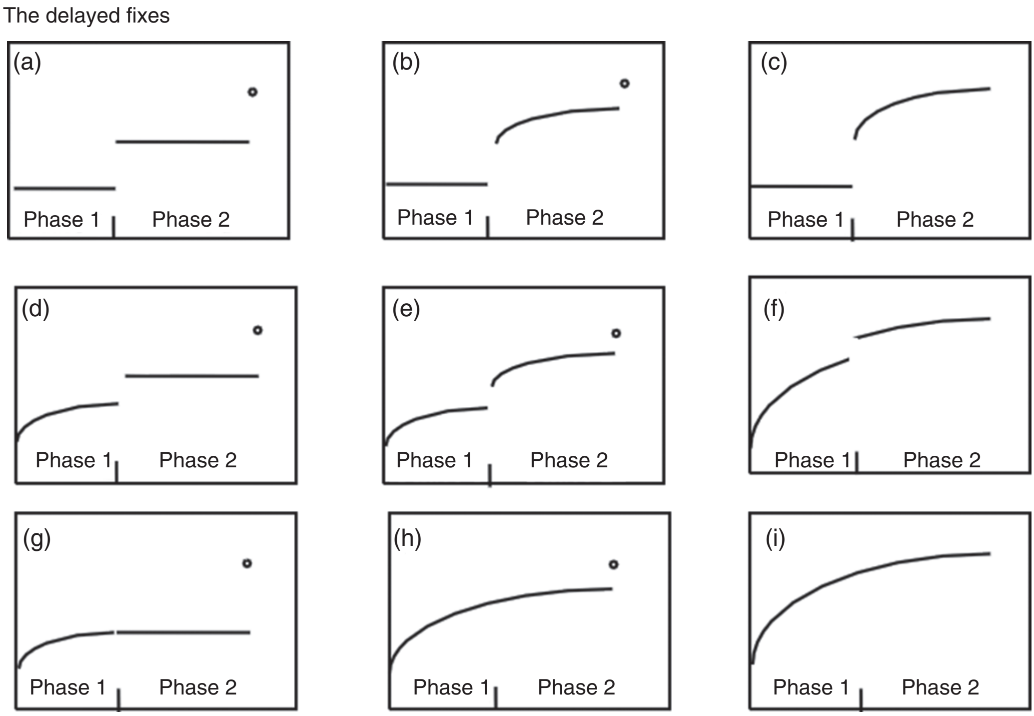


Figure 6.38 The nine possible general growth patterns for two test phases. *Source*: Based on MIL-HDBK-189C (2011). Public Domain.

$$\ln\left[\frac{n(T)}{T}\right] = -\alpha \ln(T) + b \tag{6.77}$$

or solving of $n(T)$

$$n(T) = KT^{1-\alpha} \tag{6.78}$$

where $K = e^b$. Note that if $\alpha = 0$, there is no improvement in reliability, for the number of failures expected is proportional to the testing time. For α greater than zero, the expected failures become further and further apart as the cumulative test time T increases. An upper theoretical limit is $\alpha = 1$, since with this value, Eq. (6.78) indicates that the number of failures is independent of the length of the test.

Suppose that we define the rate at which failures occur as just the time derivative of the number of failures, $N(T)$, with respect to the total testing time:

$$\Lambda(T) = \frac{d}{dT} n(T) \tag{6.79}$$

Note that Λ is *not* the same as the failure rate λ discussed at length earlier, since now each time a failure occurs, a design modification is made. Understating this difference, we may combine Eqs. (6.78) and (6.79) to obtain

$$\Lambda(T) = (1-\alpha)\, KT^{-\alpha} \tag{6.80}$$

indicating the decreasing behavior of $\Lambda(T)$ with time.

However, the Duane postulate is deterministic in the sense that it gives the expected pattern for reliability growth but does not address the associated variability of the data.

The next step to address the variability shortfall of the Duane model, Duane (1964) was taken by Dr. L.H. Crow, Crow (1975). Dr. Crow considered Duane's power law reliability growth pattern and formulated the underlying probabilistic model for failures as a nonhomogeneous Poisson process (NHPP[6]), $[N(T),\ T > 0]$, with

Expected number of failures at time T: $E[N(T)] = \lambda T^{\beta}$

Where the derivative of $E[N(T)]$, call the "Intensity" function $z(T)$:

$$Z(T) = \frac{d}{dT}\left(\lambda T^{\beta}\right) = \lambda\beta T^{\beta-1} \tag{6.81}$$

The Crow NHPP power law model has the same look and feel as the Duane model, e.g. λT^{β} is the expected number of failures by time T in both. However, the NHPP model gives the Poisson probability that $N(T)$ will assume a particular value:

$$P[N(T) = n] = \frac{\left(\lambda T^{\beta}\right)^{n} e^{\lambda T^{\beta}}}{n!}, \quad \text{for } n = 0, 1, 2, \ldots \tag{6.82}$$

Also, under the Crow model:

$$E\left(\lambda T_j^{\beta}\right) = j, \quad \text{for } j = 1, 2, \ldots$$

where T_j is the accumulated time to the jth failure.

Then we have the approximation for the expected time to the jth failure:

$$E\left[T_j\right] = \left(\frac{j}{\lambda}\right)^{\frac{t}{\beta}}, \text{where } j = 1, 2, \ldots \tag{6.83}$$

When the "shape" parameter $\beta = 1$, $z(T) = \lambda$, and the successive failures follow an exponential distribution with mean $1/\lambda$ (an HPP-Homogeneous Poisson Process), indicating no reliability growth. The intensity function $Z(T)$ is decreasing for $\beta < 1$ (positive growth), and increasing for $\beta > 1$ (negative growth).

The NHPP power law reliability growth model is a probabilistic interpretation of the Duane postulate and therefore allows for the development and use of rigorous statistical procedures for reliability growth assessments. Figure 6.39 shows how a number of different devices' cumulative failures versus time follow this power model. Along those lines, the NHPP power law model was extended by Crow in 1981 when Mil-Hbk-189 was published. Mil-Hbk-189 was the culmination of a DOD and Industry team led by Dr Larry Crow taking Duane's original idea and formalizing it from a statistical standpoint (maximum-likelihood estimation of the model parameters and system reliability, confidence interval procedures and objective goodness-of-fit tests, reliability projections, etc.).

Taking J.T. Duane's original observations and studying other possible models for reliability growth, the Mil-HBK-189 team decided that Duane's original observation was the most useful, and hence, the Larry Crow AMSAA/Duane model was born. Mil-Hbk-189 later was updated by an IEC (International Electrotechnical Commission) Committee as *ANSI/IEC/ASQ D61164-1997*

6 An NHPP is a Poisson process with a nonconstant recurrence rate with respect to time t. A Homogeneous Poisson Process (HPP) is a Poisson process such that the rate of occurrence of events is a constant with respect to time t.

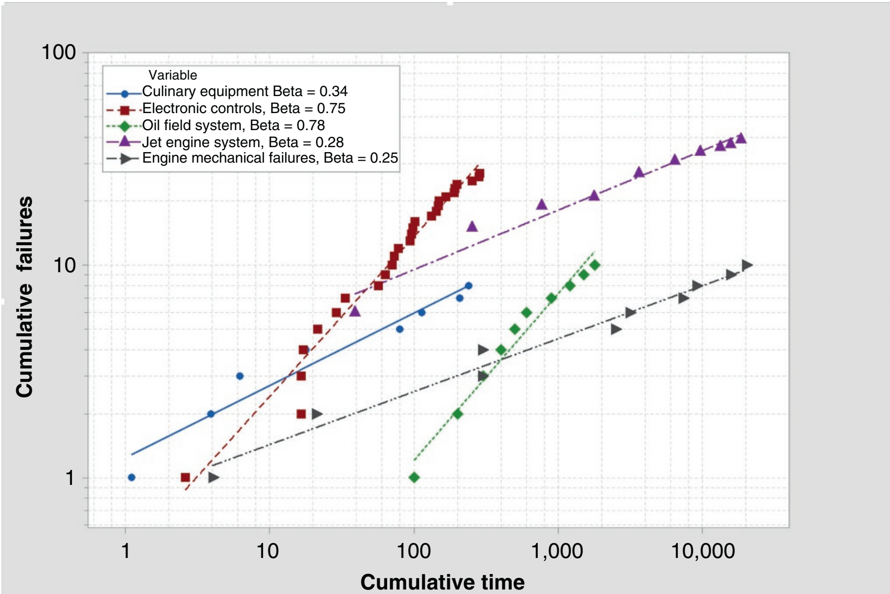


Figure 6.39 Various system cumulative failures vs time, plot as straight lines on log–log scales.

and became an international standard, formalizing further the Mil-Hbk-189 statistical accomplishments. The current version of Mil-Hbk-189 is Mil-Hbk-189C (2011).

The statistical procedures for the power law reliability growth model use the original relevant failure and time data from a test or series of field observations. Except for projecting failure rate for the future, the model is applied to the complete set of relevant failures as a whole (i.e. without subdivision into categories of failures).

Duane-AMSAA plots are very useful for predicting future failures based on your data. The technique provides a methodology, the equations are simple, the failure forecast is based on your data, and you can make reasonable forecast of future events.

Example 6.33 A first prototype for a novel laser-powered sausage slicer is built. Failures occur at the following numbers of minutes: 1.1, 3.9, 6.2, 17.8, 79.7, 113.1, 206.4, and 239.1. After each failure the design is refined to avert further failures from the same mechanism. Determine the reliability-grown coefficient β (and hence Duane's $\alpha = 1 - \beta$) for the slicer.

Solution:

Using least squares for this problem and using MINITAB "fitted line" (Figure 6.40).

Here, $\beta = 0.34$ and $\lambda = 10{*}{*}0.095 = 1.244$ or $N(T) = 1.244\text{T}^{0.34}$.

While the AMSAA-Duane model is $N(t) = \lambda t^{\beta}$, the model can be rearranged in a number of ways to satisfy a customer's demands for reporting:

$$\text{Cumulative Events}: \quad N(t) = \lambda t^{\beta} \tag{6.84}$$

$$\text{Cumulative Rate}: \quad C(t) = \frac{N(t)}{t} = \lambda t^{\beta - 1} \tag{6.85}$$

$$\text{Instantaneous Rate}: \quad c(t) = \frac{dN(t)}{dt} = \lambda \beta t^{\beta - 1} \tag{6.86}$$

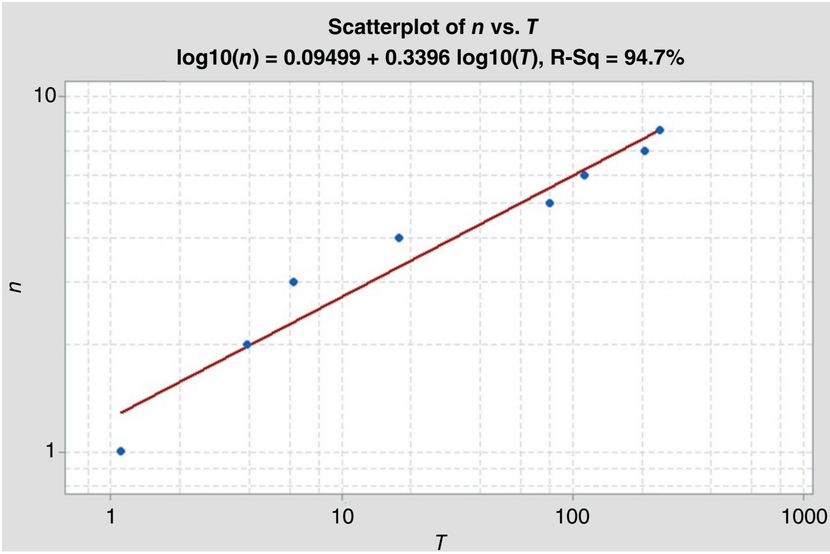


Figure 6.40 Log–log plot of cumulative events vs. cumulative time with power model fit.

$$\text{Cumulative MTBF}: \quad M(t) = \frac{1}{C(t)} = \left(\frac{1}{\lambda}\right) t^{1-\beta} \tag{6.87}$$

$$\text{Instantaneous MTBF}: \quad m(t) = \frac{1}{c(t)} = \left(\frac{1}{\lambda\beta}\right) t^{1-\beta} \tag{6.88}$$

Calculation of Reliability Growth Parameters

Maximum likelihood is most commonly used to define growth parameters. The MLE formulas for the Crow-AMSAA β & λ will be slightly different, based on the type of data.

- Time-terminated testing:

$$\hat{\beta} = \frac{N}{N \ln T - \sum_i \ln x_i} \tag{6.89a}$$

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}} \tag{6.89b}$$

where

N = Number of failures at time T
T = Cumulative test time
x_i = Cumulative time at each failure

- Failure-terminated testing:

$$\hat{\beta} = \frac{N}{(N-1) \ln x_N - \sum_i \ln x_i} \tag{6.90a}$$

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}} \tag{6.90b}$$

where

N = Number of failures at time T
x_i = Cumulative time at each failure

- Grouped data (usually from the field or warranty databases)

It may happen that a system has a "failure" in a unit that does not shut down the system. That may be due to redundancy or standby units being available. Those events are often only discovered at a scheduled inspection, which could be weekly, monthly, or longer. In those cases, the exact time of the failure is unknown; however, one can presume that it happened in the interval since the last inspection. The total number of failures in the interval between inspections is therefore the number of failures during the inspection. Such totals for each interval can be used to estimate reliability growth in accordance using the "grouped" reliability growth model if there are at least three intervals.

Grouped data: (solving for $\hat{\beta}$ first)

$$\sum_{i=1}^{k} N_i \left[\frac{t_i^{\hat{\beta}} \ln t_i - t_{i-1}^{\hat{\beta}} \ln t_{i-1}}{t_i^{\hat{\beta}} - t_{i-1}^{\hat{\beta}}} - \ln t_k \right] = 0 \tag{6.91}$$

$$\text{then, } \hat{\lambda} = \frac{\sum_{i=1}^{k} N_i}{t_k^{\hat{\beta}}} \tag{6.92}$$

where

k = number of groups/intervals
t_k = the end of the last interval
N_i = the number of failures in each interval

Goodness-of-Fit Tests for Reliability Growth Models

For Time-Terminated Testing

The null hypothesis that a nonhomogeneous Poisson process with an intensity function of the form

$$\lambda \beta t^{\beta - 1} \tag{6.93}$$

properly describes the reliability growth of a particular system is tested by the use of a Cramer von Mises statistic. An unbiased estimate of the shape parameter is used to calculate that statistic. This estimate of β is

$$\overline{\beta} = \frac{N-1}{N} \hat{\beta} \tag{6.94}$$

for a time-terminated test with N failure occurrences. The goodness-of-fit statistic is

$$C_M^2 = \frac{1}{12N} + \sum_{i=1}^{N} \left[\left(\frac{x_i}{T} \right)^{\overline{\beta}} - \frac{2i-1}{2N} \right]^2 \tag{6.95}$$

in which the failure times must be ordered so that $0 \leq x_1 \leq x_2 \leq \cdots \leq x_N$.

The null hypothesis is rejected if the statistic C_M^2 exceeds the critical value for the level of significance selected by the analyst. Critical values of C for the 0.20, 0.15, 0.10, 0.05, and 0.01 levels of significance (α) are in Supplement 3. The Cramer von Mises (C_M^2) table is indexed by a parameter labeled M. For time-terminated testing, M is equal to N, the number of failures. If the test rejects the reliability growth model, an examination of the data may reveal the reason for the lack of fit. Possible causes of rejection include the occurrence of more than one failure at the same time or the occurrence of a discontinuity in the intensity function. In the first case, an appropriate procedure may be to group the data. If a discontinuity is in the data, or the fit does appear right to the "eyeball," another reliability growth model may be called for (this is unusual). Supplement 4 reviews some of the other reliability growth models available in the literature.

For Failure-Terminated Testing

As before, the hypothesis that the AMSAA-Duane model is appropriate can be tested using a Cramer–von Mises statistic. It is important to note the difference in the calculations from those for time-terminated testing. An unbiased estimate of the shape parameter given by

$$\bar{\beta} = \frac{N-2}{N}\hat{\beta} \tag{6.96}$$

is used in the calculation of the goodness-of-fit statistic. The parameter for indexing that statistic is $M = N - 1$, where N is the number of failures. The Cramer–von Mises statistic is then

$$C_M^2 = \frac{1}{12M} + \sum_{i=1}^{M}\left[\left(\frac{x_i}{X_N}\right)^{\bar{\beta}} - \frac{2i-1}{2M}\right]^2 \tag{6.97}$$

Supplement 3 critical values for use in the test. The model is deemed inappropriate if the statistic C_M^2 exceeds the critical value for some specified level of significance (α).

For Grouped Data

A Chi-squared goodness-of-fit test can also be used to test the hypothesis that an AMSAA-Duane model adequately represents a set of grouped data. The expected number of failures predicted by the model, using (t_i), is

$$e_i = \hat{\lambda}\left(t_i^{\hat{\beta}} - t_{i-1}^{\hat{\beta}}\right) \tag{6.98}$$

Adjacent intervals may have to be combined so that the expected number of failures in any interval is at least 5. Let the number of intervals after this combination be called K, and let the number of failures in the ith interval be called N_i. The expected number of failures will be e_i as before. Calculating the statistic:

$$\chi^2 = \sum_{i=1}^{K}\frac{(N_i - e_i)^2}{e_i} \tag{6.99}$$

is approximately distributed as a χ^2 random variable with K-2 degrees of freedom. The critical value of the Chi-square can be found at the end of the chapter in a Chi-sq table (Supplement 5).

Table 6.14 Hardware failures – time-terminated test at 300 hours.

	No. 1	No. 2	Cumulative		No. 1	No. 2	Cumulative
	Hours	Hours	Hours		Hours	Hours	Hours
1	2.6[a]	0	2.6	15	60.5	37.6[a]	98.1
2	16.5[a]	0	16.5	16	61.9[a]	39.1	101.1
3	16.5[a]	0	16.5	17	76.6[a]	55.4	132
4	17.0[a]	0	17	18	81.1	61.1[a]	142.2
5	20.5	0.9[a]	21.4	19	84.1[a]	63.6	147.7
6	25.3	3.8[a]	29.1	20	84.7[a]	64.3	149
7	28.7	4.6[a]	33.3	21	94.6[a]	72.6	167.2
8	41.8[a]	14.7	56.5	22	104.8	85.9[a]	190.7
9	45.5[a]	17.6	63.1	23	105.9	87.1[a]	193
10	48.6	22.0[a]	70.6	24	108.8[a]	89.9	198.7
11	49.6	23.4[a]	73	25	132.4	119.5[a]	251.9
12	51.4[a]	26.3	77.7	26	132.4	150.1[a]	282.5
13	58.2[a]	35.7	93.9	27	132.4	153.7[a]	286.1
14	59	36.5[a]	95.5	END	132.4	167.6	300

[a] Denotes a failure.
Source: MIL-HDBK-189C (2011). Public Domain.

Example 6.34 Based on the hardware failure data in Table 6.14 where the test was terminated at 300 hours.

Using formulae (6.89a) and (6.89b):

$$\hat{\beta} = \frac{N}{N\ln(T) - \sum_i \ln(x_i)} = \frac{27}{27\ln(300) - (\ln 2.6 + \ln 6.5 + \cdots + \ln 286.1)} = 0.716$$

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}} = \frac{27}{300^{0.716}} = 0.454$$

Therefore, for this data: $N(t) = 0.454t^{0.716}$ (Figure 6.41)

In addition, see Figures 6.42 and 6.43.

Goodness-of-Fit Test:

While looking at the plots tells our "eyeball" the fits to the data are good, the goodness-of-fit test tells us that using Eqs. (6.94) and (6.95)

$$\overline{\beta} = \frac{N-1}{N}\hat{\beta} = \frac{27-1}{27}(0.716) = 0.689$$

$$C_M^2 = \frac{1}{12N} + \sum_{i=1}^{N}\left[\left(\frac{x_i}{T}\right)^{\overline{\beta}} - \frac{2i-1}{2N}\right]^2 = 0.110 < 0.172$$

(Cramer Von Mises Critical value for $N = 27$ at $\alpha = 0.10$) and our "eyeball" was pretty good! Therefore with 90% confidence we can say we have a good fit to the data.

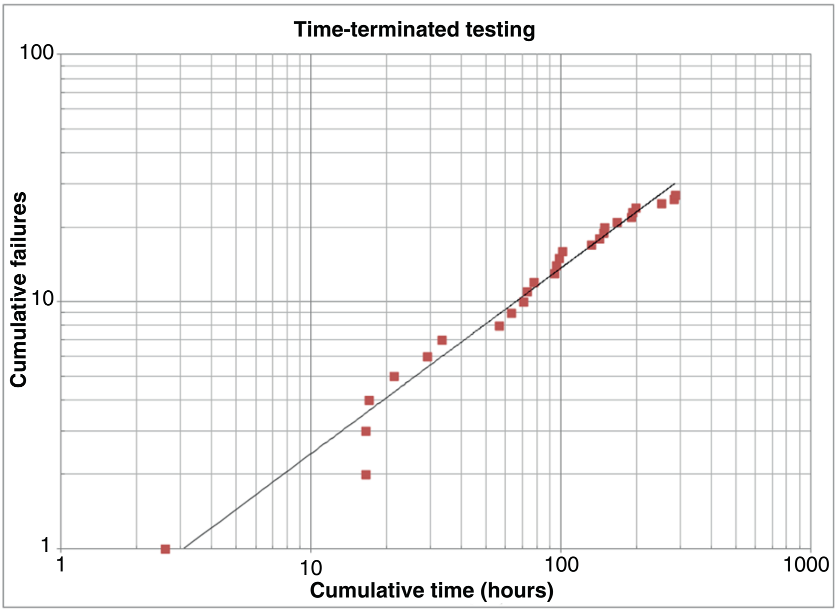


Figure 6.41 Reliability growth plot of time-terminated testing example. *Source*: Based on MIL-HDBK-189C (2011). Public Domain.

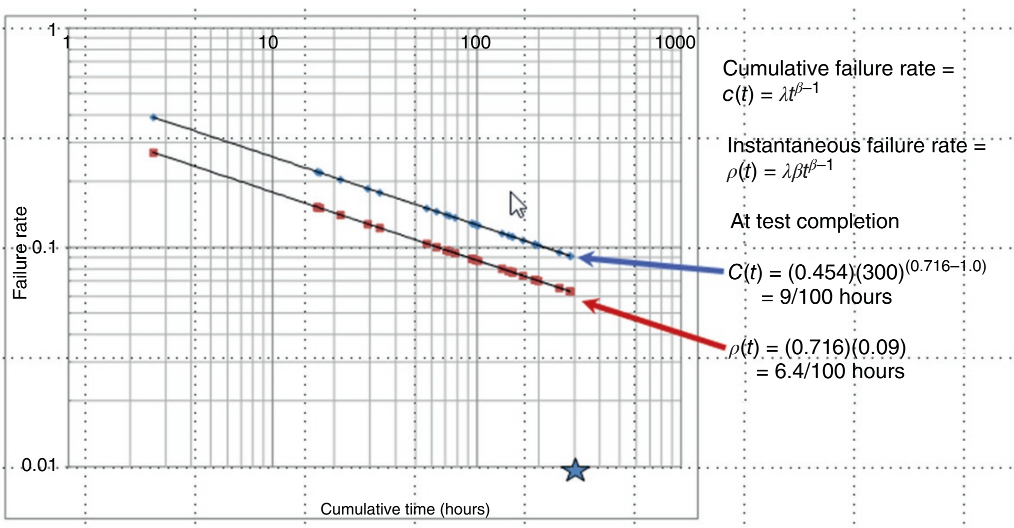


Figure 6.42 Plotting by failure rate displays an improving trend *indicates the test termination point.

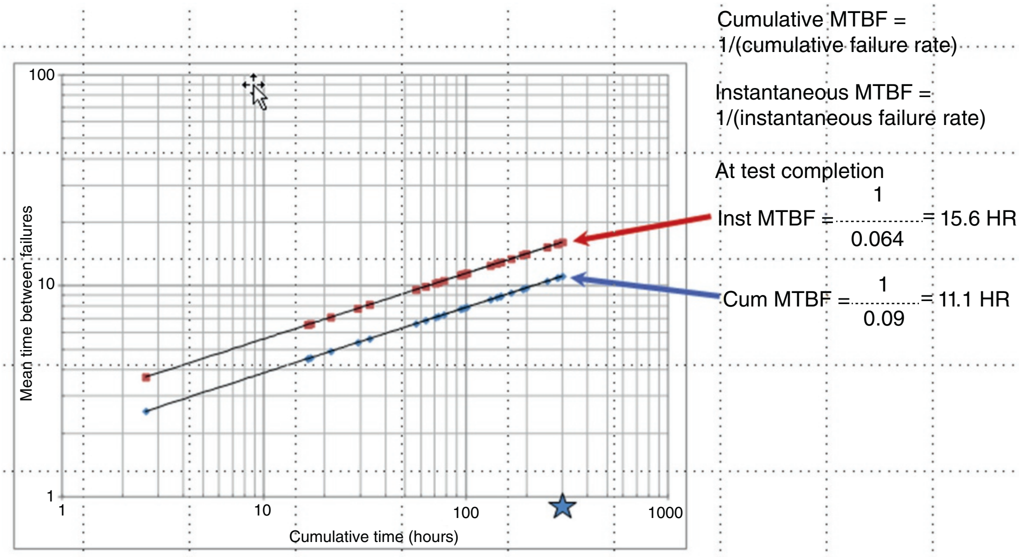


Figure 6.43 Plotting by mean time between failure (MTBF).

Example 6.35 System failure occurs repeatedly, and the test is terminated after the 26th failure.

Failures occurred at 1, 57, 187, 252,310,485,693,720,727,779, 1028, 1561, 1766, 1793, 1938, 2030, 2065, 2289, 2423, 2560, 2879, 3086, 3458, 3626, 4252, and 4582 hours.

Using Failure-terminated testing, Eqs. (6.90a) and (6.90b):

$$\hat{\beta} = \frac{N}{(N-1)\ln x_N - \sum_{i=1}^{N-1} \ln(x_i)} \quad \text{and } \hat{\lambda} = \frac{N}{T^{\hat{\beta}}}$$

$$\hat{\beta} = \frac{N}{(N-1)\ \ln x_N - \sum_{i=1}^{N-1} \ln(x_i)} = \frac{26}{(26-1)\ \ln\ (4582) - [\ln(1) + \ln(57) + \cdots + \ln(4252)]} = 0.626$$

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}} = \frac{26}{(4582)^{0.626}} = 0.1328$$

Therefore, $N(t) = 0.1328\ t^{0.626}$ (Figure 6.44).

Goodness-of-Fit Test:

Again, the goodness of fit is tested at the .10 level of significance. The critical value for M equal to 26 is determined to be 0.172 by interpolation in Cramer–von Mises table in Supplement 3.

The Cramer–von Mises statistic is $0.058 < 0.172$, which indicates that the model represents the data quite well, despite the fact that the first failure is most likely an outlier (this should be checked by engineering but will not change the β or λ significantly).

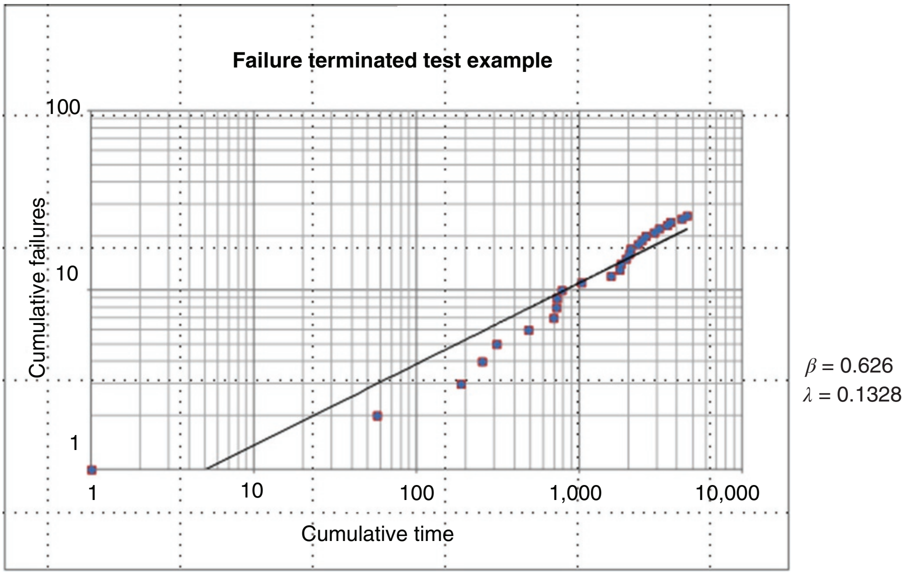


Figure 6.44 System *failure-terminated testing. Source*: Based on MIL-HDBK-189C (2011). Public Domain.

Example 6.36[7]

An aircraft has scheduled inspections at intervals of 20 flight hours. All failures that have occurred between consecutive inspections are combined with those discovered during the inspection at the end of the interval to give the total for the interval. For the first 100 hours of flight testing, the results are shown in Table 6.15:

Using Eqs. (6.91) and (6.92) for Grouped data (solving for $\hat{\beta}$ first):

$$\sum_{i=1}^{k} N_i \left[\frac{t_i^{\hat{\beta}} \ln t_i - t_{i-1}^{\hat{\beta}} \ln t_{i-1}}{t_i^{\hat{\beta}} - t_{i-1}^{\hat{\beta}}} - \ln t_k \right] = 0$$

Table 6.15 Aircraft incidents during the first 100 hours of flight testing.

Start time (*i* − 1)	**End time (*i*)**	**Incidents**
0	20	13
20	40	16
40	60	5
60	80	8
80	100	7

Source: MIL-HDBK-189C (2011). Public Domain.

7 Mil-Hbk-189, p. 140.

$$\text{then, } \hat{\lambda} = \frac{\sum_{i=1}^{k} N_i}{t_k^{\hat{\beta}}}$$

where

k = number of groups/intervals
t_k = the end of the last interval
N_i = the number of failures in each interval

And setting these equations in EXCEL™ (Tables 6.16a, 6.16b, and graphically Figure 6.45):

Goodness-of-Fit Test:
Using Eq. (6.43), with the results appearing in Table 6.17.
See Supplement 5 for a χ^2 table.

Table 6.16a Executing interval formulas iteratively in EXCEL.

i	Time interval (*i* − 1)	Time interval (*i*)	Incidents	β=	0.752850896	
1	0	20	13	=((C2^$F$1)∗LN(C2))	=C2^$F$1	=D2∗((E2/F2)-LN(100))
2	20	40	16	=((C3^$F$1)∗LN(C3))-((B3^$F$1)∗LN(B3))	=C3^$F$1-B3^$F$1	=D3∗((E3/F3)-LN(100))
3	40	60	5	=((C4^$F$1)∗LN(C4))-((B4^$F$1)∗LN(B4))	=C4^$F$1-B4^$F$1	=D4∗((E4/F4)-LN(100))
4	60	80	8	=((C5^$F$1)∗LN(C5))-((B5^$F$1)∗LN(B5))	=C5^$F$1-B5^$F$1	=D5∗((E5/F5)-LN(100))
5	80	100	7	=((C6^$F$1)∗LN(C6))-((B6^$F$1)∗LN(B6))	=C6^$F$1-B6^$F$1	=D6∗((E6/F6)-LN(100))
		Sum=	49		Sum=	−5.87312E-07
					λ=	1.529305631

Table 6.16b Spreadsheet with formulas executed – using SOLVER™.

i	Time interval (*i* − 1)	Time interval (*i*)	Incidents	β=	0.7528509	
1	0	20	13	28.574892	9.5385333	−20.922693
2	20	40	16	30.718564	6.5350351	1.5268237
3	40	60	5	30.009771	5.7377925	3.1251214
4	60	80	8	29.387835	5.2745224	7.7319028
5	80	100	7	28.861745	4.9548017	8.5388444
		Sum=	49		Sum=	−5.873E−07
					λ=	1.5293056

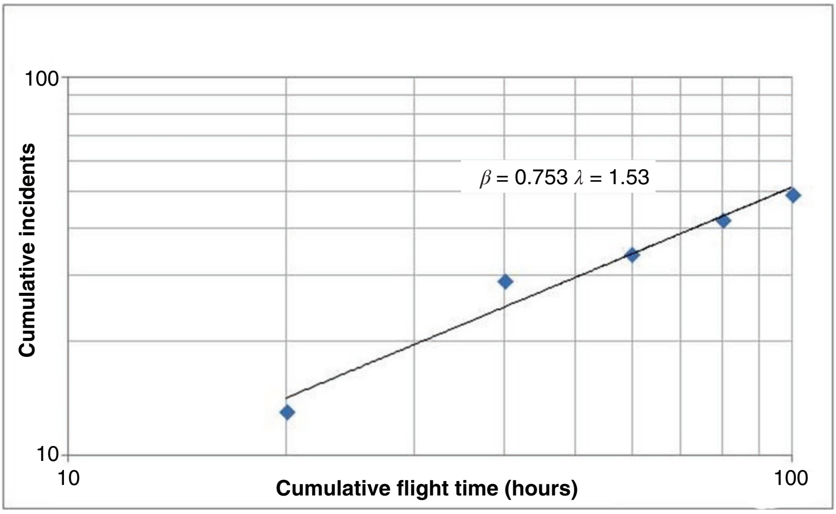


Figure 6.45 Plot of aircraft testing grouped data with growth model. *Source*: Based on MIL-HDBK-189C (2011). Public Domain.

Table 6.17 The calculation of goodness-of-fit statistic is 5.45.

i	Time interval ($i-1$)	Time interval (i)	$\beta=$ $\lambda=$ Incidents	0.752850896 1.529305631 $e_i = \hat{\lambda}\left(t_i^{\hat{\beta}} - t_{i-1}^{\hat{\beta}}\right)$	$\chi^2(k)$
1	0	20	13	14.58733262	0.172726907
2	20	40	16	9.994065906	3.609266207
3	40	60	5	8.77483841	1.623893724
4	60	80	8	8.066356846	0.000545876
5	80	100	7	7.577406216	0.043998953
				Sum=	5.450431667

The critical value for a χ^2 statistic with $k = 5 - 2 = 3$ degrees of freedom at $\alpha = 0.05$ significance level is 7.8. Since GoF statistic = 5.45 < χ^2 table value = 7.8, the model is accepted.

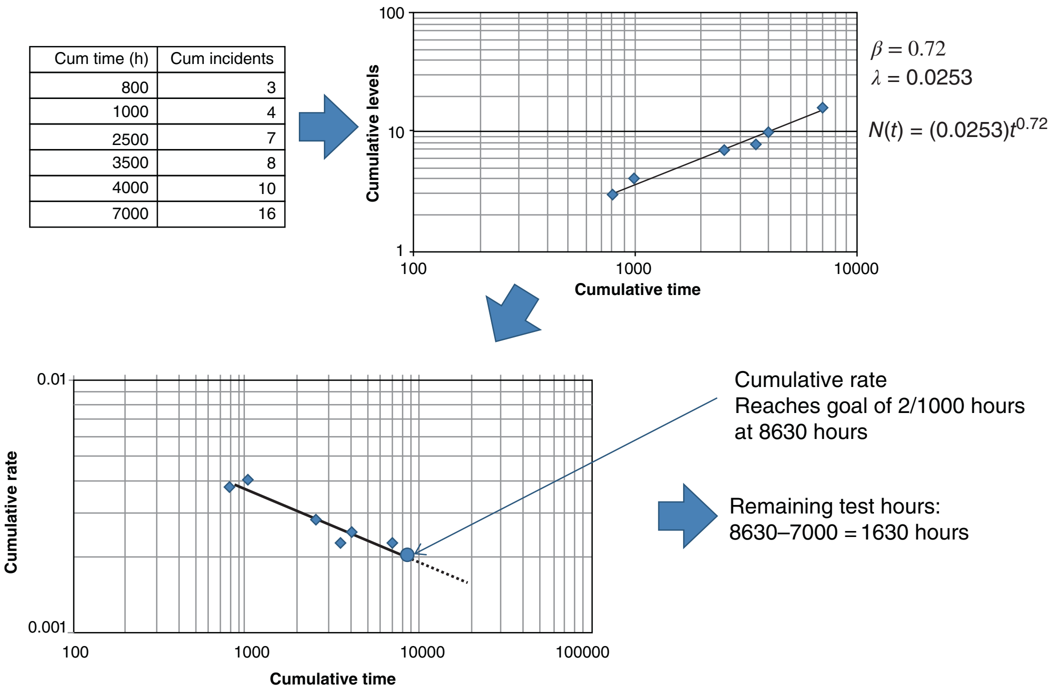
Suppose that you are now asked: How many failures will occur in the next 100 hours?

Using the AMSAA-Duane model with

$$\beta = 0.753 \text{ and } \lambda = 1.53$$
$$N(200) = 1.53^{*}200^{0.753} = 83.$$

So, over the next 100 hours, $83 - 49 = 34$ additional failures can be expected.

Example 6.37 Suppose that you are developing a new product. To effectively market this product the failure rate of your product must be 2/1000 hours or less. In testing to date, you have experienced failures at 800 hours, 1000 hours, 2500 hours, 3500 hours, 4000 hours, and 7000 hours. How much more testing (and fixing) is required to achieve your goal? See Figure 6.46 for solution.



Cum time (h)	Cum incidents
800	3
1000	4
2500	7
3500	8
4000	10
7000	16

Figure 6.46 Procedure for calculating the time remaining in development testing.

Example 6.38[8]

Suppose that we had a system that failed every 60 days for a total of 5 failures. Each corrective maintenance action was a **repair** (replacement components have the same length of life). Following the fifth failure, we added a **fix** (replacement with a longer life component) with a life of 300 days/failure. Subsequent failures will also be replaced with longer life components. The data are shown in Table 6.18.

The data and curve fit are in Figure 6.46. According to the equation, $N(t) = \lambda t^{\beta}$, which in this case is $N(t) = 0.1645t^{0.548}$.

Where β is the indicator of reliability improvements ($\beta < 1$), and the next failure (number 11 in this case) will occur at $t = (11/0.1645)^{(1/0.548)} = 2141.28$ cumulative time. The forecast of the next failure $2141.28 - 1800 = 341$ days compared to the 300 days expected from the discrete data in Table 6.18.

But in looking at the data more closely you can see there are two trends, see Figure 6.47. The first five failures have a different growth slope – steeper than the next five failures, indicating that the fix is working (Figure 6.48). So, how much has the fix helped?

By separating the data into the two "processes," the first five before the improvement and the last five after the improvement, we now can compute how many failures were prevented by the process improvement. See Table 6.19.

8 *Source*: Barringer (2003).

Table 6.18 System that will show two failure trends.

Cum time	Cum failures
60	1
120	2
180	3
240	4
300	5
600	6
900	7
1200	8
1500	9
1800	10

Source: Barringer (2003).

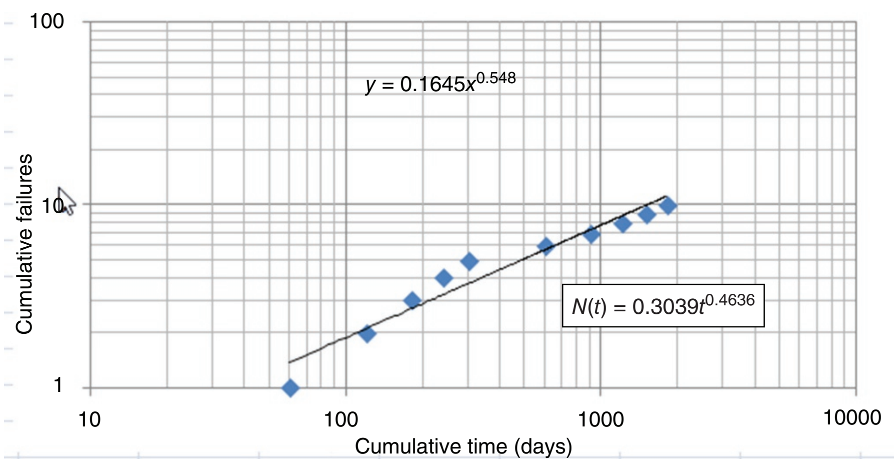


Figure 6.47 Reliability growth model fit to all data. *Source*: Barringer (2003).

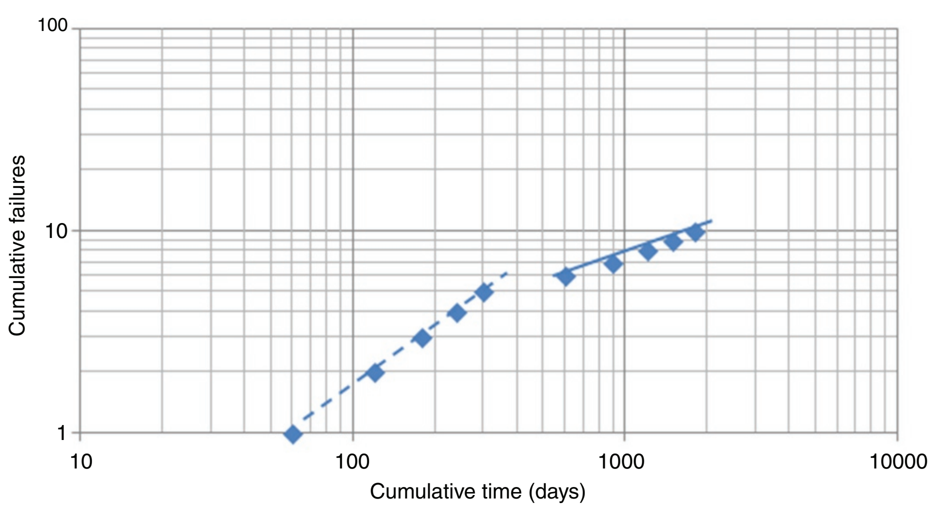


Figure 6.48 A process improvement was instituted after the fifth failure, which changed the slope of the AMSAA Duane model in the second group.

Table 6.19 Data separated by before and after process improvement.

Before process improvement		After process improvement	
Cum time	**Cum failures**	**Cum time**	**Cum failures**
60	1	300	1
120	2	600	2
180	3	900	3
240	4	1200	4
300	5	1500	5

Source: Barringer (2003).

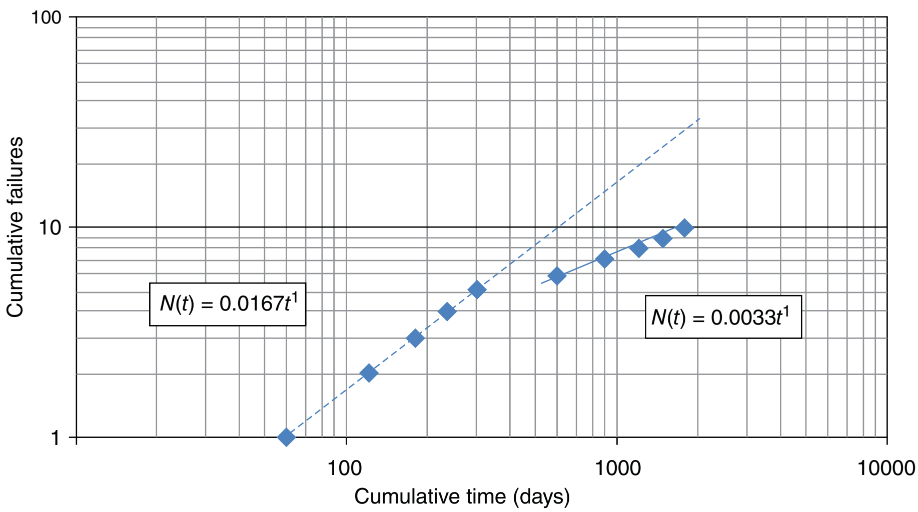


Figure 6.49 Separate models for before and after process improvement (both models used least-squares log–log regression in EXCEL™).

From Figure 6.49, for first five failures:

$N(2000) = (0.0167)*2000 = 34 - 5 = 29$ additional without the process improvement.

For second five failures (after process improvement):

$N(2000) = (0.0033)*2000 = 7 - 5 =$ two additional failures.

Process improvement saved $29 - 2 = 27$ failures.

Example 6.39 Predicting Future Failures from Your Maintenance Records[9]

Actual pump maintenance “interventions” were reported from a Brazilian chemical plant. The maintenance records are shown in Table 6.20.

9 *Source*: Barringer (2003).

Table 6.20 Maintenance "interventions," data from 1995 to 1997, forecasts 1998 to 1999.

Month	1995	1996	1997	1998 (forecast)	1999 (forecast)
January	35	12	8	8	7
February	32	13	3	7	7
March	28	12	15	7	6
April	30	11	5	7	6
May	41	11	10	7	6
June	30	11	9	7	6
July	16	15	8	7	6
August	18	9	7	7	6
September	21	8	7	7	6
October	14	8	9	7	6
November	12	10	7	7	6
December	11	10	8	7	6
Total =	288	130	96	85	74

The grouped data algorithm (Eqs. (6.91) and (6.92)) was used to solve for βs and λs and is on the combined reliability growth plots in Figure 6.52.

The cumulative failures versus cumulative time produces two straight lines. The trend line before starting a total preventive maintenance (TPM) program shows slight improvement (reliability growth slope $\beta = 0.947$).

After introducing the TPM program, operators were taught fundamental things they could do to reduce failures, and the TPM failure trend line shows a distinct change of reliability growth slope for the better because of this (a slope $\beta = 0.529$).

Using Figure 6.50 the savings from the TPM program at time $t = 36$ months is an avoidance of 516 "interventions" in 29 months. Assume that each "intervention" has an average cost of US$1000, the savings from the TPM program is $516,000 in just 29 months. Of course, the net savings for the TPM program will be the amount saved less the amount spent for introducing the TPM effort. Reliability growth plots quantify the savings and provide forecast of future failures.

Environmental Stress Screening

Environmental stress testing is based on the premise that increasing the stress levels of temperature, vibration, humidity, or other variables beyond those encountered under normal operational conditions will cause the same failure modes to appear, but at a more rapid rate. The combination of increased stress levels with failure modes analysis often provides a powerful tool for design enhancement. Typically, the procedure is initiated by identifying the key environmental factors that stress the product. Several of the prototype units are then tested for a specified period of time at the stress limits for normal operation. As a next step, voltage, vibration, temperature, or other identified factors are increased in steps beyond the specification limits until failures occur. Each failure is analyzed, and action is taken to correct it. At some level, small increases in stress will cause a dramatic increase in the number of failures. This indicates that fundamental design limits of the system have been exceeded, and further increases in stress are not indicative of the robustness of the design.

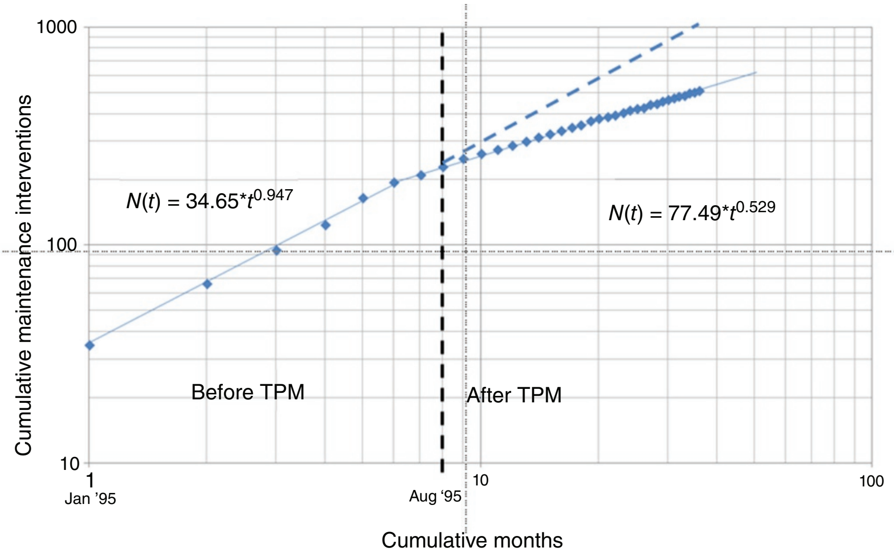


Figure 6.50 Reliability growth models show reduction in maintenance actions due to TPM. *Source*: Barringer (2003).

After the design phase, stress tests also may be applied to products taken off the production line during early parts of a run. At this point, however, the changes are typically made to the fabrication or assembly process and with the component suppliers rather than with product design. In contrast to the stress *testing* discussed thus far, whose purpose is to improve the product design or manufacturing process, e*nvironmental stress screening* (ESS) is a form of proof or acceptance test. To perform such screening, all units are operated at elevated stress levels for some specified period of time, and the failed units are removed. This is comparable to accelerating the burn-in procedure discussed in Chapter 3, for it tends to eliminate substandard units subject to infant mortality failures over a shorter period of time than simply burning them under nominal conditions. ESS and burn-in are sometimes confused in the literature due to the fact that they both have the same goal: reducing the occurrence of early field failures. The major difference is that burn-in is usually conducted under ambient conditions, whereas ESS is conducted under accelerated environmental conditions. The environmental stresses are more severe than the normal operating conditions and in some cases different than the operational conditions. ESS offers an economic advantage over burn-in in that it is capable of precipitating defects in a much shorter time period.

The objective in environmental stress screening is to reach the flat portion of the bathtub curve in a minimum time and at minimum expense before a product is shipped. This is illustrated in Figure 6.51 based on a simulation of a system with 100 components, 4 of which have a small % of latent defects caused by shipping or assembly errors or other causes that cannot be detected by usual quality control and inspection. An exponential distribution was assumed for all components.

The simulation illustrated in Figure 6.51 assumed that all 100 components assumed exponential failure distributions with η' of 10^7–10^8 and 4 (infant mortality) failure distributions to simulate latent failures not caught by usual quality system inspections.

Hence, you see a bimodal effect at the lower end of the plot. The bend in the curve as described in the previous paragraph indicates about a 2.6% failure rate due to the latent failures, which will

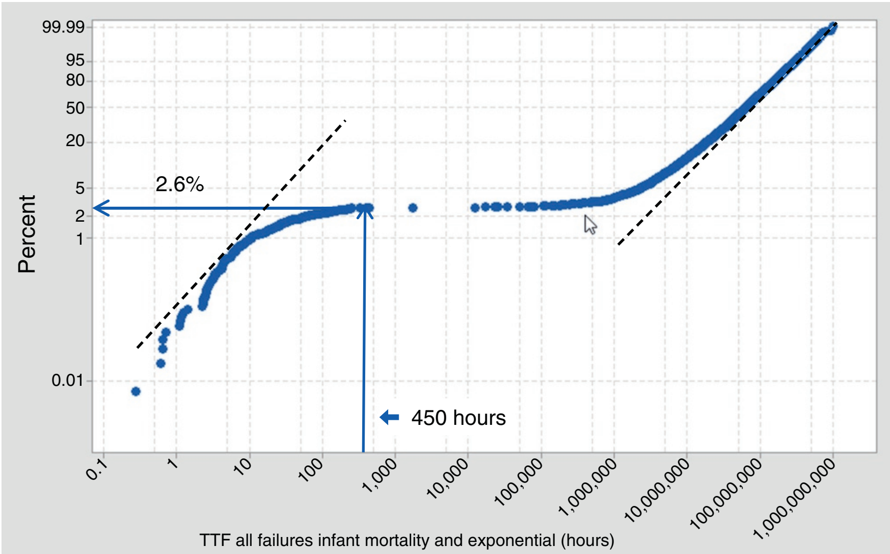


Figure 6.51 Simulated failure pattern of a system with 100 components.

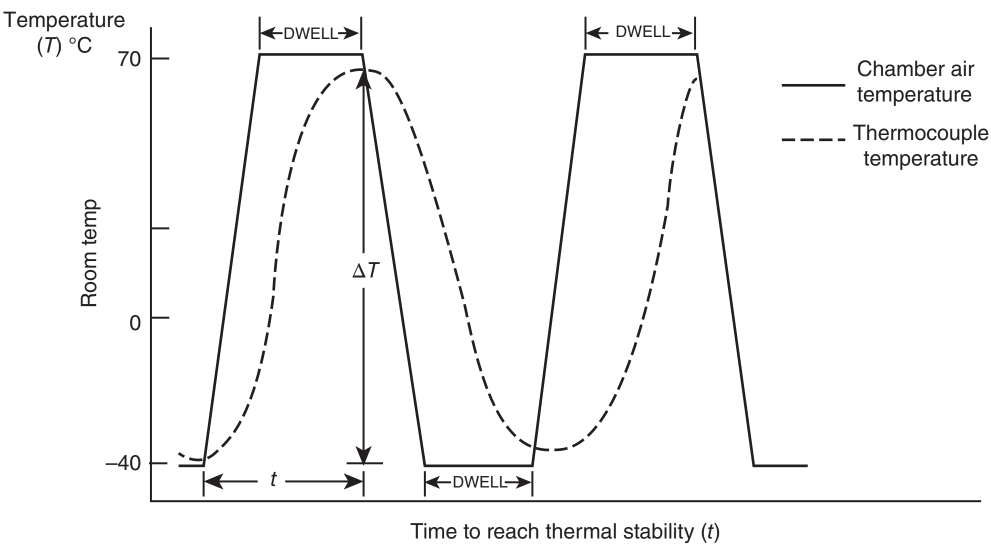


Figure 6.52 Typical thermal profile used in environmental stress testing. *Source*: Horner (1989). Public Domain.

occur after the customer receives the systems. Hence, a potential 2.6% warranty return rate ($$) and customer dissatisfaction.

In constructing programs for either environmental stress testing or screening, the selection of the stress levels and the choice of exposure times is a challenging task. While theoretical models, such as the Weibull and lognormal are helpful, the empirical knowledge gained from previous experience or industrial standards most often plays a larger role. Thermal cycling beyond the normal temperature limits is a frequent testing form. The test planner must decide on both a cycling rate and the number of cycles before proceeding to the next cycle magnitude. If too few cycles are used, the failures may not be precipitated; if too many are used, there is a diminishing return on the expenditure of time and equipment use. Often, an important factor is that of using the same test for successive products to insure that reliability is being evaluated with a common standard. Figure 6.52 illustrates one such thermal cycling prescription. Note that power on or off must be specified along with the temperature stress profile.

Take note of the following:

- ESS is *not* a test, it is a screening process
- ESS is *not* burn-in, it stresses a product to operational extremes
- ESS is used in manufacturing/production to catch latent failures
- All items in a product line are exposed to ESS.

ESS can be expensive, so a return-on-investment analysis should be done before incorporating any ESS in production. However, ESS has been shown to be a cost-effective strategy when properly implemented.

What "Screens" are used for ESS?

There are many screens that can be used at the assembly level to precipitate and detect latent defects. These screens include:

- Thermal cycling
- Random vibration
- Immersion
- Overpressure
- Voltage variation.

For electronic systems, thermal cycling and random vibration have been found to be the most effective screens available and are the most widely used. They are excellent for uncovering the microscopic defects that are present in electronic equipment. Figure 6.53 shows the types of defects precipitated by thermal cycling and random vibration. There is a lot of overlap in the defect types precipitated by these two screens. The most effective ESS program for electronic equipment should use both screens.

Thermal Cycling

Thermal cycling is the most widely used stress screen. It is an effective screen for precipitating defects at all levels of assembly, from piece part level to complete end assembly.

Thermal cycling is a relatively inexpensive screen, especially when performed at the assembly level, if units can be tested simultaneously in one chamber. This can be accomplished relatively easily for electronic systems, circuit boards, etc. BUT, it can also be accomplished for items as large as rooftop air-conditioning units or mechanical parts such as fans or air conditioner compressors.

Thermal cycling consists of changing the temperature of the equipment at a fairly high rate of change in order to induce stresses on the parts and connections. Working with the design team, the reliability engineer should finalize the temperature range, the thermal rate of change, and the number of cycles.

Defect type detected	Thermal screen	Vibration screen
Defective part	X	X
Broken part	X	X
Improperly installed part	X	X
Solder connection	X	X
PCB etch, shorts, and opens	X	X
Loose contact		X
Wire insulation	X	
Loose wire termination	X	X
Improper crimp or mating	X	
Contamination	X	X
Debris		X
Loose hardware		X
Chafed, pinched wires		X
Parameter drift	X	
Hermetic seal failure	X	
Adjacent *boards/parts* shorting		X

Figure 6.53 Assembly-level defect types precipitated by thermal and vibration screens.

Thermal cycling causes stress in the test items through the expansion and contraction of materials due to temperature change. The repeated cycling will cause different materials to expand and contract at different rates, resulting in stress at mating points, such as solder joints and connections.

Random Vibration

Random vibration has replaced sine and swept-sine vibration as a stress screen because it has been shown to be more effective in precipitating latent defects. *Sine* vibration applies energy at only one frequency and does not exercise all resonances of the equipment. In addition, the danger of fatigue failure is increased since all the energy goes into the one frequency. *Swept-sine* vibration applies energy at different frequencies sequentially. The dwell time at each frequency is not long enough to cause fatigue problems. Random vibration applies relatively constant energy in all frequencies. The energy applied at any one frequency is much smaller than that provided by sine vibration, so there is less danger of fatigue damage. Since the vibration occurs at all frequencies during the entire screen, the equipment also has time to reach a steady-state response to the input. Random vibration is also the closest approximation to the actual vibration seen by the equipment in the field. These factors all combine to make random vibration a more effective, less-damaging screen when applied correctly. However, upfront experimental surveys are essential to ensure that the equipment is not damaged by the vibratory stress levels imposed for screening.

Other Screens

The industry experience has been that thermal cycling and random vibration are the most used and most effective screens. However, for mechanical systems containing pressurized assemblies (fuel supply and pneumatics), these thermal and/or vibration stresses may not precipitate as many defects as overpressure or pressure cycling.

Immersion is a stressor used when humidity or seaborne equipment or other specialized equipment is being manufactured for a customer.

Likewise with voltage variation, anything electrical or electronic may be susceptible to being damaged by variations in voltage; hence, this stressor needs to be applied in those cases.

In electronics, when other stresses are used for screening (i.e., overpressure, immersion, etc.) they should be performed **after** thermal cycling and random vibration (if they are applied). Thermal cycling and random vibration will serve to initially stress the connections and interfaces that will then be screened through applications of other stresses.

REMINDER: The engineering and manufacturing team need to use their earlier studies and experience to point out the potential failure modes and their causes possibly using the results of a PFMEA (Process Failure Modes and Effects Analysis) and fault tree analysis to help in identifying the ESS that manufacturing will employ (see Chapter 7 for a description of FMEA and PFMEA and Chapter 11 for fault tree analysis).

Highly Accelerated Life Tests[10]

"Highly Accelerated Life Testing (HALT) is a form of accelerated testing in which the sole purpose of the test is to determine if the product can withstand the stresses to which it is being subjected. If the test unit survives, it passes the test, otherwise corrective actions will be taken to improve the product's design in order to eliminate the cause(s) of failure. In general, HALT will not quantify the life (or reliability) characteristics of the product under normal use conditions; instead, these tests will provide valuable information as to the types and levels of stresses that could be employed to design an accelerated test to assess life characteristics. A good HALT profile would quickly reveal failure modes that will occur during the life of the product under normal operating conditions. HALT supports a robust design approach."

However, one must be very cautious in using stresses (vibration, temperature cycling, etc.) beyond the design limits of the product. Failure modes may be generated by those extreme stresses but will not occur in the field because the unit will never be asked to operate at those extremes. How realistic a failure is in a HALT test should be judged by engineering.

The essence of HALT is in Figure 6.54. While historical ESS would go to the lower and upper operating limit, HALT explores the upper and lower destruct limits of a product with temperature and vibration stress. By exploring and finding the destruct limits, information on possible failure modes that may not be known to the designers has been revealed. In addition, while the customer may have asked that a product has operating margins (i.e. outside of the product specs) for "occasional" use, by exploring beyond those limits will reveal the information the customer should be aware of.

By finding the failure modes outside the spec limits, the product design team can decide if that failure mode is a shortcoming in the design and fix it if it needs to be. By repeating that process, a design will be "customer ready" when it comes out of production, meaning fewer warranty claims and higher customer satisfaction.

HALT has had a great deal of success in a number of industries, most notable of which is the electronics industry.

10 Taken from *DOD GUIDE FOR ACHIEVING RELIABILITY, AVAILABILITY, AND MAINTAINABILITY, June 2005.*

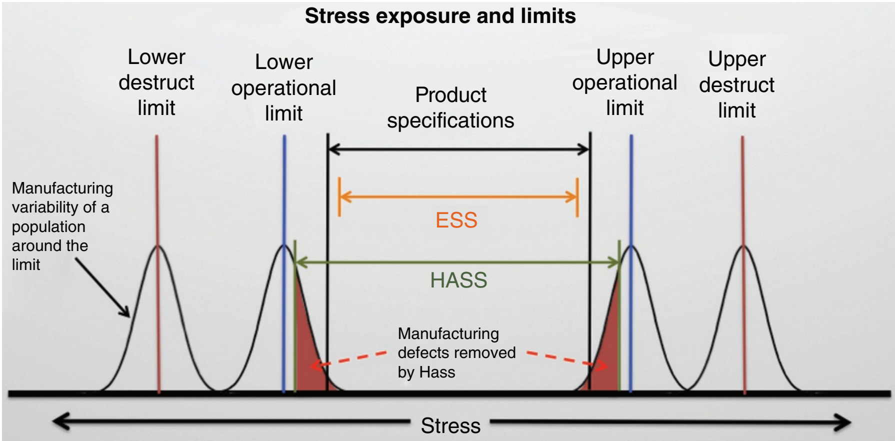


Figure 6.54 HALT/HASS stress exposure and limits. *Source*: APEX Ridge Reliability – Adam Bahret, 2021.

Highly Accelerated-Stress Screening

HALT is used in the design phase of a product, and now we introduce HASS (Highly Accelerated-Stress Screening) which will take the knowledge gained in HALT in terms of operating and destruct limits and apply them in production. Using higher temperatures and vibration than are in the specs, but identified by HALT, every product being delivered will pass a HASS test moving beyond the spec limits to the operating margins. This will produce a product that will detect latent failure modes due to production or supplier shortcomings.

Fundamentally, you must do HALT in the design phase to accomplish HASS in the production phase.

Once again, the return on investment for the extra equipment, manpower, and time involved in HALT and HASS needs to be calculated to make sure that the management buys into the HALT/HASS approach.

Bibliography

Abernethy, R. (2006). *New Weibull Handbook*, 5e.

Abernethy, R.B., Breneman, J.E., Medlin, C.H., and Reinman, G.L. (1983). *USAF Weibull Analysis Handbook*. US Air Force (AF), AFWAL-TR-83-2079.

Barringer, P. (2003). Predict Future Failures from your Maintenance Records. *Weibull News 17*, Summer .

Bazovsky, I. (1961). *Reliability Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall.

Crow, L.H. (1975). *Reliability Analysis for Complex Repairable Systems*, Technical handbook No. 138. Maryland: US AMSAA, Aberdeen Proving Ground.

Crowder, M.J., Kimber, A.C., Smith, R.L., and Sweeting, T.J. (1991). *Statistical Analysis of Reliability Data*. London: Chapman & Hall.

Dodson, B.L. and Schwab, H.L. (2006). *Accelerated Testing*. SAE.

Duane, J.T. (1964). Learning curve approach to reliability modeling. *IEEE Transactions on Aerospace* **2**: 563.

Fertig, K. and Mann, N. (1980). Life test sampling plans for 2-parameter Weibull populations. *Technometrics* **22**: 165–177.

Gupta, S. (1962). Life test sampling plans for normal and lognormal distributions. *Technometrics* **4** (2): 151–174.

Hooper, J.H. and Amster, S.J. (1990). Analysis & presentation of reliability data. In: *Handbook of Statistical Methods for Engineers & Scientists*. New York: McGraw-Hill.

Horner, W.H. (1989). AD-A206 350, Environmental Stress Screening (ESS) Guide. United States Army, Belvoir Research, Development & Engineering Center, Report 2477, January 1989.

Hur, J.-H., Lee, T.-G., Moon, S.-A. et al. (2008). Thermal reliability analysis of a BLDC motor in a high-speed axial fan by the accelerated-life test and numerical methods. *Heat and Mass Transfer* **44**: 1355–1369.

Jensen, F. and Petersen, N.K. (1982). *Burn-In*. Wiley.

Kapur, K.C. and Lamberson, L.R. (1977). *Reliability in Engineering*. New York: Wiley.

Kececioglu, D. (1993). *Reliability and Life Testing Handbook*, vol. **I/II**. Englewood Cliffs, NJ: Prentice-Hall.

Kececioglu, D. and Jacks, J. (1984). The Arrhenius, Eyring, Inverse Power Law and combination models in accelerated life testing. *Reliability Engineering* **8**: Examples 1–3.

Lawless, J.F. (1982). *Statistical Models and Methods for Lifetime Data*. New York: Wiley.

Mann, N.R., Schafer, R.E., and Singpurwalla, N.D. (1974). *Methods for Statistical Analysis of Reliability and Life Data*. New York: Wiley.

Matias, R., Trivedi, K., and Maciel, P. (2010). Using accelerated life tests to estimate time to software aging failure. 2010 IEEE 21st International Symposium on Software Reliability Engineering, San Jose, CA, USA, 1–4 Nov. 2010, p. 217.

McLean, H.W. (2009). *HALT, HASS, and HASA EXPLAINED-Accelerated Reliability Techniques*. ASQ Quality Press.

MIL-HDBK-189C. Department of Defense Handbook of Reliability Growth Management, 14 June 2011.

Montgomery, D.C. and Runger, G.C. (2011). *Applied Statistics and Probability for Engineers*, 5the. Wiley.

Nelson, W. (1982). *Applied Life Data Analysis*. New York: Wiley.

Nelson, W. (1990). *Accelerated Testing*. New York: Wiley.

Pohl, E. and Dietrich, D. (1995). Environmental stress screening strategies for complex systems: a 3-level mixed distribution model. *Microelectronic. Reliability* **35** (4): 637–656.

Reliasoft (2007). *Accelerated Life Testing Reference*. Reliasoft.

Sammons, J. (1981). Derivation and correlation of accelerated mission endurance testing. AGARD (Advisory Group for Aerospace Research and Development)- Turbine Engine Testing, January **1981**, pp. 191–194.

Tobias, P.A. and Trindade, D.C. (1986). *Applied Reliability*. New York: Van Nostrand-Reinhold.

Exercises

6.1 Suppose that "bugs" are detected and corrected in developmental software at 1.4, 6.9, 24.3, 66.1, 117.2, and 229.3 hours.

a) Estimate the reliability growth coefficient, β.

b) Calculate the expected number of failures by 1000 hours. Why is there such a low number of failures predicted over such a large time?

6.2 The wearout times of 10 emergency flares in minutes are 17.0, 20.6, 21.3, 21.4, 22.7, 25.6, 26.5, 27.0, 27.7, and 29.7. Determine which parametric failure distribution best fits this data, then using that information, determine how many tests have to be run for how long to prove that the new design emergency flare will have two times the wearout time, with 90% confidence.

6.3 A new robot system undergoes test–fix–test–fix development testing. The number of failures during each 100-hour interval in the first 700 hours of operation are recorded. They are 14, 7, 6, 4, 3, 1, and 1.

Plot the reliability growth plot in EXCEL, and what can you say about the growth trend (looking at β)?

6.4 Suppose that a device undergoing accelerated testing can be described by a Weibull distribution with a shape factor of $\beta = 2.0$. Under accelerated test conditions, with an acceleration factor (AF) = 5.0, 50% of the devices are found to fail during the first month. Under *normal operating conditions,* estimate how long the device will last before the failure probability reaches 10%. (This is referred to as the B_{10} life of the device.)

6.5 At rated voltage a microcircuit has been estimated to have an MTTF of 20,000 hours. An accelerated life test is to be carried out to verify this number. It is known that the microcircuit life is inversely proportional to the cube of the voltage. At least 10% of the test circuits must fail before the test is terminated if we are to have confidence in the result. If the test must be completed in 30 days, at what percentage of the rated voltage should the circuits be tested?

6.6 A life test with type II censoring is performed on 50 servomechanisms that are thought to have a constant failure rate. The test is terminated after the twentieth failure. The times to failure (in months) are as follows:

0.10	0.29	0.49	0.51	0.55
0.63	0.68	1.16	1.40	2.24
2.25	2.64	2.99	3.01	3.06
3.15	3.51	3.53	3.99	4.05

The failed servomechanisms are not replaced.

1) Find the most appropriate distribution to explain the data.
2) Does the data follow an exponential distribution?
3) Make a point estimate of the MTTF using the appropriate equation.
   Calculate the 90% confidence interval on the MTTF.
   How does your calculation agree with the MINITAB plot?

6.7 Suppose that in Exercise 6.6 the life test had to be stopped at 3 months because of a production deadline. Based on a 3-month test, estimate the MTTF and the corresponding 90% confidence interval.

6.8 Sets of electronic components are tested at 100 and 120 °F, and the MTTFs are found to be 80 and 35 hours, respectively. Assuming that the Arrhenius equation is applicable, estimate the MTTF at 70 °F.

6.9 A nonreplacement reliability test is carried out on 20 high-speed pumps to estimate the value of the failure rate. In order to eliminate wear failures, it is decided to terminate the test after half of the pumps have failed. The times of the first 10 failures (in hours) are 33.7, 36.9, 46.8, 56.6, 62.1, 63.6, 76.4, 79.0, 101.5, and 110.2.

a) Estimate the MTTF.
b) Determine the 90% confidence interval for the MTTF.

6.10 A replacement test is run for 30 days using 18 test setups. During the test there are 16 failures. Assuming an exponential distribution, estimate the MTTF.

6.11 A control bearing was failing prematurely due to fatigue. The bearing failures followed a Weibull distribution with β equal to 1.5 (a common value for bearing fatigue) and η equal to 3000 hours. The bearing was redesigned, and the environment in which it operated was improved to give the bearing a higher expected life. Twenty redesigned bearings were available for testing.

How long should each be tested to demonstrate, with 90% confidence, that the fatigue mode was tripled?

6.12 Assuming 1400 tests without failure, what is the demonstrated reliability at 90% confidence (assume binomial testing)?

6.13 Your company makes a product that is either good or bad, and your boss has told you that he will allow you to test 300 pieces – he wants to be *at least* 90% confident in the results and yet get the highest reliability. He wishes to have a trade-off study done so he can have his senior designers give him a consensus opinion of which test he should approve.

6.14 You have just completed 1000 tests at altitude with four failures of augmentor to light on the first try. Your customer comes in and asks for your progress in reliability demonstration and informs you that the chief engineer of his company wants to have at least a reliability = 0.95 that the augmentor will light on first try. What can you tell him?

6.15 An electronic device that normally operates at a temperature of 50 °C is subjected to a stress temperature of 100 °C. The activation energy for the failure mode is 0.8 eV. What is the acceleration factor using the Arrhenius equation?

6.16 A device that normally operates with 5 V applied is tested at two increased stress levels, $V_1 = 15$ V and $V_2 = 30$ V.

Analysis of the data from the tests indicates that 5% of the population failed at 150 hours when the high stress voltage of 30 V was used. When the stress voltage of 15 V was applied, 5% of the population failed at 750 hours.

At what time t would 5% of the population be expected to fail under the normal stress of 5 V?

6.17 What is the acceleration factor for a temperature-based test given an activation energy (A.E.) of 0.7 eV, test temperature (Tt) of 90 °C, and use temperature (Tu) of 25 °C?

6.18 Cumulative tests on an USAF engine prototype reveal that 15 test incidents occurred with ~3600 cycles of testing. It is estimated that the initial value of the cumulative MTBF at $t = 1$ cumulative cycles of testing is 300 cycles. Using the AMSAA/Duane reliability growth model, estimate the cumulative MTBF at $t = 10{,}000$ cycles of testing.

6.19 Suppose that $T_0 = 288$ K (15 °C) and $T = 303$ K (30 °C) and activation energy $E = 0.35$ V. Show that the failure rate doubles for an increase of 15 °C (i.e. $\lambda = 2\lambda_0$).

6.20 One hundred integrated circuits (ICs) are cycled in an environmental test chamber for a test that is equivalent to 1000 hours of operation. At the completion of the test it is found that two of the units failed during the test.

The binomial distribution can be used for the estimate of reliability, and the F distribution is used to calculate the confidence limit. Estimate the reliability of the IC for a mission time of 1000 hours.

6.21 An accelerated nonreplacement life test that is equivalent to 1000 hours of operation is conducted on 10 units in order to estimate the MTBF and set a lower 90% confidence limit. One unit failed at 450 hours, and a second unit failed at 800 hours. Eight units did not fail during the test. The test was time censored at 1000 hours. Assume an exponential distribution to estimate the MTBF, and the χ^2 distribution to find the lower 90% confidence limit on the MTTF.

6.22 In success testing, how many samples need to operate for one lifetime without failure to demonstrate 95% confidence of 99% reliability?

6.23 In success testing, how many samples need to operate for one lifetime without failure to demonstrate 60% confidence of 90% reliability?

6.24 Battery life has been measured as normally distributed with mean equal to 150 hours and variance of 400 hours.

Find the B10 life.

6.25 Temperature has been identified as a key stress that will affect the lifetime of a new component design. The Arrhenius model is found to be an effective accelerated life testing model for the component. Testing was completed on two samples at $T_1 = 463$ K and $T_2 = 478$ K with Weibull characteristic lives of 880 hours and 795 hours, respectively. Find the acceleration factor for a normal use temperature of 283 K given an applied stress of 478 K.

6.26 A new fan motor is available out of the design department. The customer wants a 10-year life where his application uses the fan motor ~8 hours a day (30,000 hour life) with 90% confidence. The reliability goal to minimize warranty is 0.93. Experience has shown that earlier designs have a Weibull failure distribution with a $\beta = 2$. How many fan motors should be tested and for how long?

6.27 Electronic circuit board switches are tested at 50 and 60 °C with lifetime in number of cycles as shown in the table below. What is the B10 life of the circuit board switch at its normal operating temperature of 30 °C?

50 °C	60 °C	Note:
21,045	16,551	50 °C = 323 K, 60 °C = 333 K
25,077	18,935	30 °C = 303 K
31,407	20,996	
33,812	24,363	

Cycles to failure

6.28 Design system calibration: The design system-predicted Bl life for the compressor disk is 1000 cycles. Five disks have accumulated 1500 cycles, and five have 2000 cycles without failures. If most disk low cycle fatigue failures have a β of 3.0, is this success data sufficient to increase the predicted design life?

6.29 Test substantiation: A new component has been designed. The design requirement is a Weibull with $\beta = 4.0$ and $\eta = 600$ hours. This is twice as good as the existing design which has an $\eta = 300$ hours. How many and how long should either 4 units or 8 units be tested without failure to demonstrate with 90% confidence that the new design has two times the life?

6.30 In Exercise 6.29, the program manager changed his mind after discussing the test further. Instead of 2X life, he wanted a reliability = 0.99 at 600 hours (at 90% confidence) for the new designed component. How many and how long should the new units be tested without failure to demonstrate this reliability requirement at 90% confidence ?

6.31 Suppose that you have tested 40 components in groups of 10 in an accelerated test lab. This test is a sudden death test, and you recorded the first failure in each group of 10:

Group	TTF
1	602.3
2	506.4
3	243.5
4	497.3

What is the Weibull distribution that describes the failure mode?

6.32 In Exercise 6.31, instead of testing 40 components in groups of 10, they tested 5 components in groups of 8:

Group	TTF
1	466.23
2	729.31
3	443.44
4	584.6
5	415.8
6	590.93
7	157.01
8	491.05

Compare the Weibull in Exercise 6.31 with the Weibull produced here. Are the two Weibulls significantly different at 90% confidence?

6.33 High-pressure turbine vanes were eroding beyond allowable limits. A significant percentage of the engines in service were being removed for vane repair or replacement prior to their scheduled turbine maintenance. The time to failure – determined by the worst vane in the set – followed a Weibull distribution with $\beta = 3$ and $\eta = 1300$ cycles. Through redesign and material changes the vane's durability was improved. Design a test to demonstrate the new vane's goal: no more than 5% of the engines should be removed by 2300 cycles for vane erosion (with 90% confidence). During this test, assume that the turbines are limited to running at most 5000 cycles each. Also, assume that the time to engine removal for excessive vane erosion would still follow a Weibull distribution with $\beta = 3$.

6.34 A turbine engine exhaust nozzle control bearing was failing prematurely due to fatigue. Bearing failures followed a Weibull distribution with $\beta = 1.5$ and $\eta = 3000$ hours. The bearing was redesigned, and the environment in which it operated was improved to give the bearing a higher expected life. Twenty redesigned bearings were available for testing. How long should each be tested to demonstrate, with 90% confidence, that the fatigue mode was significantly improved?

6.35 Suppose that if 50 units are put on life test (without replacement) and that the test is to be truncated, $r = 10$ of them have failed. We shall suppose, furthermore, that the first 10 failure times are 65, 110, 380, 420, 505, 580, 650, 840, 910, and 950 hours.

- Estimate the Weibull distribution from this test data.
- Can you say that this data follows the exponential distribution (Hint: look at the confidence bounds on β)?

6.36 The experiment in Exercise 6.35. was rerun as a sudden death again, but with 8 groups of 5 with the following results:

Low of 8 groups
52.28734464
48.70439991
43.16654463
39.31593549
64.82848045
79.79845537
73.44525838
55.05663793

Generate a Weibull from this data, again, realizing that each of the 8 failures were the first failure in a group of five. As such the remaining 4 in each group are censored at the failure time.

How does this Weibull compare with the Weibull generated in Exercise 6.35?

Did this Weibull need a t_0 correction?

6.37 In a continuation of a study to determine which sudden death setup would give the best answers at the minimum cost, a third set of 40 experiments were done on the same product of bulbs. This time, the experiment in Exercise 6.35. was rerun as a sudden death with 5 groups of 8 with the following results, the first failure in each of the 5 groups was:

Low of 5 groups
48.70439991
43.16654463
39.31593549
73.44525838
55.05663793

Analyze this data and compare it to Exercises 6.35 and 6.36.

6.38 Step-stress test

An avionics subsystem has a requirement of 0.99 reliability at 24 hours of continuous use.

10 Subsystems are put on test, starting. Stresses used were voltage and temperature.

First 24 hours at use conditions (at 110 V and 50 °C temperature), and then voltage and temperature were increased every hour and test continued until all 10 subsystems had failed.

TTF (h)	Freq	Censor	Conditions
30	2	1	145 V, 65 °C
32.5	3	1	160 V,70 °C
33	5	1	165 V,75 °C

Table of subsystem step-stress test results.

Has the requirement been met?

Weibull plot of step-stress results shows that 0.99 reliability requirement at 24 hours has been met, with 95% confidence!

6.39 Braking systems were tested at an accelerated rate of 800 cycles per hour.

The normal cycle's rate is 200 cycles per hour. Data from the accelerated life test fit a Weibull distribution with $\beta = 1.7$ and $\eta_{\text{stress}} = 2500$ hours. What is the expected reliability of the braking systems at 1000 hours of use under normal conditions?

6.40 Given the test results at 25 and 120 °C that provide an acceleration factor of 4, calculate the activation energy.

Hint: Use ARRHENIUS temperature acceleration model.

6.41 Consider the failure data, in hours, obtained from accelerated life testing a sample of 10 units to failure[11]:

TTF (h)				
2750	3100	3400	3800	4100
4400	4700	5100	5700	6400

11 *Source*: Kececioglu and Jacks (1984).

Assume that the accelerated life test was conducted at 150 °C(423 °K), and the expected use operating temperature is 85 °C (358 °K). Use the Arrhenius model to find the B10 life at use temperature. Use $E_A = 0.5$ eV.

6.42 Using the data in the following table[12]:

Temp (°K)	Hours	Censor	Freq
313.15	1298	1	1
313.15	1390	1	1
313.15	3187	1	1
313.15	3241	1	1
313.15	3261	1	1
313.15	3313	1	1
313.15	4501	1	1
313.15	4568	1	1
313.15	4841	1	1
313.15	4982	1	1
313.15	5000	2	90
333.15	581	1	1
333.15	925	1	1
333.15	1432	1	1
333.15	1586	1	1
333.15	2452	1	1
333.15	2734	1	1
333.15	2772	1	1
333.15	4106	1	1
333.15	4674	1	1
333.15	5000	2	11
353.15	283	1	1
353.15	361	1	1
353.15	515	1	1
353.15	638	1	1
353.15	854	1	1
353.15	1024	1	1
353.15	1030	1	1
353.15	1045	1	1
353.15	1767	1	1
353.15	1777	1	1
353.15	1856	1	1
353.15	1951	1	1
353.15	1964	1	1
353.15	2884	1	1
353.15	5000	2	1

Using the data in the table to the left, assuming an Arrhenius relation with temperature as the stressor on hours to failure, find the 90% confidence bounds on 10% life at the operating temperature of 10 °C (283.15 °K).

Using MINITAB:

Stat-Reliability/Survival > Accelerated Life Testing. Then, putting data in proper blanks, including Freq and Censor (where 2 = censored, 1 = failure), under estimate, new predictor value set = 283.15, .OK several times.

12 *Source*: Data from Hooper and Amster (1990).

6.43 Using the following condenser ALT data from Hur et al. (2008).

The stressor is temperature (°K); use Arrhenius–Weibull to project the failure time to the use temperature (323 °K).

Stress (°K)	Failure time (h)
358	950
358	988
358	912
358	922
378	266
378	257
378	251

6.44 Using the following condenser ALT data from Matias, Trevedi and Maciel (2010). This ALT uses *failure* to mean degradation in ability for a server to run based on the page size of the information, where 200 KB is usual running and above that the Server slows down.

TTF	Stress loading-page size
84	400
86	400
88	400
93	400
95	400
95	400
97	400
34	600
36	600
37	600
38	600
38	600
39	600
40	600
20	800
21	800
22	800
23	800
23	800
23	800
24	800

Since the IPL model has been shown to be useful in computer stress testing, use the Weibull inverse power law mode in MINITAB to predict the distribution of TTF for a 200-page size.

Supplement 1: Tables for Weibull Zero-failure Substantiation testing

Substantiation Testing: Characteristic Life Multipliers for Zero Failure Test at **80% Confidence**
Table 6 Sup1.1

Confidence level= 0.8

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
N	**Infant mortality**	**Random**	**Early wearout**					**Old age rapid wearout**		
2	0.6476	0.8047	0.8652	0.8971	0.9168	0.9301	0.9398	0.9471	0.9529	0.9575
3	0.2878	0.5365	0.6602	0.7324	0.7795	0.8126	0.8370	0.8558	0.8708	0.8829
4	0.1619	0.4024	0.5450	0.6343	0.6948	0.7383	0.7710	0.7964	0.8168	0.8335
5	0.1036	0.3219	0.4697	0.5674	0.6355	0.6853	0.7233	0.7532	0.7773	0.7972
6	0.0720	0.2682	0.4159	0.5179	0.5908	0.6449	0.6866	0.7197	0.7465	0.7686
7	0.0529	0.2299	0.3753	0.4795	0.5554	0.6126	0.6570	0.6925	0.7213	0.7453
8	0.0405	0.2012	0.3433	0.4485	0.5265	0.5860	0.6324	0.6697	0.7002	0.7256
9	0.0320	0.1788	0.3174	0.4229	0.5023	0.5634	0.6115	0.6503	0.6821	0.7087
10	0.0259	0.1609	0.2959	0.4012	0.4816	0.5439	0.5934	0.6334	0.6664	0.6940
11	0.0214	0.1463	0.2777	0.3825	0.4636	0.5269	0.5774	0.6185	0.6524	0.6809
12	0.0180	0.1341	0.2620	0.3662	0.4477	0.5119	0.5633	0.6052	0.6399	0.6691
13	0.0153	0.1238	0.2484	0.3519	0.4336	0.4984	0.5505	0.5932	0.6286	0.6585
14	0.0132	0.1150	0.2364	0.3391	0.4209	0.4862	0.5390	0.5823	0.6183	0.6488
15	0.0115	0.1073	0.2258	0.3276	0.4095	0.4752	0.5285	0.5723	0.6089	0.6399
16	0.0101	0.1006	0.2163	0.3172	0.3990	0.4651	0.5188	0.5632	0.6003	0.6317
17	0.0090	0.0947	0.2077	0.3077	0.3895	0.4558	0.5099	0.5547	0.5922	0.6241
18	0.0080	0.0894	0.2000	0.2990	0.3807	0.4472	0.5016	0.5468	0.5848	0.6170
19	0.0072	0.0847	0.1929	0.2910	0.3725	0.4392	0.4940	0.5395	0.5778	0.6104
20	0.0065	0.0805	0.1864	0.2837	0.3650	0.4317	0.4868	0.5326	0.5712	0.6041
21	0.0059	0.0766	0.1804	0.2768	0.3579	0.4248	0.4800	0.5262	0.5651	0.5983
22	0.0054	0.0732	0.1749	0.2705	0.3513	0.4182	0.4737	0.5201	0.5593	0.5927
23	0.0049	0.0700	0.1698	0.2645	0.3451	0.4121	0.4677	0.5143	0.5538	0.5875
24	0.0045	0.0671	0.1651	0.2590	0.3393	0.4063	0.4621	0.5089	0.5485	0.5825
25	0.0041	0.0644	0.1606	0.2537	0.3338	0.4008	0.4567	0.5037	0.5436	0.5778
26	0.0038	0.0619	0.1565	0.2488	0.3286	0.3956	0.4516	0.4988	0.5389	0.5732
27	0.0036	0.0596	0.1526	0.2441	0.3237	0.3906	0.4468	0.4941	0.5344	0.5689
28	0.0033	0.0575	0.1489	0.2397	0.3190	0.3859	0.4422	0.4896	0.5301	0.5648
29	0.0031	0.0555	0.1455	0.2356	0.3146	0.3814	0.4377	0.4854	0.5260	0.5609
30	0.0029	0.0536	0.1422	0.2316	0.3103	0.3772	0.4335	0.4813	0.5220	0.5571
40	0.0016	0.0402	0.1174	0.2006	0.2766	0.3427	0.3993	0.4479	0.4897	0.5259
50	0.0010	0.0322	0.1012	0.1794	0.2530	0.3181	0.3747	0.4236	0.4660	0.5030

Substantiation Testing: Characteristic Life Multipliers for Zero Failure Test at **90% Confidence**
Table 6 Sup1.2

Confidence level= 0.9										
					β					
	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5
N	Infant mortality	Random	Early wearout					Old age rapid wearout		
2	1.3255	1.1513	1.0985	1.0730	1.0580	1.0481	1.0411	1.0358	1.0318	1.0286
3	0.5891	0.7675	0.8383	0.8761	0.8996	0.9156	0.9272	0.9360	0.9429	0.9485
4	0.3314	0.5756	0.6920	0.7587	0.8018	0.8319	0.8540	0.8710	0.8845	0.8954
5	0.2121	0.4605	0.5963	0.6786	0.7333	0.7722	0.8013	0.8238	0.8417	0.8563
6	0.1473	0.3838	0.5281	0.6195	0.6818	0.7267	0.7606	0.7871	0.8083	0.8257
7	0.1082	0.3289	0.4765	0.5735	0.6410	0.6903	0.7278	0.7573	0.7811	0.8006
8	0.0828	0.2878	0.4359	0.5365	0.6076	0.6603	0.7006	0.7325	0.7582	0.7795
9	0.0655	0.2558	0.4030	0.5058	0.5797	0.6348	0.6774	0.7112	0.7386	0.7614
10	0.0530	0.2303	0.3757	0.4799	0.5558	0.6129	0.6573	0.6927	0.7216	0.7455
11	0.0438	0.2093	0.3525	0.4575	0.5350	0.5938	0.6397	0.6764	0.7064	0.7314
12	0.0368	0.1919	0.3327	0.4380	0.5167	0.5768	0.6240	0.6618	0.6929	0.7188
13	0.0314	0.1771	0.3154	0.4209	0.5004	0.5616	0.6098	0.6487	0.6807	0.7074
14	0.0271	0.1645	0.3002	0.4055	0.4858	0.5479	0.5971	0.6368	0.6696	0.6970
15	0.0236	0.1535	0.2867	0.3918	0.4726	0.5354	0.5854	0.6259	0.6594	0.6874
16	0.0207	0.1439	0.2746	0.3794	0.4605	0.5240	0.5747	0.6159	0.6500	0.6786
17	0.0183	0.1354	0.2637	0.3680	0.4495	0.5136	0.5649	0.6067	0.6413	0.6704
18	0.0164	0.1279	0.2539	0.3577	0.4393	0.5039	0.5557	0.5980	0.6332	0.6628
19	0.0147	0.1212	0.2449	0.3481	0.4299	0.4949	0.5472	0.5900	0.6256	0.6557
20	0.0133	0.1151	0.2367	0.3393	0.4212	0.4865	0.5392	0.5825	0.6185	0.6490
21	0.0120	0.1096	0.2291	0.3311	0.4130	0.4786	0.5318	0.5754	0.6119	0.6427
22	0.0110	0.1047	0.2221	0.3235	0.4054	0.4713	0.5247	0.5688	0.6056	0.6367
23	0.0100	0.1001	0.2156	0.3164	0.3983	0.4643	0.5181	0.5625	0.5996	0.6311
24	0.0092	0.0959	0.2096	0.3097	0.3916	0.4578	0.5119	0.5565	0.5940	0.6258
25	0.0085	0.0921	0.2039	0.3035	0.3852	0.4516	0.5059	0.5509	0.5886	0.6207
26	0.0078	0.0886	0.1987	0.2976	0.3792	0.4457	0.5003	0.5455	0.5835	0.6158
27	0.0073	0.0853	0.1937	0.2920	0.3735	0.4402	0.4949	0.5404	0.5786	0.6112
28	0.0068	0.0822	0.1891	0.2868	0.3681	0.4349	0.4898	0.5355	0.5740	0.6068
29	0.0063	0.0794	0.1847	0.2818	0.3630	0.4298	0.4849	0.5308	0.5695	0.6025
30	0.0059	0.0768	0.1806	0.2770	0.3581	0.4250	0.4802	0.5263	0.5653	0.5984
40	0.0033	0.0576	0.1491	0.2399	0.3192	0.3861	0.4423	0.4898	0.5302	0.5650
50	0.0021	0.0461	0.1285	0.2146	0.2919	0.3584	0.4150	0.4632	0.5046	0.5403

Substantiation Testing: Characteristic Life Multipliers for Zero Failure Test at **95% Confidence**

Table 6 Sup1.3

Confidence level= 0.95

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
N	**Infant mortality**	**Random**	**Early wearout**					**Old age rapid wearout**		
2	2.243603	1.497866	1.309128	1.223873	1.17541	1.144171	1.122368	1.106288	1.093941	1.084163
3	0.997157	0.998577	0.999051	0.999288	0.999431	0.999526	0.999593	0.999644	0.999684	0.999715
4	0.560901	0.748933	0.824699	0.865409	0.890794	0.908129	0.920718	0.930274	0.937775	0.943819
5	0.358976	0.599146	0.710704	0.774046	0.814729	0.843033	0.863849	0.879799	0.892407	0.902623
6	0.249289	0.499289	0.629363	0.706604	0.757427	0.793324	0.820002	0.840597	0.856973	0.870303
7	0.183151	0.427962	0.567898	0.654188	0.712134	0.75359	0.78467	0.808819	0.828114	0.843881
8	0.140225	0.374467	0.519528	0.611937	0.675095	0.720783	0.755297	0.782264	0.803902	0.821642
9	0.110795	0.332859	0.480294	0.576939	0.644027	0.693032	0.730303	0.759565	0.783133	0.802513
10	0.089744	0.299573	0.447715	0.547333	0.617449	0.669115	0.708646	0.739819	0.76501	0.785779
11	0.074169	0.272339	0.420152	0.521861	0.594353	0.648192	0.689609	0.7224	0.748978	0.770943
12	0.062322	0.249644	0.396474	0.499644	0.574022	0.629662	0.672676	0.706855	0.734635	0.757643
13	0.053103	0.230441	0.375872	0.480043	0.555935	0.613084	0.657467	0.692851	0.721683	0.74561
14	0.045788	0.213981	0.357753	0.462581	0.539697	0.598125	0.643693	0.680133	0.709896	0.734641
15	0.039886	0.199715	0.341671	0.446895	0.525007	0.584526	0.631128	0.668502	0.699095	0.724573
16	0.035056	0.187233	0.327282	0.432705	0.511627	0.572086	0.619597	0.657803	0.68914	0.715281
17	0.031053	0.17622	0.314318	0.419785	0.499369	0.560641	0.608957	0.647908	0.679918	0.70666
18	0.027699	0.16643	0.302566	0.407958	0.488081	0.55006	0.599093	0.638716	0.671336	0.698628
19	0.02486	0.15767	0.291854	0.397077	0.477639	0.540236	0.58991	0.63014	0.663318	0.691114
20	0.022436	0.149787	0.282043	0.387023	0.467939	0.531077	0.581327	0.622112	0.655801	0.684061
21	0.02035	0.142654	0.273017	0.377696	0.458895	0.52251	0.57328	0.614569	0.648729	0.677418
22	0.018542	0.13617	0.264679	0.369012	0.450435	0.51447	0.565711	0.607463	0.642057	0.671145
23	0.016965	0.130249	0.256951	0.360901	0.442497	0.506903	0.558571	0.60075	0.635746	0.665204
24	0.015581	0.124822	0.249763	0.353302	0.435027	0.499763	0.55182	0.594392	0.629761	0.659566
25	0.014359	0.119829	0.243057	0.346164	0.427982	0.493008	0.545422	0.588357	0.624074	0.654203
26	0.013276	0.11522	0.236784	0.339441	0.42132	0.486605	0.539344	0.582616	0.618659	0.649092
27	0.012311	0.110953	0.230901	0.333096	0.415007	0.480522	0.533559	0.577145	0.613492	0.644211
28	0.011447	0.10699	0.22537	0.327094	0.409014	0.474732	0.528044	0.571921	0.608554	0.639542
29	0.010671	0.103301	0.220159	0.321405	0.403313	0.469211	0.522776	0.566926	0.603827	0.635069
30	0.009972	0.099858	0.215239	0.316003	0.397881	0.463939	0.517737	0.562141	0.599295	0.630778
40	0.005609	0.074893	0.177676	0.273666	0.354631	0.421516	0.476883	0.523131	0.562181	0.595509
50	0.00359	0.059915	0.153117	0.244775	0.324349	0.391301	0.447429	0.494747	0.534984	0.569517

Substantiation Testing: Characteristic Life Multipliers for Zero Failure Test at **99% Confidence**

Table 6 sub1.4

Confidence level= 0.99

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
N	**Infant mortality**	**Random**			**Early wearout**				**Old age rapid wearout**	
2	5.301898	2.302585	1.743722	1.517427	1.396003	1.3205	1.269083	1.231839	1.203628	1.181526
3	2.356399	1.535057	1.330709	1.238974	1.186997	1.153563	1.13026	1.113092	1.09992	1.089494
4	1.325475	1.151293	1.098476	1.072983	1.057972	1.048082	1.041074	1.035849	1.031803	1.028578
5	0.848304	0.921034	0.946638	0.959705	0.967632	0.972953	0.976772	0.979645	0.981886	0.983683
6	0.5891	0.767528	0.838294	0.876087	0.899576	0.915584	0.927192	0.935995	0.9429	0.94846
7	0.432808	0.657881	0.756424	0.811099	0.845783	0.869726	0.887242	0.90061	0.911147	0.919665
8	0.331369	0.575646	0.691996	0.758714	0.801793	0.831863	0.85403	0.871042	0.884507	0.895429
9	0.261822	0.511686	0.639738	0.715322	0.764894	0.799836	0.825768	0.845767	0.861656	0.874582
10	0.212076	0.460517	0.596344	0.678614	0.733328	0.772233	0.80128	0.82378	0.841716	0.856346
11	0.175269	0.418652	0.559631	0.647033	0.705897	0.748085	0.779755	0.804384	0.824076	0.840177
12	0.147275	0.383764	0.528092	0.619487	0.681751	0.726699	0.760609	0.787075	0.808295	0.825682
13	0.125489	0.354244	0.500651	0.595184	0.660269	0.707567	0.743411	0.771482	0.794045	0.812569
14	0.108202	0.328941	0.476517	0.573534	0.640984	0.690302	0.727836	0.75732	0.781075	0.800615
15	0.094256	0.307011	0.455096	0.554086	0.623536	0.674608	0.713629	0.74437	0.769191	0.789643
16	0.082842	0.287823	0.43593	0.536492	0.607645	0.66025	0.700591	0.732456	0.758238	0.779516
17	0.073383	0.270892	0.41866 3	0.520473	0.593087	0.647042	0.68856	0.721438	0.748092	0.770122
18	0.065456	0.255843	0.40301	0.505809	0.579681	0.63483	0.677407	0.711203	0.73865	0.761368
19	0.058747	0.242377	0.388742	0.492318	0.567279	0.623492	0.667023	0.701654	0.729828	0.753179
20	0.053019	0.230259	0.375673	0.479853	0.555759	0.612922	0.657319	0.692714	0.721556	0.745492
21	0.04809	0.219294	0.363651	0.468288	0.545018	0.603034	0.648219	0.684316	0.713775	0.738253
22	0.043817	0.209326	0.352546	0.457521	0.53497	0.593756	0.63966	0.676403	0.706434	0.731416
23	0.04009	0.200225	0.342251	0.447465	0.525542	0.585023	0.631588	0.668928	0.69949	0.724943
24	0.036819	0.191882	0.332677	0.438043	0.516671	0.576782	0.623954	0.661849	0.692906	0.718798
25	0.033932	0.184207	0.323746	0.429193	0.508303	0.568986	0.616719	0.655128	0.686649	0.712953
26	0.031372	0.177122	0.31539	0.420859	0.50039	0.561596	0.609847	0.648736	0.68069	0.707383
27	0.029091	0.170562	0.307554	0.412991	0.492893	0.554575	0.603306	0.642644	0.675005	0.702063
28	0.027051	0.16447	0.300187	0.405549	0.485775	0.547893	0.59707	0.636828	0.669572	0.696976
29	0.025217	0.158799	0.293246	0.398496	0.479004	0.541522	0.591113	0.631265	0.664371	0.692101
30	0.023564	0.153506	0.28669 2	0.391798	0.472552	0.535437	0.585415	0.625938	0.659385	0.687424
40	0.013255	0.115129	0.236659	0.339307	0.421186	0.486477	0.539222	0.582501	0.61855	0.648989
50	0.008483	0.092103	0.203947	0.303485	0.385221	0.451605	0.505916	0.550895	0.588625	0.620662

Supplement 2: Tables For Weibull Zer-failure Substantiation testing using (t/Eta)

Substantiation Testing Tables for Zero Failure Test at **80% Confidence**

Table 6 Sup 2.1

Confidence level = 0.8

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
t/η	**Infant mortality**	**Random**	**Early wearout**					**Old age rapid wearout**		
0.01	17	161	1610	16,095	160,944	___	___	___	___	___
0.02	12	81	570	4024	28,452	___	___	___	___	___
0.03	10	54	310	1789	10,325	59,609	344,152	___	___	___
0.04	9	41	202	1006	5030	25,148	125,738	628,687	___	___
0.05	8	33	1 44	644	2880	12,876	57,582	257,511	___	___
0.06	7	27	1 10	448	1826	7452	30,419	124,186	506,984	___
0.07	7	23	87	329	1242	4693	17,735	67,032	253,358	___
0.08	6	21	72	252	890	3144	11,114	39,293	138,922	___
0.09	6	18	60	199	663	2208	7360	24,531	81,768	___
0.10	6	17	51	161	509	1610	5090	16,095	5 0895	160,944
0.12	5	14	39	112	323	932	2689	7762	22,406	64,680
0.14	5	12	31	83	220	587	1568	4190	1 1197	29,925
0.16	5	1 1	26	63	158	393	983	2456	6140	15,349
0.18	4	9	22	50	118	276	651	1534	3614	8518
0.20	4	9	18	41	90	202	450	1006	2250	5030
0.22	4	8	16	34	71	152	323	688	1465	3123
0.24	4	7	14	28	58	117	238	486	991	2022
0.26	4	7	13	24	47	92	180	353	691	1355
0.28	4	6	11	21	39	74	139	262	495	936
0.30	3	6	10	18	33	60	109	199	363	663
0.32	3	6	9	16	28	50	87	154	272	480
0.34	3	5	9	14	24	41	71	121	207	355
0.36	3	5	8	13	21	35	58	96	160	267
0.38	3	5	7	12	19	30	48	78	126	204
0.40	3	5	7	11	16	26	40	63	100	158
0.42	3	4	6	10	15	22	34	52	80	124
0.44	3	4	6	9	13	19	29	43	65	98
0.46	3	4	6	8	12	17	25	36	53	79
0.48	3	4	5	7	1 1	15	22	31	44	64
0.50	3	4	5	7	10	13	19	26	37	52
0.55	3	3	4	6	8	10	14	18	24	32
0.60	3	3	4	5	6	8	10	13	17	21
0.65	2	3	4	4	5	6	8	10	12	14
0.70	2	3	3	4	4	5	6	7	9	10
0.75	2	3	3	3	4	4	5	6	6	7
0.80	2	3	3	3	3	4	4	4	5	5
0.85	2	2	3	3	3	3	3	4	4	4
0.90	2	2	2	2	3	3	3	3	3	3
0.95	2	2	2	2	2	2	2	2	3	3
1.00	2	2	2	2	2	2	2	2	2	2

Substantiation Testing Tables for Zero Failure Test at **90% Confidence**

Table 6 Sup 2.2

Confidence level = 0.9

	β									
	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5
t/η	Infant mortality	Random	Early wearout					Old age rapid wearout		
0.01	24	231	2303	23,026	230,259	---	---	---	---	---
0.02	17	116	815	5757	40,705	---	---	---	---	---
0.03	14	77	444	2559	14,772	85,281	492,370	---	---	---
0.04	12	58	288	1440	7196	35,978	179,890	899,448	---	---
0.05	11	47	206	922	4119	18,421	82,380	368,414	---	---
0.06	10	39	157	640	2612	10,661	43,520	177,669	725,330	---
0.07	9	33	125	470	1777	6714	25,374	95,902	362,473	---
0.08	9	29	102	360	1273	4498	15,901	56,216	198,752	---
0.09	8	26	86	285	948	3159	10,529	35,096	116,984	---
0.10	8	24	73	231	729	2303	7282	23,026	72,815	---
0.12	7	20	56	160	462	1333	3847	11,105	32,056	---
0.14	7	17	44	118	314	840	2243	5994	16,020	---
0.16	6	15	36	90	225	563	1406	3514	8784	21,960
0.18	6	13	31	72	168	395	931	2194	5170	12,186
0.20	6	12	26	58	129	288	644	1440	3218	7196
0.22	5	11	23	48	102	217	462	983	2096	4468
0.24	5	10	20	40	82	167	340	695	1417	2892
0.26	5	9	18	35	67	132	257	504	989	1938
0.28	5	9	16	30	56	105	199	375	708	1338
0.30	5	8	15	26	47	86	156	285	520	948
0.32	5	8	13	23	40	71	125	220	389	687
0.34	4	7	12	20	35	59	101	173	296	507
0.36	4	7	11	18	30	50	83	138	229	381
0.38	4	7	10	16	26	42	69	111	180	291
0.40	4	6	10	15	23	36	57	90	143	225
0.42	4	6	9	14	21	32	48	74	115	177
0.44	4	6	8	12	18	28	41	62	93	140
0.46	4	6	8	11	17	24	35	52	76	112
0.48	4	5	7	10	15	21	31	44	63	91
0.50	4	5	7	10	14	19	27	37	53	74
0.55	4	5	6	8	11	14	19	26	34	46
0.60	3	4	5	7	9	11	14	18	23	30
0.65	3	4	5	6	7	9	11	13	16	20
0.70	3	4	4	5	6	7	9	10	12	14
0.75	3	4	4	5	5	6	7	8	9	10
0.80	3	3	4	4	5	5	6	6	7	8
0.85	3	3	3	4	4	4	5	5	5	6
0.90	3	3	3	3	3	4	4	4	4	4
0.95	3	3	3	3	3	3	3	3	3	3
1.00	3	3	3	3	3	3	3	3	3	3

Substantiation Testing Tables for Zero Failure Test at **95% Confidence**

Table 6 Sup 2.3

Confidence level = 0.95

	β									
	0.5	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
t/η	**Infant mortality**	**Random**	**Early wearout**					**Old age rapid wearout**		
0.01	30	300	2996	29,958	299,574	---	---	---	---	---
0.02	22	150	1060	7490	52,958	---	---	---	---	---
0.03	18	100	577	3329	19,218	110,954	640,588	---	---	---
0.04	15	75	375	1873	9362	46,809	234,042	117,0208	---	---
0.05	14	60	268	1199	5359	23,966	107,179	479,318	---	---
0.06	13	50	204	833	3398	13,870	56,621	231,153	943,675	---
0.07	12	43	162	612	2311	8734	33,012	124,771	471,587	---
0.08	11	38	133	469	1655	5852	20,687	73,138	258,582	---
0.09	10	34	111	370	1233	4110	13,698	45,660	152,199	---
0.10	10	30	95	300	948	2996	9474	29,958	947,34	---
0.12	9	25	73	209	601	1734	5005	14,448	417,05	---
0.14	9	22	58	153	409	1092	2918	7799	20,842	---
0.16	8	19	47	118	293	732	1829	4572	11,428	28,570
0.18	8	17	40	93	218	514	1211	2854	6727	15,855
0.20	7	15	34	75	168	375	838	1873	4187	9362
0.22	7	14	30	62	132	282	600	1279	2727	5813
0.24	7	13	26	53	107	217	443	903	1844	3763
0.26	6	12	23	45	87	171	335	656	1286	2522
0.28	6	11	21	39	73	137	258	488	922	1741
0.30	6	10	19	34	61	111	203	370	676	1233
0.32	6	10	17	30	52	92	162	286	506	893
0.34	6	9	16	26	45	77	131	225	385	660
0.36	5	9	14	24	39	65	108	179	298	496
0.38	5	8	13	21	34	55	89	144	234	379
0.40	5	8	12	19	30	47	75	118	186	293
0.42	5	8	12	17	27	41	63	97	149	230
0.44	5	7	11	16	24	36	54	80	121	182
0.46	5	7	10	15	21	31	46	67	99	146
0.48	5	7	10	14	19	28	40	57	82	118
0.50	5	6	9	12	17	24	34	48	68	96
0.55	5	6	8	10	14	19	25	33	45	60
0.60	4	5	7	9	11	14	18	24	30	39
0.65	4	5	6	8	9	11	14	17	21	26
0.70	4	5	6	7	8	9	11	13	15	18
0.75	4	4	5	6	7	8	9	10	11	13
0.80	4	4	5	5	6	6	7	8	9	10
0.85	4	4	4	5	5	5	6	6	7	7
0.90	4	4	4	4	4	5	5	5	5	6
0.95	4	4	4	4	4	4	4	4	4	4
1.00	3	3	3	3	3	3	3	3	3	3

Substantiation Testing Tables for Zero Failure Test at **99% Confidence**

Table 6 Sup 2.4

Confidence level = 0.99										
	β									
	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5
t/*η*	Infant mortality	Random	Early wearout					Old age rapid wearout		
0.01	47	461	4606	46,052	—	—	—	—	—	—
0.02	33	231	1629	11,513	81,409	—	—	—	—	—
0.03	27	154	887	5117	29,543	170,562	—	—	—	—
0.04	24	116	576	2879	14,392	71,956	—	—	—	—
0.05	21	93	412	1843	8238	36,842	164,760	—	—	—
0.06	19	77	314	1280	5223	21,321	87,040	—	—	—
0.07	18	66	249	940	3553	13,427	50,747	191,803	—	—
0.08	17	58	204	720	2545	8995	31,801	112,431	—	—
0.09	16	52	171	569	1896	6318	21,058	70,191	—	—
0.10	15	47	146	461	1457	4606	14,563	46,052	145,629	—
0.12	14	39	111	320	924	2666	7694	22,209	64,111	—
0.14	13	33	88	235	628	1679	4486	11,988	320 39	—
0.16	12	29	72	180	450	1125	2811	7027	17,568	43,919
0.18	11	26	61	143	336	790	1862	4387	10,340	24,372
0.20	11	24	52	116	258	576	1288	2879	6436	14,392
0.22	10	21	45	96	203	433	923	1966	4192	8936
0.24	10	20	40	80	164	334	680	1389	2834	5784
0.26	10	18	35	69	134	263	514	1008	1977	3876
0.28	9	17	32	59	112	210	397	750	1416	2676
0.30	9	16	29	52	94	171	312	569	1039	1896
0.32	9	15	26	45	80	141	249	440	777	1373
0.34	8	14	24	40	69	118	201	345	592	1014
0.36	8	13	22	36	60	99	165	275	457	762
0.38	8	13	20	32	52	84	137	221	359	582
0.40	8	12	19	29	46	72	114	180	285	450
0.42	8	11	17	27	41	63	96	148	229	353
0.44	7	11	16	24	36	55	82	123	186	280
0.46	7	11	15	22	33	48	70	103	152	224
0.48	7	10	14	20	29	42	61	87	126	181
0.50	7	10	14	19	27	37	53	74	105	148
0.55	7	9	12	16	21	28	38	51	68	92
0.60	6	8	10	13	17	22	28	36	46	60
0.65	6	8	9	11	14	17	21	26	32	40
0.70	6	7	8	10	12	14	17	20	23	28
0.75	6	7	8	9	10	11	13	15	17	20
0.80	6	6	7	8	9	9	11	12	13	15
0.85	5	6	6	7	7	8	9	9	10	11
0.90	5	6	6	6	6	7	7	8	8	8
0.95	5	5	5	6	6	6	6	6	6	6
1.00	5	5	5	5	5	5	5	5	5	5

Supplement 3: Critical Values for Cramer–Von Mises Goodness-of-Fit Test

Table 6 Sup 3.1 Critical values for Cramer–Von Mises goodness-of-fit test' for individual failure time data.

	α				
F	**0.20**	**0.15**	**0.10**	**0.05**	**0.01**
2	0.138	0.149	0.162	0.175	0.19
3	0.121	0.135	0.154	0.184	0.23
4	0.121	0.134	0.155	0.191	0.28
5	0.121	0.137	0.160	0.199	0.30
6	0.123	0.139	0.162	0.204	0.31
7	0.124	0.140	0.165	0.208	0.32
8	0.124	0.141	0.165	0.210	0.32
9	0.125	0.142	0.167	0.212	0.32
10	0.125	0.142	0.167	0.212	0.32
11	0.126	0.143	0.169	0.214	0.32
12	0.126	0.144	0.169	0.214	0.32
13	0.126	0.144	0.169	0.214	0.33
14	0.126	0.144	0.169	0.214	0.33
15	0.126	0.144	0.169	0.215	0.33
16	0.127	0.145	0.171	0.216	0.33
17	0.127	0.145	0.171	0.217	0.33
18	0.127	0.146	0.171	0.217	0.33
19	0.127	0.146	0.171	0.217	0.33
20	0.128	0.146	0.172	0.217	0.33
30	0.128	0.146	0.172	0.218	0.33
60	0.128	0.147	0.173	0.220	0.33
100	0.129	0.147	0.173	0.220	0.34

Source: AMSAA Reliability Growth Guide, Technical Report No.TR-652, ADA381985, U.S. Army Materiel Systems Analysis Activity, Aberdeen Proving Ground, Maryland, 2000, P.64. Public Domain.

Supplement 4: Other Reliability Growth Models that have been Proposed and Studied (see AFWAL-TR-84-2024 for details)

The major models studied by the task force included (note that Bayesian models were not represented):

(a) Deterministic Models

The form of deterministic models (models that contain no random elements) is assumed to be known. That is, it is known that reliability grows via the deterministic model. The parameters are estimated, and reliability is then calculated from the model. Examples of deterministic models reviewed are as follows:

1) The Duane model:

$$\text{Cumulative MTBF} = \gamma\,(\text{Cumulative Time})^{\alpha}$$

2) The Endless-Burn-In model:

$$\text{Instantaneous Failure Rate} = K\,(\text{Average Age})^{-\alpha} + \lambda_R$$

3) The Gompertz model:

$$\text{Cumulative Failure Rate} = K{*}A^{B*(\text{Cumulative Time})}$$

4) The Grumman model:

$$\text{Instantaneous Failure Rate} = A\,e^{-K(\text{Cumulative Time})} + B$$

(b) Poisson Process Models

This class of models does not assume that the form of the reliability-growth function is known, but only that it can be approximated statistically. Since the model form is only an approximation, the quality-of-fit tests are necessary to determine if the approximation is reasonable. The Poisson process model assumes that events occur based on a Poisson type of distribution. That is, the probability of realizing K events (failures) by some test time t is as follows:

$$P(x = k) = \frac{[M(t)]^k e^{-M(t)}}{k!}$$

Here, $M(t)$ is the mean value function. If $M(t) = \lambda t$, the process is a homogeneous Poisson process (HPP), and the time between failures follows an exponential distribution (the probability of failure by time $t = 1 - e^{-kt}$).

The Poisson process also assumes independent increments. Renewal theory generalizes the HPP by allowing time between failures to have other distributions other than the exponential. A renewal process is a sequence of random variables $[Y_1, Y_2, \ldots]$ of the form $Y_i = X_1 + X_2 + \cdots + X_i$, where each X_i comes from a common distribution $F(X)$. Therefore, the renewal model assumes that each repair returns the system to good-as-new state. If the Poisson process has a *more general* mean value function than $M(t) = \lambda t$, it is said to be a nonhomogeneous Poisson process (NHPP). The intensity function, $p(t)$, of a Poisson process is the rate at which failures are occurring and is related to the mean value function as follows:

$$M(t) = \int_0^t \rho(x)\mathrm{d}x$$

The NHPP model is the most popular since it can model a system that is wearing out. Several intensity functions have been used with the NHPP model. The following are examples:

1) The AMSAA-Duane model (presented in the section titled "Reliability Growth Modeling and Testing") and the model chosen by the task force that studied all models available at the time:

$$\rho(t) = \lambda\beta(\text{Cumulative time})^{\beta - 1}$$

2) The modified Duane model:

$$\rho(t) = \lambda\beta(\text{Cumulative time})^{\beta - 1} + \theta$$

3) The Cox-Lewis model:

$$\rho(t) = e^{\alpha + \gamma(\text{Cumulative time})}$$

(c) Markov Processes/Time Series Models

It has been shown that Markovian processes and the autoregressive moving average process were related. A Markov process is a process that moves from state i to state j with some probability P_{ij}. This probability is independent of all past states and is dependent only on the present state. The time spent in each state is an exponentially distributed random variable. If the time in residence is not exponential, the process is said to be a semi-Markov process. Markov processes usually require more data to estimate the probabilities than is generally available.

A number of noted statisticians suggested that time series methods developed by Box and Jenkins be used to model reliability growth. The Box–Jenkins Autoregressive Integrated Moving Average (ARIMA) modeling approach is attractive in that no specific model needs to be selected in advance. The models are flexible in that they can be applied to a wide range of data, and the methodology has a built-in theory of forecasting. For example, an ARIMA first difference model could be written as follows:

$$\lambda_{c,T} = \lambda_{c,T-1} + \varepsilon_T$$

where $\lambda_{c,\ T}$ is the cumulative failure rate at time T and ε_T is the random (normal(0, σ)) error at time T.

After studies using various types of data from various industries, it was decided that the AMSAA-Duane mode was the recommended model for reliability growth.

It should be noted that the time series modeling approach, while it does a slightly better job of modeling, is very mathematical and is hard to explain to an audience of general or industry managers. The author has had direct experience in trying to explain a time series model on numerous occasions and has fallen back on the AAMSAA-Duane model instead.

Source: AFWAL-TR-84-2024, RELIABILITY-GROWTH ASSESSMENT, PREDICTION, AND CONTROL FOR ELECTRONIC CONTROL(GAPCEEC), ADA163070, Aero Propulsion Lab, WPAFB, April 1984. Public Domain.

Supplement 5: Chi-Square Table

Table 6 Sup5.1 Chi-Square Table (Generated in EXCEL™, using CHIINV(α,ν).

ChiSq		Alpha level											
		0.995	0.99	0.98	0.975	0.95	0.9	0.1	0.05	0.025	0.02	0.01	0.005
	1	0.000	0.000	0.001	0.001	0.004	0.016	2.706	3.841	5.024	5.412	6.635	7.879
D	2	0.010	0.020	0.040	0.051	0.103	0.211	4.605	5.991	7.378	7.824	9.210	10.597
e	3	0.072	0.115	0.185	0.216	0.352	0.584	6.251	7.815	9.348	9.837	11.345	12.838
g	4	0.207	0.297	0.429	0.484	0.711	1.064	7.779	9.488	11.143	11.668	13.277	14.860
r	5	0.412	0.554	0.752	0.831	1.145	1.610	9.236	11.070	12.833	13.388	15.086	16.750
e	6	0.676	0.872	1.134	1.237	1.635	2.204	10.645	12.592	14.449	15.033	16.812	18.548
e	7	0.989	1.239	1.564	1.690	2.167	2.833	12.017	14.067	16.013	16.622	18.475	20.278
s	8	1.344	1.646	2.032	2.180	2.733	3.490	13.362	15.507	17.535	18.168	20.090	21.955
	9	1.735	2.088	2.532	2.700	3.325	4.168	14.684	16.919	19.023	19.679	21.666	23.589
of	10	2.156	2.558	3.059	3.247	3.940	4.865	15.987	18.307	20.483	21.161	23.209	25.188
	11	2.603	3.053	3.609	3.816	4.575	5.578	17.275	19.675	21.920	22.618	24.725	26.757
F	12	3.074	3.571	4.178	4.404	5.226	6.304	18.549	21.026	23.337	24.054	26.217	28.300
r	13	3.565	4.107	4.765	5.009	5.892	7.042	19.812	22.362	24.736	25.472	27.688	29.819
e	14	4.075	4.660	5.368	5.629	6.571	7.790	21.064	23.685	26.119	26.873	29.141	31.319
e	15	4.601	5.229	5.985	6.262	7.261	8.547	22.307	24.996	27.488	28.259	30.578	32.801
d	16	5.142	5.812	6.614	6.908	7.962	9.312	23.542	26.296	28.845	29.633	32.000	34.267
0	17	5.697	6.408	7.255	7.564	8.672	10.085	24.769	27.587	30.191	30.995	33.409	35.718
m	18	6.265	7.015	7.906	8.231	9.390	10.865	25.989	28.869	31.526	32.346	34.805	37.156
	19	6.844	7.633	8.567	8.907	10.117	11.651	27.204	30.144	32.852	33.687	36.191	38.582
	20	7.434	8.260	9.237	9.591	10.851	12.443	28.412	31.410	34.170	35.020	37.566	39.997
$(\nu = n - 1)$	21	8.034	8.897	9.915	10.283	11.591	13.240	29.615	32.671	35.479	36.343	38.932	41.401
	22	8.643	9.542	10.600	10.982	12.338	14.041	30.813	33.924	36.781	37.659	40.289	42.796
	23	9.260	10.196	11.293	11.689	13.091	14.848	32.007	35.172	38.076	38.968	41.638	44.181
	24	9.886	10.856	11.992	12.401	13.848	15.659	33.196	36.415	39.364	40.270	42.980	45.559
	25	10.520	11.524	12.697	13.120	14.611	16.473	34.382	37.652	40.646	41.566	44.314	46.928
	26	11.160	12.198	13.409	13.844	15.379	17.292	35.563	38.885	41.923	42.856	45.642	48.290
	27	11.808	12.879	14.125	14.573	16.151	18.114	36.741	40.113	43.195	44.140	46.963	49.645
	28	12.461	13.565	14.847	15.308	16.928	18.939	37.916	41.337	44.461	-5.419	48.278	50.993
	29	13.121	14.256	15.574	16.047	17.708	19.768	39.087	42.557	45.722	46.693	49.588	52.336
	30	13.787	14.953	16.306	16.791	18.493	20.599	40.256	43.773	46.979	47.962	50.892	53.672
	31	14.458	15.655	17.042	17.539	19.281	21.434	41.422	44.985	48.232	49.226	52.191	55.003
	32	15.134	16.362	17.783	18.291	20.072	22.271	42.585	46.194	49.480	50.487	53.486	56.328
	33	15.815	17.074	18.527	19.047	20.867	23.110	43.745	47.400	50.725	51.743	54.776	57.648
	34	16.501	17.789	19.275	19.806	21.664	23.952	44.903	48.602	51.966	52.995	56.061	58.964
	35	17.192	18.509	20.027	20.569	22.465	24.797	46.059	49.802	53.203	54.244	57.342	60.275
	36	17.887	19.233	20.783	21.336	23.269	25.643	47.212	50.998	54.437	55.489	58.619	61.581
	37	18.586	19.960	21.542	22.106	24.075	26.492	48.363	52.192	55.668	56.730	59.893	62.883
	38	19.289	20.691	22.304	22.878	24.884	27.343	49.513	53.384	56.896	57.969	61.162	64.181
	39	19.996	21.426	23.069	23.654	25.695	28.196	50.660	54.572	58.120	59.204	62.428	65.476
	40	20.707	22.164	23.838	24.433	26.509	29.051	51.805	55.758	59.342	60.436	63.691	66.766
	41	21.421	22.906	24.609	25.215	27.326	29.907	52.949	56.942	60.561	61.665	64.950	68.053
	42	22.138	23.650	25.383	25.999	28.144	30.765	54.090	58.124	61.777	62.892	66.206	69.336
	43	22.859	24.398	26.159	26.785	28.965	31.625	55.230	59.304	62.990	64.116	67.459	70.616
	44	23.584	25.148	26.939	27.575	29.787	32.487	56.369	60.481	64.201	65.337	68.710	71.893
	45	24.311	25.901	27.720	28.366	30.612	33.350	57.505	61.656	65.410	66.555	69.957	73.166
	46	25.041	26.657	28.505	29.160	31.439	34.215	58.641	62.830	66.617	67.771	71.201	74.437
	47	25.775	27.416	29.291	29.956	32.268	35.081	59.774	64.001	67.821	68.985	72.443	75.704
	48	26.511	28.177	30.080	30.755	33.098	35.949	60.907	65.171	69.023	70.197	73.683	76.969
	49	27.249	28.941	30.871	31.555	33.930	36.818	62.038	66.339	70.222	71.406	74.919	78.231
	50	27.991	29.707	31.664	32.357	34.764	37.689	63.167	67.505	71.420	72.613	76.154	79.490

Note: As in all χ^2 tables, $\nu = n - 1$. For $\nu > 50$, use approximation $Q(p) \approx \nu\left(1 - \frac{2}{9\nu} + Q\right)$.

7

Failure Modes and Effects Analysis – Design and Process

"You want a valve that doesn't leak and you try everything possible to develop one, but the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate."

Source: Arthur Rudolph, Saturn 5 Rocket Scientist

7.1 Introduction

Failure modes and effects analysis, usually referred to by the acronym FMEA, is one of the most widely employed techniques for enumerating the possible modes by which components may fail and for tracing through the characteristics and consequences of each mode of failure on the system as a whole. The method is primarily qualitative in nature, although in Chapter 11 (Systems Safety Analysis) we introduce an extension of FMEA called FMECA (failure modes, effects and criticality analysis) which includes estimates of failure probabilities.

What is FMEA and why should this analysis be done? It is a tool for preventing problems and reducing risk as well as a procedure for developing and implementing new or revised designs, processes, or services. Finally, FMEA serves as a diary of the design, process, or service, valuable for future reviews of performance and dependability.

In this chapter, we distinguish between three major types of FMEA: *Functional* FMEA addresses what happens if one or more of a product's functions fail to be performed, and how can such failures be prevented. *Design* FMEA deals with what happens if a design shortcoming causes a product to fail, and how that failure can be prevented. *Process* FMEA examines what happens if a process step fails to accomplish its assigned task, and what can be done to prevent such a failure. Process FMEA (PFMEA) is most often applied to manufacturing processes. However, it is also applicable to processes in service industries, software development, analysis processes, and in fact, ANY process.

The general characteristics of all three of these FMEA types follow the same path:

Failure Mode → Effect → Cause

FMEA is most straightforward to start applying in the development cycle of a product. Figure 7.1 illustrates this phenomenon. The failure modes of the system FMEA generate all the essential information for the design and PFMEA. Although the effect stays the same, the causes in the functional FMEA become the failure modes in the design, which in turn generate their own causes, which ultimately become the failure modes in the PFMEA. It is imperative that the failure modes in the manufacturing processes not be listed in the design FMEA (see Figure 7.1).

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

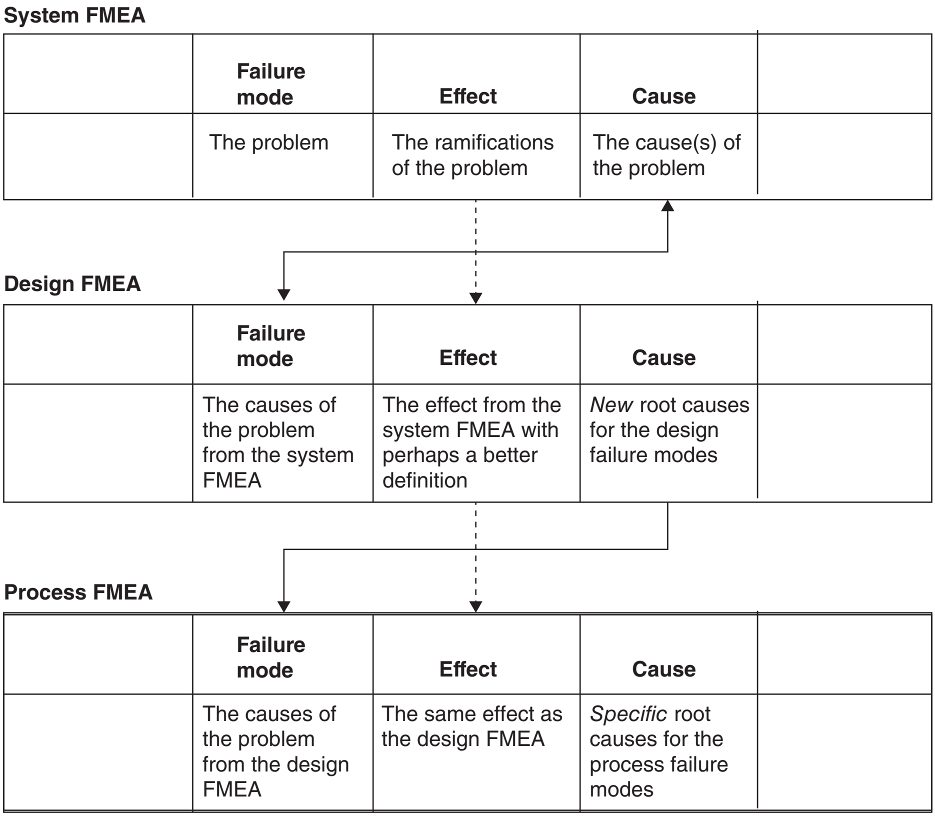


Figure 7.1 Relationship of system, design, and process FMEA. Note: System FMEA is often called "functional FMEA.". *Source:* Stamatis (1995). Figure 5.1 Relationship of system, design, and process FMEA, p. 108 with permission.

7.2 Functional FMEA

- The functional FMEA focuses on the functions of a product or process rather than on the specific hardware "piece parts." It is a high-level "top-down" approach – especially useful for complex systems. A functional FMEA is the most practical approach during the conceptual design phase – before specific hardware information is available. The functional FMEA usually begins with a functional block diagram analysis. A functional block diagram illustrates the physical and functional relationships and interfaces in a system and provides a map of energy flow within a system. The functional block diagram can also include schematics, drawings, and layouts to help in the understanding.

Example 7.1 Refrigerator functional block diagram shown in Figure 7.2a, with accompanying diagram of common household refrigerator operation in Figure 7.2b.

For the main function of a refrigerator, the functional FMEA will look as shown in Table 7.1.

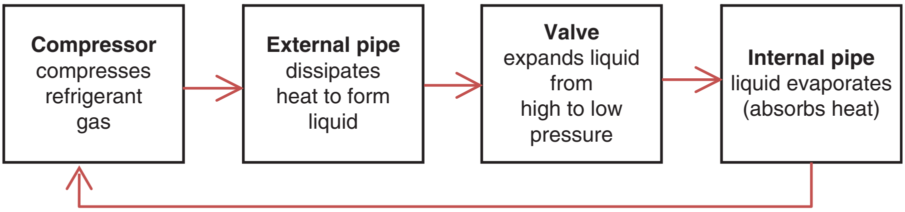


Figure 7.2a Refrigerator functional block diagram.

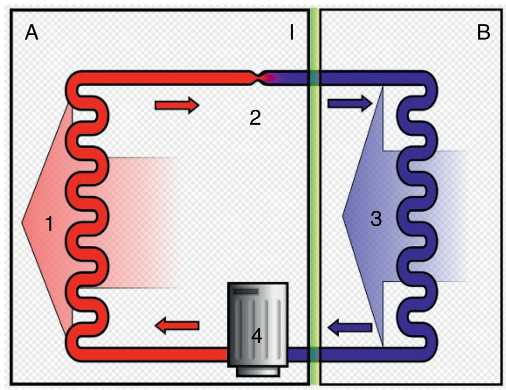


Figure 7.2b Household refrigerator flow to accompany functional flow diagram for clarity: Vapor compression cycle – A, hot compartment (kitchen); B, cold compartment (refrigerator box); I, insulation; 1, Condenser; 2, Expansion valve; 3, Evaporator unit; 4, Compressor. *Source:* Ilmari Karonen, Diagram of the vapor compression cycle used in refrigerator, Wikimedia Commons, 26 June 2010. Public Domain.

Table 7.1 Functional FMEA for refrigerator cooling.

Function	Functional failure mode	Cause of failure	Possible effects
Maintain food or beverages at desired temperatures	Does not maintain desired level	a) Compressor motor fails to operate b) Refrigerant coolant leaks c) Refrigerator door does not seal	Food spoilage

Example 7.2 Major components of Space Shuttle Main Engine (see Figure 7.3)
The functional FMEA for the hot gas manifold and heat exchanger is in Table 7.2.

In the left-hand column, the major components or subsystems are listed, and in the next column the physical modes by which each of the components may fail are given. This is followed, in the third column, by the possible causes of each of the failure modes. The fourth column lists the effects of the failure. The method becomes more quantitative if an estimate of the probability of each failure mode is made.

"Criticality" of the failure's importance may be included in order to separate the failure modes that are catastrophic from those that merely cause inconvenience or moderate economic loss. When

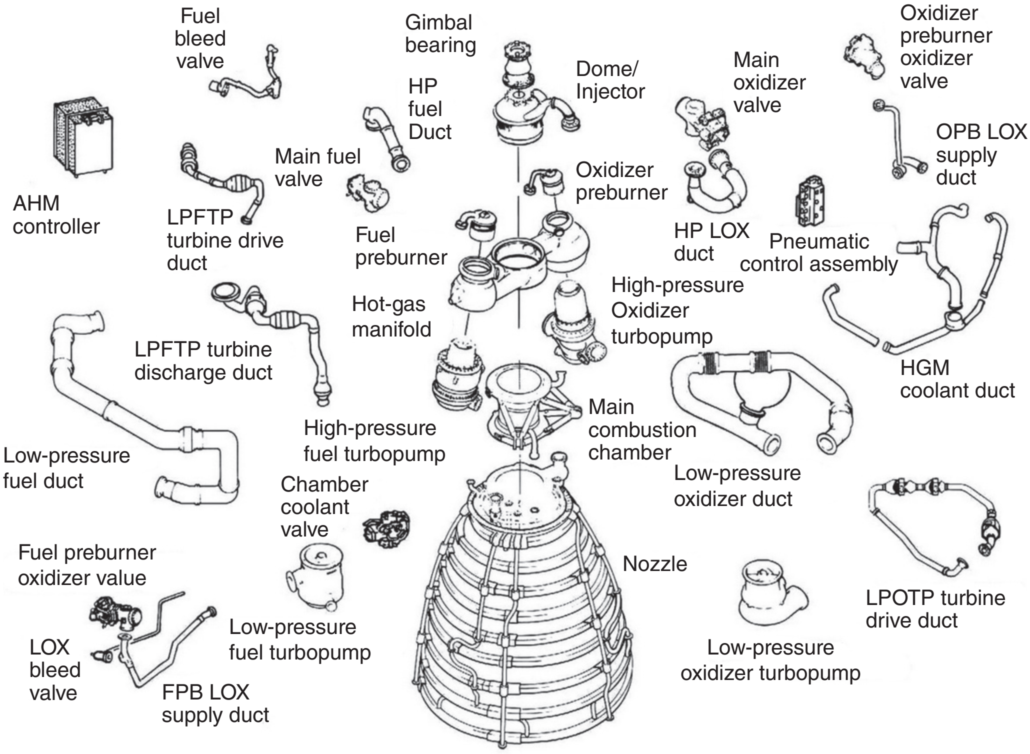


Figure 7.3 Major components of SSME with hot gas manifold/heat exchanger indicated. *Source:* "Booster System Briefs"(JSC-19041), Systems Division, Guidance and Propulsion Systems Branch, NASA Johnson Space Flight Center, Houston, Texas, October 1992. Public Domain.

"Criticality" is included, the analysis becomes a FMECA or a safety analysis, which will be discussed in more detail in Chapter 11. The final column in some FMEA charts is a listing of possible remedies. In a more extensive design FMECA, the information shown in Figures 7.2a and 7.2b may be expanded as we will see in Chapter 11 when we add the probability of an event along with the criticality as described above.

In general, the emphasis in a functional FMEA is on the basic physical phenomena that can cause a device or component to fail. Therefore, it often serves as a suitable starting point for enumerating and understanding the failure mechanisms in the early design/development phase of a project. A functional FMEA has many benefits: it helps select the optimum concept alternatives or determine changes to System Design Specifications; increases the likelihood that all potential effects of a proposed concept's failure modes are considered; identifies the system-level testing requirements; and most importantly helps determine if hardware system redundancy may be required within a design proposal.

Table 7.2 Functional FMEA of SSME Hot Gas Manifold and Heat Exchanger.

	Functional failure modes and effects analysis		
1. Subsystem________ **Item**	**2. Dwg Nr.________** **Failure modes**	**3. Prepared by______________** **Cause of failure mode**	**4. Date______________** **Possible effects**
Hot Gas Manifold	Cracks, rupture	a. Vibration and thermal b. No heat treatment c. Defective welds	Engine fire
	Loose stud fasteners	a. Wrong torque b. Repeated stretching c. Load	Hot gas leak/engine fire
	G-5 Seal and Main Combustion Chamber a. Ignition joint leaks	Installation problems	Engine fire
	Contamination	Fabrication	Performance degradation operation
Heat Exchanger	Dings, cracks, leaks	a. Mishandling b. Wrong material c. Wear, thermal fatigue d. Bad weld	Turbopump destruction Engine destruction
	Clearance problems, inclusions	a. Thermal cycling b. Fabrication errors	Coil wear, leaks, turbopump destruction

Source: Based on STUDIES AND ANALYSES OF THE SPACE SHUTTLE MAIN ENGINE," NAS 1.26:178993, NASA-CR-178993, BCD-SSME-TR-86-1, Battelle Columbus labs, December 15, 1986.

7.3 Design FMEA

A design FMEA is the most common FMEA application. It is a "bottom-up" process that tries to define all the failure modes of a part. It can break down a system to its subsystems, then to its modules, and finally, individual parts to attempt to find any failure mode that affects reliability (and hence possibly safety).

We begin with an everyday illustration of the difference between a functional and design FMEA: Let us consider first an automobile tire. The fundamental function of an automobile tire is to "keep the rim off the road." Figure 7.4 illustrates the functional FMEA with failure mode "loss of air" and the three causes for that in the functional FMEA that would be carried out in the up-front development of a tire, i.e. before "Design Go-ahead." After "Design Go-ahead," a design FMEA will be started. Then, as illustrated, the design FMEA will take each of the causes from the functional FMEA and expand it to individual failure modes with more detailed causes that can be considered in the detailed design of the tire.

Design FMEA Procedure

Design FMEAs are performed using a Design Template such as that shown in Figure 7.5. The first step in the process is to take each of the causes from the functional FMEA and enumerate the possible failure modes associated with it. Thus, the first two columns in Figure 7.5 are filled in. For simpler products, the analysis may be performed by an individual, while for more complex systems an interdisciplinary group may hold a brainstorming session in order to assure that all significant failure modes are recognized. Depending on the nature of the system, engineers familiar with failure modes of materials, structures, mechanical or electrical systems, software, human factors, and/or manufacturing processes may be called upon. It is imperative that the analysists understand the physics of failure of the particular item under scrutiny.

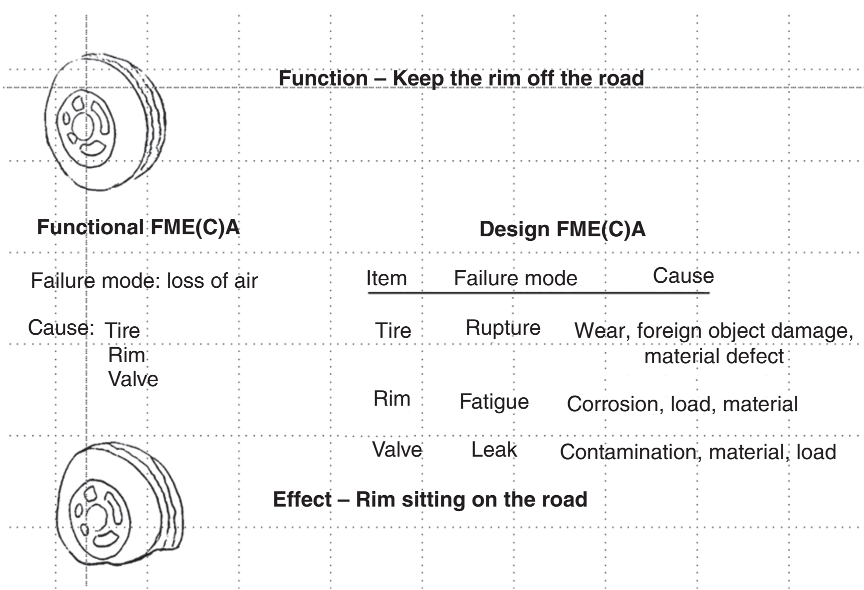


Figure 7.4 Illustration of how a functional FMEA is used by the next tier in the design of a product.

						Design									
						Failure Modes and Effects Analysis (DFMEA)									
Part/Product Name						FMEA Date (Orig) ____________			(Rev) ____________						
Product part function	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recommended actions	Resp.	Actions taken	SEV	OCC	DET	RPN
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							

Figure 7.5 Design FMEA template.

Referring to the bathtub curve, introduced in Figures 3.1–3.3, may offer a valuable perspective in identifying failure modes. For example, does a system fail because it is overstressed in some way, such as being exposed to conditions or an environment for which it was not designed? Is its maintenance faulty, or is it being used incorrectly? Such failure modes contribute to the flat part of the bathtub curve: they are essentially independent of how old the system is. Is the system susceptible to errors or other shortcomings in manufacture or construction which will aggravate infant mortality failure on the left of the bathtub curve? And finally are wear, aging, or fatigue phenomena or lack of attention to preventive maintenance likely to give rise to failure modes that aggravate the increasing failure rate on the right of the bathtub curve?

The next step in a design FMEA is to examine the overall importance of each failure mode on the same relative scale. This scale is called the "Risk Priority Number" or RPN. It is calculated as the product of Severity × Occurrence × Detection. Figure 7.6 details how each of the three factors is calculated.

The scales for each of Severity, Occurrence, and Detection were chosen so that the RPN of an Extremely Hazardous Effect (10 severity) that occurs almost certainly (10 occurrence) and was

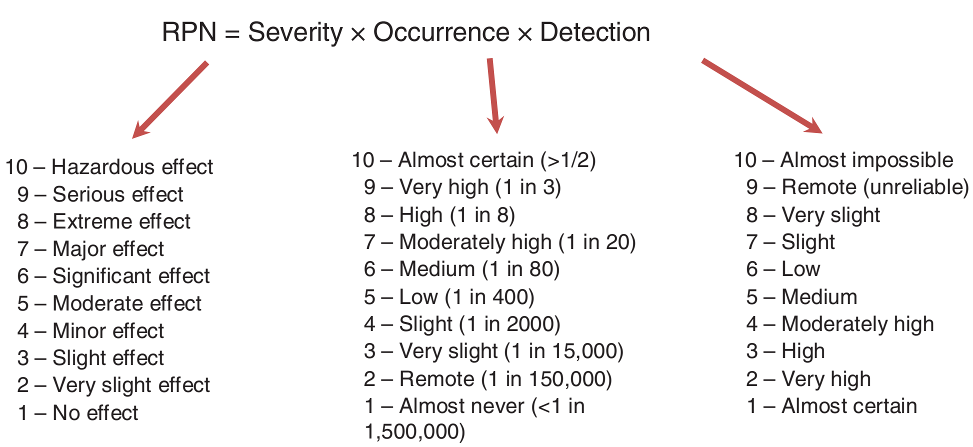


Figure 7.6 RPN (Risk Priority Number) calculation.

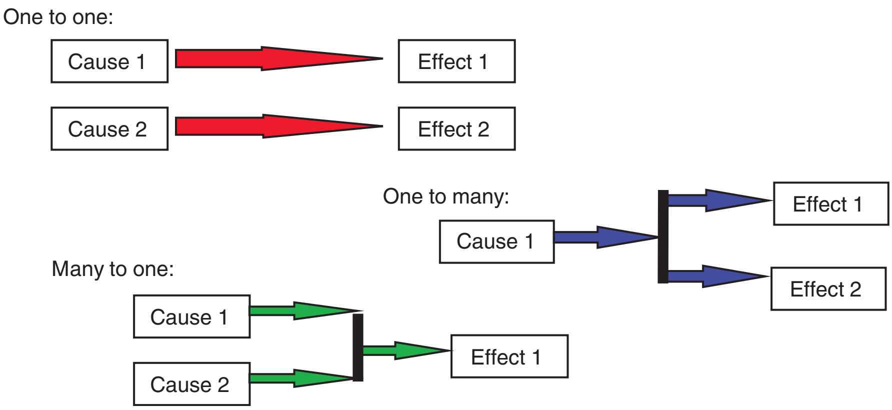


Figure 7.7 Relationships between causes and effects.

almost impossible to be detected (10 detection) would be 1000. At the same time, a failure mode that had no effect on the product (1 severity), extremely remote chance of happening (1 occurrence), and almost certainly could be detected (1 detection) would have an RPN = 1 as illustrated in Figure 7.6.

In identifying the potential causes for the effects, keep in mind that the relationship may be more complicated than simply one-to-one, as indicated in Figure 7.7.

To illustrate the construction and use of a design FMEA, we use the example of a simple product: the *design of a coffee cup*.

Example 7.3 Design of a Coffee Cup

We have been asked to participate on a design team for the design of a new paper coffee cup for a major coffee shop (the CUSTOMER). A team of five engineers, design, fabrication, general manufacturing, materials, and reliability/safety, has been selected for their expertise in producing this new coffee cup that will satisfy the needs of the CUSTOMER (determined by a QFD or Quality Function Deployment analysis[1]).

The CUSTOMER wishes to have a coffee cup in three sizes 8 oz, 9 oz, and 16 oz. Each of these sizes must be able to accomplish the following:

1) Hold coffee
2) Hold liquid
3) Be safe for the customer to handle
4) Look good
5) Must be stackable
6) Resist spills when driving.

Solution: Since the first three requirements depend on the insulation capability that must be built into the coffee cup, it was decided to do Function 3 – "insulate" – and combine the issues that will meet customer requirements 1 and 2. Thus, from the design FMEA template, we obtain Figure 7.8a.

1 2004

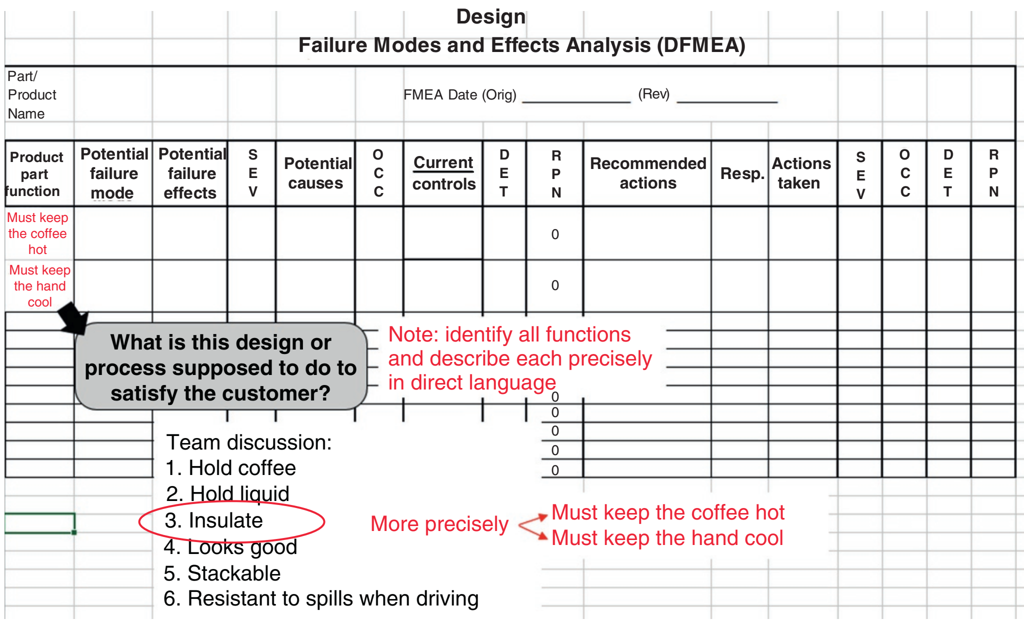


Figure 7.8a Function identification.

Next, what are the potential failure modes for each function?

Function	Failure mode
Must keep coffee hot	Coffee is cold
Must keep hand cool	Burns hand

Now, we determine the effect of each of the failure modes:
So, we ask the questions:

- In the worst case scenario, does this failure mode impact the safe operation of the system?
- What is the impact of the failure mode on the surrounding hardware and the system?

In this case, the answers are:

Function	Failure mode	Failure effects
Must keep coffee hot	Coffee is cold	Taste bad
Must keep hand cool	Burns hand	First degree burn

Next, we determine where each failure mode is on the "Severity" scale. We use the generic severity in Table 7.3: How bad are the consequences (measured on a scale from 1 to 10)?

To assign this rating, you must assume that the failure mode has occurred. Based on the effects, we choose 3 for "coffee is cold" and 9 "burns hand."

So far, we have the following:

Function	Failure mode	Failure effects	Severity
Must keep coffee hot	Coffee is cold	Taste bad	3
Must keep hand cool	Burns hand	First degree burn	9

Table 7.3 Generic severity scale.

Generic severity scale	
10 – Hazardous effect	
9 – Serious effect	← First degree burn
8 – Extreme effect	
7 – Major effect	
6 – Significant effect	
5 – Moderate effect	
4 – Minor effect	
3 – Slight effect	← Taste bad
2 – Very slight effect	
1 – No effect	

Table 7.4 Generic occurrence table.

Generic occurrence scale	Probability of occurrence
10 – Almost certain	(>1/2)
9 – Very high	(1 in 3)
8 – High	(1 in 8)
7 – Moderately high, frequent	(1 in 20)
6 – Medium	(1 in 80)
5 – Low, occasional failures expected	(1 in 400)
4 – Slight, small number of occurrences	(1 in 2,000)
3 – Very slight	(1 in 15,000)
2 – Remote, unlikely	(1 in 150,000) ←
1 – Almost never, extremely remote	(<1 in 1,500,000)

We next assign a cause and with it an occurrence estimate determined from Figure 7.6, repeated in Table 7.4. Our estimate of cause and occurrence likelihood allows us to fill in the next two columns; in this case, the occurrence for both causes is 2-Remote, unlikely.

NOTE: Any number of Quality and Statistical tools are available to help in this effort (e.g. Delphi Technique, Design Review Teams, Design of Experiments, and "5 Whys," to name a few.).

Function	Failure mode	Failure effects	Severity	Cause	Occurrence
Must keep coffee hot	Coffee is cold	Taste bad	3	Wrong material	2
Must keep hand cool	Burns hand	First degree burn	9	Material too thin	2

Continuing, we examine the current design controls for detection; i.e. What are the chances of catching the failure modes before they are delivered to the customer? Engineering analysis is the only way to detect these two failure modes, and using Table 7.5 (repeated from Figure 7.8a), we postulate that engineering analysis has very high chances of detecting both failure modes, and thus we assign them each a 2 "Detection Value". Since we now have an estimate of each of the three factors, we can calculate the RPN. We thus have Figure 7.8b.

Table 7.5 Generic detection scale.

Generic detection scale
10 – Almost impossible
9 – Remote (unreliable)
8 – Very slight
7 – Slight
6 – Low
5 – Medium
4 – Moderately high
3 – High
2 – Very high
1 – Almost certain

Design
Failure Modes and Effects Analysis (DFMEA)

Part/Product Name

FMEA Date (Orig) ____________ (Rev) ____________

Product part function	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recommended actions	Resp.	Actions taken	SEV	OCC	DET	RPN
Must keep the coffee hot	Coffee is cold	Tastes bad	3	Wrong material	2	Engrgy analysis	2	12	12						
Must keep the hand cool	Burns hand	1st degree burn	9	Material too thin	2	Engrgy analysis	2	36	36						
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							

Figure 7.8b RPN (Risk Priority Number) calculation.

Design
Failure Modes and Effects Analysis (DFMEA)

Part/ Product Name						FMEA Date (Orig) ____________			(Rev) ____________						
Product part function	**Potential failure mode**	**Potential failure effects**	**SEV**	**Potential causes**	**OCC**	**Current controls**	**DET**	**RPN**	**Recommended actions**	**Resp.**	**Actions taken**	**SEV**	**OCC**	**DET**	**RPN**
Must keep the coffee hot	**Coffee is cold**	**Tastes bad**	**3**	**Wrong material**	**2**	**Engrgy analysis**	**2**	**12**							
Must keep the hand cool	**Burns hand**	**1st degree burn**	**9**	**Material too thin**	**2**	**Engrgy analysis**	**2**	**36**	Cup material insulation capability increased to withstand burn for liquid up to 220 °F	Design team 3/1/08	Design completed with thicker material and recommendation for coffee shops to include foam "collar" for each cup of coffee served	**2**	**2**	**2**	**8**

Figure 7.8c Final design FMEA for coffee cup – first two functions.

Note that for a specific failure mode, the controls may be good related to one effect but not good for another effect of the same failure mode. Do **NOT** take into account severity or occurrence ratings when doing the detection rating.

Since the RPN on the first function is so low, we work on the second function first. To complete the design FMEA, actions must be recommended and completed as indicated in the template. For the coffee cup, the design team recommends that the cup insulation be increased to withstand 220°F without causing a burn, responsibility for the action assigned, and the actions taken and RPN obtained documents. These are included in the remaining blocks of the design FMEA template as indicated in Figure 7.8c.

Discussion of Example 3: Several comments are in order regarding the foregoing example. The FMEA responsibility for the action and a date for resolution are essential to the use of an FMEA in resolving design issues. The design team redesigned the cup/material, and the FMEA team determined that the new severity would be 2, and occurrence and detection remaining the same for an RPN = 8. The final FMEA is illustrated in Figure 7.8c. Note that the characteristics of the product identified by the design team as key to keeping the severity lower need to be documented as a Key Product Characteristic (KPC) and noted in the final FMEA. In any FMEA, a KPC should also be identified for any RPN that is called out as important and has the design team input for its lowering that RPN's occurrence or detection as well as severity.

The paper cup example was chosen for its simplicity. For more complex systems, dozens of failure modes are likely to be identified. The criteria will vary somewhat between industries. But generally, at least the top 10% of the RPNs as well as ANY mode whose severity is >7 will be chosen to undergo detailed scrutiny. Also, review the design FMEA after initial design and final design (usually those reviews are included in a design roadmap) for any changes.

The design FMEA is passed to the manufacturing and assembly departments and goes into their control plans for the product. It allows the manufacturing process to "control" any item; in the paper cup example, making sure the cup material specifications are met. In general terms for mechanical systems such as airplanes, cars, engines, and the like, any part dimension, process (e.g. chemical, etching, milling, drilling, and dimensions) that is "critical" to the reliability of the part, subsystem, or system needs to be controlled in the manufacturing process.

7.4 Process FMEA (PFMEA)

Historically, the PFMEA is based on manufacturing or assembly processes used to make the product. It begins with process flow diagrams that illustrate the flows of the parts fabrication and assembly processes, the inspection points, and the processes for handling nonconforming material. In the case of a manufacturing process or assembly process, the PFMEA assumes that the product, as designed, will meet the design intent.

The PFMEA can be used to examine processes other than in manufacturing. Some examples of other processes that have used this tool are optimizing processing of patients in a hospital, customers in a restaurant or grocery store, or passengers in a Transportation Security Administration (TSA) security inspection line. Likewise, FMEA may also be applied to engineering development process flows and for error checking in software development. A PFMEA can be used to lay out a process in a block diagram flow so that a team of knowledgeable people can examine every stage of the process for errors in input and output and "standard work" used to process the "work" through that stage.

Example of a manufacturing process flow:

Figure 7.9 is an example of a manufacturing block diagram. It illustrates the overall flow of a low-pressure turbine manufacturing line. This is the starting point for a PFMEA of that

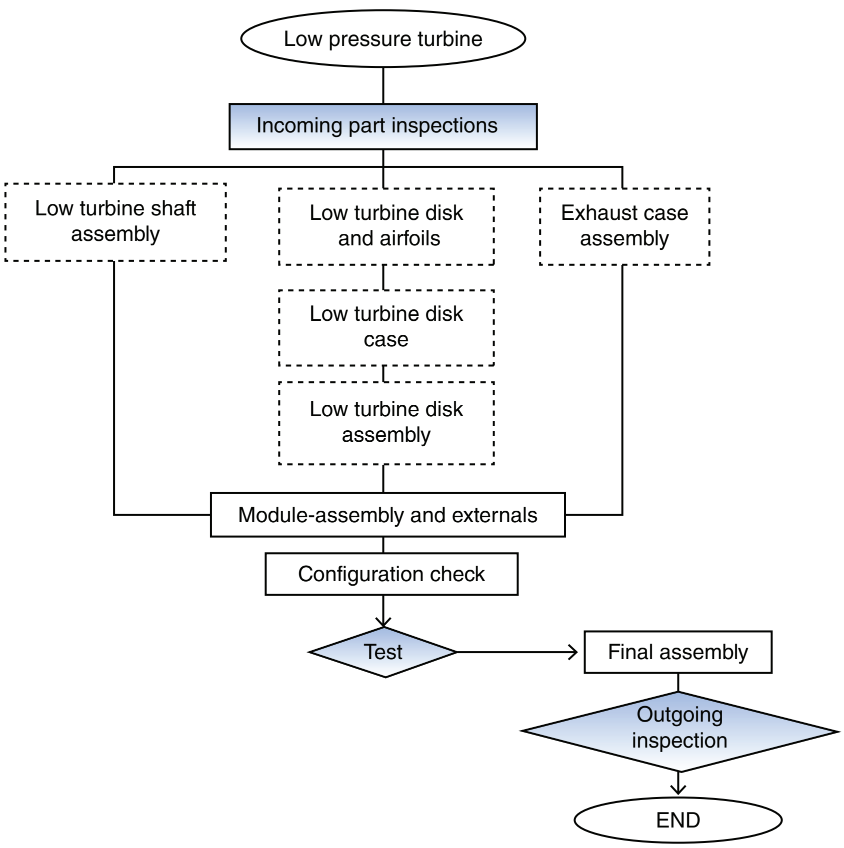
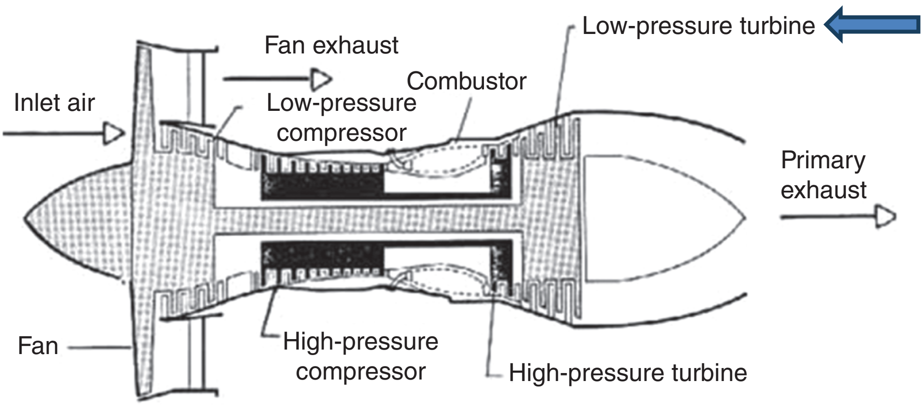


Figure 7.9 Process block diagram for low-pressure turbine manufacturing processes.

manufacturing line. Note that the low-pressure turbine is only one part of a larger manufacturing line for a two-spool turbofan engine.

Two-spool Commercial Turbofan Engine. *Source:* Drawing courtesy of NASA.GOV. Public Domain.



Whether applied to low-pressure turbines or the manufacture of any other product or system, PFMEA eliminates risks that may not be identified if only functional and design FMEAs are performed. It takes failure modes identified in design FMEA and assures that if they relate to defects in manufacturing processes they will be found and eliminated or ameliorated through changes both in process steps and statistical process controls. It feeds information on design changes required to accommodate manufacturing feasibility back to the design community. It identifies operator safety concerns, not only for manufacturing but also for field maintenance. Finally, even when applied to processes outside of manufacturing, PFMEA identifies the effects of process failure on customers and clients; it is invaluable in identifying and eliminating failure modes whenever considerations are given to introducing a new or modified part, product, or process.

To summarize: PFMEA is a tool to focus manufacturing, assembly, business processes, and engineering processes on high-risk and/or critical process steps. PFMEA also uses occurrence, detection, and severity values to determine RPN for prioritization. PFMEA develops corrective action planning or statistical process control measures for more critical process steps. PFMEA methodology is summarized in Figure 7.10.

1. Characterize/map current process
   a. Identify candidate sub-processes
   b. Breakdown entire process into steps/functions
2. Identify potential failure modes, causes and effects
3. Identify current controls
4. Assign values to occurrence, detection and severity to calculate RPN
5. Formulate corrective actions for RPN’s that are highest on Pareto chart of RPNs:
   a. design change
   b. process change
   c. process control measures
6. Recalculate RPN with benefit of additional corrective actions

Figure 7.10 Process FMEA methodology.

Process

Failure Modes and Effects Analysis (PFMEA)

Process Name

FMEA Date (Orig) ____________ (Rev) ____________

Product Step function	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recom mended actions	Resp.	Actions taken	SEV	OCC	DET	R P N
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0

Figure 7.11 PFMEA template.

We employ the form in Figure 7.11 to construct PFMEAs. This form should look familiar since it is nearly identical to the design FMEA template; it differs primarily in that heading for the first column has been changed from Item/Function to Process Step. The PFMEA also parallels the design FMEA as indicated in Figure 7.10.

A significant difference between design and PFMEA is in the construction of the numerical scales for severity, occurrence, and detection tables for PFMEA. Because of the wide variety of processes that may be considered, the construction of the scales may vary; see Table 7.6 (Severity), Table 7.7 (Occurrence), and Table 7.8 (Detection), which show generic classifications.

Table 7.6 Severity ranking.

SEVERITY of effects of failure mode		
Effect	Criteria	Ranking
Hazardous without warning	• May endanger machine or operator • Affects safe operation of product/production and/or involves noncompliance with government regulation • Failure will occur without warning	10
Hazardous with warning	• May endanger machine or operator • Affects safe operation of product/production and/or involves noncompliance with government regulation • Failure will occur with warning	9
Very high	• Major disruption to production • 100% of production may have to be scrapped • Product/equipment inoperable – loss of primary function • Customer very dissatisfied	8
High	• Minor disruption to production • Production may have to be sorted and a portion (<100%) scrapped • Product/equipment operable, but at significantly reduced level of performance, i.e. only primary function(s) • Customer dissatisfied	7

(*Continued*)

Table 7.6 (Continued)

SEVERITY of effects of failure mode		
Moderate	• Minor disruption to production • A portion of production may have to be scrapped (<100%) – no sorting • Product/equipment operable, but at reduced level of performance (some secondary functions inoperable) • Customer dissatisfied	6
Low	• Minor disruption to production • 100% of production may have to be reworked • Product/equipment operable, but at slightly reduced level of performance • Some customers dissatisfied	5
Very low	• Minor disruption to production • Production may have to be sorted and a portion (<100%) reworked • Minor nonconformance to production specification • Defect noticed by average customer	4
Minor	• Minor disruption to production • A portion of production may have to be reworked (<100%) – on-line (not in station) • Minor nonconformance to production specification • Defect noticed by average customer	3
Very minor	• Minor disruption to production • A portion of production may have to be reworked (<100%) – on-line (in station) • Minor nonconformance to production specification • Defect noticed by discriminating customer	2
None	• No effect	1

Table 7.7 Occurrence ranking.

OCCURRENCE of failure mode			
Probability of failure	**Possible failure rates**	**CpK**	**Ranking**
Very high: Failure is almost inevitable	≥1 in 2	<0.33	10
	1 in 3	≥0.33	9
High: Generally associated with processes similar to previous processes that have often failed	1 in 8	≥0.51	8
	1 in 20	≥0.67	7
Moderate: Generally associated with processes similar to previous processes that have experienced occasional failures, but not in major proportions	1 in 80	≥0.83	6
	1 in 400	≥1.00	5
	1 in 2,000	≥1.17	4
Low: Isolated failures associated with similar processes	1 in 15,000	≥1.33	3
Very low: Only isolated failures associated with almost identical processes	1 in 150,000	≥1.50	2
Remote: Failure is unlikely. No failures ever associated with almost identical processes	≤1 in 1,500,000	≥1.67	1

Table 7.8 Detection ranking.

Likelihood of DETECTION of the failure mode		
Detection	**Criteria**	**Ranking**
Almost impossible	No known control(s) available to detect failure mode	10
Very remote	Very remote likelihood current control(s) will detect failure mode	9
Remote	Remote likelihood current control(s) will detect failure mode	8
Very low	Very low likelihood current control(s) will detect failure mode	7
Low	Low likelihood current control(s) will detect failure mode	6
Moderate	Moderate likelihood current control(s) will detect failure mode	5
Moderately high	Moderately high likelihood current control(s) will detect failure mode	4
High	High likelihood current control(s) will detect failure mode	3
Very high	Very high likelihood current control(s) will detect failure mode	2
Almost certain	Current control(s) almost certain to detect the failure mode. Reliable detection controls are known with similar processes	1

Think about severity in the process environment using a parachute as an example:

- If the chute does not open, you probably die, and therefore, the severity is a 10 (failure occurs without warning).
- If you have a "smart chute" that has built-in diagnostics that emit a loud audible alarm telling me it is not going to open.
  - It still does not open but warns me I am about to die, therefore making it a Severity 9 – (not much good).
  - If an added smaller chute deploys, then I can land without dying, and the Severity is a 7 (item operable, but at a reduced level of performance. Customer dissatisfied).

Example 7.4 "Making Coffee" Process FMEA

Suppose that in this exercise we have a coffee maker, and we wish to analyze the failure modes in each step of making a pot of coffee. The first thing that we need is a flow chart. How about a simple one first (Figure 7.12).

That was not too difficult, but if you look at this flow chart and think about the process a bit more, you soon realize there are a lot of "sub-processes" involved. This initial flow chart does not have enough detail. So, if you put a bit more thought into it, working with your team, you may come up with a more detailed flowchart (Figure 7.13).

But OOPS, no ground coffee, so we have a slight diversion from our main flow chart (Figures 7.14a and 7.14b).

Now let us use our flow chart/block diagram to fill in the PFMEA template.

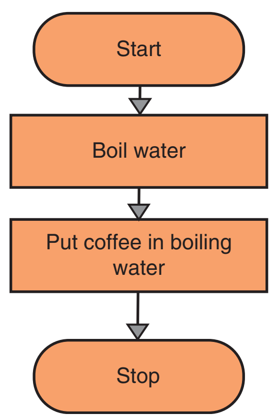


Figure 7.12 Initial flow chart for making coffee.

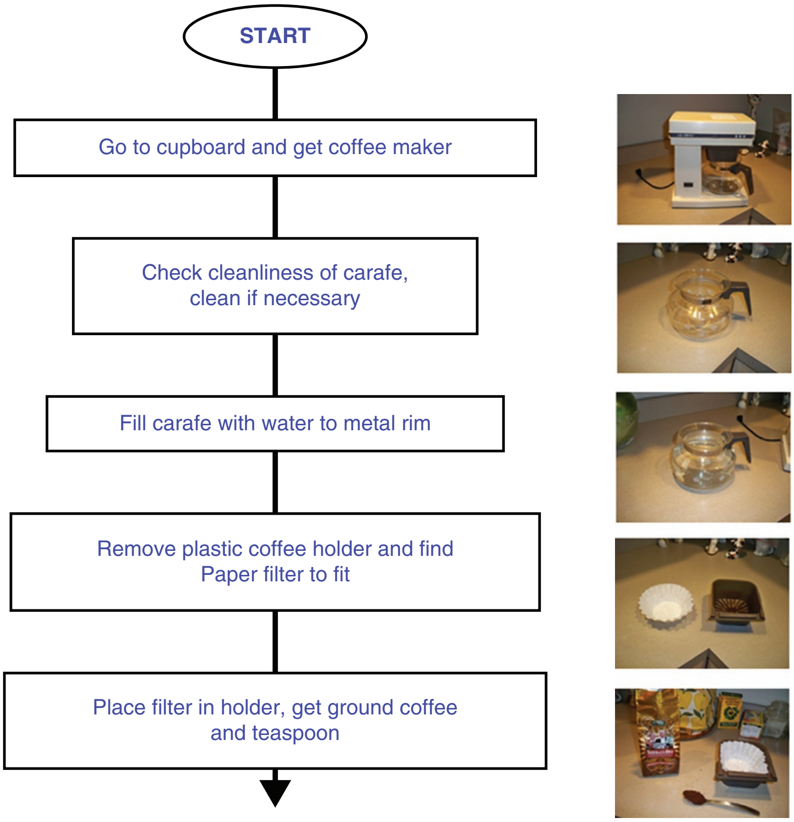


Figure 7.13 Expanded flow chart for making coffee.

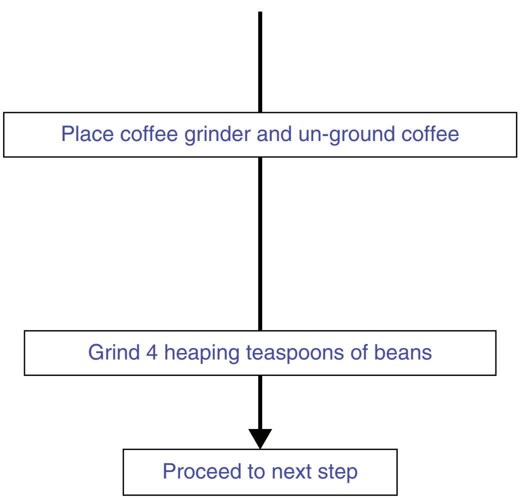


Figure 7.14a Coffee grinding flowchart.

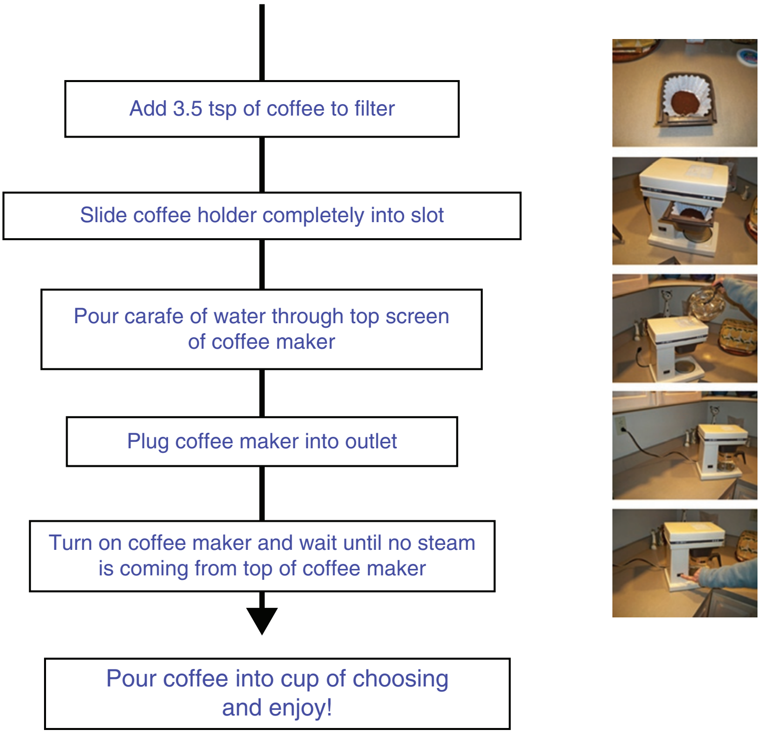


Figure 7.14b Expanded flowchart for making coffee continues.

First, a few reminders:

- RPN has no physical meaning – it is used for **relative** comparison
- Qualitative judgments must be **consistently** applied
- Should always drive actions to reduce risk

  – Severity reduction ideas might include redundancy, redesign, and new material
  – Occurrence reduction might include higher reliability components
  – Higher detection might include improved ability to detect prior to serious effect.

Using our process flow for making coffee and the PFMEA template, following each process step and thinking about what things can fail during that process step, the team completed the initial analysis of the coffee making process (see Figure 7.15).

Now generate a bar chart of the RPNs (this one was done in MINITAB, but you can use any number of programs to do a bar chart). The team decided to work on the high severity and the failure modes in the oval, as indicated in Figure 7.16.

Recommended actions for PFMEAs include:

- Corrective action should be directed first at the highest concerns as rank ordered by RPN.
- The intent of any recommended action is to reduce the occurrence, severity, and/or detection rankings.
- If NO actions are recommended for a specific cause, then this should be indicated.
- *Only a design revision* can bring about a reduction in the severity ranking.

				Process				
		Failure Modes and Effects Analysis (PFMEA)						
Process or Product Name:	Making Coffee					FMEA Date (Orig)_March 15, 2009.		
Process step	**Potential failure mode**	**Potential failure effects**	**SEV**	**Potential causes**	**OCC**	**Current controls**	**DET**	**RPN**
Go to cupboard and get coffee maker	Coffee maker broken	No coffee	10	Broke during/after last use	1	None	10	100
Fill carafe with water to metal rim	Too much water added	Coffee is weak	8	Inattention	3	None	10	240
	Too much water add	Coffee maker overflow	7	Inattention	2	Eyeball on rim	6	84
	Too little water added	Coffee is strong	6	Inattention	2	Eyeball on rim	6	72
Remove plastic coffee holder and find paper filter to fit	No filters available	No coffee	10	Failure to purchase at regular interval	1	None	10	100
	Coffee holder cracked	Coffee drips outside carafe	8	Plastic coffee holder has age hardened	1	None	10	80
Place filter in holder, get ground coffee and teaspoon	Filter placed crooked in holder	Coffee drips outside carafe	4	Inattention	1	Notice as coffee is placed in holder	6	24
	Filter torn	Grounds in coffee	9	Manufacturing defect	1	Inspection as used	4	36
Add 3.5 tsp of coffee to filter	Too little coffee added	Weak coffee	6	Spilled before adding	1	Noticeable spillage	2	12
Slide coffee holder completely into slot	Coffee holder not completely in slot	Coffee/water spills	6	Inattention	1	Inspection as user	1	6
Pour carafe of water through top screen of coffee maker	Water spillage on top/side of coffee maker	Mess to clean up	4	Inattention	1	Inspection as user	1	4
Plug coffee maker into outlet	No power to coffee maker	Coffee maker does not work	6	Inattention	1	Mind on job	1	6
Turn on coffee maker and wait until no steam is coming from top of coffee maker	No electricity	No coffee	10	Circuit breaker tripped	1	Reset breaker	1	10
	Coffee maker switch does not work	No coffee	10	Worn switch	1	Previous use worked	5	50
Pour coffee into cup of choosing	Coffe spillage	Burnt hand or coffee on counter	9	Inattention	3	Focus on task at hand	1	27

Figure 7.15 PFMEA coffee making complete, before process changes.

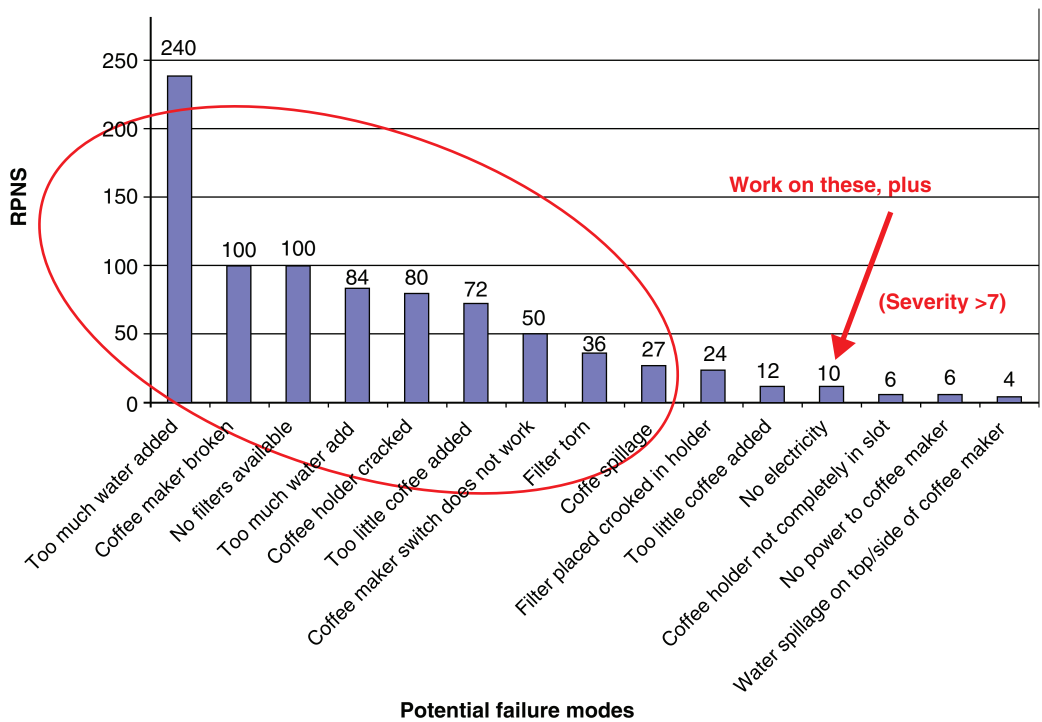


Figure 7.16 Bar chart of coffee PFMEA RPNs.

- To reduce the probability of occurrence, process and/or specification revisions are required.
  - Remove or control the causes.
  - Mistake proofing brings the frequency of occurrence to essentially zero.
- To increase the probability of detection, process control and/or inspection changes are required.
  - Improving detection controls is (typically) costly.
- Emphasis should be placed on preventing, rather than detecting, defects.
- The easy to remember mantra is **"Design it out"** – Improve controls or have controls earlier in the process and make sure lessons learned are passed back to design and are incorporated in the design process.
- **"Test it out"** – things such as environmental stress screening, running each product for xx minutes or hours, and test flights or runs.
- **"Inspect it out"** – if you cannot do the first two, you have no choice, but remember, inspection adds cost without adding value.

Bottom line: Emphasis should be placed on **preventing**, rather than detecting, defects.

After the coffee making team considered all these recommendations, the completed PFMEA is as shown in Figure 7.17.

PFMEA is a tool for preventing and fixing process problems and is a direct link to the control plans that make the improvements permanent. The design of a part is assumed to be correct; hence, the severity portion of a manufacturing PFMEA cannot be changed. In sum, PFMEA is ESSENTIAL for manufacturing and assembly processes and can be extremely useful for business and engineering processes.

Process
Failure Modes and Effects Analysis (PFMEA)

Process or Product Name: Making Coffee   FMEA Date (Orig)_March 15, 2009_________(Rev)________

Process step	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recommended actions	Resp.	Actions taken	SEV	OCC	DET	RPN
Go to cupboard and get coffee maker	Coffee maker broken	No coffee	10	Broke during/after last use	1	None	10	100	Make note at end of coffee maker use it coffee is brewed	JB	Complete	10	1	1	10
Fill carfe with water to metal rim	Too much water added	Coffee is weak	8	Inattention	3	None	10	240	Use coffee cup to measure exactly 4 cups	JB	Complete	8	1	1	8
	Too much water add	Coffee maker overflow	7	Inattention	2	Eyeball on rim	6	84	Use coffee cup to measure exactly 4 cups	JB	Complete	7	1	1	7
	Too little water added	Coffee is strong	6	Inattention	2	Eyeball on rim	6	72	Use coffee cup to measure exactly 4 cups	JB	Complete	6	1	1	6
Remove plastic coffee holder and find Paper filter to fit	No filters available	No coffee	10	Failure to purchase at regular interval	1	None	10	100	Purchase 2 box supply and put note on top of last box	JB	Complete	10	1	1	10
	Coffee holder cracked	Coffee drips outside carafe	8	Plastic coffee holder has age hardened	1	None	10	80	Purchase new coffee maker every 5 years	JB	Complete	8	1	1	8
Place filter in holder, get ground coffee and teaspoon	Filter placed crooked in holder	Coffee drips outside carafe	4	Inattention	1	Notice as coffee is placed in holder	6	24	None			0	0	0	0
	Filter torn	Grounds in coffee	9	Manufacturing defect	1	Inspection as user	4	36	Look at filer before use	JB	Complete	9	1	1	9
Add 3.5 tsp of coffee to filter	Too little coffee added	Weak coffee	6	Spilled before adding	1	Noticeable spillage	2	12	None			0	0	0	0
Slide coffee holder completely into slot	Coffee holder not completely in slot	Coffee/water spills	6	Inattention	1	Inspection as user	1	6	None			0	0	0	0
Pour carafe of water through top screen of coffee maker	Water spillage on top/side of coffee maker	Mess to clean up	4	Inattention	1	Inspection as user	1	4	None			0	0	0	0
Plug coffee maker into outlet	No power to coffee maker	Coffee maker does not work	6	Inattention	1	Mind on job	1	6	None			0	0	0	0
Turn on coffee maker and wait until no steam is coming from top of coffee maker	No electricity	No coffee	10	Circuit breaker tripped	1	Reset breaker	1	10	Make sure power is on and circuit breaker is engaged. Toaster working?)	JB	Complete	10	1	1	10
	Coffee maker switch does not work	No coffee	10	Worn switch	1	Previous use worked	5	50	pay attention to previous use	JB	Complete	10	1	1	10
Pour coffee into cup of choosing	Coffe spillage	Burnt hand or coffee on counter	9	Inattention	3	Focus on task at hand	1	27	Have wife pour coffee (morning person)	JB	Complete	9	1	1	9
								0							0

Figure 7.17 Final FMEA of the “coffee making team.”

7.5 FMEA Summary

FMEA outputs

- Functional FMEA Outputs
  - A list of potential concept failure modes.
  - A list of design actions to eliminate the causes of failure modes or reduce their rate of occurrence.
  - Recommended changes to system design specs.
  - Specific operating parameters as key specifications in the design.
  - Changes to global manufacturing standards or procedures.
- Design FMEA Outputs
  - A list of potential product failure modes.
  - A list of potential reliability critical/significant characteristics.
  - A list of design actions to eliminate the causes of product failure modes, or reduce their rate of occurrence, or improve detection.
  - Confirmation of the Design Verification Plan (DVP).
  - Feedback of design changes.
- Process FMEA Outputs

  - A list of potential process failure modes.
  - A list of confirmed critical characteristics and/or significant characteristics.
  - A list of operator safety and high-impact characteristics.
  - A list of recommended special controls for designated product; special characteristics to be entered on a control plan.
  - A list of processes or process actions to eliminate the causes of product failure modes, or reduce their rate of occurrence, and to improve product defect detection if process capability cannot be achieved.

  Changes to process sheets and assembly drawings.
  FMEA pitfalls that can be prevented!

- During development
  - Not understanding the fundamentals of FMEA
  - Inadequate representation on team from subject matter experts
  - Failure to identify the right inputs to FMEA
  - Poor planning by team lead before assembling for brainstorming and failure ranking.

- During implementation
  - Breaking session into too long a time frame, thus losing continuity
  - Using severity, occurrence, and detection scales not representative of the industry, product, or process group
  - Following too closely the “rigor” of the FMEA tool
  - Wasting time on rating debates
  - Failure to follow through on recommended actions
  - Failure to drive systemic actions
  - Failure to link design and PFMEA learning to control plans, CTQs, and CTP parameters.

- During field operation
  - Not incorporating the identified, mitigated risks into "standard work"
  - Failure to keep FMEA alive.

And, finally, remember:

FMEA is a tool for preventing problems, developing and implementing designs, processes, or services.
Functional FMEAs feed design FMEAs, which in turn feed PFMEAs, which sets in place the control plans.
FMEA helps balance risk with other design requirements.
Pitfalls to be avoided during an FMEA are numerous but surmountable.
Skills needed by FMEA team members include both "soft" and "hard" skills.

Bibliography

Akao, Y. (2004). *QFD: Quality Function Deployment - Integrating Customer Requirements into Product Design*, 1e. Productivity Press. ISBN: ISBN-10: 1563273136.
Ang, A.H.-S. and Tang, W.H. (1984). *Probability Concepts in Engineering Planning and Design*, vol. **2**. New York: Wiley.
Brockley, D. (ed.) (1992). *Engineering Safety*. London: McGraw-Hill.
Burgess, J.A. (1970). Spotting trouble before it happens. *Machine Design* **42** (23): 150.
Guttman, H.R. (1982). *Unpublished lecture notes*. Northwestern University.
Henley, E.J. and Kumamoto, H. (1981). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.
Henley, E.J. and Lynn, J.W. (ed.) (1976). *Generic Techniques in System Reliability Assessment*. Leyden, Holland: Nordhoff.
McCormick, E.J. (1976). *Human Factors in Engineering Design*. New York: McGraw-Hill.
McCormick, N.J. (1981). *Reliability and Risk Analysis*. New York: Academic Press.
Stamatis, D.H. (1995). *Failure Modes and Effect Analysis: FMEA from Theory to Execution*, 2nde. Milwaukee, WI: ASQ Quality Press.

Exercises

7.1 Given the welding FMEA created by six members of the welding department, you have been asked to help them choose the most important failure modes to work on. You have to report back to the team in one day.

Failure Modes and Effects Analysis
(Process FMEA)

Welding shop
___ Subsystems
___ Component: **Design Responsivity:** **Big John** **FMEA Number:**
Prepared by:
FMEA
Model: **Key Date:** **Date (Orig.):**

Core Team: **Welding**

Process step	Potential failure modes	Potential failure effects	Severity	Potential causes	Occurrence	Current controls	Detect	R.P.M	Recommended actions
Working with saws	Throwing sparks	Fire	6	Working adjacent to flammable materials	9	Fire extinguisher nearby	9		
Argon welding	Exposure to fumes and toxic gas	Occupational disease	9	Fail to use appropriate protective masks	8	Exhaust hoods	5		
Electric welding	Throwing sparks	Burning	5	Nature of the process	6	None	4		
	Fall from height	Injuries	9	Working at height	7	Safety training	5		
Cutting metals	Explosion of gas cylinder	Fire and injuries	7	Lack of training and poor maintenance	3	Safety training	8		
CO_2 welding	Flashback flame	Explosion	6	Equipment failure	5	Safety training	5		
Welding	Fire	Fire	5	Fail to separate full and empty cylinders	3	Safety training	8		
	Collision with obstacles	Injuries	6	Improper layout	3	Safety training	4		
	Collision with forklift	Injuries	6	No warning device	7	Safety training	4		
	Hearing loss	Deafness	6	High noise levels at work place	8	Wear proper gear	3		

7.2 In reviewing the welding FMEA in Exercise 7.1, can you fill in some of the recommended actions? Also, notice that "safety training" is a very common current control. Safety training (and retraining) is not a positive cure for failure modes. For each of the failure modes with that current control, you need to propose a REAL control not just "safety training."

7.3 Supermarket self-checkout process checkout. The self-checkout machine (example to the right).

You have seen the self-service checkout kiosks at your local supermarket. An alternative to checkout lanes staffed by cashiers is that they are introduced to offer customers more *control*, *convenience*, and a *speedier checkout option*. While retailers claim to install them to improve customer service, we also know these machines can help them redeploy their cashiers.

Key user needs

The self-checkout option is meant for shoppers who want a quick exit and prefer using the machines to dealing with store personnel. In a 2004 survey by research company IDC, respondents saw the following key benefits of self-checkout kiosk:

(1) Shorter lines, (2) Faster checkout, (3) Control, (4) Privacy, (5) Greater accuracy than checkout operator, and (6) choice of checkout

Self-checkout process pieces:
1. Lane light/store attendant call
2. Touch screen monitor
3. Basket stand
4. Barcode scanner cum weighing scale
5. Payment module
6. ATM PIN pad

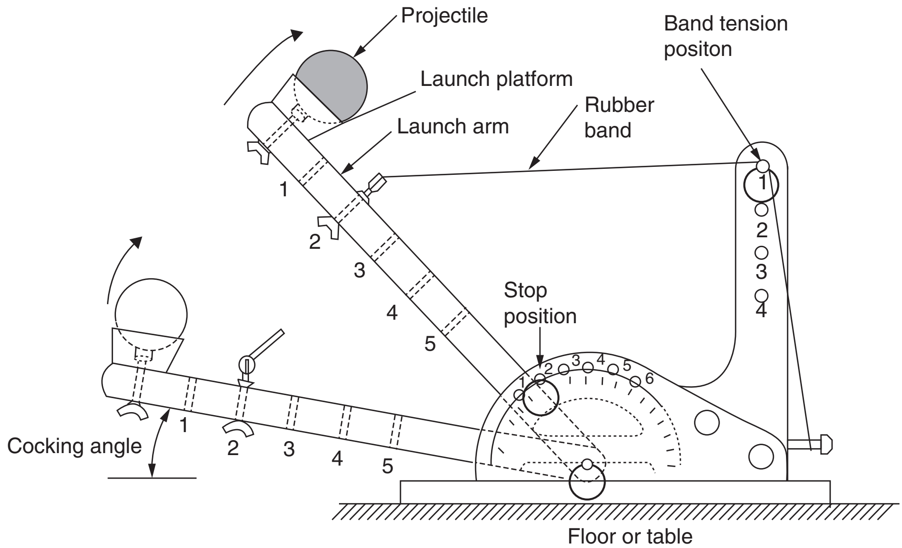
Create a process flow chart of the self-checkout process for a machine like the one illustrated.

For background, see: http://web.mit.edu/2.744/www/Project/Assignments/humanUse/lynette/2-About%20the%20machine.html

Source: By Ben Schumin – Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=17057288

7.4 (3–4 person exercise) The Romans and others until ~1200 AD used catapults in warfare. Today, a model catapult is often used to teach design of experiments. One such catapult is illustrated here:

The four variables are:



The four variables are:
1. Cocking angle (90–180°) - measured with a protractor
2. Launch position (1–5)
3. Band tension position (1–4)
4. Stop position (1–6)

Foam balls are used as the projectiles (for safety). A single rubber band is used for propulsive power.

Construct a process FMEA for this catapult, realizing that it must be used on a carpeted floor, will launch a foam ball no more than 20', and a tape measure must be used for the distance measurement as well as a sheet of paper to record (a typical 16 run experiment that varies each of the variables according to a 2^4 factorial experiment and is below) (If you know a statistician or Six Sigma BB or MBB or equivalent in your organization, contact them for the loan of a STATAPULT™).

RunOrder	CenterPt	Blocks	Hook pos.	Stop pos.	Angle	Launch	Distance
1	1	1	3	5	180	1	
2	1	1	1	5	130	1	
3	1	1	1	3	180	1	
4	1	1	1	3	130	3	
5	1	1	1	5	180	1	
6	1	1	1	3	180	3	
7	1	1	1	5	130	3	
8	1	1	3	3	130	1	
9	1	1	1	5	180	3	
10	1	1	3	5	130	1	
11	1	1	3	5	130	3	
12	1	1	3	5	180	3	
13	1	1	3	3	130	3	
14	1	1	3	3	180	3	
15	1	1	1	3	130	1	
16	1	1	3	3	180	1	

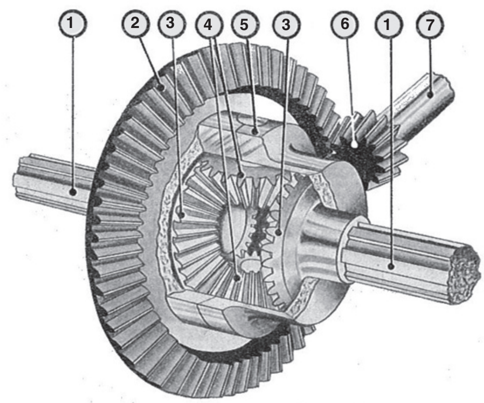
16 run experiment for STATAPULT. The follow-on to this exercise is to model the distance as a function of all factors and then pick a random distance and using MINITAB find the settings that are based on your data. Tke six "launches" and see how tight your standard deviation is.

7.5 (3–4 person team exercise) Bicycle FMEA. Items to include:
- Body [excluding accessories (mudguard, bell, reflectors, etc.)]
- Power transmission (gears, pedals, chain, etc.) excluding tires
- Brakes (cable, levers, pads)

You and your team pick the bicycle type, brand, etc.
See https://wiki.ece.cmu.edu/ddl/index.php/Bicycle_drivetrain for parts list

7.6 *Late to work* Process FMEA. Flow chart your activities from waking up in the morning to getting to your workstation. Then, take each item of the flow chart and use it to complete a process FMEA to find your highest RPN and how hence to accomplish "getting to work" easier/more efficiently.

7.7 SAE Formula cars usually use a chain, sprocket, differential for the transfer of power to engine to the axles. Components for this application vary but generally look like:



Roller chain and Differential (creative commons)

Source: EBERT/CC BY-SA 3.0.

An SAE formula team FMEA contained the following portion with these items. Using this as a beginning, complete the FMEA through recommended actions.

Item	Function	Potential failure mode	Potential effects of failure	SEV	Potential cause of failure	OCC	Current design controls	DET	RPN	Recommended actions	Actions taken	SEV	OCC	DET	RPN
Chain	Transfers torque from engine to differential sprocket	Insufficient torque	Nonuniform torque transfer	4	Wear due to insufficient lubrication, improper material selection	5	Inspection	5							
		Link breakage	Insufficient torque jerking	4	Misassembly improper siding, link stretch	4	Inspection	5							
		Fatigue	Variation in torque transfer	4	Cyclic tensile load on the tight side of the chain due to applied torque and centrifugal force	4	Inspection	4							
Sprocket	Transfers torque from chain to differential	Nonuniform torque transfer	Differential will not receive the uniform torque	5	Wear	4	Inspection	4							
		Jerking noises	Uneven torque transfer	5	Tooth crack tooth breakage	4	Inspection	4							
		Uneven torque	Differential receives varying torque	4	Improper installation leading to improper engagement, i.e. slipping between sprocket tooth and chain shoe	4	Inspection	4							
Differential	Transfers torque from sprocket to each axle	Uneven torque transfer	Axles will receive uneven torques, one more and other less	4	Wear misassembly loosening of carrier bolts	4	Inspection assembly procedures	4							
		No drive transfer to the axles	Vehicle does not move	6	Gearbox bearing seize	3	Prerace inspection	3							
		Insufficient drive transfer	Axles does not get sufficient drive	5	Gear teeth stripped	4	Prerace inspection	4							
		Lack of drive transfer	No sufficient drive from gear box	5	Improper lubrication low oil level	4	Prerace inspection	4							

7.8 FMEA of windshield wiper during cold weather conditions.

Using the three items, wiper blades, wiper arm, and wiper motor, to complete an FMEA considering cold weather operation only. To include RPN, corrective actions, modified severity, detection and occurrence, and modified RPN.

Failure mode and effect analysis (FMEA) for automotive windshield wiper/washer system during cold weather conditions

Windshield wiper

No	Item	Function/purpose	Failure mode	Subsystem effects(s) of failure	System effects(s) of failure	Severity	Detection	Cause(s)	OCC	DET	SEV	RPM	Corrective actions(s)/ status	OCC	DET	SEV	RPM
1	Wiper blades	Maintain visibility by wiping away rain, snow, and dirt off windshield	Rubber material rips/ tares	Loss of visibility, streaks on windshield	Difficulty driving, cannot see road	4	Visible by eye	Worn out, bad material	5	1	5						
			Rubber material degrades due to sun	Loss of visibility, streaks on windshield	Difficulty driving, cannot see road	4	Visible by eye	Worn out, bad material	4	1	5						
			Blade frame ices/freezes	Loss of visibility, blade does not clean windshield	Difficulty driving, cannot see road	2	Visible by eye	Moisture, snow, sleet, build up during snowy or cold conditions	6	1	7						
			Dirty blades	Loss of visibility, dirt residue smear	Difficulty driving, cannot see road	4	Visible by eye	Dirt, sand, and salt build up	9	1	3						
2	Wiper arm	Hold wiper blades	Corrosion	Loss of strength to arm	Appearance, difficult to remove wipers	4	Visible by eye	Bad paint, lack of washing area	1	1	2						
			Loss of tension	Loss of visibility, streaks on windshield	Difficulty driving, cannot see road	4	Blades not touching properly	Fatigue to spring	3	1	3						
3	wiper motor	Operate the wipers	Bums out	Loss of visibility, cannot move arm	Difficulty driving, cannot see road	2	Do not hear motor	Worn out, bad material	2	1	8						
			Blown fuse	Loss of visibility, cannot move arm	Difficulty driving, cannot see road	2	No operation after flip switch	Operate wipers when frozen to windshield	6	1	3						

7.9 Complete the following partial design FMEA and select the first next step.

Line reference	Function	Potential failure mode	Potential effect of failure	SEV	Potential causes	OCC	Current design controls	DET	RPX
1	Power switch providing on/off function to a power tool	Switch unable to turn on unit	No power	7	Worn parts	6	Select part rated for expected use; power cycling life test	3	
2		Switch intermittent behavior	Notable to power off tool	9	Corroded contacts	4	Select part rated for expected environment; power cycling life test	2	
3		Switch unable to turn unit off	Notable to power off tool	9	Switch hard to reach when operating	2	Switch has high contract color; power cycling life test	3	

- Provide an alternate means to power on the unit to lower the detection score of line 1
- Provide an alternate means to power down the unit to lower the occurrence score of line 2
- Provide an alternate location of the switch to lower the occurrence score of line 3
- Provide a safety switch that bypasses the power switch to reduce the severity score of lines 2 and 3

7.10 Baking cookies is a favorite FUN pastime for an FMEA. You can use your favorite recipe or use this one:

PUMPKIN CHOCOLATE CHIP COOKIES

MIX TOGETHER

1 ½ cups Olive Oil — 1 ½ tsp Vanilla
¾ cup Honey — 1 can (15 oz.) Pumpkin (***not*** Pie Mix)

ADD and MIX,

3 cups Whole Wheat Flour — 1 tsp Salt
1 ½ tsp Baking Soda — 3 cups Oatmeal (uncooked)
½ tsp Baking Powder — 1 cup Walnuts
1 ½ tsp Cinnamon — 1 cup Chocolate Chips

Batter should be rather thick; if not, add a little milk; if a little too thin, add a little flour or oatmeal.
Drop by spoonfuls on cookie sheet.
Bake in 350deg pre-heated oven for 20-25 min. until cookies are slightly firm.
Cool and enjoy. Since there are no preservatives, refrigerate/freeze if there are any left after a day or so.so.

Do a process flow of the baking process, noting possible failure modes in each stage, and then
do an FMEA of the process.

7.11 Pick out the best answer in each of these multiple choice questions (put your ENGINEERING hat on):

a) When prioritizing actions to be taken in an FMEA, which of the following priority rankings should be considered first?
   - Overall RPN (Risk Priority Number)
   - Highest severity ranking
   - Highest occurrence ranking
   - Highest severity times occurrence ranking.

b) An FMEA is being constructed for the manufacture of a syringe cartridge. The team has developed risk ranking scale criteria for calculating the Risk Priority Number (RPN). The team has assigned 5 values for ranking likelihood of occurrence (O), 10 values for ranking the risk associated with severity (S), and 5 values for ranking the risk associated with detection (D). Using this method will most likely:
   - Ensure all values for O, S, and D are equally represented in RPN
   - Give severity a disproportionate representation in RPN
   - Give occurrence and severity an equal representation in RPN
   - Ensure RPN reflects the priority for addressing failure modes

c) Which of following is NOT a part of Risk Priority Number for FMEA?
   - Severity.
   - Catastrophic.
   - Occurrence.
   - Detection.

d) All of the following are examples of design FMEA detection controls EXCEPT for:
   - Whole system testing
   - Finite Element Analysis (FEA)
   - Lab testing
   - Adding extra thickness to a part's notched area

e) The intent of a recommended action in an FMEA is to reduce rankings in which of the following orders of priority?
   - Severity, Occurrence, Detection
   - Occurrence, Severity, Detection
   - Severity, Detection, Occurrence
   - Occurrence, Detection, Severity

f) A potential infant mortality failure has been identified as the failure mode with the highest RPN in a design FMEA. What should you do next?
   - Take no action until the failure modes actually occur.
   - Tell the boss that reliability targets will not be achieved.
   - Start a team to identify possible factors that can cause poor product quality during manufacturing in order to identify corrective action for this failure mode.
   - Institute a burn-in test for each product to find infant mortality failure modes before delivery to the customer.

g) A potential failure mode for an electronics device is the complete inability of the power switch to activate (or power on) the device. In an FMEA, this failure mode would be considered in which category?

- No function
- Partial degraded function
- Intermittent function
- Unintended function

h) Which of the following is a good design control to reduce severity or occurrence that is identified in a design FMEA?
- Change the system requirements to reduce system function
- Add additional inspection(s) in production
- Enhance design validation testing
- Modify the design to reduce stress on a component.

Supplement 1: Shortcut Tables for Stalled FMEA Teams

One additional thought on severity, occurrence, and detection.

If a 1–10 scale is causing "analysis paralysis" (i.e. continuous arguing over whether it is "6" or "7", etc.)

Use 1–4–7–10 *only* for each of severity, occurrence, and detection. Remember, an FMEA is a qualitative upfront tool to help prevent failure modes from occurring. … NOT an exact science!

The modified severity, occurrence, and detection tables for a 1–4–7–10 approach.

Figure 7 Sup1.1 Modified ranking severity, occurrence, and detection tables.

SEVERITY of effects of failure mode		
Effect	**Criteria**	**Ranking**
Hazardous-without warning	• May endanger machine, or operator • Affects safe operation of product / production and / or involves non-compliance with government regulation • Failure will occur without warning	10
High	• Minor disruption to production • Production may have to be sorted and a portion (<100%) scrapped • Product / equipment operable, but at significantly reduced level of performance, ie. only primary function(s) • Customer dissatisfied	7
Very low	• Minor disruption to production • Production may have to be sorted and a portion (<100%) re-worked • Minor non-conformance to production specification • Defect noticed by average customer	4
None	• No effect	1

OCCURRENCE of failure mode			
Probability of failure	**Possible failure rates**	**CpK**	**Ranking**
Very high: Failure is almost inevitable	≥ 1 in 2	< 0.33	10
High: Generally associated with processes similar to previous processes that have often failed	1 in 20	≥ 0.67	7
Moderate: Generally associated with processes similar to previous processes which have experienced occasional failures, but not in major proportions	1 in 2,000	≥ 1.17	4
Remote: Failure is unlikely. No failures ever associated with almost identical processes	≤ 1 in 1,500,000	≥ 1.67	1

Likelihood of DETECTION of the failure mode		
Detection	**Criteria**	**Ranking**
Almost impossible	No known control(s) available to detect failure mode	10
Very low	Very low likelihood current control(s) will detect failure mode	7
Moderately high	Moderately high likelihood current control(s) will detect failure mode	4
Almost certain	Current control(s) almost certain to detect the failure mode. Reliable detection controls are known with similar processes	1

Supplement 2: Future Changes in FMEA Approaches

Changes are being made to FMEAs (Failure Mode and Effects Analysis) by the AIAG (Automotive Industries Advisory Group. The new AIAG-VDA FMEA Handbook comes out periodically as changes are made in FMEA thinking since the AIAG FMEA Handbook is used by most of the auto industry. A great deal of the AIAG Handbook is based on the cooperative work of Fiat Chrysler, GM, and Ford on SAE J1739, "Potential Failure Mode and Effects Analysis in Design (design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (process FMEA) and Effects Analysis for Machinery (Machinery FMEA)", first published in 2002, with updates since.

Other industries have their own homegrown FMEA templates that will have minor changes in format. An example is Department of Defense.

The DFMEA and PFMEA templates here are generic, as are the severity–occurrence–detection tables.

Supplement 3: DFMEA and PFMEA Forms

Figure 7 Sup3.1 Design FMEA template.

						Design									
				Failure Modes and Effects Analysis (DFMEA)											
Part/ Product Name						FMEA Date (Orig) ______________ (Rev) ______________									
Product/ part function	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recom mended actions	Resp.	Actions taken	SEV	OCC	DET	R P N
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0

Figure 7 Sup3.2 Process FMEA template.

						Process									
				Failure Modes and Effects Analysis (PFMEA)											
Process Name						FMEA Date (Orig) ______________ (Rev) ______________									
Process step function	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current controls	DET	RPN	Recom mended actions	Resp.	Actions taken	SEV	OCC	DET	R P N
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0
								0							0

8

Loads, Capacity, and Reliability

"Adopt a self-reliant attitude to "own your work."
Invest the time necessary to be sure of yourself and your designs."
Source: Stan R. Caldwell; SEC 20: 5 Tips for Structural Engineers: Become the Best Version of Yourself. Retrieved from: https://engineeringmanagementinstitute.org/tsec-20-top-5-tips-structural-engineers/

8.1 Introduction

In the preceding chapters, failure rates were used to emphasize the strong dependence of reliability on time. Empirically, these failure rates are found to increase with system complexity and also with loading. In this chapter, we explore the concepts of loads and capacity and examine their relationship to reliability. This examination allows us both to relate reliability to traditional design approaches using safety factors and to gain additional insight into the relations between failure rates, infant mortality, random failures, and aging.

Safety factors and margins are defined in the following way: Suppose that we define l as the load on a system, structure, or piece of equipment and c as the corresponding capacity. The safety factor is then defined as

$$v = \frac{c}{l} \tag{8.1}$$

Alternately, the safety margin may be used. It is defined by

$$m = c - l \tag{8.2}$$

Failure then occurs if the safety factor falls to a value less than 1, or if the safety margin becomes negative.

The concepts of load and capacity are employed most widely in structural engineering and related fields, where the load is usually referred to as stress, and the capacity as strength. However, they have much wider applicability. For example, if a piece of electric equipment is under consideration, we may speak of electric load and capacity. A telecommunications system load and capacity may be measured in terms of telephone calls per unit time, and for an energy conversion system thermal units for load and capacity may be used. The point is that a wide variety of applications can be

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

formulated in terms of load and capacity. For a given application, however, l and c must have the same units.

In the traditional approach to design, the safety factor or margin is made large enough to more than compensate for uncertainties in the values of both the load and the capacity of the system under consideration. Thus, although these uncertainties cause the load and the capacity to be viewed as random variables, the calculations are deterministic, using for the most part the best estimates of load and capacity. The probabilistic analysis of loads and capacities necessary for estimating reliability clarifies and rationalizes the determination and use of safety factors and margins. This analysis is particularly useful for situations in which no fixed bound can be put on the loading, for example, with earthquakes, floods, and other natural phenomena, or for situations in which flaws or other shortcomings may result in systems with unusually small capacities. Similarly, when economics rather than safety is the primary criteria for setting design margins, the trade-off of performance versus reliability can best be studied by examining the increase in the probability of failure as load and capacity approach one another.

The expression for reliability in terms of the random variables **l** and **c** comes from the notion that there is always some small probability of failure that decreases as the safety factor is increased. We may define the failure probability as

$$p = P\{\mathbf{l} \geq \mathbf{c}\} \tag{8.3}$$

In this context, the reliability is defined as the nonfailure probability or

$$r = 1 - p \tag{8.4}$$

which may also expressed as

$$r = P\{\mathbf{l} < \mathbf{c}\} \tag{8.5}$$

In treating loads and capacities probabilistically, we must exercise a great deal of care in expressing the types of loads and the behavior of the capacity. If this is done, we may use the resulting formalism not only to provide a probabilistic relation between safety factors and reliability but also to gain a better understanding of the relations between loading, capacities, and the time dependence of failure rates as exhibited, for example in the bathtub curve.

In Section 8.2, we develop reliability expressions for a single loading, and then, in Section 8.3, relate the results to the probabilistic interpretation of safety factors. In Section 8.4, we take up repetitive loading to demonstrate how the time dependence of failure rate curves stems from the interactions of variable loading with capacity variability and deterioration. In Section 8.5, a failure rate model for the bathtub curve is synthesized in which variable capacity, variable loading, and capacity deterioration, respectively, are related to infant mortality, random failures, and aging.

8.2 Reliability with a Single Loading

In this section, we derive the relations between load, capacity, and reliability for systems that are loaded only once. The resulting reliability does not depend on time, for the reliability is just the probability that the system survives the application of the load. Nevertheless, before the expressions for the reliability can be derived, the restrictions on the nature of the loads and capacity must be clearly understood.

Load Application

In referring to the load on a system, we are in fact referring to the maximum load from the beginning of application until the load is removed. Figure 8.1 indicates the time dependence of several loading patterns that may be treated as single on loading *l*, provided that appropriate restrictions are met.

Figure 8.1a represents a single loading of finite duration. Missiles during launch, flashbulbs, and any number of other devices that are used only once have such loadings. Such one-time-only loads are also a ubiquitous feature of manufacturing processes, occurring, for instance when torque is applied to a bolt, or pressure is applied to a rivet. Loading often is not applied in a smooth manner, but rather as a series of shocks, as shown in Figure 8.1b. This behavior would be typical of the vibrational loading on a structure during an earthquake and of the impact loading on an aircraft during landing. In many situations, the extreme value of many short-time loadings may be treated as a single loading, provided that there is a definite beginning and end to the disturbance giving rise to it.

The duration of the load in Figure 8.1a and b is short enough that no weakening of the system capacity takes place. If no decrease in system capacity is possible, the situations shown in Figure 8.1c and d may also be viewed as single loadings, even though they are not of finite duration. The loading shown in Figure 8.1c is typical of the dead loads from the weight of structures; these increase during construction and then remain at a constant value. This formulation of the loading is widely used in structural analysis when the load-bearing capacity not only may remain constant but may in some instances increase somewhat with time because of the curing of concrete or the work-hardening of metals.

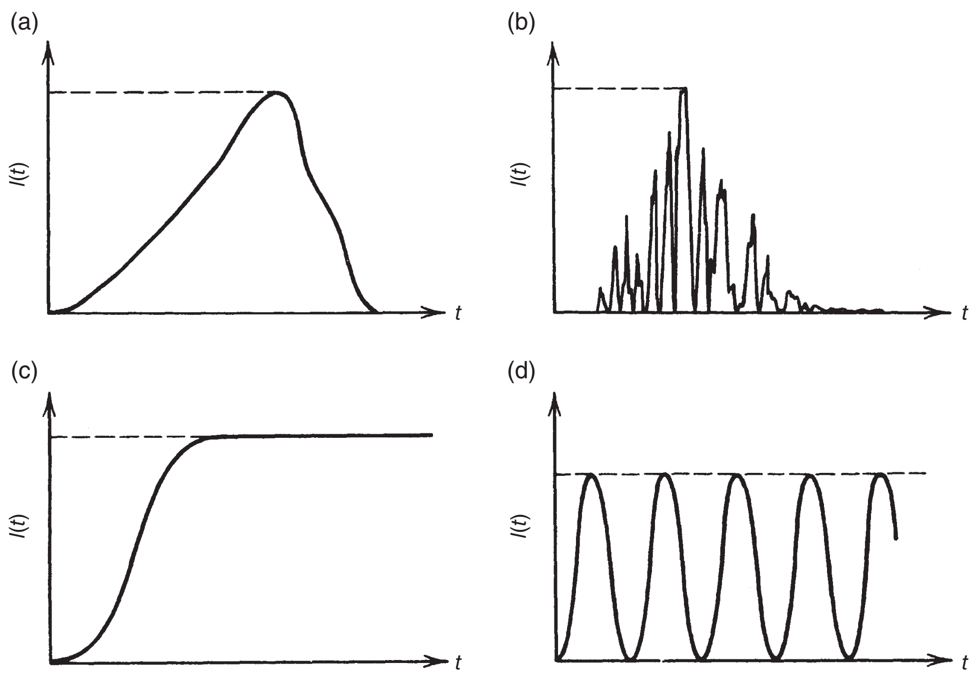


Figure 8.1 Time-dependent loading patterns.

Subject to the same restrictions, the patterns shown in Figure 8.1d may be viewed as a single loading. Provided the peaks are of the same magnitude, the system will either fail the first time the load is applied or will not fail at all. Under such cyclic loading, however, the assumption that the system capacity will not decrease with time should be suspected. Metal fatigue and other wear effects are likely to weaken the capacity of the system gradually. Similarly, if the values of peak magnitudes vary from cycle to cycle, we must consider the time dependence of reliability explicitly, as in Section 8.4.

Thus far, we have assumed that a system is subjected to only one load and that reliability is determined by the capacity of the system as a whole to resist this load. In reality, a system is invariably subjected to a variety of different loads; if it does not have the capacity to sustain any one of these, it will fail. An obvious example is a piece of machinery or other equipment, each of whose components are subjected to different loads; failure of any one component will make the system fail. A more monolithic structure, such as a dam, is subject to static loads from its own weight, dynamic loads from earthquakes, flood loadings, and so on. Nevertheless, the considerations that follow remain applicable, provided that the loads are considered in terms of the probability of a particular failure mode or of the loading of a particular component. If the failure modes can be assumed to be approximately independent of one another, the reliability of the overall system can be calculated as the product of the failure mode reliabilities, as discussed in Chapter 3.

Definitions

To derive an expression for the reliability, we must first define independent PDFs for the load, **1**, and for the capacity, **c**. Let

$$f_l(l)\,dl = P\{l \le \mathbf{l} \le l + dl\} \tag{8.6}$$

be the probability that the load is between l and $l + dl$. Similarly, let

$$f_c(c)\,dc = P\{c \le \mathbf{c} < c + dc\} \tag{8.7}$$

be the probability that the capacity has a value between c and $c + dc$. Thus, $f_{ll}(l)$ and $f_{\mathbf{c}}(c)$ are the necessary PDFs; we include the subscripts to avoid any possible confusion between the two. The corresponding CDFs may also be defined. They are

$$F_{\mathbf{c}}(c) = \int_0^c f_{\mathbf{c}}(c')\,dc' \tag{8.8}$$

$$F_l(l) = \int_0^l f_l(l')\,dl' \tag{8.9}$$

We first consider a system with a known capacity c and a distribution of possible loads, as shown in Figure 8.2a. For fixed c, the reliability of the system is just the probability that $\mathbf{1} < c$, which is the shaded area in the figure. Thus,

$$r(c) = \int_0^c f_l(l)\,dl \tag{8.10}$$

The reliability, therefore, is just $F_1(c)$, the CDF of the load evaluated at c. Clearly, for a system of known capacity, the reliability is equal to one as $c \to \infty$, and to zero as $c \to 0$.

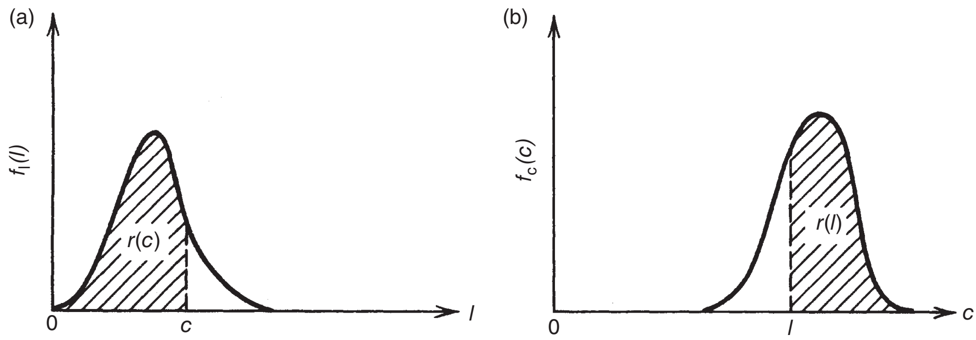


Figure 8.2 Area interpretation of reliability: (a) variable load, fixed capacity and (b) variable capacity, fixed load.

Now suppose that the capacity also involves uncertainty; it is described by the PDF $f_c(c)$. The expected value of the reliability is then obtained from averaging over the distribution of capacities:

$$r = \int_0^\infty r(c)\, f_c(c)\, dc \tag{8.11}$$

Substituting in Eq. (8.10), we have

$$r = \int_0^\infty \left[\int_0^c f_l(l)\, dl\right] f_c(c)\, dc \tag{8.12}$$

The failure probability may then be determined from Eq. (8.4) to be

$$p = 1 - \int_0^\infty \left[\int_0^c f_l(l)\, dl\right] f_c(c)\, dc \tag{8.13}$$

Alternately, we may substitute the condition on the load PDF,

$$\int_0^c f_l(l)\, dl = 1 - \int_c^\infty f_l(l)\, dl \tag{8.14}$$

into Eq. (8.12). Then, using the condition

$$\int_0^\infty f_c(c)\, dc = 1 \tag{8.15}$$

we obtain for the failure probability

$$p = \int_0^\infty \left[\int_c^\infty f_l(l)\, dl\right] f_c(c)\, dc \tag{8.16}$$

As shown in Figure 8.3, the probability of failure is loosely associated with the overlap of the PDFs for load and capacity in the sense that if there is no overlap, the failure probability is zero, and $r = 1$.

Example 8.1 The bending moment on a match stick during striking is estimated to be distributed exponentially. It is found that match sticks of a given strength break 20% of the time. Therefore, the manufacturer increases the strength of the matches by 50%. What fraction of the strengthened matches are expected to break as they are struck?

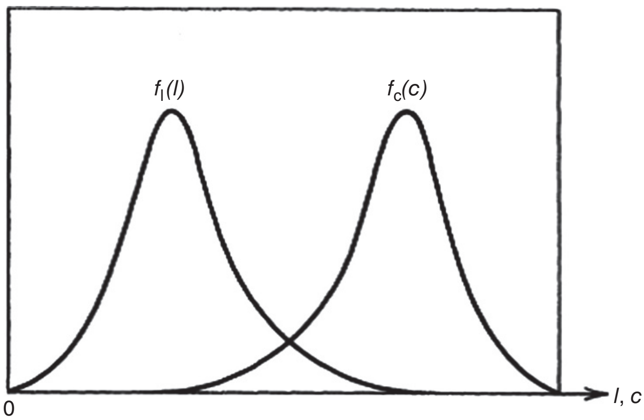


Figure 8.3 Graphical reliability interpretation with variable load and capacity.

Solution:
Assume that the strength (capacity) is known; then, for the standard matches, we have

$$0.8 = r = \int_0^c f_l(l)\,dl = \int_0^c \lambda e^{-\lambda l}\,dl = 1 - e^{-\lambda c}$$

Therefore, $e^{-\lambda c} = 0.2$ or $\lambda c = -\ln(0.2)$, where λ is the unknown parameter of the exponential loading distribution. For the strengthened matches

$$r' = \int_0^{1.5c} f_l(l)\,dl = \int_0^{1.5c} \lambda e^{-\lambda l} dl = 1 - e^{-1.5\lambda c}$$

$$p' \equiv 1 - r' = \exp\left[+1.5 \times \ln(0.2)\right] = 0.2^{1.5} = 0.089$$

Thus, about 9% of the strengthened matches are expected to break.

Another derivation of r and p is possible. Although the derivation may be shown to yield results that are identical to Eqs. (8.12) and (8.13), the intermediate results are useful for different sets of circumstances. To illustrate, let us consider a system with known load but uncertain capacity represented by the distribution $f_c(c)$. The reliability for this system with known load is then given by the shaded area in Figure 8.2b.

$$r(l) = \int_l^{\infty} f_c(c)\,dc \tag{8.17}$$

or equivalently,

$$r(l) = 1 - \int_0^l f_c(c)\,dc \tag{8.18}$$

For a system in which the load is also represented by a distribution, the expected value of the reliability is obtained by averaging over the load distribution,

$$r = \int_0^{\infty} f_l(l)\,r(l)\,dl \tag{8.19}$$

or more explicitly,

$$r = \int_0^\infty f_l(l) \left[\int_l^\infty f_c(c)\, dc \right] dl \tag{8.20}$$

Similarly, we may consider the variation of the capacity first in deriving an expression for the failure probability. For a system with a fixed load, the failure probability will be the unshaded area under the curve in Figure 8.2b:

$$p(l) = \int_0^l f_c(c)\, dc \tag{8.21}$$

Then, averaging over the distribution of loads, we have

$$p = \int_0^\infty f_l(l) \left[\int_0^l f_c(c)\, dc \right] dl \tag{8.22}$$

It is easily shown that Eqs. (8.12) and (8.20) are the same. First, write Eq. (8.12) as the double integral

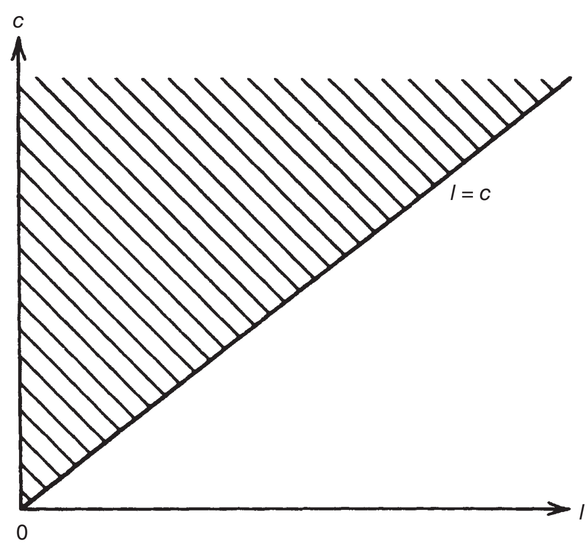
$$r = \int_0^\infty \left[\int_0^c f_c(c)\, f_l(l)\, dl \right] dc \tag{8.23}$$

where the shaded domain of integration appears in Figure 8.4. If we reverse the order of integration, taking the c integration first, we have

$$r = \int_0^\infty \left[\int_1^\infty f_c(c)\, f_l(l)\, dc \right] dl \tag{8.24}$$

Putting $f_{[1}(l)$ outside the integral over c, we obtain Eq. (8.20).

Figure 8.4 Domain of integration for reliability calculation.



To recapitulate, Eqs. (8.12) and (8.20) may be shown to be identical, as may Eqs. (8.16) and (8.22). However, the intermediate results for $r(c)$, $p(c)$, $r(l)$, and $p(l)$ are useful when considering systems whose capacity varies little compared to their load or vice versa.

8.3 Reliability and Safety Factors

In the preceding section, reliability for a single loading is defined in terms of the independent PDFs for load and capacity. Similarly, it is possible to define safety factors in terms of these distributions. Two of the most widely accepted definitions are as follows. In the central safety factor, the values of load and capacity in Eq. (8.1) are taken to be the mean values

$$\bar{l} = \int_{-\infty}^{\infty} l f_l(l)\, dl \tag{8.25}$$

$$\bar{c} = \int_{-\infty}^{\infty} c f_c(c)\, dc \tag{8.26}$$

Thus, the safety factor is

$$\nu = \bar{c}/\bar{l} \tag{8.27}$$

There is a second alternative if we express the safety factor in terms of the most probable values l_o and c_0 at the load and capacity distributions. The safety factor in Eq. (8.1) is then

$$\nu = c_0/l_0 \tag{8.28}$$

These definitions are naturally associated with loads and capacities represented in terms of normal or lognormal distributions, respectively. Then, the reliability can be expressed in terms of the safety factor along with measures of the uncertainty in load and capacity. Other distributions may also be used in relating reliability to safety factors. Such is the case with the extreme-value distribution. With such analysis, the effects of design changes and quality control can be evaluated. Design determines the mean, $\bar{c}$, or most probable value, c_0, of the capacity, whereas the degree of quality control in manufacture or construction influences primarily the variance of $f_{\mathbf{c}}(c)$ about the mean. Similarly, the conditions under which operations take place determine the load distribution $f_1(l)$ as well as the mean value $\bar{l}$.

Normal Distributions

The normal distribution is widely used for relating safety factors to reliability, particularly when small variations in materials and dimensional tolerances and the inability to determine loading precisely make capacity and load uncertain. The normal distribution is appropriate when variability in loads, capacity, or both is caused by the sum of many effects, no one of which is dominant. An appropriate example is the load and capacity of an elevator large enough to carry several people. Since the load is the sum of the weights of the people, the variability of the weight is likely to be very close to a normal distribution for the reasons discussed in Chapter 4. The variability in the weight of any one person is unlikely to have an overriding effect on the total load. Similarly, if the elevator cable is made up of many independent strands of wire, its capacity will be the sum of the strengths of the individual strands. Since the variability in strength of any one strand will not have much effect on the cable capacity, the normal distribution may be used to model the cable capacity.

Suppose that the load and capacity are represented by normal distributions,

$$f_l(l) = \frac{1}{\sqrt{2\pi}\,\sigma_l}\exp\left[-\frac{1}{2}\frac{\left(l-\bar{l}\right)^2}{\sigma_l^2}\right] \tag{8.29}$$

and

$$f_c(c) = \frac{1}{\sqrt{2\pi}\,\sigma_c}\exp\left[-\frac{1}{2}\frac{(c-\bar{c})^2}{\sigma_c^2}\right] \tag{8.30}$$

where the mean values of the load and capacity are denoted by $\bar{l}$ and $\bar{c}$, and the corresponding standard deviations are σ_l and σ_c. Substituting these expressions into Eq. (8.12), we obtain for the reliability

$$r = \int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}\,\sigma_c}\exp\left[-\frac{1}{2}\frac{(c-\bar{c})^2}{\sigma_c^2}\right]\times\left\{\int_{-\infty}^{c}\frac{1}{\sqrt{2\pi}\,\sigma_l}\exp\left[-\frac{1}{2}\frac{\left(l-\bar{l}\right)^2}{\sigma_l^2}\right]dl\right\}dc \tag{8.31}$$

This expression[1] for the reliability may be reduced to a much simpler form involving only a single normal integral. To accomplish this, however, involves a significant amount of algebraic manipulation. We begin by transforming variables to the dimensionless quantities

$$x = (c-\bar{c})/\sigma_c \tag{8.32}$$

$$y = \left(l-\bar{l}\right)/\sigma_l \tag{8.33}$$

Eq. (8.31) may then be rewritten as

$$r = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left\{\int_{-\infty}^{\left(\sigma_c x+\bar{c}-\bar{l}\right)/\sigma_l}\exp\left[-\frac{1}{2}\left(x^2+y^2\right)\right]dy\right\}dx \tag{8.34}$$

This double integral may be viewed geometrically as an integral over the shaded part of the $x-y$ plane shown in Figure 8.5. The line demarking the edge of the region of integration is determined by the upper limit of the y integration in Eq. (8.34):

$$y = \frac{1}{\sigma_l}\left(\sigma_c x+\bar{c}-\bar{l}\right) \tag{8.35}$$

By rotating the coordinates through the angle θ, we may rewrite the reliability as a single standardized normal function. To this end, we take

$$x' = x\cos\theta + y\sin\theta \tag{8.36}$$

and

$$y' = -x\sin\theta + y\cos\theta \tag{8.37}$$

It may then be shown that

$$x^2+y^2 = x'^2+y'^2 \tag{8.38}$$

1 Note that we have extended the lower limits on the integrals to $-\infty$ in order to accommodate the use of normal distributions. The effect on the result is negligible for $\bar{c}\gg\sigma_c$ and $\bar{l}\gg\sigma_i$.

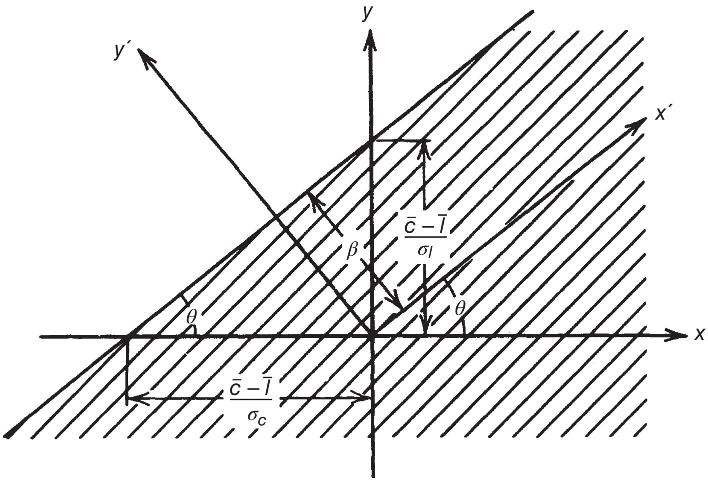


Figure 8.5 Domain of integration for normal load and capacity.

and

$$dx\,dy = dx'dy' \tag{8.39}$$

allowing us to write the reliability as

$$r = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left\{\int_{-\infty}^{\beta}\exp\left[-\frac{1}{2}(x'^2 + y'^2)\right]dy'\right\}dx' \tag{8.40}$$

The upper limit on the y' integration is just the distance β_R shown in Figure 8.5. With elementary trigonometry, β_R may be shown to be a constant given by

$$\beta_R = \frac{\bar{c}-\bar{l}}{\left(\sigma_c^2 + \sigma_l^2\right)^{1/2}} \tag{8.41}$$

The quantity β_R *is referred to as the safety or reliability index.*[2] Since β_R is a constant, the order of integration may be reversed. Then, since

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} e^{-\frac{1}{2}x'^2}\,dx' = \Phi(\infty) = 1 \tag{8.42}$$

the remaining integral, in y', may be written as a standardized normal CDF to yield the reliability in terms of the safety index β_R:

$$r = \Phi(\beta_R) \tag{8.43}$$

The results of this equation may be put in a more graphic form by expressing them in terms of the safety factor, Eq. (8.27). A standard measure of the dispersion about the mean is the coefficient of variation, defined as the standard deviation divided by the mean:

$$\rho = \sigma/\mu \tag{8.44}$$

2 β_R is used in this text so that there is no confusion with the Weibull slope β.

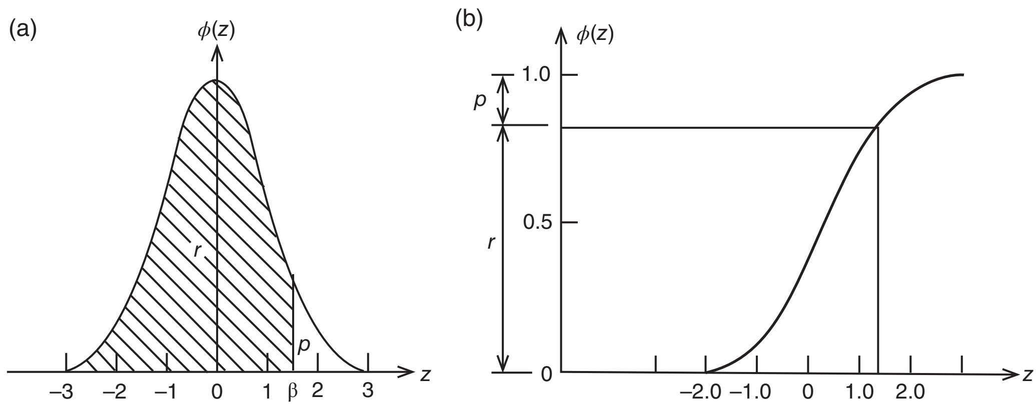


Figure 8.6 Standard normal distribution: (a) probability density function (PDF) and (b) cumulative distribution function (CDF).

Thus, we may write

$$\rho_c = \sigma_c/\bar{c} \tag{8.45}$$

and

$$\rho_l = \sigma_l/\bar{l} \tag{8.46}$$

With these definitions we may express the safety index in terms of the central safety factor and the coefficients of variation:

$$\beta_R = \frac{\nu - 1}{\left(\rho_c^2 \nu^2 + \rho_l^2\right)^{1/2}} \tag{8.47}$$

In Figure 8.6, the standardized normal distribution is plotted. The area under the curve to the left of β_R is the reliability r; the area to the right is the failure probability p. In Figure 8.6b, the CDF for the normal distribution is plotted. Thus, given a value of β_R, we can calculate r and p. Conversely, if the reliability is specified, and the coefficients of variation are known, we may determine the value of the safety factor. In Figures 8.7a and 8.7b, the relation between safety factor and probability of failure is indicated for some representative values of the coefficients of variation. Figure 8.7a has $\rho_c = 0.1$, and Figure 8.7b has $\rho_c = 0.2$.

Example 8.2 Suppose that the coefficients of variation are $\rho_c = 0.1$ and $\rho_l = 0.15$. If we assume normal distributions, what safety factor is required to obtain a failure probability of no more than 0.005?

Solution:
$p = 0.005$; $r = 0.995$; $r = \Phi(\beta_R) = 0.995$. Therefore, from Appendix C, $\beta_R = 2.575$. We must solve Eq. (8.47) for ν. We have

$$\beta_R{}^2\left(\rho_c^2 \nu^2 + \rho_l^2\right) = (\nu - 1)^2 \quad \text{or} \quad \left(1 - \beta_R{}^2 \rho_c^2\right)\nu^2 - 2\nu + \left(1 - \beta_R{}^2 \rho_l^2\right) = 0$$

Solving this quadratic equation in ν, we have

$$\nu = \frac{2 \pm \left[4 - 4\left(1 - \beta^2 \rho_l^2\right)\left(1 - \beta^2 \rho_c^2\right)\right]^{1/2}}{2\left(1 - \beta^2 \rho_c^2\right)}$$

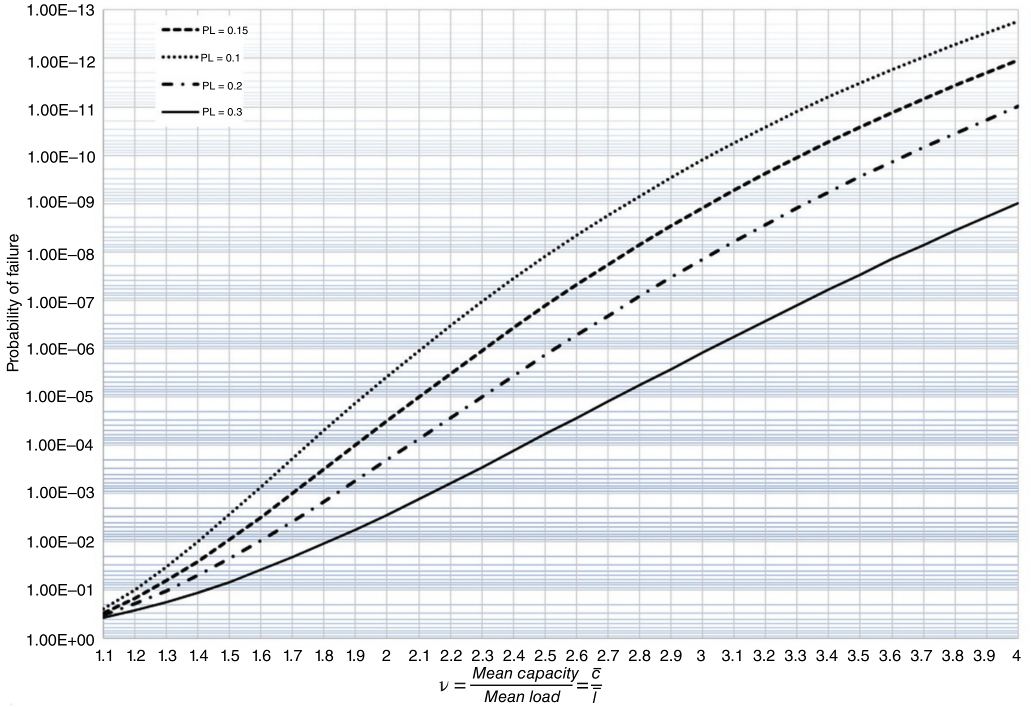


Figure 8.7a Probability of failure for normal load and capacity ($\rho_l = 0.1$).

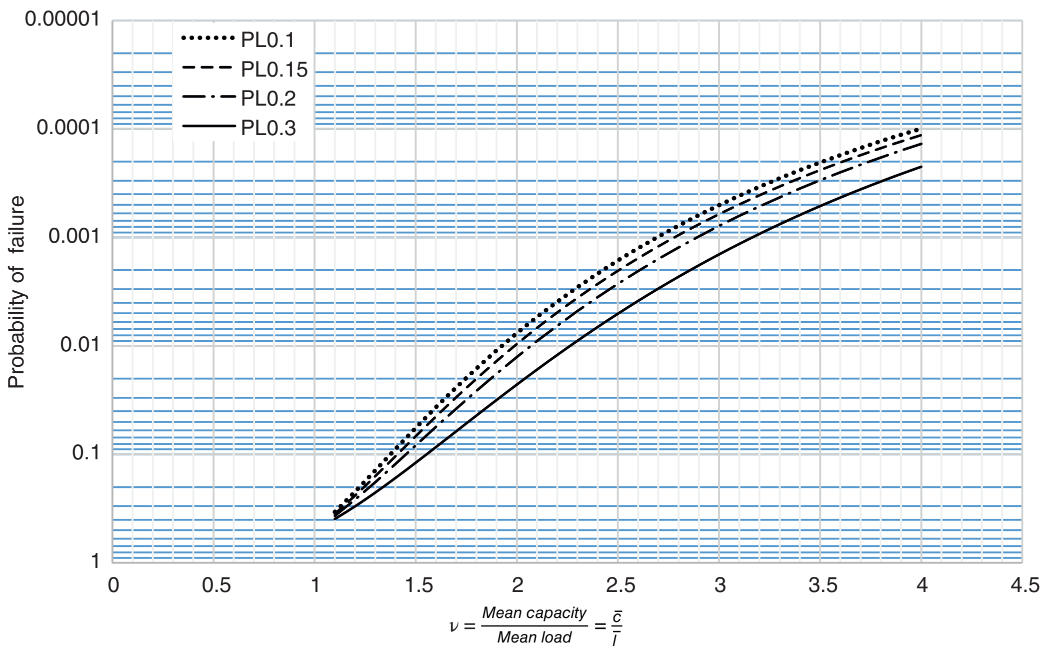


Figure 8.7b Probability of failure for normal load and capacity ($\rho_l = 0.2$).

or

$$\nu = \frac{2 \pm 2(1 - 0.8508 \times 0.9337)^{1/2}}{2 \times 0.9336} = \frac{1 \pm 0.4534}{0.9337}$$
$$= 1.56$$

since the second solution, 0.5853, will not satisfy Eq. (8.47).

In using Eqs. (8.43) and (8.47) to estimate reliability, we assume that the load and capacity are normally distributed and that the means and variances can be estimated. In practice, the paucity of data often does not allow us to say with any certainty what the distributions of load and capacity are. In these situations, however, the sample mean and variance can often be obtained. They can then be used to calculate the reliability index defined by Eq. (8.47); often, the reliability can be estimated from Eq. (8.43). Such approaches are referred to as second-moment methods, since only the zero and second moments of the load and capacity distributions need to be estimated.

Second-moment methods (Cornell 1969; Ang and Tang 1984) have been widely employed, for they represent the logical next step beyond the simple use of safety factors in that they also account for the variance of the distributions. Such methods must be employed with care, however, for when the distributions deviate greatly from normal distributions, the resulting formulas may be in serious error. This may be seen from the different expressions for reliability when lognormal or extreme-value distributions are employed.

Lognormal Distributions

The lognormal distribution is useful when the uncertainty about the load, or capacity, or both is relatively large. Often, it is expressed as having 90% confidence that the load or the capacity lies within some factor, say 2, of the best estimates l_0 or c_0. In Chapter 4, the properties of the lognormal distribution were presented. As indicated there, the lognormal distribution is most appropriate when the value of the variable is determined by the product of several different factors. For load and capacity, we rewrite Eq. (4.67) for the PDFs as

$$f_l(l) = \frac{1}{\sqrt{2\pi}\,\omega_l l} \exp\left\{-\frac{1}{2\omega_l^2}\left[\ln\left(\frac{l}{l_0}\right)\right]^2\right\}, \quad 0 < l \leq \infty \tag{8.48}$$

and

$$f_c(c) = \frac{1}{\sqrt{2\pi}\,\omega_c c} \exp\left\{-\frac{1}{2\omega_c^2}\left[\ln\left(\frac{c}{c_0}\right)\right]^2\right\}, \quad 0 < c \leq \infty \tag{8.49}$$

If Eqs. (8.48) and (8.49) are substituted into Eq. (8.12), the resulting expression for the reliability is

$$\begin{aligned} r = &\int_0^\infty \frac{1}{\sqrt{2\pi}\omega_c c} \exp\left\{-\frac{1}{2\omega_c^2}\left[\ln\left(\frac{c}{c_0}\right)\right]^2\right\} \\ &\times \left(\int_0^c \frac{1}{\sqrt{2\pi}\,\omega_l l} \exp\left\{-\frac{1}{2\omega_l^2}\left[\ln\left(\frac{l}{l_0}\right)\right]^2\right\} dl\right) dc \end{aligned} \tag{8.50}$$

Note, however, that with the substitution

$$y = \frac{1}{\omega_l}\ \ln\left(\frac{l}{l_0}\right) \tag{8.51}$$

and

$$x = \frac{1}{\omega_l}\ \ln\left(\frac{c}{c_0}\right) \tag{8.52}$$

We obtain

$$r = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left\{\int_{-\infty}^{(1/\omega_l)[\omega_c x + \ln(c_0/l_0)]} \exp\left[-\frac{1}{2}\left(x^2 + y^2\right)\right] dy\right\} dx \tag{8.53}$$

The forms of the reliability in Eq. (8.34) and in this equation are identical if in the upper limit of the y integration we substitute ω_l and ω_c for σ_l and σ_s, respectively, and replace $\bar{c} - \bar{l}$ with $\ln(c_0/l_0)$. Thus, the reliability still has the form of a standardized normal distribution given by Eq. (8.43). Now, however, the argument β_R is given by

$$\beta_R = \frac{\ln(c_0/l_0)}{\left(\omega_c^2 + \omega_l^2\right)^{1/2}} \tag{8.54}$$

Example 8.3 Suppose that both the load and the capacity on a device are known within a factor of 2 with 90% confidence. What value of the safety factor, c_0/l_0, must be used if the failure probability is to be no more than 1.0%?

Solution:
For $\Phi(\beta_R) = r = 1 - p = 0.99$, we find from Appendix C that $\beta_R = 2.33$. From Eq. (4.77) for 90% confidence with a factor of $n = 2$ uncertainty, we have for both load and capacity $\omega_c = \omega_l = \omega = (1/1.645)\ \ln(n) = (1/1.645)\ \ln(2) = 0.4214$. Solve Eq. (8.54) for c_0/l_0:

$$\begin{aligned}\frac{c_0}{l_0} &= \exp\left[\beta\left(\omega_c^2 + \omega_l^2\right)^{1/2}\right] = \exp\left(\beta\sqrt{2}\omega\right)\\ &= \exp(2.33 \times 1.414 \times 0.4214) = 4.01\end{aligned}$$

Combined Distributions

In general, it is difficult to evaluate analytically the expressions given for reliability when the load and capacity are given by different distributions. However, when the load or capacity is given by an extreme-value distribution and the other by a normal distribution, both analytical results and some insight can be obtained Equations (8.12) and (8.20) may be used to numerically estimate the reliability if the probability density function of the load and capacity were known, or if load and capacity distribution data were empirically known. In the latter case, using Monte Carlo simulation.

Consider first a system whose capacity is approximated by the smallest extreme-value distribution introduced in Chapter 5, but about whose loading there is only a small amount of uncertainty. This situation is depicted in Figure 8.8a. We assume that $\bar{l}$, the mean value of the load, is much

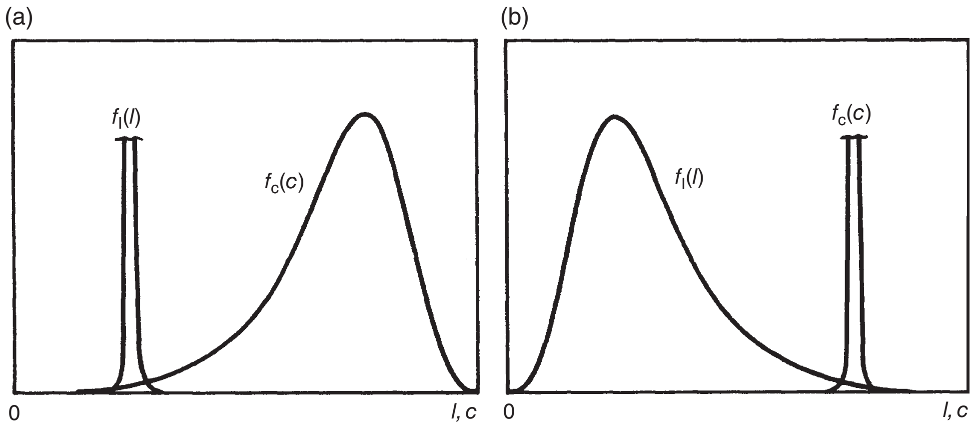


Figure 8.8 Graphical representations of reliability: (a) smallest extreme-value distribution for capacity and (b) largest extreme-value distribution for loading.

smaller than the mean, $\bar{c} \equiv u - \Theta\gamma$, of the smallest extreme-value distribution that represents the capacity: $\bar{l} \ll \bar{c}$. For known loading, the reliability is given by Eq. (8.18). Thus, using CDF from Eq. (5.34), we have

$$r(l) = \exp\left[-e^{(l-u)/\Theta}\right] \tag{8.55}$$

which for small enough values of l (i.e. $l \ll u$) becomes

$$r(l) \approx 1 - \exp\left(\frac{l-u}{\Theta}\right) \tag{8.56}$$

Now suppose that we want to take into account some natural variation in the loading on the system. If this is represented by a distribution with small variance of the load about the mean, Eq. (8.19) may be employed to express the reliability as

$$r = 1 - \int_0^\infty f_l(l) \exp\left(\frac{l-u}{\Theta}\right) dl \tag{8.57a}$$

Again, it must be assumed that the variance of the load is not large, $\sigma_l \ll \bar{c} - \bar{l}$, so that the expansion, Eq. (8.56), is valid over the entire range of l, where $f_1(l)$ is significantly greater than zero. We obtain for the reliability

$$r = 1 - \exp\left[\frac{1}{2}\left(\frac{\sigma_l}{\theta}\right)^2\right] \exp\left(\frac{\bar{l}-u}{\Theta}\right) \tag{8.57b}$$

where $u \equiv \bar{c} + \Theta\gamma \gg \bar{l}$, and γ is Euler's constant.

In the converse situation the capacity has only a small degree of uncertainty, whereas the loading is represented by a maximum extreme-value distribution, again with the stipulation that $\bar{c} \gg \bar{l}$.

This situation is depicted in Figure 8.8b. The reliability at known capacity is first obtained by substituting the maximum extreme-value distribution from Eq. (5.19) into Eq. (8.10),

$$r(c) = F_l(c) = \exp\left[-e^{-(c-u)/\Theta}\right] \tag{8.58}$$

or for large c,

$$r(c) \approx 1 - e^{-(c-u)/\Theta} \tag{8.59}$$

Thus, from Eq. (8.11), we have

$$r = \int_0^\infty f_c(c)\left[1 - \exp\left(\frac{u-c}{\Theta}\right)\right] dc \tag{8.60}$$

provided that the variance in $f_c(c)$ is small enough that Eq. (8.59) is valid. The resulting reliability is

$$r = 1 - \exp\left[-\frac{1}{2}\left(\frac{\sigma_c}{\Theta}\right)^2\right] 1 - \exp\left(\frac{u-\bar{c}}{\Theta}\right) \tag{8.61}$$

where $u \equiv \bar{l} - \Theta\gamma \ll \bar{c}$, and γ is Euler's constant.

8.4 Repetitive Loading

We have considered time only implicitly, or not at all, in conjunction with load–capacity interference theory. Load has been represented as the maximum load over the life of the device or system. Therefore, with longer lives, the load distribution in Figure 8.3 would shift to the right, causing the reliability to decrease. Likewise, aging effects have been taken into account only in the conservatism in which the capacity distribution is chosen; it should take weakening with age into account.

Time, however, is arguably the most important variable in many reliability considerations. The bathtub curve representation of failure rate curve pictured in Figure 3.1 is ubiquitous in characterizing the reliability losses that cause infant mortality, random failures, and aging. In this and the following section, we demonstrate how load and capacity interact under repetitive loading and result in these three failure mechanisms. Specifically, infant mortality is closely associated with capacity variability, random failures with loading variability, and aging with capacity deterioration. These associations provide a rational for the bathtub shapes of failure rate curves and clarify the relationship between the three failure classes and the corresponding causes of quality loss enumerated by Taguchi: product noise, outer noise, and inner noise.

Loading Variability

Consider a system subject to repetitive loading, and assume that the magnitude of each load is determined by a random variable **1**, described by a probability density $f_l(l)$. Suppose, for now, that we specify a system with a known capacity $c(t)$ at time t. The probability that a load occurring at time t will cause system failure is then just the probability that $l > c(t)$, or

$$p = \int_{c(t)}^{\infty} f_l(l)\, dl \tag{8.62}$$

Repetitive loading may occur at either equal or random time intervals, as pictured in Figures 8.9a or b, respectively. The model that follows is based on random intervals, although when the mean time between loads becomes small, the two models yield nearly identical results. We model the random times at which the loads occur by specifying that during a vanishingly small time increment, Δt, the probability of load occurrence is $\gamma\ \Delta t$, where Δt is so small that $\gamma\ \Delta t \ll 1$. The probability of a load occurring at any time is then independent of the time at which the last loading occurred; the loading is then said to be Poisson distributed in time with a frequency γ. The probability of a load that is large enough to cause failure occurring between t and $t + \Delta t$ is thus $p\gamma\ \Delta t$ or, using Eq. (8.62),

$$\gamma \int_{c(t)}^{\infty} f_l(l)\, dl\, \Delta t \tag{8.63}$$

The system, however, can fail only once. Thus, it will fail between t and $t + \Delta t$ only if it has survived to time t *and* the failing load occurs during Δt.

But $R(t)$, the reliability, is just the probability that the system has survived to t. Thus, the failure probability during Δt is $R(t)\ p\gamma\ \Delta t$. Likewise, the reliability at $t + \Delta t$ is just the probability that the system survived to t *and* that no failure load occurred during Δt. Since we take the *and* to represent independent events, we may write

$$R(t + \Delta t) = \left[1 - \gamma \int_{c(t)}^{\infty} f_l(l)\, dl\, \Delta t\right] R(t) \tag{8.64}$$

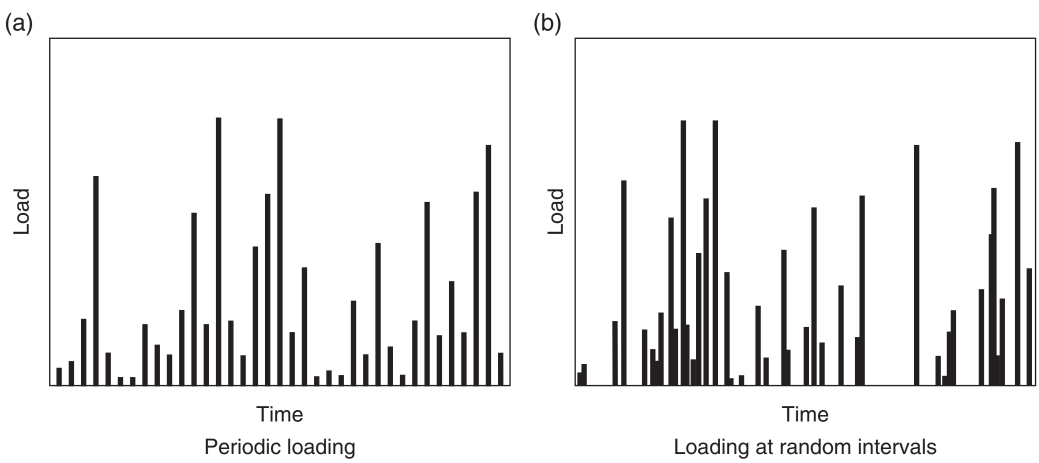


Figure 8.9 Repetitive loads of random magnitudes: (a) periodic loading and (b) loading at random intervals.

Rearranging terms yields

$$\frac{R(t+\Delta t)-R(t)}{\Delta t} = -\gamma\int_{c(t)}^{\infty} f_l(l)\,dl\,R(t) \tag{8.65}$$

Taking the limit as $\Delta t \to 0$ then yields the same form as Eq. (3.15),

$$\lambda(t) = -\frac{1}{R(t)}\frac{d}{dt}R(t) \tag{8.66}$$

where the failure rate is given in terms of the load distribution as

$$\lambda(t) = \gamma\int_{c(t)}^{\infty} f_l(l)\,dl \tag{8.67}$$

This equation clearly indicates that if the capacity of the system is time independent, so that $c(t) \to c_0$, then time also disappears from the failure rate, yielding the constant failure rate model

$$\lambda = \gamma\int_{c(t)}^{\infty} f_l(l)\,dl \tag{8.68}$$

and the common exponential distribution $R(t) = \exp(-\lambda t)$ results.

Example 8.4 A microwave transmission tower is to be constructed at a location where an average of 15 lightning strikes per year are expected. The mean value of the peak current is estimated to be 20,000 amperes, and the peak currents are modeled by an exponential distribution. The MTTF is to be no less than 10 years.

a) What value of the failure rate is acceptable?
b) For what peak amperage must the protection system be designed?

Solution:

a) For a constant failure rate phenomenon, we have

$$\lambda = 1/\text{MTTF} = 1/10 = 0.1\ \text{year}^{-1}$$

b) From Eq. (3.24), we may write the exponential load distribution as $F_l(l) = 1 - e^{-l/\bar{l}}$, where the mean load $\bar{l} = \ = 20,000$, and $\gamma = 15/\text{year}$. Using the relationship between $f_l(l)$ and $F_l(l)$, we may write Eq. (8.68) as

$$\lambda = \gamma\int_{c_0}^{\infty} f_l(l)\,dl = \gamma\,[1 - F_l(c_0)] = \gamma\,\exp\left(-c_0/\bar{l}\right)$$

Since $\text{MTTF} = 1/\lambda$, we have

$$\text{MTTF} = \frac{1}{\gamma}\,\exp\left(-c_0/\bar{l}\right)$$

or inverting,

$$\left(c_0/\bar{l}\right) = \ln(\gamma\text{MTTF}) = \ln(15\cdot 10) = 5.0$$

or

$$c_0 = 20,000 \times 5.0 = 100,000 \text{ Amperes}$$

Aging is present if the capacity decreases with time. We represent this deterioration as

$$c(t) = c_0 - g(t) \tag{8.69}$$

where c_0 is the initial capacity, at $t = 0$, and $g(t)$ is a monotonically increasing function of time, with $g(0) = 0$. Clearly, if the capacity decreases as time elapses, the failure rate will grow, since the lower limit on the integral in Eq. (8.67) then moves toward zero. The rate at which the failure rate increases, however, will be sensitive to the loading distribution as well as to $c(t)$.

Once the failure rate is known, the reliability can be obtained from Eq. (3.18). Thus,

$$R(t \mid c_0) = \exp\left[-\int_0^t dt'\gamma\int_{c(t')}^{\infty} f_l(l)dl\right] \tag{8.70}$$

where $c(t)$ is given by Eq. (8.69).

Example 8.5 Assume that the capacity of the microwave tower in Example 8.4 deteriorates at a constant rate of 1% per year.

a) What is the 10 year % decrease in capacity?
b) What is the 10 year % increase in failure rate?
c) What is the probability that a damaging lightning strike will take place in the first 10 years without deterioration and
d) with deterioration?

Solution:

a) Let $c(t) = c_0(1 - \alpha t)$, where $\alpha = 0.01$/year. After 10 years, the capacity decrease is $0.01 \times 10 = 10\%$.
b) Replacing c_0 by $c(t)$ in Example 8.4, we have

$$\lambda(t) = \gamma \exp\left[-c_0(1-\alpha t)/\bar{l}\right] = \lambda(0)\exp\left(\alpha t c_0/\bar{l}\right)$$

Since $\alpha t = 0.1$ and $\left(c_0/\bar{l}\right) = 5.0$, we have

$$\lambda(10) = \lambda(0)e^{0.1\times5.0} = 1.65\ \lambda(0).$$

Thus, the increase is 65%.

c) $1 - R(10) = 1 - e^{-\lambda(0)\ t} = 1 - e^{0.1\times10} = 0.632$

$$\int_0^t \lambda(t')\,dt' = \lambda(0)\int_0^t e^{\alpha t' c_0/\bar{l}}dt' = \lambda(0)\left(\alpha c_0/\bar{l}\right)^{-1}\left(e^{\alpha t c_0/\bar{l}} - 1\right)$$

$$\int_0^{10} \lambda(t')\,dt' = 0.1(0.01 \times 5.0)^{-1}\left(e^{0.1\times50} - 1\right) = 1.3$$

$$1 - R(10) = 1 - \exp\left(-\int_0^{10}\lambda(t')\,dt'\right) = 1 - e^{-1.3} = 0.727$$

Variable Capacity[3]

We next consider situations where not every unit of a system or device has exactly the same initial capacity. In reality, they would not, since variability in manufacturing processes inevitably leads to some variability in capacity. We model this variability by letting c_0 become a random variable which is described by the probability density function $f_c(c_0)$. We next consider the ensemble of such units, each with its own capacity. The system reliability is then an ensemble average over c_0:

$$R(t) = \int_0^\infty dc_0 f_c(c_0) R(t \mid c_0) \tag{8.71}$$

Inserting Eq. (8.70) then yields

$$R(t) = \int_0^\infty dc_0 f_c(c_0) \exp\left[-\int_0^t dt' \gamma \int_{c(t')}^\infty f_l(l) dl\right] \tag{8.72}$$

To focus on the effect of variable capacity on failure rates, we ignore deterioration for the moment by setting $c(t) = c_0$ and assume that some fraction, say p_d, of the systems under consideration are flawed in a serious way. This situation may be modeled by writing the PDF of capacities in terms of the Dirac delta functions as

$$f_c(c_0) = (1 - p_d)\delta(c_0 - c_\tau) + p_d \delta(c_0 - c_d) \tag{8.73}$$

The first term on the right-hand side corresponds to the probability that the system will be a properly built system with target design capacity of c_τ. Using the Dirac delta function, we are assuming that the capacity variability of the properly built systems can be ignored. The second term corresponds to the probability that the system will be defective and have a reduced capacity $c_d < c_\tau$. Such a situation might arise, for example if a critical component were to be left out of a small fraction of the systems in assembly, or if, in construction, members were not properly assembled with some probability p_d.

The reliability is obtained by first substituting Eq. (8.73) into (8.72) and using the Dirac delta distribution property given in Eq. (8Sup1.7) to evaluate the integrals,

$$R(t) = (1 - p_d)\exp(-\lambda_\tau t) + p_d \exp(-\lambda_d t) \tag{8.74}$$

where for brevity, we have defined the failure rates

$$\lambda_\tau = \gamma \int_{c_\tau}^\infty f_l(l)\, dl \tag{8.75}$$

and

$$\lambda_d = \gamma \int_{c_d}^\infty f_l(l) dl \tag{8.76}$$

Since the failure rate must increase with decreased capacity, $\lambda_\tau < \lambda_d$. We now use the definition of the time-dependent failure rate given in Eq. (8.66) to obtain, after evaluating the derivative,

$$\lambda(t) = \lambda_\tau \left\{ \frac{1 + \dfrac{p_d}{1 - p_d} \dfrac{\lambda_d}{\lambda_\tau} \exp[-(\lambda_d - \lambda_\tau)t]}{1 + \dfrac{p_d}{1 - p_d} \exp[-(\lambda_d - \lambda_\tau)t]} \right\} \tag{8.77}$$

3 This section uses Supplement 1 – The Dirac Delta Distribution.

The decreasing failure rate associated with infant mortality may be seen to appear as a result of the presence of the units with substandard capacities. For clarity, we consider the extreme example of a system for which the probability of defective construction is small, $p_d \ll 1$, but for which the defect greatly increases the failure rate, $\lambda_d \gg \lambda_\tau$. In this case, Eq. (8.77) reduces to

$$\lambda(t) = \lambda_\tau\left(1 + p_d\frac{\lambda_d}{\lambda_\tau}e^{-\lambda d^t}\right) \tag{8.78}$$

Thus, the failure rate decreases from a value of $\approx\lambda_\tau + p_d\lambda_d$ at zero time to the value of λ_τ for the unflawed systems that remain after all defective units have failed.

Example 8.6 A servomechanism is designed to have a constant failure rate and a design-life reliability of 0.99 in the absence of defects. A common manufacturing defect, however, is known to cause the failure rate to increase by a factor of 100. The purchaser requires the design-life reliability to be at least 0.975.

a) What fraction of the delivered servomechanisms may contain the defect if the reliability criterion is to be met?
b) If 10% of the servomechanisms contain the defect, how long must they be worn in before delivery to the purchaser?

Solution:

a) Without the defect, the failure rate $\lambda_\tau \equiv \lambda(c_\tau)$ may be found in terms of the design life T by $R_0(T) = e^{-\lambda_\tau T}$; then,

$$\lambda_\tau T = \ln\left[\frac{1}{R(T)}\right] = \ln\left(\frac{1}{0.99}\right) = 0.01005$$

To determine *p,* the acceptable fraction of units with defects, solve Eq. (8.74); with $t = T$ for p_d:

$$p_d = \frac{1 - R(T)\exp[+\lambda_\tau T]}{1 - \exp[-(\lambda_d - \lambda_\tau)T]}$$

With $\lambda_d \equiv \lambda\,(c_d) = 100\,\lambda_\tau$, $R(T) = 0.975$, and $\lambda_\tau T = 0.01005$,

$$p_d = \frac{1 - 0.975e^{+0\ 01005}}{1 - e^{-99\times 0.01005}} = 0.024$$

b) Recall the definition for reliability with wear-in from Eq. (3.51). Combining Eq. (8.74) with this expression, we have, for a wear-in period T_w,

$$R(T \mid T_\omega) = \frac{(1-p_d)\exp[-\lambda_\tau(T \mid T_\omega)] + p_d\exp[-\lambda_d(T + T_\omega)]}{(1-p_d)\exp(-\lambda_\tau T_\omega) + p_d\exp(-\lambda_d T_\omega)}$$

Solve for T_ω:

$$T_\omega = \frac{1}{\lambda_d - \lambda_\tau}\ln\left[\frac{p_d}{1-p_d}\,\frac{R(T \mid T_\omega)\exp(-\lambda_d T)}{\exp(-\lambda_\tau t) - R(T \mid T_\omega)}\right]$$

With $R(T|T_\omega) = 0.975$, $p_d = 0.1$, $\lambda_\tau T = 0.01005$, and $\lambda_d T = 1.005$,

$$T_\omega = \frac{T}{99} \ln \left(\frac{0.1}{1-0.1} \frac{0.975 - e^{-100 \times 0.01005}}{e^{-0\ 01005} - 0.975} \right)$$

$$= 0.015\,T \quad \text{or} \quad 1\tfrac{1}{2}\% \text{ of the design life.}$$

8.5 The Bathtub Curve – Reconsidered

The preceding examples illustrate the constant failure rate that results from loading variability, the increasing failure rates resulting from the combined effects of loading variability and product deterioration, and the decreasing failure rates from loading and initial capacity variability. We next look at the three classes of failure individually and in combination to show how the bathtub curve arises. Table 8.1 lists the eight combinations that may be considered. We next write a general expression for the failure rate that includes all three modes. Since the failure rate is defined in terms of the reliability by Eq. (8.66), we may insert Eq. (8.72) for the reliability and perform the derivative to yield

$$\lambda(t) = \frac{\gamma \int_0^\infty dc_0 f_c(c_0) \int_{c(t)}^\infty f_l(l) dl \exp\left[-\gamma \int_0^t dt' \int_{c(t')}^\infty f_l(l) dl \right]}{\int_0^\infty dc_0 f_c(c_0) \exp\left[-\gamma \int_0^t dt' \int_{c(t')}^\infty f_l(l) dl \right]} \tag{8.79}$$

Equations (8.69), (8.72), and (8.79) constitute a reliability model in which infant mortality, random failures, and aging are represented explicitly in terms of capacity variability, loading variability, and capacity degradation.

The relationships are summarized in the first two columns of Table 8.2. Any phenomenon may be eliminated from consideration as indicated in the third column. The fourth column exhibits the particular load and capacity distributions used in the numerical examples that follow. These are normal distributions of load and capacity; in these, we use $\nu = 1.5$ for the safety factor, with $\rho_l = 0.15$ and $\rho_c = 0.10$ for the load and capacity coefficients of variation. We examine the failure modes and their interactions by considering individually each of the eight combinations enumerated in Table 8.1. For each case, load and capacity are plotted versus time in Figure 8.10 for schematic realizations of the stochastic loading process. The normal distribution plotted on the vertical axis is used to denote cases with variable capacity; the vertical lines denote loading magnitudes at random time intervals.

Table 8.1 Failure modes and their interactions.

	Case	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
I.	Infant mortality	No	No	No	Yes	No	Yes	Yes	Yes
II.	Random failures	No	No	Yes	No	Yes	No	Yes	Yes
III.	Aging	No	Yes	No	No	Yes	Yes	No	Yes

Table 8.2 Failure mode characterization.

	Failure mode	Governing property	Mode absent	Mode[a] present
I.	Infant Mortality (variable capacity)	$f_c(c_0)$	$f_c(c_0) = \delta(c_0 - \bar{c}_0)$	$f_c(c_0) = \phi[(c_0 - \bar{c}_0)/\sigma_c]$
II.	Random Failures (variable load)	$f_l(l)$	$f_l(l) = \delta(l - \bar{l})$	$f_l(l) = \phi[(l - \bar{l})/\sigma_l]$
III.	Aging (deteriorating capacity)	$g(t)$	$g(t) = 0$	$g(t) = \alpha c_0 (t/t_0)^\beta$

[a] $\phi(\mu) \equiv (2\pi)^{-1/2} \exp\left(-\frac{1}{2}u^2\right)$.

Single Failure Modes

Of the eight cases, the first is trivial since, as indicated in Figure 8.10, the absence of both variability and aging leads to a vanishing failure rate and a reliability equal to one. In cases two and three, there is no capacity variability, and therefore Eqs. (8.72) and (8.79) reduce to Eqs. (8.70) and (8.67). In case two, only mode III, aging, is present. Thus, the loading is represented by the Dirac delta function, and we may further reduce Eqs. (8.67) and (8.70) to

$$\lambda(t) = \begin{Bmatrix} 0, & t < t_f \\ \gamma, & t > t_f \end{Bmatrix} \tag{8.80}$$

where $t_f = g^{-1}(c_0 - \bar{l})$.Thus,

$$R(t) = \begin{Bmatrix} 1, & t < t_f \\ e^{-\gamma(t - t_f)}, & t > t_f \end{Bmatrix} \tag{8.81}$$

This system does not fail before time t_f, but at the first loading thereafter, causing the rapid exponential decay in the reliability. In case three, where only mode II, random failure, due to load variability is present, we replace $c(t)$ by c_0 in Eq. (8.70) to obtain a constant failure rate and the characteristic exponential decay of the reliability.

In case four, where only mode I, infant mortality, caused by variable capacity, is present, the situation is somewhat more complex. Setting $c(t)$ equal to c_0 and using the Dirac delta function for loading in Eqs. (8.72) and (8.79), we obtain

$$R(t) = 1 - (1 - e^{-\gamma t}) \int_0^{\bar{l}} f_c(c_0)\, dc_0 \tag{8.82}$$

and a corresponding failure rate of

$$\lambda(t) = \frac{\gamma e^{-\gamma t} \int_0^{\bar{l}} f_c(c_0)\, dc_0}{1 - (1 - e^{-\gamma t}) \int_0^{\bar{l}} f_c(c_0) dc_0} \tag{8.83}$$

In this situation, the fraction of the system population for which $c_0 < \bar{l}$ fails at the first loading, causing the reliability to drop sharply and then stabilize; the failure rate decreases exponentially at a very rapid rate.

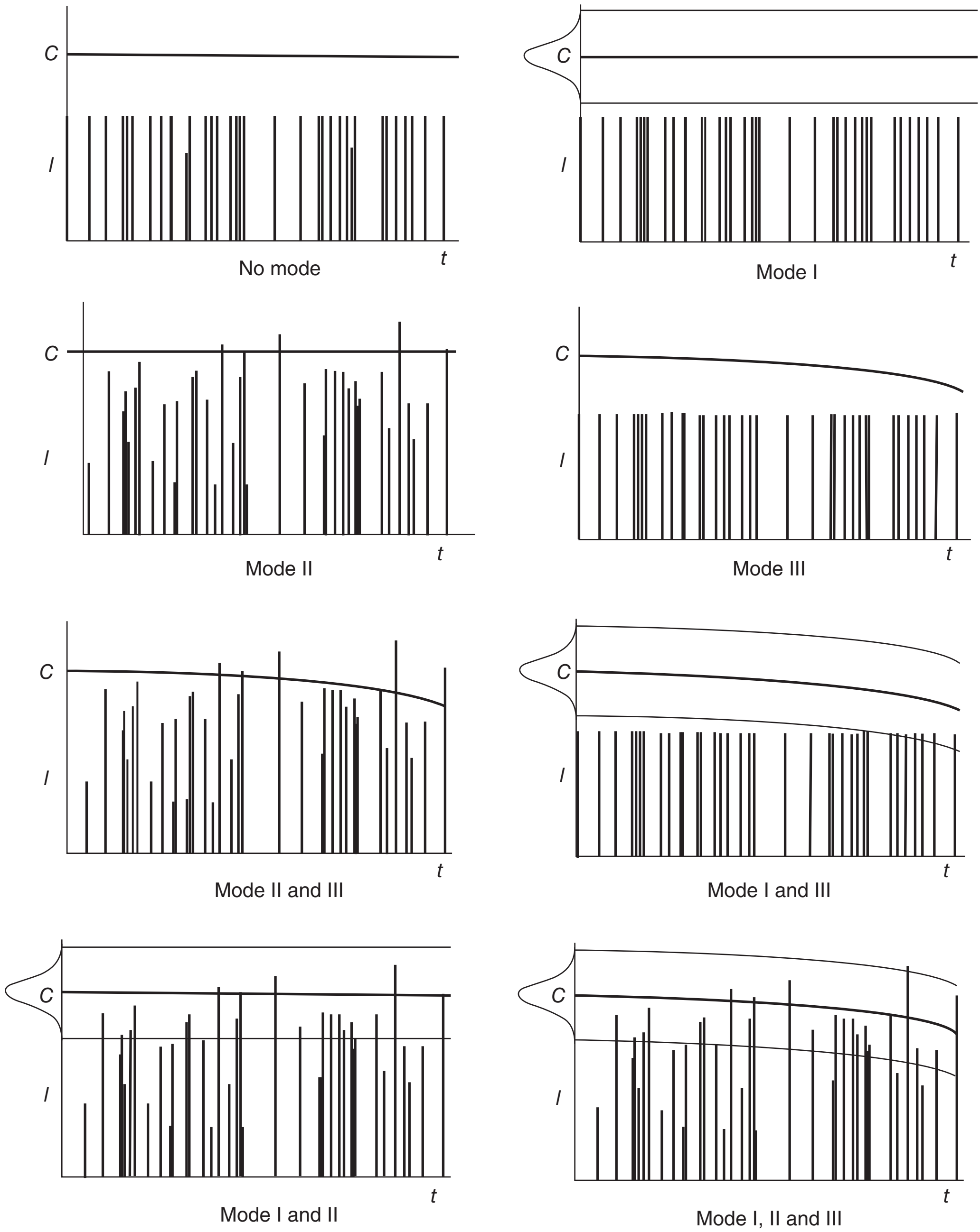


Figure 8.10 Load and capacity realizations vs. time for failure mode combinations (I – infant mortality, II – random, and III – aging).

In each of the preceding three cases, only one failure mode is present. The modes are compared through the schematic diagrams of reliability and failure rate given in Figure 8.11a and b. The failure rate curves, in particular, are instructive since they show that the cases of pure infant mortality, random failures, and aging failures to some extent resemble the bathtub curve. The differences,

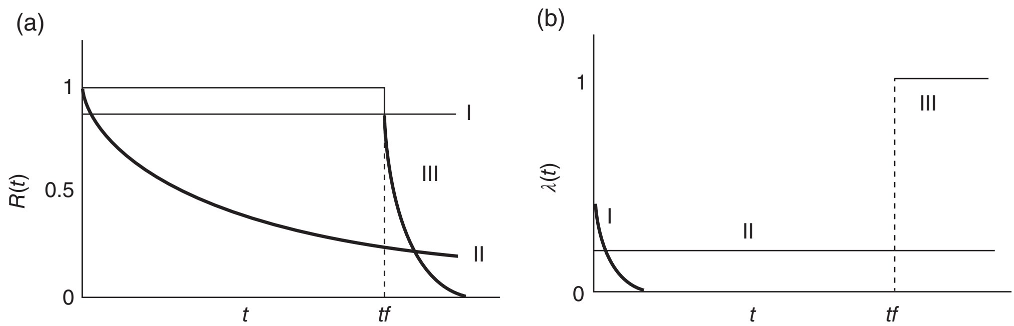


Figure 8.11 Effects of single failure modes: (a) reliability and (b) failure rate.

however, are striking. The infant mortality contribution drops quickly to zero, since if the system does not fail at the first loading it does not fail at all. Unlike bathtub curves, the failure rate from aging is zero until t_f, at which time it jumps to a value of γ, causing the reliability to drop sharply to zero. Thus, it is clear that simple superposition of the failure rates depicted in Figure 8.11 do not accurately represent the bathtub curve. To obtain realistic results we must also examine the interactions between failure modes.

Combined Failure Modes

Next, we consider combinations of two failure modes. Equations (8.70) and (8.67) describe case five, which combines random failures and aging, modes II and III. Aging is modeled by a power law

$$g(t) = 0.1c_0(t/t_0)^{\beta} \tag{8.84}$$

where we take $\gamma t_0 = 100$. In Figure 8.12, the failure rate is shown to be increasing with time with a behavior which is closely correlated to exponent m in the aging model.

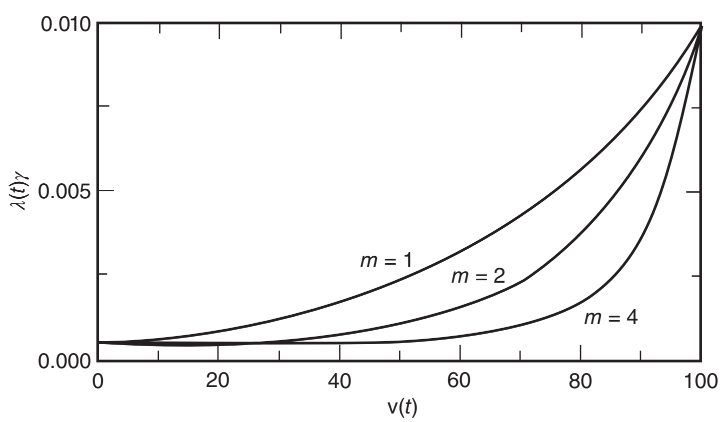


Figure 8.12 Combined random and aging failure rates (modes II and III) vs. time for several values of m.

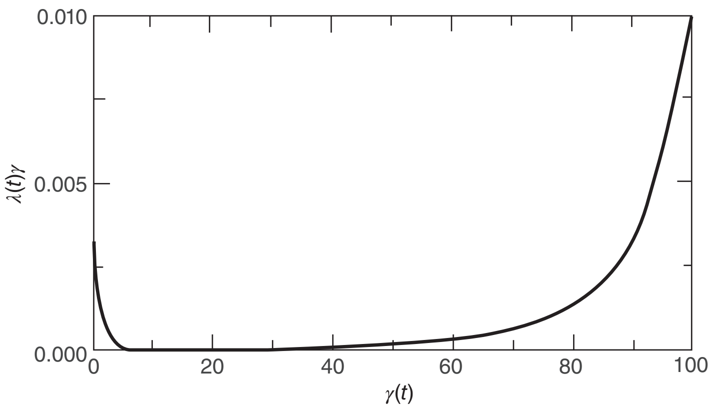


Figure 8.13 Combined infant mortality and aging failure rates (modes I and III) vs. time.

In case six, infant mortality and aging modes I and III occur together in the absence of random failures. The reliability and failure rate are obtained by replacing the load PDF in Eqs. (8.72) and (8.79) by a Dirac delta function. The reduced expressions are

$$R(t) = 1 - (1 - e^{-\gamma t})\int_0^{\bar{l}} f_c(c_0)\, dc_0 - \int_{\bar{l}}^{\bar{l}+g(t)} \left\{1 - e^{-\gamma[t-g^{-1}(c_0-\bar{l})]}\right\} f_c(c_0)\, dc_0 \tag{8.85}$$

for the reliability and

$$\lambda(t) = \frac{\gamma e^{-\gamma t}\left[\int_0^{\bar{l}} f_c(c_0)dc_0 + \int_{\bar{l}}^{\bar{l}+g(t)} e^{\gamma g^{-1}(c_0-\bar{l})} f_c(c_0)dc_0\right]}{1 - (1-e^{-\gamma t})\int_0^{\bar{l}} f_c(c_0)dc_0 - \int_{\bar{l}}^{\bar{l}+g(t)}\left\{1 - e^{-\gamma[t-g^{-1}(c_0-\bar{l})]}\right\} f_c(c_0)dc_0} \tag{8.86}$$

for the failure rate. The failure rate is plotted in Figure 8.13. This situation resembles that encountered frequently in fatigue testing, where the loading magnitude is carefully controlled. After that fraction of the population for which the initial capacity is less than the load is removed at the first loading, the failure rate is vanishingly small until the effects of aging become significant.

In case seven, infant mortality and random failures, modes I and II, are present in the absence of aging. Results obtained by setting $c(t) = c_0$ in Eqs. (8.72) and (8.79) are shown in Figure 8.14. The interaction of infant mortality and random failure modes causes the characteristic decreasing failure rate frequently observed in electronic equipment.

Finally, we consider the eighth case where all three failure modes are present, using Eqs. (8.72) and (8.79) for reliability and failure rate. The bathtub curve characteristics are shown in Figure 8.15 where we have also included curves for various combinations of two failure modes. These are obtained by removing one failure mode, but keeping the remaining parameters fixed. These results illuminate the origins of the three failure modes: infant mortality with capacity variability, random failures with loading variability, and aging with capacity deterioration. Moreover, while changes in load or capacity distribution often have large effects on the quantitative behavior of the failure rate cures, the qualitative behavior remains essentially the same. The model indicates, however, that the interactions between the three modes are very important in determining the failure rate cure. Thus, only if the three failure modes arise from independent failure mechanisms or in different components is it legitimate simply to sum the failure rate contributions.

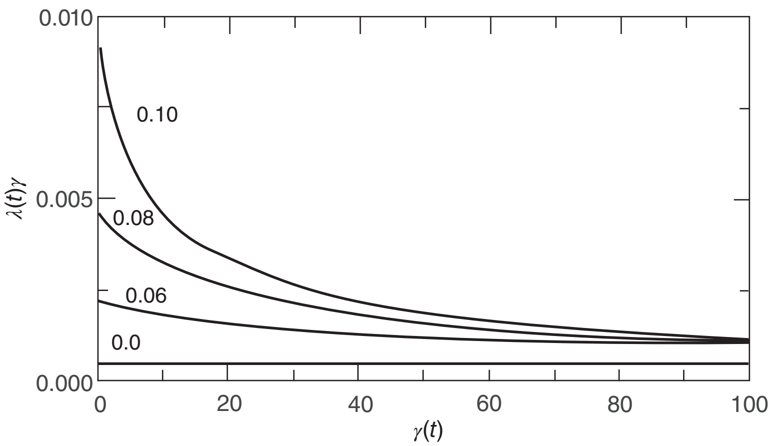


Figure 8.14 Combined infant mortality and random failure rates (modes I and II) vs. time for several values of ρ_c.

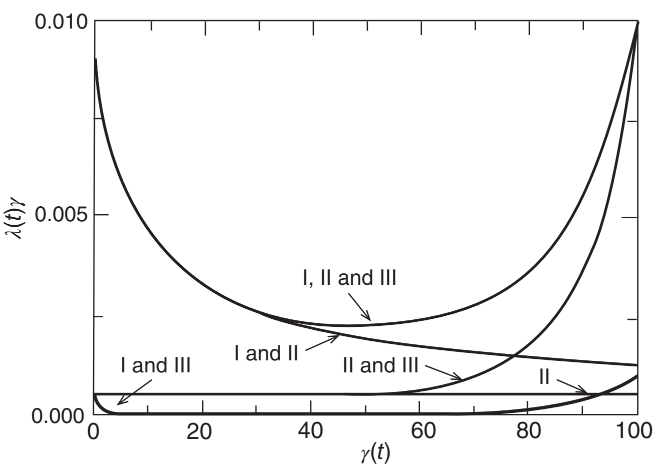


Figure 8.15 Failure rates vs. time for various combinations of failure modes.

Bibliography

Ang, A.H.-S. and Tang, W.H. (1975). *Probability Concepts in Engineering Planning and Design*, vol. 1. New York: Wiley.

Ang, A.H.-S. and Tang, W.H. (1984). *Probability Concepts in Engineering Planning and Design*, vol. 2. New York: Wiley.

Brockley, D. (ed.) (1992). *Engineering Safety*. London: McGraw-Hill.

Cornell, C.A. (1969). Structural Safety Specifications Based on Second-Moment Reliability. Symposium of the International Association of Bridge and Structural Engineers, London.

Freudenthal, A.M., Garrelts, J.M., and Shinozuka, M. (1966). The analysis of structural safety. *Journal of the Structural Division ASCE ST* 1: 267–325.

Gumbel, E.J. (1958). *Statistics of Extremes*. New York: Columbia University Press.
Haugen, E.B. (1980). *Probabilistic Mechanical Design*. New York: Wiley.
Haviland, R.D. (1964). *Engineering Reliability and Long Life Design*. New York: Van Nostrand.
Kapur, K.C. and Lamberson, L.R. (1977). *Reliability in Engineering Design*. New York: Wiley.
Lewis, E.E. and Chen, H.-C. (1994). Load-capacity interference and the bathtub curve. *IEEE Transactions on Reliability* 43: 470–475.
Rao, S.S. (1992). *Reliability-Based Design*. New York: McGraw-Hill Inc.
Thoft-Chirstensen, P. and Baker, M.J. (1982). *Structural Reliability Theory and Its Application*. Berlin: Springer-Verlag.

Exercises

8.1 A design engineer knows that one-half of the lightning loads on a surge protection system are greater than 500 V. Based on previous experience, such loads are known to follow the PDF:

$$f(v) = \gamma e^{-\gamma v}, \quad 0 \leq v < \infty .$$

a) Estimate γ per volt.
b) What is the mean load?
c) For what voltage should the system be designed if the failure probability is not to exceed 5%?

8.2 Given the following distributions of capacity and load, determine the failure probability:

$$\begin{aligned} f_c(c) &= 5c^4; \quad && 0 < c < 1 \\ &= 0; && \text{otherwise} \\ f_l(l) &= 2; && 0 < l < 1/2 \\ &= 0; && \text{otherwise} \end{aligned}$$

8.3 Suppose that the PDFs for load and capacities are

$$f_1(l) = \gamma e^{-\lambda l}, \qquad 0 \leq l \leq \infty$$

$$f_c(c) = \begin{cases} 0, & 0 \leq c < a \\ 1/a, & a \leq c \leq 2a \\ 0, & 2a < c \leq \infty \end{cases}$$

Determine the reliability; evaluate all integrals.

8.4 The impact loading on a railroad coupling is expressed as an exponential distribution:

$$f_1(l) = \beta e^{-\beta l}$$

The coupling is designed to have a capacity $\mathbf{c} = c_m$. However, because of material flaws, the PDF for the capacity is more accurately expressed as

$$f_c(c) = \begin{cases} \dfrac{\alpha e^{\alpha c}}{\exp(\alpha c_m) - 1}, & 0 \le c \le c_m \\ 0, & c > c_m \end{cases}$$

a) Determine the reliability for a single loading, assuming that the flaws can be neglected.
b) Recalculate a using the capacity distribution with the flaws included.
c) Show that the result of b reduces to that of a as $\alpha \to \infty$.
d) Show that for $\alpha = 0$, the reliability is

$$r = 1 - \frac{1}{\beta c_m}\left[1 - e^{-\beta c_m}\right]$$

8.5 It is estimated that the capacity of a newly designed structure is $\bar{c} = 10,000$ kips, $\sigma_c = 6000$ kips, normally distributed. The anticipated load on the structure will be $\bar{l} = 5000$ kips, with an uncertainty of $\sigma_l = 1500$ kips, also normally distributed. Find the *un*reliability of the structure.

8.6 A structural code requires that the reliability index of a cable must have a value of at least $\beta_R = 5.0$. If the load and capacity may be considered to be normally distributed with coefficients of variation of $\rho_l = 0.2$ and $\rho_c = 0.1$, respectively, what safety factor must be used?

8.7 Steel cable strands have a normally distributed strength with a mean of 5000 lb and a standard deviation of 150 lb. The strands are incorporated into a crane cable that is proof tested at 50,000 lb. It is specified that no more than 2% of the cables may fail the proof test. How many strands should be incorporated into the cable, assuming that the cable strength is the sum of the strand strengths?

8.8 **Substitute** the normal distributions for load and capacity, Eqs. (8.29) and (8.30), into the reliability expression, Eq. (8.20). Show that the resulting integral reduces to Eqs. (8.41) and (8.43).

8.9 The twist strength of a standard bolt is 23 N m with a standard deviation of 1.3 N m. The wrenches used to tighten such bolts have an uncertainty of $\sigma = 2.0$ N m in their torsion settings. If no more than 1 bolt in 1000 may fail from excessive tightening, what should the setting be on the wrenches? (Assume normal distributions.)

8.10 Suppose that a car hits potholes spaced at random distances at a rate of 20/hour. The loading on the wheel bolts caused by these potholes is exponentially distributed.

$$f_l(l) = 0.6\exp(-0.6l), \quad 0 \le l \le \infty$$

What will the failure rate be if the bolt capacity is designed to be exactly eight times the mean value of the pothole loading?

8.11 Suppose that both load and capacity are known to a factor of 2 with 90% confidence. Assuming lognormal distributions, determine the safety factor c_0/l_0 necessary to obtain a reliability of 0.995.

8.12 Show in detail that Eq. (8.61) follows from Eqs. (8.30) and (8.60).

8.13 The loading on industrial fasteners of fixed capacity is known to follow an exponential distribution. Thirty percent of the fasteners fail. If the fasteners are redesigned to double their capacity, what fraction will be expected to fail?

8.14 Consider a pressure vessel for which the capacity is defined as p, the maximum internal pressure that the vessel can withstand without bursting. This pressure is given by $p = \tau_0\sigma_m/2R$, where τ_0 is the unflawed thickness, σ_m is the stress at which failure occurs, and R is the radius. Suppose that the vessel thickness is τ ($\geq\tau_0$), but the PDF for the maximum depths of undetected crack in steel piping is distribution of crack depths is

$$f(x) = \frac{1}{\gamma}\frac{e^{-x/\gamma}}{(1-e^{-\tau/\gamma})} \quad \text{where } \tau \text{ is the pipe thickness, and } \gamma = 6.25\text{ mm.}$$

Show that the PDF for capacity is

$$f_{\rm p}(p) \equiv \begin{cases} \dfrac{2R}{\gamma\sigma_m}\dfrac{1}{e^{\tau/\gamma}-1}\exp\left(\dfrac{2R}{\gamma\sigma_m}p\right), & 0 \leq p \leq \dfrac{\tau\sigma_m}{2R} \\ 0, & p > \dfrac{\tau\sigma_m}{2R} \end{cases}$$

a) Normalize to $\tau\sigma_m/2R = 1$ and then plot $f_{\rm p}(p)$ for $\gamma = \tau$, $0.5\ \tau$, and $0.1\ \tau$.
b) Physically interpret the results of your plots.

8.15 In Exercise 8.14, suppose that the vessel is proof tested at a pressure of $p = \tau\sigma_m/4R$. What is the probability of failure if
a) $\gamma = 0.5\ \tau$?
b) $\gamma = 0.1\ \tau$?

8.16 A system under a constant load, l, has a known capacity that varies with time as $c(t) = c_0(1 - 0.02\ t)$. The safety factor at $t = 0$ is 2.
a) Sketch $R(t)$.
b) What is the MTTF?
c) What is the variance of the time to failure?

8.17 Suppose that steel wire has a mean tensile strength of 1200 lb. A cable is to be constructed with a capacity of 10,000 lb. How many wires are required for a reliability of 0.999
a) if the wires have a 2% coefficient of variation?
b) if the wires have a 5% coefficient of variation?
(*Note:* Assume that the strengths are normally distributed and that the cable strength is the sum of the wire strengths.)

8.18 Consider a chain consisting of N links that is subjected to M loads. The capacity of a single link is described by the PDF $f_c(c)$. The PDF for any one of the loads is described by $f_1(l)$. Derive an expression in terms of $f_c(c)$ and $f_1(l)$ for the probability that the chain will fail from the M loadings.

8.19 Suppose that the CDF for loading on a cable is

$$F_1(l) = 1 - \exp\left[-\left(\frac{l}{500}\right)^3\right]$$

where l is in pounds. To what capacity should the cable be designed if the probability of failure is to be no more than 0.5%?

8.20 Suppose that the design criteria for a structure is that the probability of an earthquake severe enough to do structural damage must be no more than 1.0% over the 40-year design life of the building.

a) What is the probability of one or more earthquakes of this magnitude or greater occurring during any one year?
b) What is the probability of the structure being subjected to more than one damaging earthquake over its design life?

8.21 The total load on a building may often be represented as the sum of three contributions: the dead load **d**, from the weight of the structure; the live load **l**, from human beings, furniture, and other movable weights; and the wind load **w**. Suppose that the loads from each of the sources on a support column are represented as normal distributions with the following properties:

$$\mu_d = 6.0 \text{ kips}, \quad \sigma_d = 0.4 \text{ kips}$$
$$\mu_l = 9.2 \text{ kips}, \quad \sigma_l = 1.2 \text{ kips}$$
$$\mu_w = 4.6 \text{ kips}, \quad \sigma_w = 1.1 \text{ kips}$$

a) Determine the mean and standard deviation of the total load.
b) Assume that the column is to be built with a safety factor of 1.6. If the strength of the column is normally distributed with a 20% coefficient of variation, what is the probability of failure?

8.22 Prove that Eqs. (8.72) and (8.79) reduce to Eqs. (8.82) and (8.83) under the assumptions of constant loading and no capacity deterioration.

8.23 The impact load on a landing gear is known to follow an extreme-value distribution with a mean value of 2500 and a variance of 25×10^4. The capacity is approximated by a normal distribution with a mean value of 15,000 and a coefficient of variation of 0.05. Find the probability of failure per landing.

8.24 Prove that Eqs. (8.72) and (8.79) reduce to Eqs. (8.85) and (8.86) under the assumption of constant loading.

8.25 A dam is built with a capacity to withstand a flood with a return period (i.e. mean time between floods) of 100 years. What is the probability that the capacity of the dam will be exceeded during its 40-year design life?

8.26 Suppose that the capacity of a system is given by

$$f_c(c) = \frac{1}{\sqrt{2\pi}\sigma_c} \exp\left\{-\frac{1}{2\sigma_c^2}[c-\bar{c}(t)]^2\right\}$$

where

$$\bar{c}(t) = c_0(1-\alpha t)$$

If the system is placed under a constant load l,

a) Find $f(t)$, the PDF for time to failure.
b) Put $f(t)$ into a standard normal form and find σ_t and the MTTF.

8.27 A manufacturer of telephone switchboards was using switching circuits from a single supplier. The circuits were known to have a failure rate of 0.06/year. In its new board, however, 40% of the switching circuits came from a new supplier. Reliability testing indicates that the switchboards have a composite failure rate that is initially 80% higher than it was with circuits from the single supplier. The failure rate, however, appears to be decreasing with time.

a) Estimate the failure rate of the circuits from the new supplier.
b) What will the failure rate per circuit be for long periods of time?
c) How long should the switchboards be worn in if the average failure rate of circuits should be no more than 0.1/year?

Note: See Example 8.6.

8.28 Suppose that a system has a time-independent failure rate that is a linear function of the system capacity c,

$$\lambda(c) = \lambda_0[1 + b(c_m - c)], \quad b > 0$$

where c_m is the design capacity of the system. Suppose that the presence of flaws causes the PDF or capacity of the system to be given by $f_c(c)$ in Exercise 8.4.

a) Find the system failure rate.
b) Show that it decreases with time.

8.29 The most probable strength of a steel beam is given by $24N^{-0.05}$ kips, where N is the number of cycles. This value is known to be within 25% with 90% confidence.

a) How many cycles will elapse before the beam loses 20% of its strength?
b) Suppose that the cyclic load on the beam is 10 kips. How many cycles can be applied before the probability of failure reaches 10%?

Note: Assume a lognormal distribution.

Supplement 1: The Dirac Delta Distribution

If the normal distribution is used to describe a random variable $\mathbf{x}$, the mean μ is the measure of the average value of x, and the standard deviation σ is a measure of the dispersion of x about μ. Suppose that we consider a series of measurements of a quantity μ with increasing precision. The PDF for the measurements might look like Figure 8Sup.1. As the precision is increased – decreasing the uncertainty – the value of σ decreases. In the limit where there is no uncertainty $\sigma \to 0$, $\mathbf{x}$ is no longer a random variable, for we know that $\mathbf{x} = \mu$.

The Dirac delta function is used to treat this situation. It may be defined as

$$\delta(x-\mu) = \lim_{\sigma \to 0} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \tag{8Sup1.1}$$

Figure 8Sup.1 Normal distributions with different values of the variance.

Two extremely important properties immediately follow from this definition:

$$\delta(x-\mu) = \begin{cases} \infty & x = \mu \\ 0 & x = 0 \end{cases} \tag{8Sup1.2}$$

and

$$\int_{\mu-\varepsilon}^{\mu+\varepsilon} \delta(x-\mu)dx = 1 \tag{8Sup1.3}$$

Specifically, even though $\delta(0)$ is infinite, the area under the curve is equal to one.

The primary use of the Dirac delta function in this book is to simplify integrals in which one of the variables has a fixed value. This appears, for example in the treatment of expected values.

Suppose that we want to calculate the expected value of $g(x)$, as given by Eq. (4.17) when $f(x) = \delta(x - x_0)$; then,

$$E\{g(x)\} = \int_{-\infty}^{\infty} g(x)\delta(x-x_0)dx \tag{8Sup1.4}$$

may be written as

$$E\{g(x)\} = \int_{x_0-\varepsilon}^{x_0+\varepsilon} g(x)\delta(x-x_0)dx \quad \varepsilon > 0 \tag{8Sup1.5}$$

since $\delta(x - x_0) = 0$ away from $x = x_0$. If $g(x)$ is continuous, we may pull it outside the integral for very small ε to yield

$$E\{g(x)\} = g(x_0)\int_{x_0-\varepsilon}^{x_0+\varepsilon} \delta(x-x_0)dx \tag{8Sup1.6}$$

Therefore, for arbitrarily small ε, we obtain

$$E\{g(x)\} \equiv \int_{x_0-\varepsilon}^{x_0+\varepsilon} g(x)\delta(x-x_0)dx = g(x_0) \tag{8Sup1.7}$$

A more rigorous proof may be provided using Eq. (8Sup1.1) in Eq. (8Sup1.4) and expanding $g(x)$ in a power series about x_0.

9

Maintained Systems

> "A little neglect may breed great mischief…
> for want of a nail the shoe was lost;
> for want of a shoe the horse was lost;
> and for want of a horse the rider was lost."
>
> *Source*: Benjamin Franklin; Poor Richard's Almanac (1758). Public Domain

9.1 Introduction

Relatively few systems are designed to operate without maintenance of any kind, and for the most part they must operate in environments where access is very difficult, in outer space or high-radiation fields, for example or where replacement is more economical than maintenance. For most systems there are two classes of maintenance, one or both of which may be applied. In preventive maintenance, parts are replaced, lubricants changed, or adjustments made before failure occurs. The objective is to increase the reliability of the system over the long term by staving off the aging effects of wear, corrosion, fatigue, and related phenomena. In contrast, repair or corrective maintenance is performed after failure has occurred in order to return the system to service as soon as possible. Although the primary criteria for judging preventive-maintenance procedures is the resulting increase in reliability, a different criterion is needed for judging the effectiveness of corrective maintenance. The criterion most often used is the system availability, which is defined roughly as the probability that the system will be operational when needed.

The amount and type of maintenance that is applied depends strongly on its costs as well as the cost and safety implications of system failure. Thus, for example in determining the maintenance for an electric motor used in a manufacturing plant, we would weigh the costs of preventive maintenance against the money saved from the decreased number of failures. The failure costs would need to include, of course, both those incurred in repairing or replacing the motor and those from the loss of production during the unscheduled downtime for repair. For an aircraft engine the trade-off would be much different: the potentially disastrous consequences of engine failure would eliminate repair maintenance as a primary consideration. Concern would be with how much preventive maintenance can be afforded and with the possibility of failures induced by faculty maintenance.

In both preventive and corrective maintenance, human factors play a very strong role. It is for this reason that laboratory data are often not representative of field data. In field service, the quality of preventive maintenance is not likely to be as high. Moreover, repairs carried out in the field are

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

likely to take longer and to be less than perfect. The measurement of maintenance quantities thus depends strongly on human reliability so that there is great difficulty in obtaining reproducible data. The numbers depend not only on the physical state of the hardware but also on the training, vigilance, and judgment of the maintenance personnel. These quantities in turn depend on many social and psychological factors that vary to such an extent that the probabilities of maintenance failures and repair times are generally more variable than the failure rates of the hardware.

In this chapter, we first examine preventive maintenance. Then, we define and discuss availability and other quantities needed to treat corrective maintenance. Subsequently, we examine the repair of two types of failure: those that are revealed (i.e. immediately obvious) and those that are unrevealed (i.e. are unknown until tests are run to detect them). Finally, we examine the relation of a system to its components from the point of view of corrective maintenance.

9.2 Preventive Maintenance

In this section, we examine the effects of preventive maintenance on the reliability of a system or component. We first consider ideal maintenance in which the system is restored to an as-good-as-new condition each time maintenance is applied. We then examine more realistic situations in which the improvement in reliability brought about by maintenance must be weighed against the possibility that faulty maintenance will lead to system failure. Finally, the effects of preventive maintenance on redundant systems are examined.

Idealized Maintenance

Suppose that we denote the reliability of a system without maintenance as $R(t)$, where t is the operation time of the system; it includes only the intervals when the system is actually operating and not the time intervals during which it is shut down. If we perform maintenance on the system at time intervals T, then, as indicated in Figure 9.1, for $t < T$ maintenance will have no effect on reliability. That is, if $R_M(t)$ is the reliability of the maintained system,

$$R_M(t) = R(t), \quad 0 \le t < T \tag{9.1}$$

Now suppose that we perform maintenance at T, restoring the system to an as-good-as-new condition. This implies that the maintained system at $t > T$ has no memory of accumulated wear effects for times before T. Thus, in the interval $T < t \le 2T$, the reliability is the product of the probability R

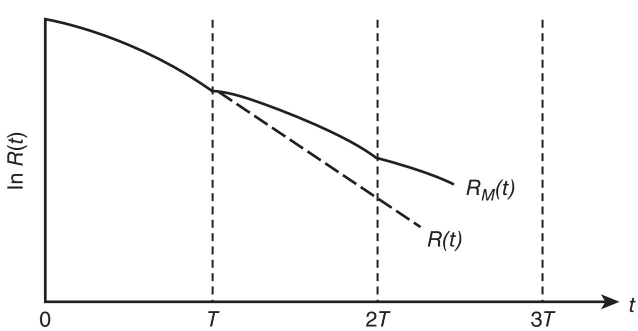


Figure 9.1 The effect of preventive maintenance on reliability.

(T) that the system survived to T, and the probability $R(t - T)$ that a system as good as new at T will survive for a time $t - T$ without failure:

$$R_M(t) = R(T)R(t-T), \quad T \leq t < 2T \tag{9.2}$$

Similarly, the probability that the system will survive to time t, $2T \leq t < 3T$, is just the reliability $R_M(2T)$ multiplied by the probability that the newly restored system will survive for a time $t - 2T$:

$$R_M(t) = R(T)^2 R(t-2T), \quad 2T \leq t < 3T \tag{9.3}$$

The same argument may be used repeatedly to obtain the general expression

$$R_M(t) = R(T)^N R(t-NT), \quad NT \leq t < (N+1)T, \quad N = 0, 1, 2, \ldots. \tag{9.4}$$

The mean time to failure (MTTF) for a system with preventive maintenance can be determined by replacing $R(t)$ by $R_M(t)$ in Eq. (3.22):

$$\text{MTTF} = \int_0^\infty R_M(t)\, dt \tag{9.5}$$

To evaluate this expression, we first divide the integral into time intervals of length T:

$$\text{MTTF} = \sum_{N=0}^{\infty} \int_{NT}^{(N+1)T} R_M(t)\, dt \tag{9.6}$$

Then, inserting Eq. (9.4), we have

$$\text{MTTF} = \sum_{N=0}^{\infty} \int_{NT}^{(N+1)T} R(T)^N R(t-NT)\, dt \tag{9.7}$$

Setting $t' = t - NT$ then yields

$$\text{MTTF} = \sum_{N=0}^{\infty} R(T)^N \int_0^T R(t')\, dt' \tag{9.8}$$

Then, evaluating the infinite series,

$$\sum_{n=0}^{\infty} R(T)^N = \frac{1}{1 - R(T)} \tag{9.9}$$

we have

$$\text{MTTF} = \frac{\int_0^T R(t)\, dt}{1 - R(T)} \tag{9.10}$$

We would now like to estimate how much improvement, if any, in reliability we derive from the preventive maintenance. The first point to be made is that in random or chance failures (i.e. those represented by a constant failure rate λ), idealized maintenance has no effect. This is easily proved by putting $R(t) = e^{-\lambda t}$ on the right-hand side of Eq. (9.4). We obtain

$$R_M(t) = \left(e^{-\lambda t}\right)^N e^{-\lambda(t-NT)} = e^{-N\lambda t} e^{-\lambda(t-NT)} = e^{-\lambda t} \tag{9.11}$$

or simply

$$R_M(t) = R(t), \quad 0 \leq t \leq \infty \tag{9.12}$$

Preventive maintenance has a quite definite effect, however, when aging or wear causes the failure rate to become time dependent. To illustrate this effect, suppose that the reliability can be represented by the two-parameter Weibull distribution described in Chapter 5. For the system without maintenance, we have

$$R(t) = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \tag{9.13}$$

Equation (9.4) then yields for the maintained system

$$R_M(t) = \exp\left[-N\left(\frac{T}{\eta}\right)^{\beta}\right]\exp\left[-\left(\frac{t-NT}{\eta}\right)^{\beta}\right], \quad NT \le t < (N+1)T, \quad N = 0, 1, 2, ... \tag{9.14}$$

To examine the effect of maintenance, we calculate the ratio $R_M(t)/R(t)$. The relationship is simplified if we calculate this ratio at the time of maintenance $t = NT$:

$$\frac{R_M(NT)}{R(NT)} = \exp\left[-N\left(\frac{T}{\eta}\right)^{\beta} + \left(\frac{NT}{\eta}\right)^{\beta}\right] \tag{9.15}$$

Thus, there will be a gain in reliability from maintenance only if the argument of the exponential is positive, that is if $(NT/\eta)^{\beta} > N(T/\eta)^{\beta}$. This reduces to the condition

$$N^{\beta-1} - 1 > 0. \tag{9.16}$$

This states simply that β must be greater than 1 for maintenance to have a positive effect on reliability; it corresponds to a failure rate that is increasing with time through aging. Conversely, for $\beta < 1$, preventive maintenance decreases reliability. This corresponds to a failure rate that is decreasing with time through early failure. Specifically, if new defective parts are introduced into a system that has already been "worn in," increased rates of failure may be expected. These effects on reliability are illustrated in Figure 9.2, where Eq. (9.14) is plotted for both increasing ($\beta > 1$) and decreasing ($\beta < 1$) failure rates, along with random failures ($\beta = 1$).

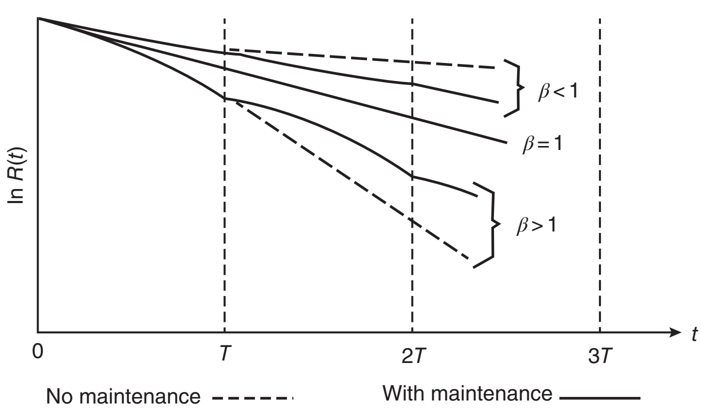


Figure 9.2 The effect of preventive maintenance on reliability: $\beta > 1$, increasing failure rate; $\beta < 1$, decreasing failure rate; $\beta = 1$, constant failure rate.

Naturally, a system may have several modes of failure corresponding to increasing and decreasing failure rates. For example, in Chapter 3 we note that the bathtub curve for a device may be expressed as the sum of Weibull distributions:

$$\int_0^t \lambda(t')\ dt' = \left(\frac{t}{\eta_1}\right)^{\beta_1} + \left(\frac{t}{\eta_2}\right)^{\beta_2} + \left(\frac{t}{\eta_3}\right)^{\beta_3} \tag{9.17}$$

For this system, we must choose the maintenance interval for which the positive effect on wearout time is greater than the negative effect on wearin time. In practice, the terms in Eq. (9.17) may be due to different components of the system. Thus, we would perform preventive maintenance only on the components for which the wearout effect dominates. For example, we may replace worn spark plugs in an engine without even considering replacing a fuel injection system with a new one, which might itself be defective.

Example 9.1 A compressor is designed for five years of operation. There are two significant contributions to the failure rate. The first is due to wear of the thrust bearing and is described by a Weibull distribution with $\eta = 7.5$ year and $\beta = 2.5$. The second, which includes all other causes, is a constant failure rate of $\lambda_0 = 0.013$/year.

a) What is the reliability if no preventive maintenance is performed over the five-year design life?
b) If the reliability of the five-year design life is to be increased to at least 0.9 by periodically replacing the thrust bearing, how frequently must it be replaced?

Solution:
Let $T_d = 5$ be the design life.
(a) The system reliability may be written as

$$R(T_d) = R_0(T_d)R_M(T_d)$$

where

$$R_0(T_d) = e^{-\lambda_0 T_d} = e^{-0.013\times 5} = 0.9371$$

is the reliability if only the constant failure rate is considered. Similarly,

$$R_M(T_d) = e^{-(T_d/\eta)^\beta} = e^{-(5/7.5)^{2.5}} = 0.6957$$

is the reliability if only the thrust bearing wear is considered. Thus,

$$R(T_d) = 0.9371 \times 0.6957 = 0.6519$$

(b) Suppose that we divide the design life into N equal intervals; the time interval, T, at which maintenance is carried out is then $T = T_d/N$. Correspondingly, $T_d = NT$. For bearing replacement at time interval T, we have from Eq. (9.14),

$$R_M(T_d) = \exp\left[-N\left(\frac{T_d}{N\eta}\right)^\beta\right] = \exp\left[-N^{1-\beta}\left(\frac{T_d}{\eta}\right)^\beta\right]$$

For the criterion to be met, we must have

$$R_M(T_d) = \frac{R(T_d)}{R_0(T_d)} \geq \frac{0.9}{0.9371} = 0.9604$$

With $(T_d/\eta)^\beta = (5/7.5)^{2.5} = 0.36289$, we calculate
$R_M(T_d) = \exp(-0.36289^{-1.5})$

N	1	2	3	4	5
$R_M(T_d)$	0.696	0.880	0.933	0.956	0.968

Thus, the criterion is met for $N = 5$, and the time interval for bearing replacement is $T = T_d/N = \frac{5}{5} = 1$ year.

In Chapter 3, we state that even when wear is present, a constant failure rate model may be a reasonable approximation, provided that preventive maintenance is carried out, with timely replacement of wearing parts. Although this may be intuitively clear, it is worthwhile to demonstrate it with our present model. Suppose that we have a system for which wearin effects can be neglected, allowing us to ignore the first term in Eq. (9.17) and write

$$R(t) = \exp\left[-\frac{t}{\eta_2} - \left(\frac{t}{\eta_3}\right)^{\beta_3}\right] \tag{9.18}$$

The corresponding expression for the maintained system given by Eq. (9.4) becomes

$$R_M(t) = \exp\left[-N\left(\frac{T}{\eta_3}\right)^{\beta_3}\right]\exp\left[-\frac{t}{\eta_2} - \left(\frac{t-NT}{\eta_3}\right)^{\beta_3}\right], \quad NT \le t \le (N+1)T \tag{9.19}$$

For a maintained system, the failure rate may be calculated by replacing R by R_M in Eq. (3.15):

$$\lambda_M(t) = -\frac{1}{R_M(t)}\frac{d}{dt}R_M(t) \tag{9.20}$$

Thus, taking the derivative, we obtain

$$\lambda_M(t) = \frac{1}{\eta_2} + \frac{\beta_3}{\eta_3}\left(\frac{t-NT}{\eta_3}\right)^{\beta_3 - 1}, \quad NT \le t < (N+1)T \tag{9.21}$$

Provided that the second term, the wear term, is never allowed to become substantial compared to the first, the random-failure term, the overall failure rate may be approximated as a constant by averaging over the interval T. This is illustrated for a typical set of parameters in Figure 9.3.

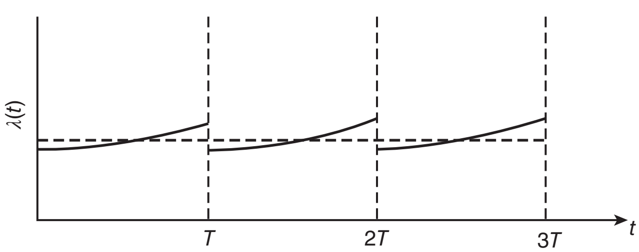


Figure 9.3 Failure rate for a system with preventive maintenance.

Imperfect Maintenance

Next, consider the effect of a less-than-perfect human reliability on the overall reliability of a maintained system. This enters through a finite probability p that the maintenance is carried out unsatisfactorily in such a way that the faulty maintenance causes a system failure immediately thereafter. To take this into account in a simple way, we multiply the reliability by the maintenance nonfailure probability, $1 - p$, each time that maintenance is performed. Thus, Eq. (9.4) is replaced by

$$R_M(t) = R(T)^N(1-p)^N R(t-NT), \quad NT < t < (N+1)T, \quad N = 0, 1, 2, \ldots. \tag{9.22}$$

The trade-off between the improved reliability from the replacement of wearing parts and the degradation that can come about because of maintenance error may now be considered. Since random failures are not affected by preventive maintenance, we consider the system in which only aging is present using Eq. (9.13) with $\beta > 1$. Once again, the ratio R_M/R after the Nth preventive maintenance is a useful indication of performance. Note that for $p \ll 1$, we may approximate

$$(1-p)^N \approx e^{-Np} \tag{9.23}$$

to obtain

$$\frac{R_M(NT)}{R(NT)} = \exp\left[-N\left(\frac{T}{\eta}\right)^\beta - Np + \left(\frac{NT}{\eta}\right)^\beta\right] \tag{9.24}$$

For there to be an improvement from the imperfect maintenance, the argument of the exponential in this expression must be positive. This reduces to the condition

$$p < \left(N^{\beta-1} - 1\right)\left(\frac{T}{\eta}\right)^\beta \tag{9.25}$$

Consequently, the benefits from imperfect maintenance are not seen until a long time, when either N or T is large. This is plausible because after a long time wear effects degrade the reliability enough that the positive effect of maintenance compensates for the probability of maintenance failure. This is illustrated in Figure 9.4.

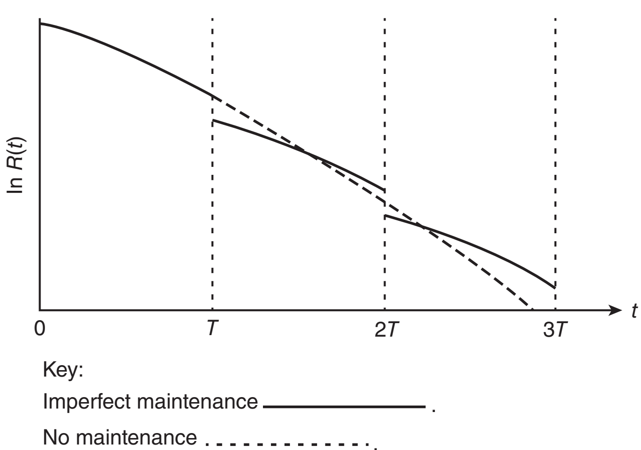


Figure 9.4 The effect of imperfect preventive maintenance on reliability.

Example 9.2 Suppose that in Example 9.1 the probability of faulty bearing replacement causing failure of the compressor is $p = 0.02$. What will the design-life reliability be with the annual replacement program?

Solution:
At the end of the design life ($T_d = 5$ years) maintenance will have been performed four times. From the preceding problem we take the perfect maintenance result to be

$$R(T_d) = R_0 R_M = 0.907 \times 0.968 = 0.907$$

With imperfect maintenance,

$$R(T_d) = R_0 R_M (1 - p)^4 = 0.907 \times 0.98^4 = 0.907 \times 0.922 = 0.836$$

In evaluating the trade-off between maintenance and aging, we must examine the failure mode very closely. Suppose, for example that we consider the maintenance of an engine. If after maintenance the engine fails to start, but no damage is done, the failure may be corrected by redoing the maintenance. In this case, p may be set equal to zero in the model just given, with the understanding that preventive maintenance includes a checkout and a repair of maintenance errors.

The situation is potentially more serious if the maintenance failure damages the system or is delayed because it is an induced early failure. We consider each of these problems separately. Suppose first that after maintenance the engine is started and is irreparably damaged by the maintenance error. Whether maintenance is desirable in these circumstances strongly depends on the failure mode that the maintenance is meant to prevent. If the engine's normal mode of failure is simply to stop running because a component is worn, with no damage to the remainder of the engine, it is unlikely that even the increased reliability provided by the preventive maintenance is economically worthwhile. Provided that there are no safety issues at stake, it may be more expedient to wait for failure, and then repair, rather than to chance damage to the system through faulty maintenance. If we are concerned about servicing an *aircraft* engine, however, the situation is entirely different. Damaging or destroying an occasional engine on the ground following faulty maintenance may be entirely justified in order to decrease the probability that wear will cause an engine to fail in flight.

Consider, finally, the situation in which the maintenance does not cause immediate failure but adds a wearin failure rate. This may be due to the replacement of worn components with defective new ones. However, it is equally likely to be due to improper installation or reassembly of the system, thereby placing excessive stress on one or more of the components. After the first repair, we then have a failure rate described by a bathtub curve, as in Eq. (9.17), with the first term stemming at least in part from imperfect maintenance. The reliability is then determined by inserting Eq. (9.17) into Eq. (9.4). If we assume that the early failure term is due to faulty maintenance, it may be shown by again calculating $R_M(NT)/R(NT)$ that the reliability is improved only if

$$\left(1 - N^{\beta_1 - 1}\right)\left(\frac{T}{\eta_1}\right)^{\beta_1} < \left(N^{\beta_3 - 1} - 1\right)\left(\frac{T}{\eta_3}\right)^{\beta_3}, \quad \beta_1 < 1, \beta_3 > 1 \tag{9.26}$$

Whether or not an increase in overall reliability is the only criterion to be used once again depends on whether the failure modes are comparable in the system damage that is done. If no safety questions are involved, it is primarily a question of weighing the costs of repairing the failures caused by aging against those induced by maintenance errors. This might be the case, for example with an automobile engine. With an aircraft engine, however, prevention of failure in flight must be the overriding criterion; the cost of repairing the engine following failure, of course, is not relevant if the plane crashes. In this, and similar situations, the more important consideration is often the effect of maintenance errors on redundant systems because maintenance is one of the primary causes of common-mode failures. We examine these next.

Redundant Components

The foregoing expressions for $R_M(t)$ may be used in calculating the reliability of redundant systems as in Chapter 3, but only if the maintenance failures on different components are independent of one another. This stipulation is frequently difficult to justify. Although some maintenance failures are independent, such as the random neglect to tighten a bolt, they are more likely to be systematic; if the wrong lubricant is put in one engine, it is likely to be put in a second one also.

The common-mode failure model introduced in Chapter 3 may be applied with some modification to treat such dependent maintenance failures. As an example we consider a parallel system consisting of two identical components. If the maintenance is imperfect but independent, we may insert Eq. (9.22) into Eq. (9.5) to obtain

$$R_I(t) = 2R(T)^N(1-p)^N R(t-NT) - R(T)^{2N}(1-p)^{2N} R(t-NT)^2, \quad NT \le t < (N+1)T \quad N = 0,\ 1,\ 2, \ldots \tag{9.27}$$

Suppose that a maintenance failure on one component implies that the same failure occurs simultaneously in the other. We account for this by separating out the maintenance failures into a series component, much as we did with the common-mode failure rate λ_c in Chapter 3. Thus, the system failure is modeled by taking the reliability for perfect maintenance (i.e. $p = 0$) and multiplying by $1-p$ for each time that maintenance is performed. Thus, for dependent maintenance failures,

$$R_D(t) = \left\{2R(T)^N R(t-NT) - R(T)^{2N} R(t-NT)^2\right\}(1-p)^N, \quad NT \le t < (N+1)T, \quad N = 0, 1, 2, \ldots \tag{9.28}$$

The degradation from maintenance-induced common-mode failures is indicated by the ratio of Eqs. (9.28) to (9.27). We find

$$\frac{R_D(NT)}{R_I(NT)} = \frac{1 - \frac{1}{2}R(T)^N}{1 - \frac{1}{2}(1-p)^N R(T)^N} \tag{9.29}$$

The value of this ratio is less than 1, and it decreases each time imperfect preventive maintenance is performed.

9.3 Corrective Maintenance

With or without preventive maintenance, the definition of reliability has been central to all our deliberations. This is no longer the case, however, when we consider the many classes of systems in which corrective maintenance plays a substantial role. Now, we are interested not only in the probability of failure but also in the number of failures and, in particular, in the times required to make repairs. For such considerations, two new reliability parameters become the focus of attention. Availability is the probability that a system is available for use at a given time. Roughly, it may be viewed as a fraction of time that a system is in an operational state. Maintainability is a measure of how fast a system may be repaired following failure. Both availability and maintainability, however, require more formal definitions if they are to serve as a quantitative basis for the analysis of repairable systems.

Availability

For repairable systems a fundamental quantity of interest is the availability. It is defined as follows:

$$A(t) = \text{probability that a system is performing satisfactory at time } t \tag{9.30}$$

This is referred to as the point availability. Often, it is necessary to determine the interval or mission availability. The interval availability is defined by

$$A^*(T) = \frac{1}{T}\int_0^T A(t)\,dt \tag{9.31}$$

It is just the value of the point availability averaged over some interval of time, T. This interval may be the design life of the system or the time to accomplish some particular mission. Finally, it is often found that after some initial transient effects the point availability assumes a time-independent value. In these cases, the steady-state or asymptotic availability is defined as

$$A^*(\infty) = \lim_{T\to\infty}\frac{1}{T}\int_0^T A(t)\,dt \tag{9.32}$$

If a system or its components cannot be repaired, the point availability is just equal to the reliability. The probability that it is available at t is just equal to the probability that it has not failed between 0 and t:

$$A(t) = R(t) \tag{9.33}$$

Combining Eqs. (9.31) and (9.33), we obtain

$$A^*(T) = \frac{1}{T}\int_0^T R(t)\,dt \tag{9.34}$$

Thus, as T goes to infinity, the numerator, according to Eq. (3.22), becomes the MTTF, a finite quantity. The denominator, T, however, becomes infinite. Thus, the steady-state availability of a nonrepairable system is

$$A^*(\infty) = 0 \tag{9.35}$$

Since all systems eventually fail, and there is no repair, the availability averaged over an infinitely long time span is zero.

Example 9.3 A nonrepairable system has a known MTTF and is characterized by a constant failure rate. The system mission availability must be 0.95. Find the maximum design life that can be tolerated in terms of the MTTF.

Solution:
For a constant failure rate, the reliability is $R = e^{-\lambda t}$. Insert this into Eq. (9.34) to obtain

$$A^*(T) = \frac{1}{\lambda T}\left(1 - e^{-\lambda T}\right)$$

Expanding the exponential then yields

$$A(T) = \frac{1}{\lambda T}\left(1 - 1 + \lambda T - \frac{1}{2}(\lambda T)^2 + \cdots\right)$$

Thus, $A(T) \approx 1 - \frac{1}{2}\lambda T$, for $\lambda T \ll 1$ or $0.95 = 1 - \frac{1}{2}\lambda T$. Then, $\lambda T = 0.1$, but MTTF $= 1/\lambda$. Therefore, $T = 0.1 \times$ MTTF.

Maintainability

We may now proceed to the quantitative description of repair processes and the definition of maintainability. Suppose that we let $\mathbf{t}$ be the time required to repair a system, measured from the time of failure. If all repairs take the same length of time, $\mathbf{t}$ is just a number, say $\mathbf{t} = \tau$. In reality, repairs require different lengths of time, and even the time to perform a given repair is uncertain because circumstances, skill level, and a host of other factors vary. Therefore, $\mathbf{t}$ is normally not a constant but rather a random variable. This variable can be considered in terms of distribution functions as follows.

Suppose that we define the probability density function (PDF) for repair as

$$m(t)\,\Delta t = P\{t \le \mathbf{t} \le t + \Delta t\} \tag{9.36}$$

That is, $m(t)\,\Delta t$ is the probability that repair will require a time between t and $t + \Delta t$. The CDF corresponding to Eq. (9.36) is defined as the maintainability

$$M(t) = \int_0^t m(t')\,dt' \tag{9.37}$$

and the *mean time to repair* or MTTR is then

$$\text{MTTR} = \int_0^\infty t m(t)\,dt \tag{9.38}$$

Analogous to the derivations of the failure rate given in Chapter 3, we may define the *instantaneous repair rate* as

$$v(t)\,\Delta t = \frac{P\{t \le \mathbf{t} \le t + \Delta t\}}{p\{\mathbf{t} > t\}} \tag{9.39}$$

$\nu(t)\,\Delta t$ is the conditional probability that the system will be repaired between t and $t + \Delta t$, given that it is failed at t. Noting that

$$M(t) = P\{\mathbf{t} \le t\} = 1 - P\{\mathbf{t} \ge t\} \tag{9.40}$$

we then have

$$v(t) = \frac{m(t)}{1 - M(t)} \tag{9.41}$$

Equations (9.37) and (9.41) may be used to express the maintainability and the PDF in terms of the repair rate. To do this, we differentiate Eq. (9.37) to obtain

$$m(t) = \frac{d}{dt}M(t) \tag{9.42}$$

and combine this result with Eq. (9.41) to yield

$$v(t) = [1 - M(t)]^{-1}\frac{d}{dt}M(t) \tag{9.43}$$

Moving dt to the left and integrating between 0 and t, we obtain

$$\int_0^1 v(t')\,dt' = \int_0^{M(t)} \frac{dM}{1-M} \tag{9.44}$$

Evaluating the integral on the right-hand side and solving for the maintainability, we have

$$M(t) = 1 - \exp\left[-\int_0^t v(t')\,dt'\right] \tag{9.45}$$

Finally, we may use Eq. (9.42) to express the PDF for repair times as

$$m(t) = v(t)\,\exp\left[-\int_0^t v(t')\,dt'\right] \tag{9.46}$$

A great many factors go into determining both the mean time to repair and the PDF, $m(t)$, by which the uncertainties in repair time are characterized. These factors range from the ability to diagnose the cause of failure, on the one hand, to the availability of equipment and skilled personnel to carry out the repair procedures on the other. The determining factors in estimating repair time vary greatly with the type of system that is under consideration. This may be illustrated with the following comparison.

In many mechanical systems the causes of the failure are likely to be quite obvious. If a pipe ruptures, a valve fails to open, or a pump stops running, the diagnoses of the component in which the mechanical failure have occurred may be straightforward. The primary time entailed in the repair is then determined by how much time is required to extract the component from the system and install the new component, for each of these processes may involve a good deal of metal cutting, welding, or other time-consuming procedures.

In contrast, if a computer fails, maintenance personnel may spend most of the repair procedure time in diagnosing the problem, for it may take considerable effort to understand the nature of the failure well enough to be able to locate the circuit board, chip, or other component that is the cause. Conversely, it may be a rather straightforward procedure to replace the faulty component once it has been located.

In both of these examples we have assumed that the necessary repair parts are available at the time they are needed and that it is obvious how much of the system should be replaced to eliminate the fault. In fact, both the availability of parts and the level of repair involve subtle economic trade-offs between the cost of inventory, personnel, and system downtime.

For example, suppose that the pump fails because bearings have burned out. We must decide whether it is faster to remove the pump from the line and replace it with a new unit or to tear it down and replace only the bearings. If the entire pump is to be replaced, on-site inventories of spare pumps will probably be necessary, but the level of skill needed by repair personnel to install the new unit may not be great. Conversely, if most of the pump failures are caused by bearing failures, it may make sense to stock only bearings on site and to repack the bearings. In such a case, repair personnel will need different and perhaps greater training and skill. Such trade-offs are typical of the many factors that must be considered in maintainability engineering, the discipline that optimizes $M(t)$ at a high level with as low a cost as possible.

9.4 Repair: Revealed Failures

In this section, we examine systems for which the failures are revealed, so that repairs can be immediately initiated. In these situations, two quantities are of primary interest, the number of failures over a given span of time and the system availability. The number of failures is needed in order to calculate a variety of quantities including the cost of repair and the necessary repair parts inventory. Provided that the MTTR is much smaller than the MTTF, reasonable estimates for the number of failures can be obtained using the Poisson distribution as in Chapter 2, and neglecting the system downtime for repair. For availability calculations, repair time must be considered or else we would obtain simply $A(t) = 1$. Ordinarily, this is not an acceptable approximation, for even small values of the unavailability $\widetilde{A}(t)$ are frequently important, whether they be due to the risk incurred through the unavailability of a critical safety system or to the production loss during the downtimes of an assembly line.

In what follows, two models for repair are developed to estimate the availability of a system, constant repair rate and constant repair time. It will be clear from comparing these that most of the more important results depend primarily on the MTTR, not on the details of the repair distribution.

Constant Repair Rates

To calculate availability, we must take the repair rate into account, even though it may be large compared to the failure rate. We assume that the distribution of times to repair can be characterized by a constant repair rate

$$v(t) = v \tag{9.47}$$

The PDF of times to repair is then exponential,

$$m(t) = ve^{-vt} \tag{9.48}$$

and the mean time to repair is simply

$$\text{MTTR} = 1/v \tag{9.49}$$

Although the exponential distribution may not reflect the details of the distribution very accurately, it provides a reasonable approximation for predicting availabilities, for these tend to depend more on the MTTR than on the details of the distribution. As we illustrate, even when the PDF of the repair is bunched about the MTTR rather than being exponentially distributed, the constant repair rate model correctly predicts the asymptotic availability.

Suppose that we consider a two-state system; it is either operational, state 1, or it is failed, state 2. Then, $A(t)$ and $\widetilde{A}(t)$, the availability and unavailability, are the probabilities that the state is operational or failed, respectively, at time t, where t is measured from the time at which the system operation commences. We therefore have the initial conditions $A(0) = 1$ and $\widetilde{A}(0) = 0$, and of course,

$$A(t) + \widetilde{A}(t) = 1 \tag{9.50}$$

A differential equation for the availability may be derived in a manner similar to that used for the Poisson distribution in Chapter 2. We consider the change in $A(t)$ between t and $t + \Delta t$. There are two contributions. Since $\lambda\,\Delta t$ is the conditional probability of failure during Δt, given that the system is available at t, the loss of availability during Δt is $\lambda\,\Delta t\,A(t)$. Similarly, the gain in availability is equal to $\nu \ \Delta t \ \widetilde{A} \ (t)$, where $\nu \ \Delta t$ is the conditional probability that the system is repaired during Δt, given that it is unavailable at t. Hence, it follows that

$$A(t + \Delta t) = A(t) - \lambda \ \Delta t A(t) + \nu \Delta t \widetilde{A}(t) \tag{9.51}$$

Rearranging terms and eliminating $\overline{A}(t)$ with Eq. (9.50), we obtain

$$\frac{A(t + \Delta t) - A(t)}{\Delta t} = -(\lambda + \nu)A(t) + \nu \tag{9.52}$$

Since the expression on the left-hand side is just the derivative with respect to time, Eq. (9.52) may be written as the differential equation,

$$\frac{d}{dt}A(t) = -(\lambda + \nu)A(t) + \nu \tag{9.53}$$

We now may use an integrating factor of $e^{\lambda+\nu}$, along with the initial condition $A(0) = 1$ to obtain

$$A(t) = \frac{\nu}{\lambda + \nu} + \frac{\lambda}{\lambda + \nu}e^{-(\lambda + \nu)t} \tag{9.54}$$

Note that the availability begins at $A(0) = 1$ and decreases monotonically to an asymptotic value $1/(1 + \lambda/\nu)$, which depends only on the ratio of failure to repair rate. The interval availability may be obtained by inserting Eq. (9.54) into Eq (9.31) to yield

$$A^*(T) = \frac{\nu}{\lambda + \nu} + \frac{\lambda}{(\lambda + \nu)^2 T}\left[1 - e^{-(\lambda + \nu)T}\right] \tag{9.55}$$

and the asymptotic availability is obtained by letting T go to infinity. Thus,

$$A^*(\infty) = \frac{\nu}{\lambda + \nu} \tag{9.56}$$

Finally, note from Eqs. (9.54) and (9.56) that for constant repair rates

$$A^*(\infty) = A(\infty) \tag{9.57}$$

Since, in most instances, repair rates are much larger than failure rates, a frequently used approximation comes from expanding Eq. (9.56) and deleting higher terms in λ/ν. We obtain after some algebra

$$A^*(\infty) \approx 1 - \lambda/\nu \tag{9.58}$$

The ratio in Eq. (9.56) may be expressed in terms of the mean time between failures and the mean time to repair. Since MTTF = $1/\lambda$ and MTTR = $1/\nu$, we have

$$A(\infty) = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \tag{9.59}$$

This expression is sometimes used for the availability even though neither failure or repair is characterized well by the exponential distribution. This is often quite adequate, for, in general, when availability is averaged over a reasonable period T of time, it is insensitive to the details of the failure or repair distributions. This is indicated for constant repair times in the following section.

Example 9.4 In the following table are times (in days) over a six-month period at which failure of a production line occurred (t_f) and times (t_r) at which the plant was brought back on line following repair.

i	t_{fi}	t_{ri}	i	t_{fi}	t_{ri}
1	12.8	13.0	6	56.4	57.3
2	14.2	14.8	7	62.7	62.8
3	25.4	25.8	8	131.2	134.9
4	31.4	33.3	9	146.7	150.0
5	35.3	35.6	10	177.0	177.1

a) Calculate the six-month-interval availability from the plant data.
b) Estimate MTTF and MTTR from the data.
c) Estimate the interval availability using the results of *b* and Eq. (9.59), and compare this result to that of *a*.

Solution:
During the six months (182.5 days) there are 10 failures and repairs.

a) From the data we find that $\widetilde{A}(T)$ is just the fraction of that time for which the system is inoperable. Thus, we find that

$$\widetilde{A}(T) = \frac{1}{T}\sum_{i=1}^{10}(t_{ri} - t_{fi})$$
$$= \frac{1}{182.5}(0.2 + 0.6 + 0.4 + 1.9 + 0.3 + 0.9 + 0.1 + 3.7 + 3.3 + 0.1)$$
$$\widetilde{A}(T) = 0.0630$$
$$A(T) = 1 - 0.063 = 0.937$$

b) Taking $t_{r_0} = 0$, we first estimate the MTTF and MTTR from the data:

$$\text{MTTF} = \frac{1}{N}\sum_{i=1}^{10}(t_{fi} - t_{ri-1})$$
$$= \frac{1}{10}(12.8 + 1.2 + 10.6 + 5.6 + 2.0 + 20.8 + 5.4 + 68.4 \div 11.8 + 27.0)$$
$$\text{MTTF} = \frac{1}{10}\,165.6 = 16.56.$$
$$\text{MTTR} = \frac{1}{N}\sum_{i=1}^{10}(t_{ri} - t_{fi}) = \frac{T}{10}\frac{1}{T}\sum_{i=1}^{10}(t_{fi} - t_{ri}) = \frac{18205}{10}\widetilde{A}(T)$$
$$= 1.15\text{ days}$$

c) $$A(T) = \frac{v}{v+\lambda} = \frac{1}{1+\dfrac{\text{MTTR}}{\text{MTTF}}} = \frac{1}{1+\dfrac{0.85}{16.5}} = 0.935$$

Constant Repair Times

In the foregoing availability model we have used a constant repair rate, as we will also do throughout much of the remainder of this chapter. Before proceeding, however, we repeat the calculation of the system availability using a repair model that is quite different; all the repairs are assumed to require exactly the same time, τ. Thus, the PDF for time to repair has the form

$$m(t) = \delta(t-\tau) \tag{9.60}$$

where δ is the Dirac delta function discussed in Chapter 8, Supplement 1. Although the availability is more difficult to calculate with this model, the result is instructive. It will be seen that while the details of the time dependence of $A(t)$ differ, the general trends are the same, and the asymptotic value is still given by Eq. (9.59).

A differential equation may be obtained for the availability, with the initial condition $A(0) = 1$. Since all repairs require a time τ, there are no repairs for $t < \tau$. Thus, instead of Eq. (9.51), we have only the failure term on the right-hand side,

$$A(t+\Delta t) = A(t) - \lambda\,\Delta t\,A(t), \quad 0 \le t \le \tau \tag{9.61}$$

which corresponds to the differential equation

$$\frac{d}{dt}A(t) = -\lambda A(t), \quad 0 \le t \le \tau \tag{9.62}$$

For times greater than $\boldsymbol{\tau}$, repairs are also made; the number of repairs made during Δt is just equal to the number of failures during Δt at a time τ earlier: $\lambda\,\Delta t\,A(t-\tau)$. Thus, the change in availability during Δt is

$$A(t+\Delta t) = A(t) - \lambda\,\Delta t\,A(t) + \lambda\,\Delta t\,A(t-\tau), \quad t > \tau \tag{9.63}$$

which corresponds to the differential equation

$$\frac{d}{dt}A(t) = -\lambda A(t) + \lambda A(t-\tau), \quad t > \tau \tag{9.64}$$

Equations (9.63) and (9.64) are more difficult to solve than those for the constant repair rate. During the first interval, $0 \le t \le \tau$, we have simply

$$A(t) = e^{-\lambda t}, \quad 0 \le t \le \tau \tag{9.65}$$

For $t > \tau$, the solution in successive intervals depends on that of the preceding interval. To illustrate, consider the interval $N\boldsymbol{\tau} \le t \le (N+1)\boldsymbol{\tau}$. Applying an integrating factor $e^{\lambda t}$ to Eq. (9.64), we may solve for $A(t)$ in terms of $A(t-\tau)$:

$$A(t) = A(N\tau)\,e^{-\lambda(t-N\tau)} + \int_{NT}^{t} dt'\lambda e^{-\lambda(t-t')}A(t'-\tau), \quad N\tau \le t \le (N+1)\tau \tag{9.66}$$

For $N = 1$, we may insert Eq. (9.65) on the right-hand side to obtain

$$A(t) = e^{-\lambda t} + \lambda(t-\tau)e^{-\lambda(t-\tau)}, \quad \tau \le t \le 2\tau \tag{9.67}$$

For $N = 2$, there will be three terms on the right-hand side, and so on. The general solution for arbitrary N appears quite similar to the Poisson distribution:

$$A(t) = \sum_{n=0}^{N} \frac{[\lambda(t-n\tau)^{\mathrm{n}}]}{n!}\,e^{-\lambda(t\text{-}n\tau)}, \quad N\tau \le t \le (N+1)\tau \tag{9.68}$$

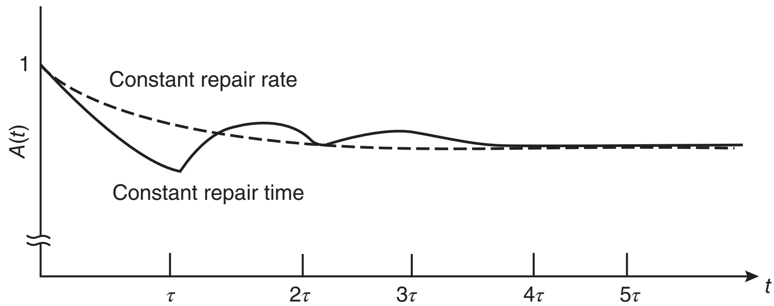


Figure 9.5 Availability for different repair models.

The solutions for the constant repair rate and the constant repair time models are plotted for the point availability $A(t)$ in Figure 9.5 for $\tau = 1/\nu$. Note that the discrete repair time leads to breaks in the slope of the availability curve, whereas this is not the case with the constant failure rate model. However, both curves follow the same general trend downward and converge to the same asymptotic value. Thus, if we are interested only in the general characteristics of availability curves, which ordinarily is the case, the constant repair rate model is quite adequate, even though some of the structure carried by a more precise evaluation of the repair time PDF may be lost. Moreover, to an even greater extent than with failure rates, not enough data are available in most cases to say much about the spread of repair times about the MTTR. Therefore, the single-parameter exponential distribution may be all that can be justified, and Eq. (9.59) provides a reasonable estimate of the availability.

9.5 Testing and Repair: Unrevealed Failures

As long as system failures are revealed immediately, the time to repair is the primary factor in determining the system availability. When a system is not in continuous operation, however, failures may occur but remain undiscovered. This problem is most pronounced in backup or other emergency equipment that is operated only rarely, or in stockpiles of repair parts or other materials that may deteriorate with time. The primary loss of availability then may be due to failures in the standby mode that are not detected until an attempt is made to use the system.

A primary weapon against these classes of failures is periodic testing. As we will see, the more frequently testing is carried out, the more failures will be detected and repaired soon after they occur. However, this must be weighed against the expense of frequent testing, the loss of availability through downtime for testing, and the possibility of excessive component wear from too-frequent testing.

Idealized Periodic Tests

Suppose that we first consider the effect of a simple periodic test on a system whose reliability can be characterized by a constant failure rate:

$$R(t) = e^{-\lambda t} \tag{9.69}$$

The first thing that should be clear is that system testing has no positive effect on reliability. For unlike preventive maintenance the test will only catch failures after they occur.

Testing, however, has a very definite positive effect on availability. To see this in the simplest case, suppose that we perform a system test at time interval T_0. In addition, we make the following three assumptions: (i) The time required to perform the test is negligible, (ii) the time to perform repairs is negligible, and (iii) the repairs are carried out perfectly and restore the system to an as-good-as-new condition. Later, we examine the effects of relaxing these assumptions.

Suppose that we test a system with reliability given by Eq. (9.69) at time interval T_0. As indicated, if there is no repair, the availability is equal to the reliability. Thus, before the first test,

$$A(t) = R(t), \quad 0 \le t \le T_0 \tag{9.70}$$

Since the system is repaired perfectly and restored to an as-good-as-new state at $t = T_0$, we have $R(T_0) = 1$. Then, since there is no repair between T_0 and $2T_0$, the availability will again be equal to the reliability, but now the reliability is evaluated at $t - T_0$:

$$A(t) = R(t - T_0), \quad T_0 \le t \le 2T_0 \tag{9.71}$$

This pattern repeats itself as indicated in Figure (9.16). The general expression is

$$A(t) = R(t - NT_0), \quad NT_0 \le T < (N+1)T_0 \tag{9.72}$$

For the situation indicated in Figure 9.6, the interval and the asymptotic availability have the same value, provided that the integral in Eq. (9.31) is taken over a multiple of T_0, say mT_0. We have

$$A^*(mT_0) = \frac{1}{mT_0}\int_0^{mT_0} A(t)\,dt = \frac{1}{T_0}\int_0^{T_0} A(t)\,dt \tag{9.73}$$

Since the interval availability is independent of the number of intervals over which $A^*(T)$ is calculated, so will the asymptotic availability $A^*(\infty)$:

$$A^*(\infty) = \lim_{m\to\infty} \frac{1}{mT_0}\int_0^{mT_0} A(t)\,dt = \frac{1}{T_0}\int_0^{T_0} A(t)\,dt \tag{9.74}$$

The effect of the testing interval on availability may be seen by combining Eqs. (9.69) and (9.74). We obtain

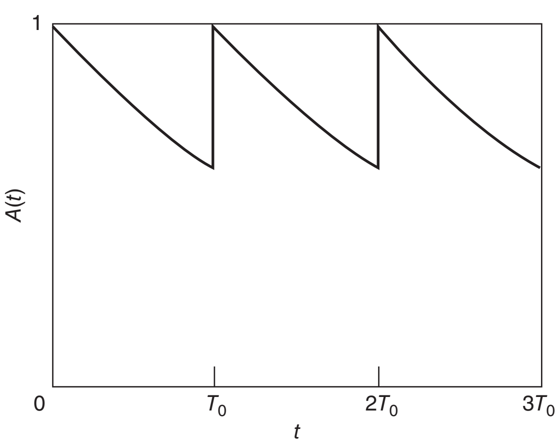


Figure 9.6 Availability with idealized periodic testing for unrevealed failures.

$$A^*(\infty) = \frac{1}{\lambda T_0}\left(1 - e^{-\lambda T_0}\right) \tag{9.75}$$

Ordinarily, the test interval would be small compared to the MTTF: $\lambda T_0 \ll 1$. Therefore, the exponential may be expanded, and only the leading terms are retained to make the approximation

$$A^*(\infty) \approx 1 - \frac{1}{2}\lambda T_0 \tag{9.76}$$

Example 9.5 Annual inspection and repair are carried out on a large group of smoke detectors of the same design in public buildings. It is found that 15% of the smoke detectors are not functional. If it is assumed that the failure rate is constant,

a) In what fraction of fires will the detectors offer protection?
b) If the smoke detectors are required to offer protection for at least 99% of fires, how frequently must inspection and repair be carried out?

Solution:
With inspection and repair at interval T_0 the fraction of detectors that are operational at the time of inspection will be

$$R = e^{-\lambda T_0} = 0.85$$

Then, $\lambda T_0 = -\ln(0.85) = 0.162$. Since $T_0 = 1$ year, $\lambda = 0.162$/year.

a) If we assume that the fires are uniformly distributed in time, the fractional protection is just equal to the interval availability; from Eq. (9.75)

$$A^*(\infty) = \frac{1}{\lambda T_0}\left(1 - e^{-\lambda T_0}\right) = \frac{1}{0.162}(1 - 0.85) = 0.926$$

b) For this high availability, the rare-event approximation, Eq. (9.76), may be used:

$$0.99 = A^*(\infty) \approx 1 - \frac{1}{2}\lambda T_0$$

Thus, from Eq. (9.76),

$$\begin{aligned} T_0 &= \frac{2[1 - A^*(\infty)]}{\lambda} = \frac{2(1 - 0.99)}{0.162} = 0.123\,\text{year} \\ &= 0.123 \times 12\,\text{months} \approx 1\frac{1}{2}\,\text{months} \end{aligned}$$

Real Periodic Tests

Equation (9.76) indicates that we may achieve availabilities as close to one as desired merely by decreasing the test interval T_0. This is not the case, however, for as the test interval becomes smaller, a number of other factors – test time, repair time, and imperfect repairs – become more important in estimating availability.

When we examine these effects, it is useful to visualize them as modifications in the curve shown in Figure 9.6. The interval or asymptotic availability may be pictured as proportional to the area under the curve within one test interval, divided by T. Thus, we may view each of the factors listed earlier in terms of the increase or decrease that it causes in the area under the curve. In particular, with reasonable assumptions about the ratios of the various parameters involved, we may derive approximate expressions similar to Eq. (9.76) that are quite simple but at the same time are not greatly in error.

Consider first the effect of a nonnegligible test time, t_t. During the test we assume that the system must be taken off line, and the system has an availability of zero during the test. The point availability will then appear as the solid line in Figure 9.7. Provided that we again assume that $\lambda T_0 \ll 1$, so that Eq. (9.76) holds, and that $t_t \ll T_o$, the test time, is small compared to the test interval, we may approximate the contribution of the test to system downtime as t_t/T_0. The availability indicated in Eq. (9.76) is therefore decreased to

$$A^*(\infty) \approx 1 - \frac{1}{2}\lambda t T_0 - \frac{t_1}{T_0} \tag{9.77}$$

We next consider the effect of a nonzero time to repair on the availability. The probability of finding a failed system at the time of testing is just one minus the point availability at the time the test is carried out. For small T_0 this probability may be shown to be approximately $\lambda\ T_0$. Since $1/\nu$ is the mean time to repair, the contribution to be unavailability over the period T_0 is $\lambda T_0/\nu$, or dividing by the interval T_0, we find, as in Eq. (9.58), the loss of availability to be approximately λ/ν. We may therefore modify our availability by subtracting this term to yield

$$A^*(\infty) \approx 1 - \frac{1}{2}\lambda T_0 - \frac{t_1}{T_0} - \frac{\lambda}{\nu} \tag{9.78}$$

The effect of this contribution to the system unavailability is indicated by the dotted line in Figure 9.7.

Examination of Eq. (9.78) is instructive. Clearly, decreases in failure rate and in test time t_t increase the availability, as do increases in the repair rate ν. It may also be shown that the more perfect the repair, the higher the availability. Decreasing the test interval, however, may either

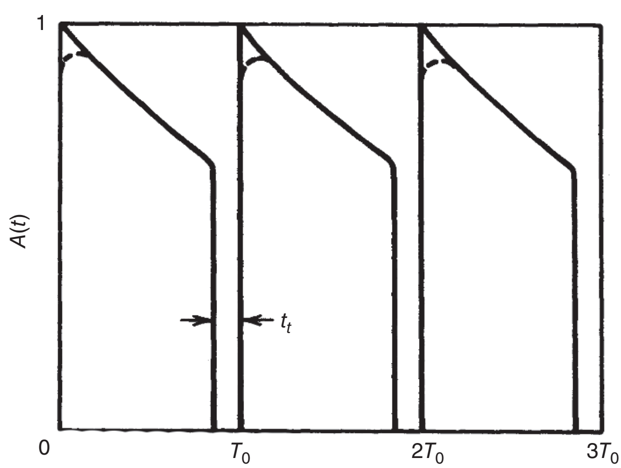


Figure 9.7 Availability with realistic periodic testing for unrevealed failures.

increase or decrease the availability, depending on the value of the other parameters. For, as indicated in Eq. (9.78), it appears in both the numerator and the denominator of terms.

Suppose that we differentiate Eq. (9.78) with respect to T_0 and set the result equal to zero in order to determine the maximum availability:

$$\frac{d}{dt}A^*(\infty) = -\frac{1}{2}\lambda + \frac{t_t}{T_0^2} = 0 \tag{9.79}$$

The optimal test interval is then

$$T_0 = \left(\frac{2t_t}{\lambda}\right)^{1/2} \tag{9.80}$$

Substitution of this expression back into Eq. (9.78) yields a maximum availability of

$$A^*(\infty) = 1 - (2\lambda t_t)^{1/2} - \frac{\lambda}{\nu} \tag{9.81}$$

If the test interval is longer than Eq. (9.80), undetected failures will lower availability. However, if a shorter test interval is employed, the loss of availability during testing will not be fully compensated for by earlier detection of failures. The test interval should increase as the failure rate decreases and decrease as the testing time can be decreased. Other trade-offs may need to be considered as well. For example, will hurrying to decrease the test time increase the probability that failures will be missed?

Example 9.6 A sulfur dioxide scrubber is known to have a MTBF of 137 days. Testing the scrubber requires half a day, and the mean time to repair is 4 days. (a) Choose the test period to maximize the availability. (b) What is the maximum availability?

Solution:

a) From Eq. (9.80), with MTBF = $1/\lambda$,

$$T_0 = (2t_t\,\text{MTBF})^{1/2} = (2 \times 0.5 \times 137)^{1/2} = 11.7\ \text{days}$$

b) From Eq. (9.81),

$$A^*(\infty) = 1 - \left(\frac{2t_t}{\text{MTBF}}\right)^{1/2} - \frac{\text{MTTR}}{\text{MTBF}}$$

$$A^*(\infty) = 1 - \left(\frac{2 \times 0.5}{137}\right)^{1/2} - \frac{4}{137} = 0.885$$

9.6 System Availability

Thus far, we have examined only the effects on the availability of the failure and repair of a system as a whole. But just as for reliability, it is often instructive to examine the availability of a system in terms of the component availabilities. Not only are data more likely to be available at the component level, but the analysis can provide insight into the gains made through redundant configurations and through different testing and repair strategies.

Since availability, like reliability, is a probability, system availabilities can be determined from parallel and series combinations of component availabilities. In fact, the techniques developed in Chapter 3 for combining reliabilities are also applicable to point availabilities, but only provided that both the failure and repair rates for the components are **independent** of one another. **If this is not the case**, either the ξ-factor method described in Chapter 3 or the Markov methods discussed in the following chapter may be required to model the component dependencies. In this chapter, we consider situations in which the component properties are independent of one another, deferring analysis of component dependencies (using Markov Chains) to the following chapter.

In what follows we estimate point availabilities of systems in terms of components. The appropriate integral is then taken to obtain interval and asymptotic availabilities. When the component availabilities become time independent after a long period of operation, steady-state availabilities may be calculated simply by letting $t \to \infty$ in the point availabilities. In testing or other situations in which there is a periodicity in the point availability, the point availability must be averaged over a test period, even though the system has been in operation for a substantial length of time. Very often, when repair rates are much higher than failure rates, simplifying approximations, in which λ/ν is assumed to be very small, are of sufficient accuracy and lead to additional physical insight in comparing systems.

For systems without redundancy the availability obeys the product law introduced in Chapter 8. Suppose that we let $\widetilde{X}$ represent the failed state of the system, and X the unfailed or operational state of the system. Similarly, let $\widetilde{X}_i$ represent the failed state of component i, and X_i, the unfailed state of the same component. In a nonredundant system, all the components must be available for the system to be available:

$$X = X_1 \cap X_2 \cap \ \ldots \ \cap X_M \tag{9.82}$$

Since the availability is defined as just the probability that the system is available, we have

$$A(t) = \prod_i A_i(t) \tag{9.83}$$

where the $A_i(t)$ are the independent component availabilities.

For redundant (i.e. parallel) systems, all the components must be unavailable if the system is to be unavailable. Thus, if $\widetilde{X}$ signifies a failed system, and $\widetilde{X}_i$ the failed state of component i, we have

$$\widetilde{X} = \widetilde{X}_1 \cap \widetilde{X}_2 \cap \widetilde{X}_3 \cap \cdots \cap \widetilde{X}_M \tag{9.84}$$

Since the unavailability is one minus the availability, we have

$$1 - A(t) = [1 - A_1(t)][1 - A_2(t)]\cdots[1 - A_M(t)] \tag{9.85}$$

or more compactly,

$$A(t) = 1 - \prod_i [1 - A_i(t)] \tag{9.86}$$

Comparing Eqs. (9.83) and (9.86) with Eqs. (9.1) and (9.38) indicates that the same relationships hold for point availabilities as for reliabilities. The other relationships derived in Chapter 3 also hold when the assumption that the components are mutually independent is made throughout.

Revealed Failures

Suppose that we now apply the constant repair rate model to each component. According to Eq. (9.54), the component availabilities are then

$$A_i(t) = \frac{\nu_i}{\nu_i + \lambda_i} + \frac{\lambda_i}{\nu_i + \lambda_i} e^{-(\lambda_i + \nu_i)t} \tag{9.87}$$

This relationship may be applied in the foregoing equations to estimate system availability.

If we are interested only in asymptotic availability, we may delete the second term of Eq. (9.87) to obtain

$$A_i(\infty) = \frac{\nu_i}{\nu_i + \lambda_i} \tag{9.88}$$

Combining this expression with Eq. (9.83), we have for a nonredundant system

$$A(\infty) = \prod_i \frac{\nu_i}{\nu_i + \lambda_i} \tag{9.89}$$

If we further make the reasonable assumption that repair rates are large compared to failure rates, $\nu_i \gg \lambda_i$, then

$$A_i(\infty) \approx 1 - \frac{\lambda_i}{\nu_i} \tag{9.90}$$

With this expression substituted into Eq. (9.83) to estimate the availability of a nonredundant system, we obtain

$$A(\infty) \approx \prod \left(1 - \frac{\lambda_i}{\nu_i}\right) \tag{9.91}$$

But since we have already deleted higher order terms in the ratios λ_i/ν_i, for consistency we also should eliminate them from this equation. This yields

$$A(\infty) \approx 1 - \sum_i \frac{\lambda_i}{\nu_i} \tag{9.92}$$

Thus, the rapid deterioration of the availability with an increased number of components is seen. If we further assume that all the repair rates can be replaced by an average value $\nu_i = \nu$, Eq. (9.92) becomes

$$A(\infty) \approx 1 - \lambda/\nu \tag{9.93}$$

where

$$\lambda = \sum_i \lambda_i \tag{9.94}$$

Therefore, we obtain the same result as given for the system as a whole, provided that we sum the component failure rates as in Chapter 3.

The effect of redundancy may be seen by inserting Eq. (9.88) into Eq. (9.86), the availability of a parallel system. For N identical units with $\lambda_i = \lambda$ and $\nu_i = \nu$, we have

$$A(\infty) = 1 - \left(\frac{\lambda}{\lambda + \nu}\right)^N \tag{9.95}$$

If we consider the case where $\nu \gg \lambda$, then

$$A(\infty) \approx 1 - \left(\frac{\lambda}{\nu}\right)^N \tag{9.96}$$

or correspondingly for the unavailability,

$$\tilde{A}(\infty) \approx \left(\frac{\lambda}{\nu}\right)^N \tag{9.97}$$

The analogy to the reliability of parallel systems is clear; both unreliability and unavailability are proportional to the Nth power of the failure rate. The foregoing relationships assume that there are no common-mode failures. If there are, the ξ-factor method of Chapter 3 may be adapted, putting a fictitious component in series with a failure and a repair rate for the common-mode failure. Once again, the presence of common-mode failure limits the gains that can be made through the use of parallel configurations, although not as severely as for systems that cannot be repaired. Suppose that we consider as an example N units in parallel, each having a failure rate λ divided into independent and common-mode failures as in Eqs. (9.24) through (9.30). We have

$$A(\infty) = \left\{1 - [1 - A_I(\infty)]^N\right\} A_c(\infty), \tag{9.98}$$

where A_I *are* the availabilities with only the independent failure rate λ_I taken into account, and A_c is the common-mode availability with failure rate λ_c. We assume that both common and independent failure modes have the same repair rate. Thus,

$$A(\infty) = \left[1 - \left(\frac{\lambda_I}{\lambda_I + \nu}\right)^N\right] \frac{\nu}{\lambda_c + \nu}. \tag{9.99}$$

This may also be written in terms of ξ factors by recalling that $\lambda_I \equiv (1 - \xi)\,\lambda$ and $\lambda_c \equiv \xi\lambda$.

Example 9.7 A system has a ratio of $\nu/\lambda = 100$. What will the asymptotic availability be (a) for the system, (b) for two of the systems in parallel with no common-mode failures, and (c) for two systems in parallel with $\xi = 0.2$?

Solution:

a) $A(\infty) = \dfrac{100}{1 + 100} = 0.990$

b) $A(\infty) = 1 - \left(\dfrac{1}{1 + 100}\right)^2 = 0.99990$

c) $\dfrac{\lambda_I}{\nu} = (1 - \xi)\dfrac{\lambda}{\nu} = (1 - 0.2)\dfrac{1}{100} = 0.8 \times 10^{-2}$

$$\frac{\lambda_c}{\nu} = \xi\frac{\lambda}{\nu} = 2 \times 10^{-3}$$

Therefore, from Eq. (9.99),

$$A(\infty) = \left[1 - \left(\frac{0.8 \times 10^{-2}}{1 + 0.8 \times 10^{-2}}\right)^2\right] \frac{1}{2 \times 10^{-3} + 1} = 0.9979$$

Unrevealed Failures

In the derivations just given it is assumed that component failures are detected immediately and that repair is initiated at once. Situations are also encountered in which the component failures go undetected until periodic testing takes place. The evaluation of availability then becomes more complex, for several testing strategies may be considered. Not only is the test interval T_0 subject to change, but the testing may be carried out on all the components simultaneously or in a staggered sequence. In either event, the calculation of the system availability is now more subtle, for the point availabilities will have periodic structures, and they must be averaged over a test period in order to estimate the asymptotic availability.

To illustrate, consider the effects of simultaneous and staggered testing patterns on two simple component configurations: the nonredundant configuration consisting of two identical components in series and the completely redundant configuration consisting of two identical components in parallel. For clarity, we consider the idealized situation in which the testing time and the time to repair can be ignored. The failure rates are assumed to be constant.

We begin by letting $A_1(t)$ and $A_2(t)$ be the component point availabilities. Since the testing is carried out at intervals of T_0, we need only to determine the system point availability $A(t)$ between $t = 0$ and $t = T_0$, for the asymptotic mission availability is then obtained by averaging $A(t)$ over the test period:

$$A^*(\infty) = A^*(T_0) = \frac{1}{T_0}\int_0^{T_0} A(t)\, dt \tag{9.100}$$

Simultaneous Testing

When both components are tested at the same time, $t = 0$, T_0, $2\ T_0$, ..., the point availabilities are given by

$$A_1(t) = e^{-\lambda t}, \quad 0 \le t < T_0 \tag{9.101}$$

and

$$A_2(t) = e^{-\lambda t}, \quad 0 \le t < T_0 \tag{9.102}$$

For the series system, we have

$$A(t) = A_1(t)A_2(t) \tag{9.103}$$

or

$$A(t) = e^{-2\lambda t}, \quad 0 \le t < T_0 \tag{9.104}$$

For the parallel system, we obtain

$$A(t) = A_1(t) + A_2(t) - A_1(t)A_2(t) \tag{9.105}$$

or

$$A(t) = 2e^{-\lambda t} - e^{-2\lambda t}, \quad 0 \le t < T_0 \tag{9.106}$$

The availabilities are plotted as solid lines in Figure 9.8a and b, respectively. The asymptotic availability obtained from Eq. (9.100) for the series system is

$$A_s^*(T_0) = \frac{1}{2\lambda T_0}\left(1 - e^{-2\lambda T_0}\right) \tag{9.107}$$

whereas that of the parallel system is

$$A_p^*(T_0) = \frac{1}{2\lambda T_0}\left(3 - 4e^{-\lambda T_0} + e^{-2\lambda T_0}\right) \tag{9.108}$$

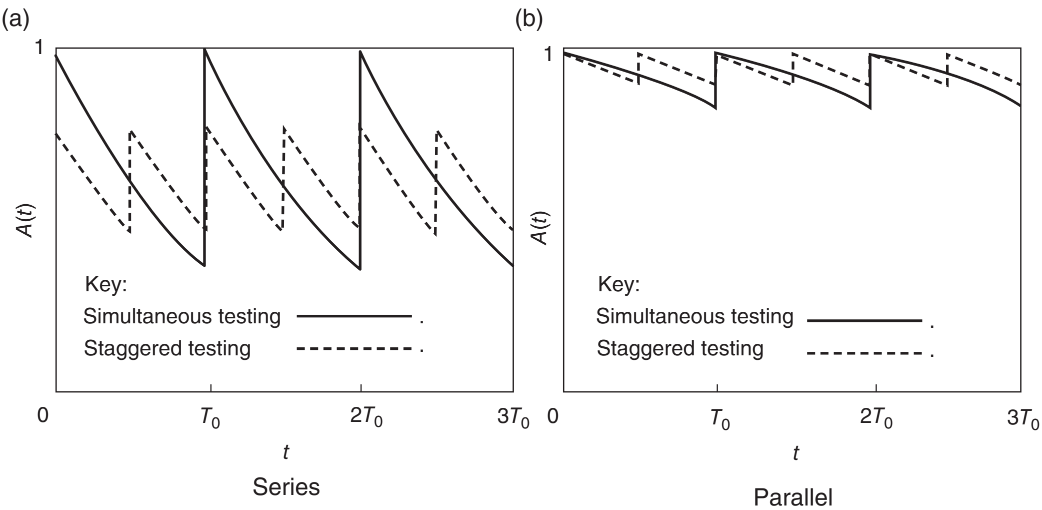


Figure 9.8 Availability for a two-component system with unrevealed failures.

Staggered Testing

We now consider the testing of components at staggered intervals of $T_0/2$. We assume that component 1 is tested at 0, T_0, $2T_0$, ..., whereas component 2 is tested at the half-intervals $T_0/2$, $3T_0/2$, ... The point availabilities within any interval after the first one are given by

$$A_1(t) = e^{-\lambda t}, \quad 0 \le t < T_0 \tag{9.109}$$

and

$$A_2(t) = \begin{cases} \exp\left[-\lambda\left(t + \dfrac{T_0}{2}\right)\right] & 0 \le t < \dfrac{T_0}{2} \\ \exp\left[-\lambda\left(t - \dfrac{T_0}{2}\right)\right] & \dfrac{T_0}{2} \le t < T_0 \end{cases} \tag{9.110}$$

To determine the point system availability, we combine these two equations with Eqs. (9.103) and (9.105), respectively, for the series and parallel configurations. The results are plotted as dotted lines in Figures 9.8a and b.

To calculate the asymptotic availabilities for staggered testing, we first note from Figure 9.8 that the system point availabilities for both series and parallel situations have a periodicity over the half-intervals $T_0/2$. Therefore, instead of averaging $A(t)$ over an entire interval as in Eq. (9.100), we need to average it over only the half-interval. Hence,

$$A^*(T_0) = \frac{2}{T_0}\int_0^{T_0/2} A(t)\,dt \tag{9.111}$$

For the series configuration we calculate $A_1(t)A_2(t)$ from Eqs. (9.109) and (9.110), substitute the result into Eq. (9.111), and carry out the integral to obtain

$$A_s^*(T_0) = \frac{1}{2\lambda T_0}\left(e^{-\lambda T_0/2} - e^{-3\lambda T_0/2}\right) \tag{9.112}$$

Table 9.1 Availability $A^*(T_0)$ for unrevealed failures.

Testing	Series system	Parallel system
Simultaneous	$1-\lambda T_0+\frac{2}{3}(\lambda T_0)^2$	$1-\frac{1}{3}(\lambda T_0)^2$
Staggered	$1-\lambda T_0+\frac{13}{24}(\lambda T_0)^2$	$1-\frac{5}{24}(\lambda T_0)^2$

Similarly, for the parallel configuration we form $A(t)$ by substituting Eqs. (9.109) and (9.110) into Eq. (9.105), combine the result with Eq. (9.111), and perform the integral to obtain

$$A_p^*(T_0)=\frac{1}{\lambda T_0}\left(2-2e^{-\lambda T_0}-e^{-\lambda T_0/2}+e^{-3\lambda T_0/2}\right) \quad (9.113)$$

Although the point availabilities plotted as dotted lines in Figure 9.8 are interesting in understanding the effects of staggering on the availability, the asymptotic values are often more useful, for they allow us to compare the strategies with a single number. Evaluation of the appropriate expressions indicates that in the nonredundant (series) configuration higher availability is obtained from simultaneous testing, whereas staggered testing yields the higher availability for redundant (parallel) configurations.

This behavior can be understood explicitly if the expressions for the asymptotic availability are expanded in powers of λT_0, since for small failure rates the lowest order terms in λT_0 will dominate the expressions. The results of such expansions are presented in Table 9.1.

The effects of staggered testing become more pronounced when repair time, testing time, or both are not negligible. We can see, for example that even for a zero failure rate, the testing time t_t will decrease the availability of the series system by t_t/T_0 if the systems are tested simultaneously. If the tests are staggered in the series system, the availability will decrease by $2t_t/T_0$. Conversely, in the parallel system simultaneous testing with no failures will decrease the availability by t_t/T_0, but if the tests are staggered so that they do not take both components out at the same time, the availability does not decrease.

Example 9.8 A voltage monitor achieves an average availability of 0.84 when it is tested monthly; the repair time is negligible. Since the 0.84 availability is unacceptably low, two monitors are placed in parallel. What will the availability of this twin system be (a) if the monitors are tested monthly at the same time and (b) if they are tested monthly at staggered intervals?

Solution:
First, we must find λT_0. Try Eq. (9.76), the rare-event approximation:

$$0.84=1-\frac{1}{2}\lambda T_0;\quad \lambda T_0\approx 0.32$$

This is too large for the exponential expansion to be used. Therefore, we use Eq. (9.75) instead. We obtain a transcendental equation

$$0.84=\frac{1}{\lambda T_0}\left(1-e^{-\lambda T_0}\right)$$

Solving iteratively, we find that

λT_0	0.320	0.340	0.360	0.380
$(1/0.84)(1-e^{-\lambda T_0})$	0.326	0.343	0.3599	0.376

Therefore,

$$\lambda T_0 \approx 0.36$$

a) From Eq. (9.108), we find for simultaneous testing

$$A_p^*(T_0) = \frac{1}{2 \times 0.36}\left(3 - 4e^{-0.36} + e^{-2 \times 0.36}\right) = 0.967$$

b) From Eq. (9.113), we find for staggered testing

$$A_p^*(T_0) = \frac{1}{0.36}\left(2 - 2e^{-0.36} - e^{-0.36/2} + e^{-3 \times 0.36/2}\right) = 0.978.$$

These results can be generalized to combinations of series and parallel configurations. However, the evaluation of the integral in Eq. (9.100) over the test period may become tedious. Moreover, the evaluation of maintenance, testing, and repair policies becomes more complex in real systems that contain combinations of revealed and unrevealed failures, large numbers of components, and dependencies between components. Some of the more common types of dependencies are included in the following chapter.

Bibliography

Ascher, H. and Feingold, H. (1984). *Repairable Systems Reliability: Modeling, Inference, Misconceptions, and Their Causes*, *Lecture Notes in Statistics Series*, vol. **7**. New York: Marcel Deckkr.

Barlow, R.E. and Proschan, F. (1965). *Mathematical Theory of Reliability*. New York: Wiley.

Gertsbakh, I.B. (1977). *Models for Preventive Maintenance*. Amsterdam: North-Holland Publishing Co.

Jardine, A.K.S. (1973). *Maintenance, Replacement, and Reliability*. New York: Wiley.

Sandler, G.H. (1963). *System Reliability Engineering*. Englewood Cliffs, NJ: Prentice-Hall.

Smith, D.J. (1993). *Reliability, Maintainability and Risk*, 46e. Oxford: Butterworth-Heinemann.

Exercises

9.1 Without preventive maintenance the reliability of a condensate demineralizer is characterized by

$$\int_0^t \lambda(t')\,dt' = 1.2 \times 10^{-2} t + 1.1 \times 10^{-9} t^2$$

where t is in hours. The design life is 10,000 hours.

(a) What is the design-life reliability?

(b) Suppose that by overhaul the demineralizer is returned to as-good-as-new condition. How frequently should such overhauls be performed to achieve a design-life reliability of at least 0.95?

(c) Repeat *b* for a target reliability of at least 0.975.

9.2 Discuss under what conditions preventative maintenance can increase the reliability of a simple active parallel system, even though the component failure rates are time independent. Justify your results.

9.3 Repeat *b* of Exercise 9.1 assuming that there is a 1% probability that faulty overhaul will cause the demineralizer to fail destructively immediately following start-up. Is it possible to achieve the 0.95 reliability? If so, how many overhauls are required?

9.4 Derive an equation analogous to Eqs. (9.27) and (9.28) that includes a probability p_I of independent maintenance failure and a probability p_c of common-mode maintenance failure.

9.5 Suppose that a device has a failure rate of

$$\lambda(t) = (0.015 + 0.02t)/\text{year}$$

where t is in years.

a) Calculate the reliability for a five-year design life assuming that no maintenance is performed.
b) Calculate the reliability for a five-year design life assuming that annual preventive maintenance restores the system to an as-good-as-new condition.
c) Repeat *b* assuming that there is a 5% chance that the preventive maintenance will cause immediate failure.

9.6 A machine has a failure rate given by $\lambda(t) = at$. Without maintenance the reliability at the end of one year is $R(1) = 0.86$.

a) Determine the value of "a."
b) If as-good-as-new preventive maintenance is performed at two-month intervals, what will the one-year reliability be?
c) If in *b* there is a 2% probability that each maintenance will cause system failure, what will be the value of the reliability at the end of one year?

9.7 Suppose that the times to failure of an unmaintained component may be given by a Weibull distribution with $\beta = 2$. Perfect preventive maintenance is performed at intervals $T = 0.25\eta$.

a) Find the MTTF of the maintained system in terms of η.
b) Determine the percentage increase in the MTTF over that of the unmaintained system.

9.8 Solve Exercise 9.7 approximately for the situation in which $T \ll \eta$.

9.9 The reliability of a device is given by the Rayleigh distribution

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

The MTTF is considered to be unacceptably short. The design engineer has two alternatives: a second identical system may be set in parallel or (perfect) preventive maintenance may be performed at some interval T. At what interval T must the preventive maintenance be performed to obtain an increase in the MTTF equal to what would result from the parallel configuration without preventive maintenance? (*Note*: See the solution for Exercise 9.19.)

9.10 Show that preventive maintenance has no effect on the MTTF for a system with a constant failure rate.

9.11 The following table gives a series of times to repair (man-hours) obtained for a diesel engine.

11.6	7.9	27.7	17.8	8.9	22.5
3.3	33.3	75.3	9.4	28.5	5.4
9.13	1.1	7.8	41.9	13.3	5.3

a) Estimate the MTTR.
b) Estimate the repair rate and its 90% confidence interval assuming that the data is exponentially distributed.

9.12 Find the asymptotic availability for the systems shown in Exercise 9.38, assuming that all the components are subject only to revealed failures and that the repair rate is ν. Then, approximate your result for the case $\nu/\lambda \gg 1$.

9.13 A computer has an MTTF = 34 hours and an MTTR = 2.5 hours.
a) What is the availability?
b) If the MTTR is reduced to 1.5 hours, what MTTF can be tolerated without decreasing the availability of the computer?

9.14 A generator has a long-term availability of 72%. Through a management reorganization the MTTR (mean time to *repair*) is reduced to one half of its former value. What is the generator availability following the reorganization?

9.15 A system consists of two subsystems in series, each with $\nu/\lambda = 10^2$ as its ratio of repair rate to failure rate. Assuming revealed failures, what is the availability of the system after an extended period of operation?

9.16 A robot has a failure rate of 0.05 hour^{-1}. What repair rate must be achieved if an asymptotic availability of 95% is to be maintained?

9.17 Reliability testing has indicated that without repair a voltage inverter has a six-month reliability of 0.87; make a rough estimate of the MTTR that must be achieved if the inverter is to operate with an availability of 0.95. (Assume revealed failures and a constant failure rate.)

9.18 The control unit on a fire sprinkler system has an MTTF for unrevealed *failures* of 30 months. How frequently must the unit be tested/repaired if an average *availability* of 99% is to be maintained.

9.19 A device has a constant failure rate, and the failures are unrevealed. It is found that with a test interval of six months the interval availability is 0.98. Use the "rare-event" approximation to estimate the failure rate. (Neglect test and repair times.)

9.20 Starting with Eqs. (9.107) and (9.112), derive the results for series systems with simultaneous and staggered testing given in Table 9.1.

9.21 The following table gives the times at which a system failed (t_f) and the times at which the subsequent repairs were completed (t_r) over a 2000-hours period.

t_f	t_r	t_f	t_r
51	52	1127	1134
90	92	1236	1265
405	412	1297	1303
507	529	1372	1375
535	539	1424	1439
615	616	1531	1552
751	752	1639	1667
760	766	1789	1795
835	839	1796	1808
881	884	1859	1860
933	941	1975	1976
1072	1091		

a) Calculate the average availability over the time interval $0 \le t \le t_{max}$ directly from the data.
b) Assuming constant failure and repair rates, estimate λ and μ from the data.
c) Use the values of λ and μ obtained in *b* to estimate $A(t)$ and the time-averaged availability for the interval $0 \le t \le t_{max}$. Compare your results to *a*.

9.22 Starting with Eqs. (9.108) and (9.113), derive the results for parallel systems with simultaneous and staggered testing given in Table 9.1.

9.23 An auxiliary feedwater pump has an availability of 0.960 under the following conditions: The failures are unrevealed; periodic testing is carried out on a monthly (30-day) basis; and testing and repair require that the system be shut down for eight hours.
a) What will the availability be if the shutdown time can be reduced to two hours?
b) What will the availability be if the tests are performed once per week, with the eight-hours shutdown time?
c) Given the eight-hours shutdown time, what is the optimal test interval?

9.24 A pressure relief system consists of two valves in parallel. The system achieves an availability of 0.995 when the valves are tested on a staggered basis, each valve being tested once every three months.
a) Estimate the failure rate of the valves.
b) If the test procedures were relaxed so that each valve is tested once in six months, what would the availability be?

9.25 In annual test and replacement procedures 8% of the emergency respirators at a chemical plant are found to be inoperable.
a) What is the availability of the respirators?
b) How frequently must the test and replacement be carried out if an availability of 0.99 is to be reached? (Assume constant failure rates.)

9.26 Consider three units in parallel, each tested at equally staggered intervals of T_0. Assume constant failure rates.

a) What is $A(t)$?
b) Plot $A(t)$.
c) What is $A^*(T_0)$?
d) Find the rare-event approximate for $A^*(T_0)$.

9.27 Unrevealed bearing failures follow a Weibull distribution with $\beta = 2$ and $\eta = 5000$ operating hours. How frequently must testing and repair take place if bearing availability is to be maintained at least 95%?

9.28 The reliability of a system is represented by the Rayleigh distribution

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

Suppose that all failures are unrevealed. The system is tested and repaired to an as-good-as-new condition at intervals of T_0. Neglecting the times required for test and repair, and assuming perfect maintenance:
a) Derive an expression for the asymptotic availability $A^*(\infty)$.
b) Find an approximation for $A^*(\infty)$ when $T_0 \ll \eta$.
c) Evaluate $A^*(\infty)$ for $T_0/\eta = 0.1$, 0.5, 1.0, and 2.0.

10

Failure Interactions

"If anything can go wrong, it will."

Source: Murphy's law

10.1 Introduction

In reliability analysis, perhaps the most pervasive technique is that of estimating the reliability of a system in terms of the reliability of its components. In such analysis, it is frequently assumed that the component failure and repair properties are mutually independent. In reality, this is often not the case. Therefore, it is necessary to replace the simple products of probabilities with more sophisticated models that take into account the interactions of component failures and repairs.

Many component failure interactions – as well as systems with independent failures – may be modeled effectively as Markov processes, provided that the failure and repair rates can be approximated as time independent. Indeed, we have already examined a particular example of a Markov process, the derivation of the Poisson process contained in Chapter 3. In this chapter, we first formulate the modeling of failures as Markov processes and then apply them to simple systems in which the failures are independent. This allows us both to verify that the same results are obtained as in Chapter 3 and to familiarize ourselves with Markov processes. We then use Markov methods to examine failure interactions of two particular types, shared-load systems and standby systems, and follow with demonstrations of how to incorporate such failure dependencies into the analysis of larger systems. Finally, the analysis is generalized to take into account operational dependencies such as those created by shared repair crews.

10.2 Markov Analysis

We begin with the Markov formulation by designating all the possible states of a system. A state is defined to be a particular combination of operating and failed components. Thus, for example if we have a system consisting of three components, we may easily show that there are eight different combinations of operating and failed components and therefore eight states. These are enumerated in Table 10.1, where O indicates an operational component, and X a failed component. In general, a system with N components will have 2^N states so that the number of states increases much faster than the number of components.

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

Table 10.1 Markov states of three-component systems.

	State #							
Component	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
a	*O*	*X*	*O*	*O*	*X*	*X*	*O*	*X*
b	*O*	*O*	*X*	*O*	*X*	*O*	*X*	*X*
c	*O*	*O*	*O*	*X*	*O*	*X*	*X*	*X*

Note: O = operating; X = failed.

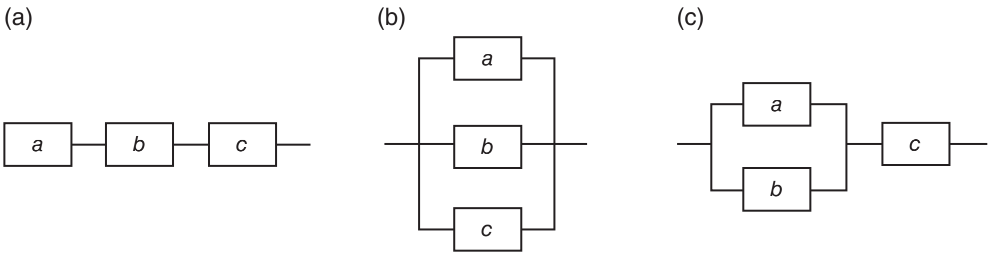


Figure 10.1 Reliability block diagrams for three-component systems.

For the analysis that follows we must know which of the states correspond to system failure. This, in turn, depends on the configuration in which the components are used. For example, three components might be arranged in any of the three configurations shown in Figure 10.1. If all the components are in series, as in Figure 10.1a, any combination of one or more component failures will cause system failure. Thus, states 2 through 8 in Table 10.1 are failed-system states. Conversely, if the three components are in parallel as in Figure 10.1b, all three components must fail for the system to fail. Thus, only state 8 is a system failure state. Finally, for the configuration shown in Figure 10.1c, both components 1 and 2 or component 3 must fail for the system to fail. Thus, states 4 through 8 correspond to system failure.

The object of Markov analysis is to calculate $P_i(t)$, the probability that the system is in state i at time t. Once this is known, the system reliability can be calculated as a function of time from

$$R(t) = \sum_{i \in O} P_i(t) \tag{10.1}$$

where the sum is taken over all the operating states (i.e. over those states for which the system is not failed). Alternately, the reliability may be calculated from

$$R(t) = 1 - \sum_{i \in X} P_i(t) \tag{10.2}$$

where the sum is over the states for which the system is failed.

In what follows, we designate state 1 as the state for which all the components are operating, and we assume that at $t = 0$, the system is in state 1.

Therefore,

$$P_1(0) = 1 \tag{10.3}$$

and

$$P_i(0) = 0, \quad i \neq 1 \tag{10.4}$$

Since at any time the system can only be in one state, we have

$$\sum_i P_i(t) = 1 \tag{10.5}$$

where the sum is over all possible states.

To determine the $P_i(t)$, we derive a set of differential equations, one for each state of the system. These are sometimes referred to as state transition equations because they allow the $P_i(t)$ to be determined in terms of the rates at which transitions are made from one state to another. The transition rates consist of superpositions of component failure rates, repair rates, or both. We illustrate these concepts first with a very simple system, one consisting of only two independent components, a and b.

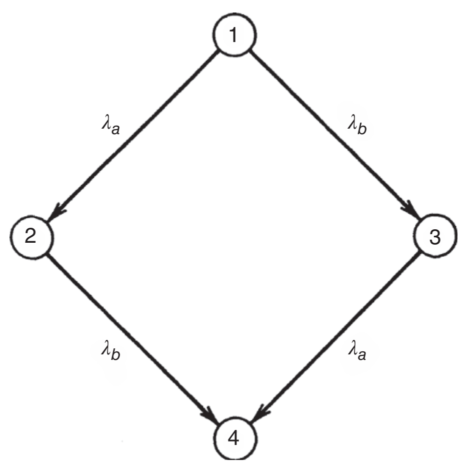
Two Independent Components

A two-component system has only four possible states, those enumerated in Table 10.2. The logic of the changes of states is best illustrated by a state transition diagram shown in Figure 10.2. The failure rates λ_a and λ_b for components a and b indicate the rates at which the transitions are made between states. Since $\lambda_a \, \Delta t$ is the probability that a component will fail between times t and

Table 10.2 Markov states of three-component systems.

	State #			
Component	**1**	**2**	**3**	**4**
a	O	X	O	X
b	O	O	X	X

Figure 10.2 State transition diagram with independent failures.



$t + \Delta t$, given that it is operating at t (and similarly for λ_b), we may write the net change in the probability that the system will be in state 1 as

$$P_1(t + \Delta t) - P_1(t) = -\lambda_a \Delta t P_1(t) - \lambda_b \Delta t P_1(t) \tag{10.6}$$

or in differential form

$$\frac{d}{dt} P_1(t) = -\lambda_a p_1(t) - \lambda_b P_1(t) \tag{10.7}$$

To derive equations for state 2, we first observe that for every transition out of state 1 by failure of component *a,* there must be an arrival in state 2. Thus, the number of arrivals during Δt is $\lambda_a \Delta t P_1(t)$. Transitions can also be made out of state 2 during Δt; these will be due to failures of component *b,* and they will make a contribution of $-\lambda_b \Delta t P_2(t)$. Thus, the net increase in the probability that the system will be in state 2 is given by

$$P_2(t + \Delta t) - P_2(t) = \lambda_a \Delta t P_1(t) - \lambda_b \Delta t P_2(t) \tag{10.8}$$

or dividing by Δt and taking the derivative, we have

$$\frac{d}{dt} P_2(t) = \lambda_a P_1(t) - \lambda_b P_2(t) \tag{10.9}$$

Identical arguments can be used to derive the equation for $P_3(t)$. The result is

$$\frac{d}{dt} P_3(t) = \lambda_b P_1(t) - \lambda_a P_3(t) \tag{10.10}$$

We may derive one more differential equation, which is for state 4. We note from the diagram that the transitions into state 4 may come either as a failure of component *b* from state 2 or as a failure of component *a* from state 3; the transitions during Δt are $\lambda_b \Delta t P_2(t)$ and $\lambda_a \Delta t P_3(t)$, respectively. Consequently, we have

$$P_4(t + \Delta t) - P_4(t) = \lambda_b \Delta t P_2(t) + \lambda_a \Delta t P_3(t) \tag{10.11}$$

or, correspondingly,

$$\frac{d}{dt} P_4(t) = \lambda_b P_2(t) + \lambda_a P_3(t) \tag{10.12}$$

State 4 is called an absorbing state, since there is no way to get out of it. The other states are referred to as nonabsorbing states.

From the foregoing derivation we see that we must solve four coupled ordinary differential equations in time in order to determine the $P_i(t)$. We begin with Eq. (10.7) for $P_1(t)$, since it does not depend on the other $P_i(t)$. By substitution, it is clear that the solution to Eq. (10.7) that meets the initial condition, Eq. (10.3), is

$$P_1(t) = e^{-(\lambda_a + \lambda_b)t} \tag{10.13}$$

To find $P_2(t)$, we first insert Eq. (10.13) into Eq. (10.9),

$$\frac{d}{dt} P_2(t) = \lambda_a e^{-(\lambda_a + \lambda_b)t} - \lambda_b P_2(t) \tag{10.14}$$

yielding an equation in which only $P_2(t)$ appears. Moving the last term to the left-hand side, and multiplying by an integrating factor $e^{\lambda_a t}$, we obtain

$$\frac{d}{dt}\left[e^{\lambda_b t}P_2(t)\right] = \lambda_a e^{-\lambda_a t} \tag{10.15}$$

Multiplying by *dt,* and integrating the resulting equation from time equals zero to *t,* we have

$$\left[e^{\lambda_b t}P_2(t)\right]_0^t = \lambda_a \int_0^t e^{-\lambda_a t'}dt' \tag{10.16}$$

Carrying out the integral on the right-hand side, utilizing Eq. (10.4) on the left-hand side, and solving for $P_2(t)$, we obtain

$$P_2(t) = e^{-\lambda_b t} - e^{-(\lambda_a + \lambda_b)t} \tag{10.17}$$

Completely analogous arguments can be applied to the solution of Eq. (10.10). The result is

$$P_3(t) = e^{-\lambda_a t} - e^{-(\lambda_a + \lambda_b)t} \tag{10.18}$$

We may now solve Eq. (10.11) for $P_4(t)$. However, it is more expedient to note that it follows from Eq. (10.5) that

$$P_4(t) = 1 - \sum_{i=1}^{3} P_i(t) \tag{10.19}$$

Therefore, inserting Eqs. (10.13), (10.17), and (10.18) into this expression yields the desired solution

$$P_4(t) = 1 - e^{-\lambda_a t} - e^{-\lambda_b t} - e^{-(\lambda_a + \lambda_b)t} \tag{10.20}$$

With the $P_i(t)$ known, we may now calculate the reliability. This, of course, depends on the configuration of the two components, and there are only two possibilities, series and parallel. In the series configuration, any failure causes system failure. Hence

$$R_s(t) = P_1(t) \tag{10.21}$$

or

$$R_s(t) = e^{-(\lambda_a + \lambda_b)t} \tag{10.22}$$

Since for the active parallel configuration both components *a* and *b* must fail to have system failure,

$$R_p(t) = P_1(t) + P_2(t) + P_3(t) \tag{10.23}$$

or, using Eq. (10.19), we have

$$R_p(t) = 1 - P_4(t) \tag{10.24}$$

Therefore,

$$R_p(t) = e^{-\lambda_a t} + e^{-\lambda_b t} - e^{-(\lambda_a + \lambda_b)t} \tag{10.25}$$

This analysis assumes that the failure rate of each component is independent of the state of the other component. As can be seen from Figure 10.2, the transitions $1 \to 2$ and $3 \to 4$, which involve the failure of component *a,* have the same failure rate, even though one takes place with component *b* in operating order and the other with failed component *b*. The same argument applies in comparing the transitions $1 \to 3$ and $2 \to 4$. Since the failure rates – and therefore the failure probabilities – are independent of the system state, they are mutually independent. Therefore, the expressions derived in Chapter 3 should still be valid. That this is the case may be seen from the following. For constant failure rates, the component reliabilities derived in Chapter 3 are

$$R_i(t) = e^{-\lambda_l t}, \quad l = a, b \tag{10.26}$$

Thus, the series expression, Eq. (10.22), reduces to

$$R_S(t) = R_a(t)\, R_b(t) \tag{10.27}$$

and the parallel expression, Eq. (10.25), is

$$R_p(t) = R_a(t) + R_b(t) - R_a(t)R_b(t) \tag{10.28}$$

These are just the expressions derived earlier for independent components, without the use of Markov methods.

Load-Sharing Systems

The primary value of Markov methods appears in situations in which component failure rates can no longer be assumed to be independent of the system state. One of the common cases of dependence is in load-sharing components, whether they be structural members, electric generators, or mechanical pumps or valves. Suppose, for example that two electric generators share an electric load that either generator has enough capacity to meet. It is nevertheless true that if one generator fails, the additional load on the second generator is likely to increase its failure rate.

To model load-sharing failures, consider once again two components, a and b, in parallel. We again have a four-state system, but now the transition diagram appears as in Figure 10.3. Here, λ_a^* and λ_b^* denote the increased failure rates brought about by the higher loading after one failure has taken place.

The Markov equations can be derived as for independent failures if the changes in failure rates are included. Comparing Figures 10.2 with 10.3, we see that the resulting generalizations of Eqs. (10.7), (10.9), (10.10), and (10.12) are

$$\frac{d}{dt} P_1(t) = -\left(\lambda_a + \lambda_b\right) P_1(t) \tag{10.29}$$

$$\frac{d}{dt} P_2(t) = \lambda_a P_1(t) - \lambda_b^* P_2(t) \tag{10.30}$$

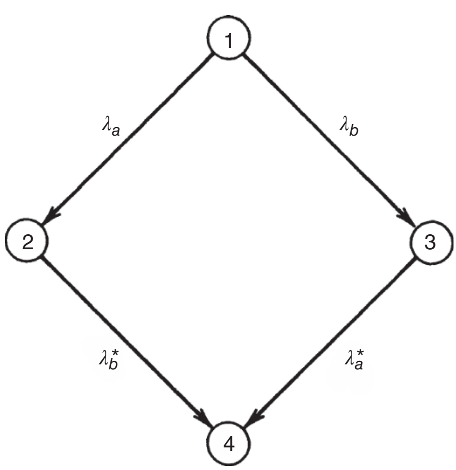


Figure 10.3 State transition diagram with load sharing.

$$\frac{d}{dt}P_3(t) = \lambda_b P_1(t) - \lambda_a^* P_3(t) \tag{10.31}$$

and

$$\frac{d}{dt}P_4(t) = \lambda_b^* P_2(t) + \lambda_a^* P_3(t) \tag{10.32}$$

The solution procedure is also completely analogous. The results are

$$P_1(t) = e^{-(\lambda_a + \lambda_b)t} \tag{10.33}$$

$$P_2(t) = \frac{\lambda_a}{(\lambda_a + \lambda_b - \lambda_b{}^*)}\left(e^{-\lambda_b{}^* t} - e^{-(\lambda_a + \lambda_b)t}\right) \tag{10.34}$$

$$P_3(t) = \frac{\lambda_b}{(\lambda_a + \lambda_b - \lambda_a{}^*)}\left(e^{-\lambda_a{}^* t} - e^{-(\lambda_a + \lambda_b)t}\right) \tag{10.35}$$

and

$$P_4(t) = 1 - P_1(t) - P_2(t) - P_3(t) \tag{10.36}$$

Finally, since both components must fail for the system to fail, the reliability is equal to $P_1(t) + P_2(t) + P_3(t)$. Thus, setting $\lambda_c = \lambda_a + \lambda_b$, we have

$$R_p(t) = \frac{\lambda_b}{\lambda_c - \lambda_a{}^*}e^{-\lambda_a{}^* t} + \frac{\lambda_a}{\lambda_c - \lambda_b{}^*}e^{-\lambda_b{}^* t} - \frac{\lambda_a\lambda_b{}^* + \lambda_b\lambda_a{}^* - \lambda_a{}^*\lambda_b{}^*}{(\lambda_c - \lambda_b{}^*)(\lambda_c - \lambda_b{}^*)}e^{-\lambda_c t} \tag{10.37}$$

It is easily seen that if $\lambda_a^* = \lambda_a$ and $\lambda_b^* = \lambda_b$, there is no dependence between failure rates, and Eq. (10.37) reduces to Eq. (10.25). The effects of increased loading on a load-sharing redundant system can be seen graphically by considering the situation in which the two components are identical: $\lambda_a = \lambda_b = \lambda$ and $\lambda_a^* = \lambda_b^* = \lambda*$. Equation (10.37) then reduces to

$$R(t) = (2\lambda - \lambda^*)^{-1}\left(2\lambda e^{-\lambda^* t} - \lambda^* e^{-2\lambda t}\right) \tag{10.38}$$

In Figure 10.4 we have plotted *R*(*t*) for the two-component parallel system, while varying the increase in failure rate caused by increased loading (i.e. the ratio $\lambda*/\lambda$). The two extremes are

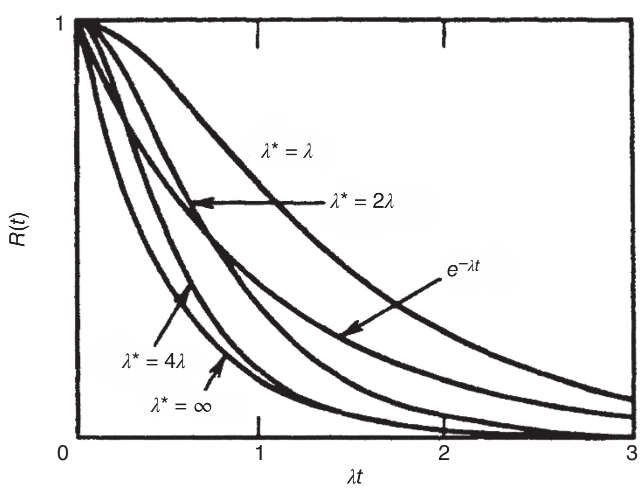


Figure 10.4 Reliability of load-sharing systems.

the system in which the two components are independent, $\lambda* = \lambda$, and the totally dependent system in which the failure of one component brings on the immediate failure of the other, $\lambda* = \infty$. Notice that these two extremes correspond to Eqs. (10.25) and (10.22), for independent failures of parallel and series configurations, respectively.

Example 10.1 Two diesel generators of known MTTF are hooked in parallel. Because the failure of one of the generators will cause a large additional load on the other, the design engineer estimates that the failure rate will double for the remaining generator. For how many MTTF can the generator system be run without the reliability dropping below 0.95?

Solution:
Placing $\lambda^* = 2\lambda$ in Eq. (11.38) will yield 0/0. Instead, we take $\lambda^* = 2\lambda - \varepsilon$, and then from Eq. (10.38):

$$\lim_{\varepsilon \to 0} R(t) = \lim_{\varepsilon \to 0} \varepsilon^{-1}(2\lambda e^{\varepsilon t} - 2\lambda + \varepsilon)e^{-2\lambda t} = (1 + 2\lambda t)e^{-2\lambda t}$$

or

$$0.95 = (1 + 2\lambda t)e^{-2\lambda t}$$

where t is the time at which $R(t) = 0.95$. Solving graphically for λt yields $\lambda t = 0.178$. Therefore, since $\lambda = 1/\text{MTTF}$ for the diesel generators, the maximum time of operation is $t = 0.178/\lambda = 0.178$ MTTF. Note that if only a single generator had been used, it could have operated only $t = \ln(1/R)/\lambda = 0.0513$ MTTF without violating the criterion.

10.3 Reliability With Standby Systems

Standby or backup systems are a widely applied type of redundancy in fault-tolerant systems, whether they be in the form of extra logic chips, navigation components, or emergency power generators. They differ, however, from active parallel systems in that one of the units is held in reserve and only brought into operation in the event that the first unit fails. For this reason they are often referred to as passive parallel systems. By their nature, standby systems involve dependency between components; they are nicely analyzed by Markov methods.

Idealized System

We first consider an idealized standby system consisting of a primary unit a and a backup unit b. If the states are numbered according to Table 10.2, the system operation is described by the transition diagram, Figure 10.5. When the primary unit fails, there is a transition $1 \rightarrow 2$, and then when the backup unit fails, there is a transition $2 \rightarrow 4$, with state 4 corresponding to system failure. Note that there is no possibility of the system's being in state 3, since we have assumed that the backup unit does not fail while in the standby state. Hence, $P_3(t) = 0$. Later, we consider the possibility of failure in this standby state as well as the possibility of failures during the switching from primary to backup unit.

From the transition diagram we may construct the Markov equations for the three states quite easily. For state 1, there is only a loss term from the transition $1 \rightarrow 2$. Thus,

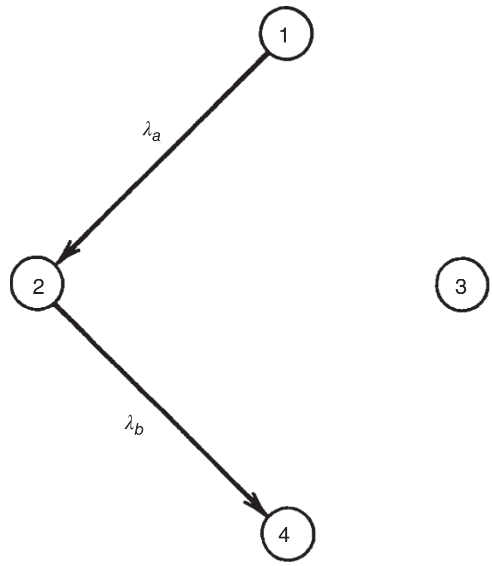


Figure 10.5 State transition diagram for a standby configuration.

$$\frac{d}{dt}P_1(t) = -\lambda_a P_1(t) \tag{10.39}$$

For state 2, we have one source term, from the $1 \rightarrow 2$ transition, and one loss term from the $2 \rightarrow 4$ transition. Thus,

$$\frac{d}{dt}P_2(t) = \lambda_a P_1(t) - \lambda_b P_1(t) \tag{10.40}$$

Since state 4 results only from the transition $2 \rightarrow 4$, we have

$$\frac{d}{dt}P_4(t) = \lambda_b P_2(t) \tag{10.41}$$

The foregoing equations may be solved sequentially in the same manner as those of the preceding sections. We obtain

$$P_1(t) = e^{-\lambda_a t} \tag{10.42}$$

$$P_2(t) = \frac{\lambda_a}{\lambda_b - \lambda_a}\left(e^{-\lambda_a t} - e^{-\lambda_b t}\right) \tag{10.43}$$

$$P_3(t) = 0 \tag{10.44}$$

and

$$P_4(t) = 1 - \frac{1}{\lambda_b - \lambda_a}\left(\lambda_b\, e^{-\lambda_a t} - \lambda_a\, e^{-\lambda_b t}\right) \tag{10.45}$$

where we have again used the initial conditions, Eqs. (10.3) and (10.4). Since state 4 is the only state corresponding to system failure, the reliability is just

$$R(t) = P_1(t) + P_2(t) \tag{10.46}$$

or

$$R(t) = e^{-\lambda_a t} + \frac{\lambda_a}{\lambda_b - \lambda_a}\left(e^{-\lambda_a t} - e^{-\lambda_b t}\right) \tag{10.47}$$

This, in turn, may be simplified to

$$R(t) = \frac{1}{\lambda_b - \lambda_a}\left(\lambda_b\, e^{-\lambda_a t} - \lambda_a\, e^{-\lambda_b t}\right) \tag{10.48}$$

The properties of standby systems are nicely illustrated by comparing their reliability versus time with that of an active parallel system. For brevity, we consider the situation $\lambda_a = \lambda_b = \lambda$. In this situation, we must be careful in evaluating the reliability, for both Eqs. (10.47) and (10.48) contain $\lambda_b - \lambda_a$ in the denominator. We begin with Eq. (10.47) and rewrite the last term as

$$R(t) = e^{-\lambda_a t} + \frac{\lambda_a}{\lambda_b - \lambda_a}\, e^{-\lambda_a t}\left[1 - e^{-(\lambda_b - \lambda_a)t}\right] \tag{10.49}$$

Then, going to the limit as λ_b approaches λ_a, we have $(\lambda_b - \lambda_a)\, t \ll 1$, and we can expand

$$e^{-(\lambda_b - \lambda_a)t} = 1 - (\lambda_b - \lambda_a)t + \frac{1}{2}(\lambda_b - \lambda_a)^2 t^2 - \cdots \tag{10.50}$$

Combining Eqs. (10.49) and (10.50), we have

$$R(t) = e^{-\lambda_a t} + \lambda_a\, e^{-\lambda_a t}\left[t - \frac{1}{2}(\lambda_a - \lambda_b)t^2 + \cdots\right] \tag{10.51}$$

Thus, as λ_b and λ_a become equal, only the first two terms remain, and we have for $\lambda_b = \lambda_a = \lambda$:

$$R(t) = (1 + \lambda t)\, e^{-\lambda t} \tag{10.52}$$

In Figure 10.6 are compared the reliabilities of active and standby parallel systems whose two components have identical failure rates. Note that the standby parallel system is more reliable than the active parallel system because the backup unit cannot fail before the primary unit, even though the reliability of the primary unit is not affected by the presence of the backup unit.

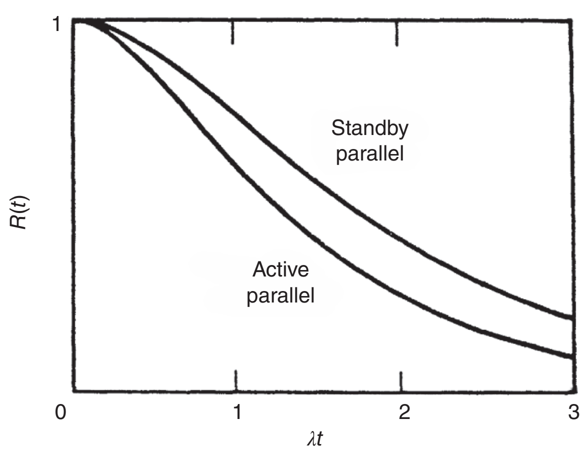


Figure 10.6 Reliability comparison for standby and active parallel systems.

The gain in reliability is further indicated by the increase in the system MTTF for the standby configuration, relative to that for the active configuration. Substituting Eq. (10.52) into Eq. (3.22), we have for the standby parallel system

$$\mathrm{MTTF} = 2/\lambda \tag{10.53}$$

compared to a value of

$$\mathrm{MTTF} = 3/2\lambda \tag{10.54}$$

for the active parallel system.

Failures in the Standby State

We next model the possibility that the backup unit fails before it is required. We generalize the state transition diagram as shown in Figure 10.7. The failure rate λ_b^+ represents failure of the backup unit while it is inactive; state 3 represents the situation in which the primary unit is operating, but there is an undetected failure in the backup unit.

There are now two paths for transition out of state 1. Thus, for $P_1\ (t)$, we have

$$\frac{d}{dt} P_1(t) = -\lambda_a P_1(t) - \lambda_b^+\ P_1(t) \tag{10.55}$$

The equation for state 2 is unaffected by the additional failure path; as in Eq. (10.40), we have

$$\frac{d}{dt} P_2(t) = -\lambda_a P_1(t) - \lambda_b P_2(t) \tag{10.56}$$

We must now set up an equation to determine $P_3(t)$. This state is entered through the $1 \rightarrow 3$ transition with rate λ_b^+ and is exited through the $3 \rightarrow 4$ transition with rate λ_a. Thus,

$$\frac{d}{dt} P_3(t) = -\lambda_b^+\ P_1(t) - \lambda_a P_3(t) \tag{10.57}$$

Finally, state 4 is entered from either states 2 or 3;

$$\frac{d}{dt} P_4(t) = -\lambda_b P_2(t) - \lambda_a P_3(t) \tag{10.58}$$

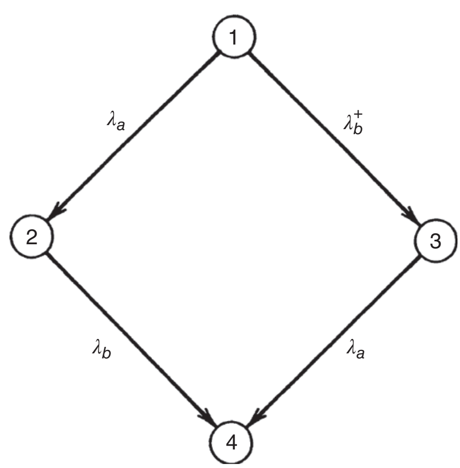


Figure 10.7 State transition diagram with failure in the backup mode.

The Markov equations may be solved in the same manner as before. We obtain, with the initial conditions Eqs. (10.3) and (10.4),

$$P_1(t) = e^{-\left(\lambda_a + \lambda_b^+\right)t} \tag{10.59}$$

$$P_2(t) = \frac{\lambda_a}{\lambda_a + \lambda_b^+ - \lambda_b}\left[e^{-\lambda_b t} - e^{-\left(\lambda_a + \lambda_b^+\right)t}\right] \tag{10.60}$$

and

$$P_3(t) = e^{-\lambda_a t} - e^{-\left(\lambda_a + \lambda_b^+\right)t} \tag{10.61}$$

There is no need to solve for $P_4(t)$, since once again it is the only state for which there is system failure, and therefore,

$$R(t) = P_1(t) + P_2(t) + P_3(t) \tag{10.62}$$

yielding

$$R(t) = e^{-\lambda_a t} + \frac{\lambda_a}{\lambda_a + \lambda_b^+ - \lambda_b}\left[e^{-\lambda_b t} - e^{-\left(\lambda_a + \lambda_b^+\right)t}\right] \tag{10.63}$$

Once again, it is instructive to examine the case $\lambda_a = \lambda_b = \lambda$ and $\lambda_b^+ = \lambda^+$ in which Eq. (10.63) reduces to

$$R(t) = \left(1 + \frac{\lambda}{\lambda^+}\right)e^{-\lambda t} - \frac{\lambda}{\lambda^+}\,e^{-(\lambda + \lambda^+)t} \tag{10.64}$$

In Figure 10.8, the results are shown, having values of λ^+ ranging from zero to λ. The deterioration of the reliability is seen with increasing λ^+. The system MTTF may be found easily by inserting Eq. (10.64) into Eq. (3.22). We have

$$\text{MTTF} = \frac{1}{\lambda} + \frac{1}{\lambda^+} - \frac{\lambda}{\lambda^+}\frac{1}{\lambda + \lambda^+} \tag{10.65}$$

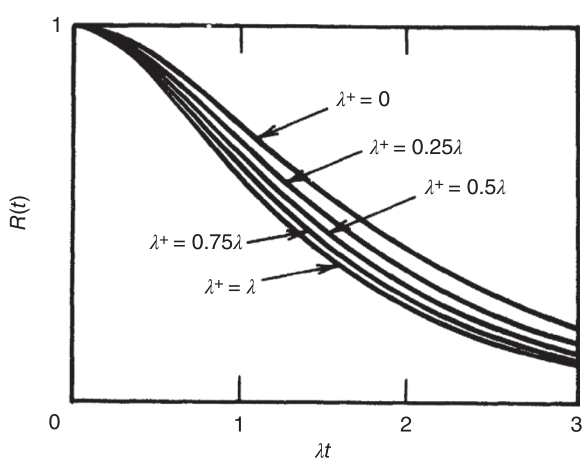


Figure 10.8 Reliability of a standby system with different rates of failure in the backup mode.

When $\lambda^+ = \lambda$, the foregoing results reduce to those of an active parallel system. This is sometimes referred to as a "hot-standby system," since both units are then running, and only a switch from one to the other is necessary. Fault-tolerant control systems, which can use only the output of one device at a time but which cannot tolerate the time required to start up the backup unit, operate in this manner. Unlike active parallel systems, however, they must switch from primary unit to backup unit. We consider switching failures next.

Example 10.2 A fuel pump with an MTTF of 3000 hour is to operate continuously on a 500-hour mission.

a) What is the mission reliability?
b) Two such pumps are put in a standby parallel configuration. If there are no failures of the backup pump while in the standby mode, what is the system MTTF and the mission reliability?
c) If the standby failure rate is 15% of the operational failure rate, what is the system MTTF and the mission reliability?

Solution:

a) The component failure rate is $\lambda = 1/3000 = 0.333 \times 10^{-0}$/hour. Therefore, the mission reliability is

$$R(T) = \exp\left(-\frac{1}{3000} \times 500\right) = 0.846$$

b) In the absence of standby failures, the system MTTF is found from Eq. (10.53) to be

$$\text{MTTF} \simeq \frac{2}{\lambda} = 2 \times 3000 = 6000\,\text{hour}$$

The system reliability is found from Eq. (10.52) to be

$$R(500) = \left(1 + \frac{1}{3000} \times 500\right) \times \exp\left(-\frac{1}{3000} \times 500\right) = 0.988$$

c) We find the system MTTF from Eq. (10.65) with $\lambda^+ = 0.15/3000 = 0.5 \times 10^{-4}$/hour:

$$\begin{aligned}\text{MTTF} = &\frac{1}{0.333 \times 10^{-3}} + \frac{1}{0.5 \times 10^{-4}} \\ &- \frac{0.333 \times 10^{-3}}{0.5 \times 10^{-4}} \frac{1}{0.333 \times 10^{-3} + 0.5 \times 10^{-4}} \\ \text{MTTT} = &\ 5609\,\text{hour}\end{aligned}$$

From Eq. (10.64) the system reliability for the mission is $R(500) = 0.986$.

Switching Failures

A second difficulty in using standby systems stems from the switch from the primary unit to the backup. This switch may take action by electric relays, hydraulic valves, electronic control circuits, or other devices. There is always the possibility that the switching device will have a demand failure probability p large enough that switching failures must be considered. For brevity, we do not consider backup unit failure while it is in the standby mode.

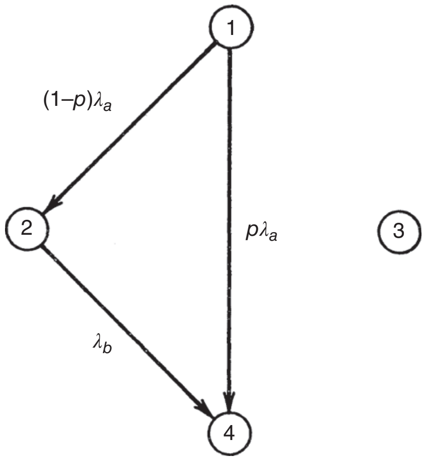


Figure 10.9 State transition diagram with standby switching failures.

The state transition diagram with these assumptions is shown in Figure 10.9. Note that the transition out of state 1 in Figure 10.5 has been divided into two paths. The primary failure rate is multiplied by $1-p$ to get the successful transition into state 2 in which the backup system is operating. The second path with rate $p\lambda_a$ indicates a transition directly to the failed-system state that results when there is a demand failure on the switching mechanism.

For the situation depicted in Figure 10.9, state 1 is still described by Eq. (10.39). Now, however, the $1 \rightarrow 2$ transition is decreased by a factor $1-p$, and so, instead of Eq. (10.40), state 2 is described by

$$\frac{d}{dt}P_2(t) = (1-p)\,\lambda_a\,P_1\,(t) - \lambda_b P_2\,(t) \tag{10.66}$$

and state 4 is described by

$$\frac{d}{dt}\,P_4(t) = \lambda_b\,P_2\,(t) + p\lambda_a\,P_1\,(t) \tag{10.67}$$

Since $P_1(t)$ is again given by Eq. (10.42), we need to solve only Eq. (10.66) to obtain

$$P_2(t) = (1-p)\frac{\lambda_a}{\lambda_b-\lambda_a}\,\left(e^{-\lambda_a t} - e^{-\lambda_b t}\right) \tag{10.68}$$

Accordingly, since state 4 is the only failed state and $P_3(t) = 0$, we may write

$$R(t) = P_1(t) + P_2(t) \tag{10.69}$$

or inserting Eqs. (10.42) and (10.68), we obtain for the reliability

$$R(t) = e^{-\lambda_a t} + \frac{(1-p)\,\lambda_a}{\lambda_b-\lambda_a}\,\left(e^{-\lambda_a t} - e^{-\lambda_b t}\right) \tag{10.70}$$

Once again it is instructive to consider the case $\lambda_a = \lambda_b = \lambda$ for which we obtain

$$R(t) = [1 + (1-p)\,\lambda t]e^{-\lambda t} \tag{10.71}$$

Clearly, as p increases, the value of the backup system becomes less and less, until finally if p is one (i.e. certain failure of the switching system), the backup system has no effect on the system reliability.

Example 10.3 An annunciator system has a mission reliability of 0.9. Because reliability is considered too low, a redundant annunciator of the same design is to be installed. The design engineer must decide between an active parallel and a standby parallel configuration. The engineer knows that failures in standby have a negligible effect, but there is a significant probability of a switching failure.

a) How small must the probability of a switching failure be if the standby configuration is to be more reliable than the active configuration?
b) Discuss the switching failure requirement of a for very short mission times.

Solution:

a) Assuming a constant failure rate, we know that for the mission time T,

$$\lambda T = \ln\left[\frac{1}{R(T)}\right] = \ln\left(\frac{1}{0.9}\right) = 0.1054$$

To find the failure probability, we equate Eq. (10.71) with Eq. (3.104) for the active parallel system:

$$[1 + (1-p)\lambda T]e^{-\lambda T} = 2e^{-\lambda T} - e^{-2\lambda T}$$

Thus,

$$p = 1 - \frac{1}{\lambda T}\left(1 - e^{-\lambda T}\right)$$
$$= 1 - \frac{1}{0.1054}\left(1 - e^{-0.1054}\right) = 0.05$$

(b) For active parallel system, Eq. (3.112), the exponential gives the short mission time approximation:

$$R_a \simeq 1 - (\lambda t)^2$$

For standby parallel system, we expand (10.71) for small λt:

$$R_{sb} = [1 + (1-p)\lambda t]e^{-\lambda t} = [1 + (1-p)\,\lambda t]\left[1 - \lambda t + \frac{1}{2}(\lambda t)^2 \ldots\right]$$
$$\simeq 1 - p\lambda t - \left(\frac{1}{2} - p\right)(\lambda t^2)$$

Then, we calculate p for $R_a - R_{sb} = 0$:

$$1 - (\lambda t)^2 - 1 + p\lambda t + \left(\frac{1}{2} - p\right)(\lambda t)^2 = 0$$

or

$$p = \frac{\frac{1}{2}\lambda t}{1 - \lambda t} \simeq \frac{1}{2}\lambda t$$

The shorter the mission, the smaller p must be, or else switching failures will be more probable than the failures of the second annunciator in the active parallel configuration.

The combined effects of failures in the standby mode and switching failures may be included in the foregoing analysis. For two identical units, the reliability may be shown to be

$$R(t) = \left[1 + (1-p)\,\frac{\lambda}{\lambda^+}\right] e^{-\lambda t} - (1-p)\,\frac{\lambda}{\lambda^+}\, e^{-(\lambda+\lambda^+)t} \tag{10.72}$$

which reduces to Eq. (10.71) as $\lambda^+ \to 0$. For a hot-standby system in which identical primary and backup systems are both running so that $\lambda^+ = \lambda$, we obtain from Eq. (10.72)

$$R(t) = (2-p)\,e^{-\lambda t} - (1-p)e^{-2\lambda t} \tag{10.73}$$

Thus, the reliability is less than that of an active parallel system because there is a probability of switching failure. As stated earlier, in hot-standby systems, such as for control devices, the output of only one unit can be used at a time. If the probability of switching failure is too great, an alternative is to add a third unit and use a 2/3 voting system, as discussed in Chapter 3.

Primary System Repair

Two considerable benefits are to be gained using redundant system components. The first is that more than one failure must occur in order for the system to fail. A second is that components can be repaired while the system is on line. Much higher reliabilities are possible if the failed component has a high probability of being repaired before a second one fails.

Component repair increases the reliability of either active parallel or standby parallel systems. Moreover, either system may be analyzed using Markov methods. In what follows, we derive the reliability for a system consisting of a primary and a backup unit. We assume that the primary unit can be repaired on line. For clarity, we assume that failure of the backup unit in standby mode and switching failures can be neglected.

The state transition diagram shown in Figure 10.10 differs from Figure 10.5 only in that the repair transition has been added. This creates an additional source term of $\nu P_2(t)$ in Eq. (10.39),

$$\frac{d}{dt}\,P_1(t) = -\lambda_a\,P_1(t) + \nu P_2(t) \tag{10.74}$$

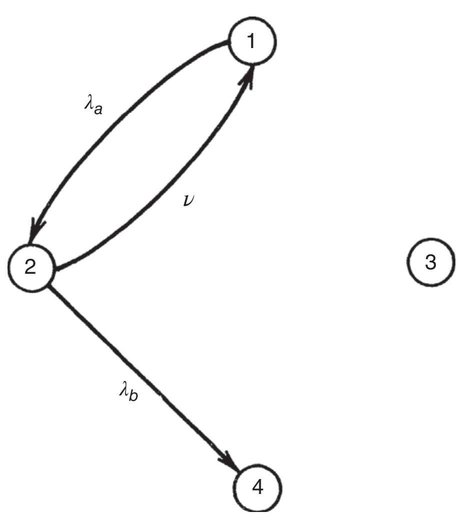


Figure 10.10 State transition diagram with primary system repair.

and the corresponding loss term is subtracted from Eq. (10.40),

$$\frac{d}{dt}P_2(t) = -\lambda_a P_1(t) + (\lambda_b + \nu)P_2(t) \tag{10.75}$$

The reliability, once again, is calculated from Eq. (10.46).

The equations can no longer be solved one at a time, sequentially, as in the previous examples, for now $P_1(t)$ depends on $P_2(t)$. Laplace transforms may be used to solve Eqs. (10.74) and (10.75), but to avoid introducing additional nomenclature we use the following technique instead. Suppose that we look for solutions of the form

$$P_1(t) = Ce^{-\alpha t}; \quad P_2(t) = C'e^{-\alpha t} \tag{10.76}$$

where C, C', and α are constants. Substituting these expressions into Eqs. (10.74) and (10.75), we obtain

$$-\alpha C = -\lambda_a C + \nu C'; \quad -\alpha C' = \lambda_a C - (\lambda_b + \nu)C' \tag{10.77}$$

The constants C and C' may be eliminated between these expressions to yield the form

$$\alpha^2 - (\lambda_a + \lambda_b + \nu)\,\alpha + \lambda_a\lambda_b = 0 \tag{10.78}$$

Solving this quadratic equation, we find that there are two solutions for α:

$$\alpha_\pm = \frac{\nu + \lambda_a + \lambda_b}{2} \pm \frac{1}{2}\left[(\nu + \lambda_a + \lambda_b)^2 - 4\lambda_a\lambda_b\right]^{½} \tag{10.79}$$

Thus, our solutions have the form

$$P_1(t) = C_+ e^{-\alpha_+ t} + C_- e^{-\alpha_- t} \tag{10.80}$$

$$P_2(t) = C'_+ e^{-\alpha_+ t} + C'_- e^{-\alpha_- t} \tag{10.81}$$

We must use the initial conditions along with Eq. (10.79) to evaluate $C_\pm$ and $C'_\pm$. Combining Eqs. (10.80) and (10.81) with the initial conditions $P_1(0) = 1$ and $P_2(0) = 0$, we have

$$C_+ + C_- = 1; \quad C'_+ + C'_- = 0 \tag{10.82}$$

Furthermore, adding Eq. (10.77), we may write, for α_+ and α_-,

$$\alpha_\pm C_\pm = (\lambda_b - \alpha_\pm)C_\pm \tag{10.83}$$

These four equations can be solved for $C_\pm$ and $C'_\pm$. Then, after some algebra, we may add Eqs. (10.80) and (10.81) to obtain from Eq. (10.46)

$$R(t) = \frac{\alpha_+}{\alpha_+ - \alpha_-}e^{-\alpha_- t} - \frac{\alpha_-}{\alpha_+ - \alpha_-}e^{-\alpha_+ t} \tag{10.84}$$

The improvement in reliability with standby systems is indicated in Figure 10.11, where the two units are assumed to be identical, $\lambda_a = \lambda_b = \lambda$, and plots are shown for different ratios of ν/λ. In the usual case, where $\nu \gg \lambda$, it is easily shown that $\alpha_+ \gg \alpha_-$, so that the second term in Eq. (10.84) can be neglected, and that $\alpha_- \approx -\lambda_a\lambda_b/\nu$. Hence, we may write, approximately,

$$R(t) \approx \exp\left(-\frac{\lambda_a\lambda_b}{\nu}t\right) \tag{10.85}$$

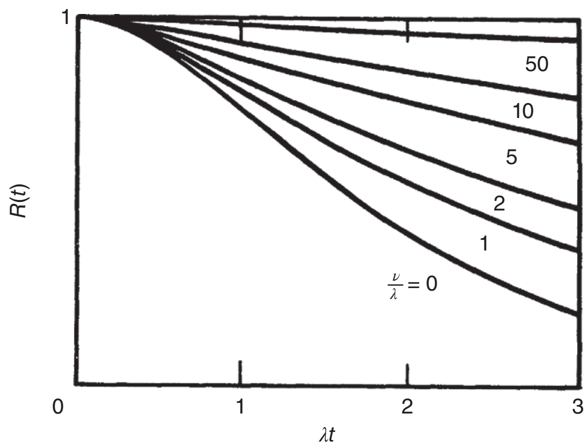


Figure 10.11 The effect of primary system repair rate on the reliability of a standby system.

In the situation in which $\nu \gg \lambda_a, \lambda_b$, the deterioration of reliability is likely to be governed not by the possibility that the backup system will fail before the primary system is repaired but rather by one of the two other possibilities: (i) that switching to the backup system will fail or (ii) that the backup system has failed. These failures are dealt with either by improving the switching and standby mode reliabilities or by utilizing an active parallel system with repairable components. Then, the switching is obviated, and the configuration is more likely to be designed so that failures in either component are revealed immediately.

10.4 Multicomponent Systems

The models described in the two preceding sections concern the dependencies between only two components. In order to make use of Markov methods in realistic situations, however, it is often necessary to consider dependencies between more than two components or to build the dependency models into many-component systems. In this section, we first undertake to generalize Markov methods for the consideration of dependencies between more than two components. We then examine how to build dependency models into larger systems in which some of the component failures are independent of the others.

Multicomponent Markov Formulations

The treatment of larger sets of components by Markov methods is streamlined by expressing the coupled set of state transition equations in matrix form. Moreover, the resulting coefficient matrix can be used to check on the formulation's consistency and to gain some insight into the physical processes at play. To illustrate, we first put one of the two-component, four-state systems discussed earlier into matrix form. The generalization to larger systems is then obvious.

Consider the backup configuration shown in Figure 10.7 in which we allow for the failure of the unit in the standby mode. The four equations for the $P_i(t)$ are given by Eqs. (10.55) through (10.58). If we define a vector $\mathbf{P}(t)$, whose components are $P_1(t)$ through $P_4(t)$, we may write the set of simultaneous differential equations as

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix} = \begin{bmatrix} -\lambda_a - \lambda_b^+ & 0 & 0 & 0 \\ \lambda_a & -\lambda_b & 0 & 0 \\ \lambda_b^+ & 0 & -\lambda_a & 0 \\ 0 & \lambda_b & \lambda_a & 0 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix} \tag{10.86}$$

Consider next a system with three components in parallel, as shown in Figure 10.1b. Suppose that this is a load-sharing system in which the component failure rate increases with each component failure:

λ_1 = component failure rate with no component failures,
λ_2 = component failure rate with one component failure,
λ_3 = component failure rate with two component failures.

If we again enumerate the possible system states in Table 10.1, the state transition diagram will appear as in Figure 10.12. From this diagram, we may construct the equations for the $P_i(t)$. In matrix form, they are

$$\frac{d}{dt}\begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_5(t) \\ P_6(t) \\ P_7(t) \\ P_8(t) \end{bmatrix} = \begin{bmatrix} -3\lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_1 & -2\lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_1 & 0 & -2\lambda_2 & 0 & 0 & 0 & 0 & 0 \\ \lambda_1 & 0 & 0 & -2\lambda_2 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2 & \lambda_2 & 0 & -\lambda_3 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & \lambda_2 & 0 & -\lambda_3 & 0 & 0 \\ 0 & 0 & \lambda_2 & \lambda_2 & 0 & 0 & -\lambda_3 & 0 \\ 0 & 0 & 0 & 0 & \lambda_3 & \lambda_3 & \lambda_3 & 0 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_5(t) \\ P_6(t) \\ P_7(t) \\ P_8(t) \end{bmatrix} \tag{10.87}$$

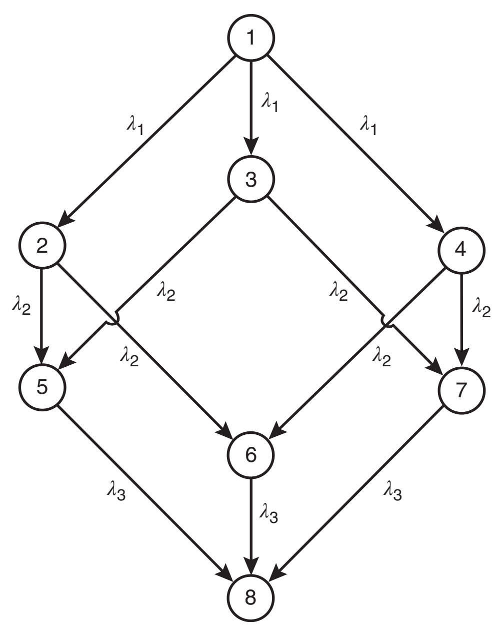


Figure 10.12 Slate transition diagram for a three-component parallel system.

where there are now $2^3 = 8$ states in all. The generalization to more components is straightforward, provided that the logical structure of the dependencies is understood.

Equations (10.86) and (10.87) may be used to illustrate an important property of the coefficient matrix, one which serves as an aid in constructing the set of equations from the state transition diagram. Each transition out of a state must terminate in another state. Thus, for each negative entry in the coefficient matrix, there must be a positive entry in the same column, and the sum of the elements in each column must be zero. Thus, the matrix may be constructed systematically by considering the transitions one at a time. If the transition originates from the ith state, the failure rate is subtracted from the ith diagonal element. If the transition is to the jth state, the failure rate is then added to the jth row of the same column.

A second feature of the coefficient matrix involves the distinction between operational and failed states. In reliability calculations we do not allow a system to be repaired once it fails. Hence, there can be no way to leave a failed state. In the coefficient matrix this is indicated by the zero in the diagonal element of each failed state. This is not the case, however, when availability rather than reliability is being calculated. Availability calculations are discussed in the following section.

For larger systems of equations it is often more convenient to write Markov equations in the matrix form

$$\frac{d}{dt} P(t) = MP(t) \tag{10.88}$$

where P is a column vector with components $P_1(t)$, $P_2(t)$,..., and M is referred to as the Markov transition matrix. Instead of repeating the entire set of equations, as in Eqs. (10.86) and (10.87), we need to write out only the matrix. Thus, for example the matrix for Eq. (10.86) is

$$M = \begin{bmatrix} -\lambda_a - \lambda_b^+ & 0 & 0 & 0 \\ \lambda_a & -\lambda_b & 0 & 0 \\ \lambda_b^+ & 0 & -\lambda_a & 0 \\ 0 & \lambda_b & \lambda_a & 0 \end{bmatrix} \tag{10.89}$$

The dimension of the matrix increases as 2^N, where N is the number of components. For larger systems, particularly those whose components are repaired, the simple solution algorithms discussed earlier become intractable. Instead, more general Laplace transform techniques may be required. If there are added complications, such as time-dependent failure rates, the equations may require solution by numerical integration or by Monte Carlo simulation.

Example 10.4 A 2/3 system is constructed as follows. After the failure of either component a or c, whichever comes first, component b is switched on. The system fails after any two of the components fail. The components are identical with the failure rate λ.

a) Draw a state transition diagram for the system.
b) Write the corresponding Markov transition matrix.
c) Find the system reliability $R(t)$.
d) Determine the reliability when time is set equal to the MTTF one component.

Solution:
For this three-component system, there are eight states. We define these according to Table 10.1.

a) The state transition diagram is shown in Figure 10.13. Note that states 3 and 8 are not reachable.
b) The Markov transition matrix is

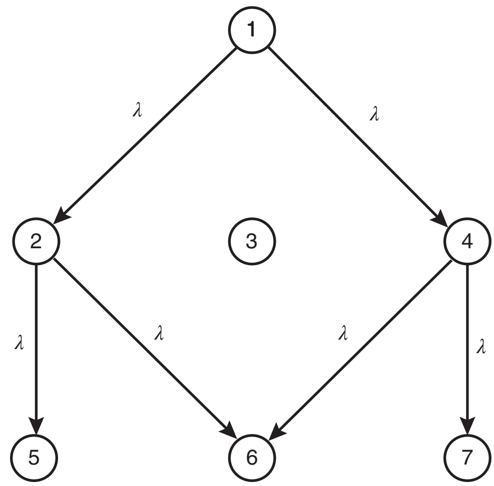


Figure 10.13 State transition diagram for Example 10.4.

$$M = \begin{bmatrix} -2\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda & -2\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda & 0 & 0 & -2\lambda & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

c) The reliability is given by $R(t) = P_1(t) + P_2(t) + P_4(t)$; thus, only three of the eight equations need be solved. First, $dP_1 / dt = -2\lambda P_1$, with $P_1(0) = 1$ yields $P_1(t) = e^{-2\lambda t}$. The equations for $P_2 + P_4$ are the same:

$$\frac{dP_n}{dt} = \lambda P_1 - 2\lambda P_n, \quad P_n(0) = 0; \quad n = 2, 4$$

Therefore,

$$\frac{dP_n}{dt} = \lambda e^{-2\lambda t} - 2\lambda P_n$$

We use the integrating factor $e^{2\lambda t}$ to obtain

$$\frac{d}{dt}\left(P_n e^{-2\lambda t}\right) = \lambda$$

Then, integrating between 0 and t, we obtain

$$P_n(t)\, e^{2\lambda t} - P_n(0) = \lambda t$$

Thus,

$$P_n(t) = \lambda t e^{-2\lambda t}, \quad n = 2, 4$$

Substituting into $R(t) = P_1 + P_2 + P_4$ yields

$$R(t) = (1 + 2\lambda t)e^{-2\lambda t}$$

d) $t = \text{MTTF} \equiv 1/\lambda$. Then,

$$R\,(\text{MTTF}) = (1 + 2 \times 1)\,e^{-2 \times 1} = 0.406$$

Combinations of Subsystems

In principle, we can treat systems of many components using Markov methods. However, with 2^N equations the solutions soon become unmanageable. A more efficient approach is to define one or more subsystems containing the components with dependencies between them. These subsystems can then

be treated as single blocks in a reliability block diagram, and the system reliability can be calculated using the techniques of Chapter 3, since the failures in the subsystem defined in this way are independent of one another.

To understand this procedure, consider the system configurations shown in Figure 10.14. In Figure 10.14a is shown the convention for drawing a two-component standby system of the type discussed in the preceding section as a reliability block diagram. In Figure 10.14b, the standby parallel subsystem, consisting of components *a* and *b,* is in series with two other components. The reliability of the standby subsystem (with no switching errors) is given by Eq. (10.63). Therefore, we define the reliability of the standby subsystem as

$$R_{sb}(t) = e^{-\lambda_a t} + \frac{\lambda_a}{\lambda_a + \lambda_b^+ - \lambda_b}\left[e^{-\lambda_b t} - e^{-\left(\lambda_a + \lambda_b^+\right)t}\right] \tag{10.90}$$

Then, if the failures in components *c* and *d* are independent of those in the standby subsystem, the system reliability can be calculated using the product rule

$$R(t) = R_{sb}(t)R_c(t)\,R_d(t) \tag{10.91}$$

Generalization of this technique to more complex configurations is straightforward.

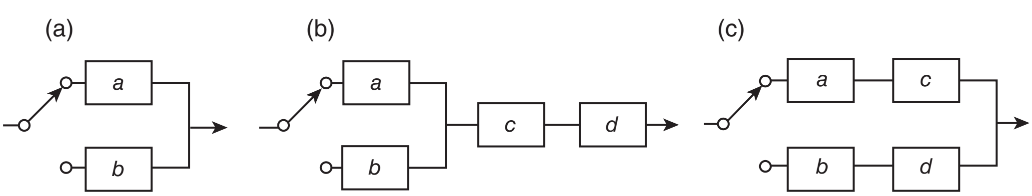


Figure 10.14 Standby configurations.

The configuration in Figure 10.14c illustrates a somewhat different situation. Here, the primary and standby subsystems themselves each consist of two components, a and c, and b and d, respectively. Here, we may simplify the Markov analysis by first combining the four components into two subsystems, each having a composite failure rate. Thus, we define

$$\lambda_{ac} = \lambda_a + \lambda_c \tag{10.92}$$

$$\lambda_{bd} = \lambda_b + \lambda_d \tag{10.93}$$

and

$$\lambda_{bd}^+ = \lambda_b^+ + \lambda_d^+ \tag{10.94}$$

We may again apply Eq. (10.90) to calculate the system reliability if we replace λ_a, λ_b, and λ_b^+ with λ_{ac}, λ_{bd}, and λ_{bd}^+, respectively.

10.5 Availability

In availability, as well as in reliability, there are situations in which the component failures cannot be considered independent of one another. These include shared-load and backup systems in which all the components are repairable. They may also include a variety of other situations in which the dependency is introduced by the limited number of repair personnel or by replacement parts that may be called on to put components into working order. Thus, for example the repair of two redundant components cannot be considered independent if only one crew is on station to carry out the repairs.

The dependencies between component failure and repair rates may be approached once more with Markov methods, provided that the failures are revealed, and that the failure and repair rates are time independent. Although we have already treated the repair of components in reliability calculations, there is a fundamental difference in the analysis that follows. In reliability calculations, components can be repaired only as long as the system has not failed; the analysis terminates with the first system failure. In availability calculations, we continue to repair components after a system failure in order to bring the system back on line, that is to make it available once again.

The differences between Markov reliability and availability calculations for systems with repairable components can be illustrated best in terms of the matrix notion developed in the preceding section. For this reason, we first illustrate an availability calculation with a system for which the reliability was calculated in the preceding section, standby redundance. We then illustrate the limitation placed on the availability of an active parallel configuration by the availability of only one repair crew.

Standby Redundancy

Suppose that we consider the reliability of a two-component system, consisting of a primary and a backup unit. We assume that switching failures and failure in the standby mode can be neglected. In the preceding section, the analysis of such a system is carried out assuming that the primary unit can be repaired with a rate ν. Since there are only three states with nonzero probabilities the state transition diagram may be drawn as in Figure 10.15a, where state 3 is the

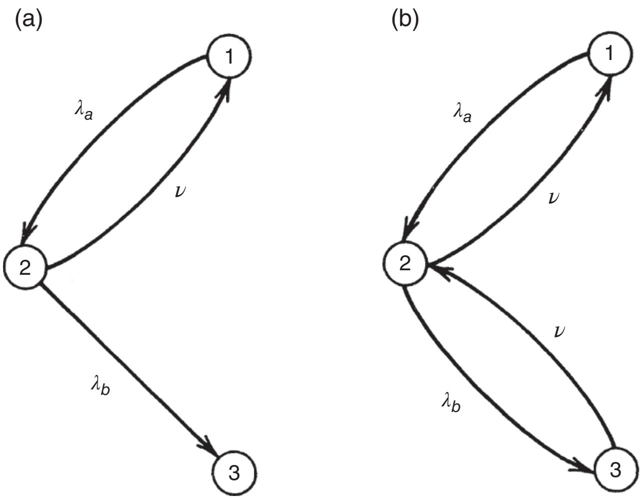


Figure 10.15 State transition diagrams for a standby system: (a) for reliability and (b) for availability.

failed state. The transition matrix for Eq. (10.88) is then given by

$$M = \begin{bmatrix} -\lambda_a & \nu & 0 \\ \lambda_a & -\lambda_b - \nu & 0 \\ 0 & \lambda_b & 0 \end{bmatrix} \tag{10.95}$$

The estimate of the availability of this system involves one additional state transition. In order for the system to go back into operation after both units have failed, we must be able to repair the backup unit. This requires an added repair transition from state 3 to state 2, as indicated in Figure 10.15b. This repair transition is represented by two additional terms in the Markov transition matrix. We have

$$M = \begin{bmatrix} -\lambda_a & \nu & 0 \\ \lambda_a & -\lambda_b - \nu & \nu \\ 0 & \lambda_b & -\nu \end{bmatrix} \tag{10.96}$$

Here, we assume that when both units have failed, the backup unit will be repaired first; we also assume that the repair rates are equal. More general cases may also be considered.

An important difference can be seen in the structures of Eqs. (10.95) and (10.96). In Eq. (10.96), all the diagonal elements are nonzero. This is a fundamental difference from reliability calculations. In availability calculations, the system must always be able to recover from any failed state. Thus, there can be no zero diagonal elements, for these would represent an absorbing or inescapable failed state; transitions can always be made out of operating states through the failure of additional components.

The availability of the system is given by

$$A(t) = \sum_{i \in 0} P_i(t) \tag{10.97}$$

where the sum is over the operational states. The Markov equations, Eq. (10.88), may be solved using Laplace transforms or other methods to determine the $\mathbf{P}(t)$, and Eq. (10.97) may be evaluated for the detailed time dependence of the point availability.

We are usually interested in the asymptotic or steady-state availability, $A(\infty)$, rather than in the time dependence. This quantity may be calculated more simply. We note that as $t \to \infty$, the derivative on the right-hand side of Eq. (10.88) vanishes, and we have the time-independent relationship

$$\mathbf{MP}(\infty) = 0 \tag{10.98}$$

In our problem, this represents the three simultaneous equations

$$-\lambda_a P_1(\infty) + \nu P_2(\infty) = 0 \tag{10.99}$$

$$\lambda_a P_1(\infty) - (\lambda_b + \nu)P_2(\infty) + \nu P_3(\infty) = 0 \tag{10.100}$$

and

$$\lambda_b P_2(\infty) - \nu P_3(\infty) = 0 \tag{10.101}$$

This set of three equations is not sufficient to solve for the $P_i(\infty)$. For all Markov transition matrices are singular; that is, the equations are linearly dependent, yielding only $N-1$ (in our case two) independent relationships. This is easily seen, since adding Eqs. (10.99) and (10.101) yields Eq. (10.100). The needed piece of additional information is the condition that all of the probabilities must sum to 1:

$$\sum_i P_i(\infty) = 1 \tag{10.102}$$

In the situation in which we take $\lambda_a = \lambda_b = \lambda$, our problem is easily solved. Combining Eqs. (10.99), (10.101), and (10.102), we obtain

$$P_1(\infty) = \left[1 + \frac{\lambda}{\nu} + \left(\frac{\lambda}{\nu}\right)^2\right]^{-1} \tag{10.103}$$

$$P_2(\infty) = \left[1 + \frac{\lambda}{\nu} + \left(\frac{\lambda}{\nu}\right)^2\right]^{-1} \frac{\lambda}{\nu} \tag{10.104}$$

and

$$P_3(\infty) = \left[1 + \frac{\lambda}{\nu} + \left(\frac{\lambda}{\nu}\right)^2\right]^{-1} \left(\frac{\lambda}{\nu}\right)^2 \tag{10.105}$$

The steady-state availability may be found by setting $t = \infty$ in Eq. (10.97):

$$A(\infty) = 1 - \left[1 + \frac{\lambda}{\nu} + \left(\frac{\lambda}{\nu}\right)^2\right]^{-1} \left(\frac{\lambda}{\nu}\right)^2 \tag{10.106}$$

If we further assume that $\lambda/\nu \ll 1$, we may write

$$A(\infty) \approx 1 - \left(\frac{\lambda}{\nu}\right)^2 \tag{10.107}$$

Example 10.5 Suppose that the system availability for standby systems must be 0.9. What is the maximum acceptable value of the failure to repair rate ratio λ/ν?

Solution:
Let $x = \lambda/\nu$ in Eq. (10.106). Then,

$$A(\infty) = 1 - \left(1 + x + x^2\right)^{-1} (x)^2$$

Converting to a quadratic equation, we have $x^2 - \gamma x - \gamma = 0$, where

$$\gamma = \frac{1-A}{A} = \frac{1-0.9}{0.9} = \frac{1}{9}$$

and

$$\frac{\lambda}{\nu} \equiv x = \frac{+\gamma + \gamma\sqrt{1+4/\gamma}}{2} = 0.393$$

If instead the rare-event approximation is used,

$$\frac{\lambda}{\nu} \approx \sqrt{1-A(\infty)} = \sqrt{1-0.9} = 0.316$$

Other configurations are also possible. If two repair crews are available, repairs may be carried out on the primary and backup units simultaneously; the result is the four-state system of Table 10.2. As indicated in Figure 10.16a, it is possible to get the primary unit running before the backup unit is repaired. In this situation, states 1, 2, and 3 are the operating states and must be included in the sum in Eq. (10.97). The Markov matrix now becomes

$$M = \begin{bmatrix} -\lambda_a & \nu & \nu & 0 \\ \lambda_a & -\nu-\lambda_b & 0 & \nu \\ 0 & 0 & -\nu-\lambda_a & \nu \\ 0 & \lambda_b & \lambda_a & -2\nu \end{bmatrix} \tag{10.108}$$

Other possibilities may also be added. For example, if switching failures and failures of the backup unit while in standby are not negligible, the state transition diagram is modified as shown in Figure 10.16b, where p represents the probability of failure in switching from the primary to the backup, and λ_b^+ the standby failure rate of the backup unit. The Markov transition matrix corresponding to Figure 10.16b is

$$M = \begin{bmatrix} -\lambda_a-\lambda_b^+ & \nu & \nu & 0 \\ (1-p)\lambda_a & -\lambda_b-\nu & 0 & \nu \\ \lambda_b^+ & 0 & -\lambda_a-\nu & \nu \\ p\lambda_a & \lambda_b & \lambda_a & -2\nu \end{bmatrix} \tag{10.109}$$

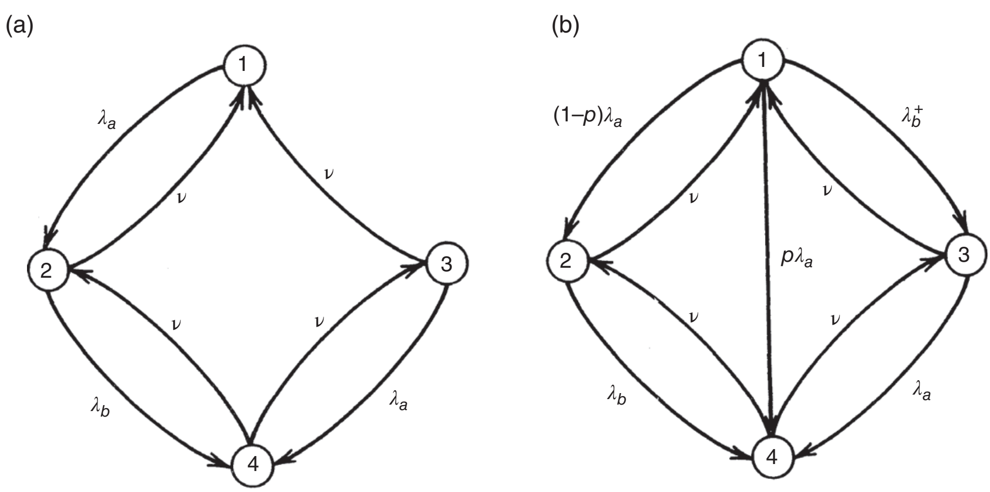


Figure 10.16 State transition diagrams for repairable standby systems.

To recapitulate, steady-state availability problems are solved by the same procedure. Any $N-1$ of the N equations represented by Eq. (10.98) are combined with the condition, Eq. (10.102), that the probabilities must add to 1, to solve for the components of $P(\infty)$. These are then substituted into Eq. (10.97) with the sum taken over all operating states to obtain the availability.

Shared Repair Crews

We conclude with the analysis of an active parallel system consisting of two identical units. We assume that the failure rates are identical and that they are independent of the state of the other unit. We also assume that the repair rates for the two units are the same. In this situation the failures and repairs of the two units are independent, provided that each unit has its own repair crew. The availability is then given by Eq. (10.95). The dependency is introduced not by a hardware failure, as in the case of standby redundance, but by an operational decision to provide a single repair crew that can handle only one unit at a time.

The state transition diagram for the system using two repair crews is shown in Figure 10.17a. Since the availability can be calculated from the component availabilities, as in Eq. (10.95), we will not pursue the Markov solution further. Our attention is directed to the system using one repair crew, indicated by the state transition diagram given in Figure 10.17b.

The transition matrix corresponding to Figure 10.17b is

$$M = \begin{bmatrix} -2\lambda & \nu & \nu & 0 \\ \lambda & -\lambda-\nu & 0 & \nu \\ \lambda & 0 & -\lambda-\nu & 0 \\ 0 & \lambda & \lambda & -\nu \end{bmatrix} \tag{10.110}$$

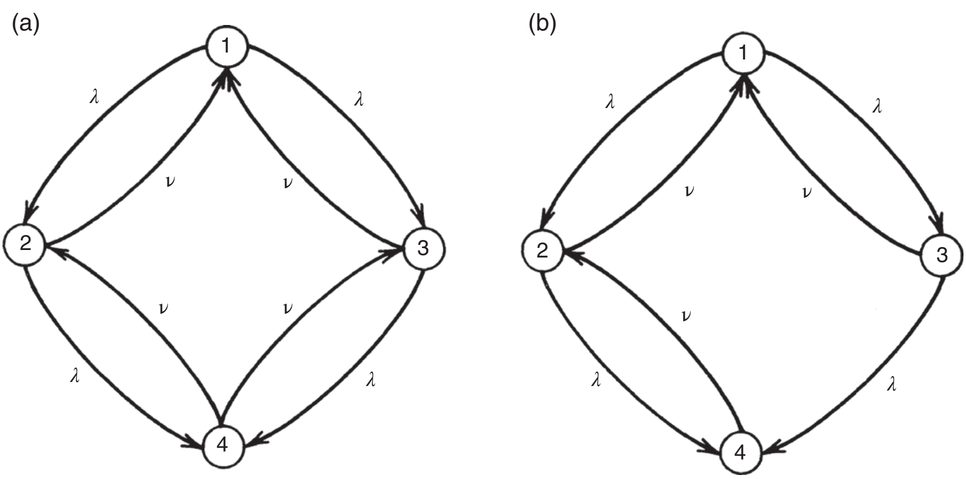


Figure 10.17 State transition diagrams for an active parallel system: (a) two repair crews and (b) one repair crew.

We solve the equations obtained from this matrix along with Eq. (10.102) to yield, after some algebra,

$$P_1(\infty) = \left[1 + 2\frac{\lambda}{v} + 2\left(\frac{\lambda}{v}\right)^2\right]^{-1} \tag{10.111}$$

$$P_2(\infty) + P_3(\infty) = \left[1 + 2\frac{\lambda}{v} + 2\left(\frac{\lambda}{v}\right)^2\right]^{-1} \frac{2\lambda}{v} \tag{10.112}$$

and

$$P_4(\infty) = \left[1 + 2\frac{\lambda}{v} + 2\left(\frac{\lambda}{v}\right)^2\right]^{-1} \frac{2\lambda^2}{v^2} \tag{10.113}$$

Substitution of the results into Eq. (10.97) then yields for the steady-state availability

$$A(\infty) = 1 - \left[1 + 2\frac{\lambda}{v} + 2\left(\frac{\lambda}{v}\right)^2\right]^{-1} \frac{2\lambda^2}{v^2} \tag{10.114}$$

For the usual case where $\lambda/v \ll 1$, this may be approximated by

$$A(\infty) \simeq 1 - 2\left(\frac{\lambda}{v}\right)^2 \tag{10.115}$$

The loss in availability because a second repair crew is not on hand can be determined by comparing these expressions to those obtained for system availability when there are two repair crews. From Eq. (10.95), with $N = 2$, we have

$$A(\infty) = 1 - \left[1 + 2\frac{\lambda}{v} + 2\left(\frac{\lambda}{v}\right)^2\right]^{-1} \left(\frac{\lambda}{v}\right)^2 \tag{10.116}$$

or for the case where $\lambda/v \ll 1$,

$$A(\infty) \simeq 1 - \left(\frac{\lambda}{v}\right)^2 \tag{10.117}$$

Thus, the unavailability is roughly doubled if only one repair crew is present.

Example 10.6 A system has an availability of 0.90. Two such systems, each with its own repair crew, are placed in parallel. What is the availability

a) for a standby parallel configuration with perfect switching and no failure of the unit in standby?
b) for an active parallel configuration?
c) What is the availability if only one repair crew is assigned to the active parallel configuration?

Solution:
The system availability is given by $A(\infty) = v/(v + \lambda)$. Therefore, $v/\lambda = A(\infty)/[1 - A(\infty)] = 0.9/(1 - 0.9) = 9$; $\lambda/v = 0.1110$.

a) From Eq. (10.106),

$$A(\infty) = 1 - \frac{(0.1111)^2}{1 + 0.1111 + (0.1111)^2} = 0.989$$

b) From Eq. (10.116),

$$A(\infty) = 1 - \frac{(0.1111)^2}{1 + 2 \times 0.1111 + (0.1111)^2} = 0.990$$

c) From Eq. (10.114),

$$A(\infty) = 1 - \frac{2 \times (0.1111)^2}{1 + 2 \times 0.1111 + 2 \times (0.1111)^2} = 0.980$$

Example 10.7 Aircraft at Airfield XX each have probability 0.95 of being available on any given day, and therefore a (1 – 0.95=) 0.05 probability of not being available. If it is not available, there is a 0.4 probability of being available in 1 day. What is the probability the aircraft will be available in 4 days?

First, using the *Probability Tree* approach in Figure 10.18, and summing the P(Oper) in each branch:

$$\text{Therefore, } P(\text{Available after 4 days}) = \sum_i P(\text{Available}_i) = 0.899$$

Recall that the one-step transition matrix for a Markov chain with states $S = \{0, 1, 2\}$ is

$$\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{bmatrix} \tag{10.118}$$

where $p_{ij} = \Pr\{X_1 = j \mid X_0 = i\}$ are the transition probabilities. This means that the future behavior of the system depends only on the current state i and not on any of the previous states.

Then, using Eq. (10.88), in its form as the N-step transition probability matrix of Chapman–Kolmogorov, since the n-step transition probabilities $P_{ij}^{(n)} = P(X_n = j \mid X_0 = i)$ obey the following law (for arbitrary $m < n$:)

$$P_{ij}^{(n)} = \sum_k P_{kj}^{(n-m)} P_{ik}^{m} \tag{10.119}$$

So, the transition data in this example is

		Next day status	
		Available	**Not available**
Current	Available	0.95	0.05
Aircraft status	Not available	0.4	0.6

and the transition matrix:

$$\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} = \begin{bmatrix} 0.95 & 0.05 \\ 0.4 & 0.6 \end{bmatrix}$$

So, if we want operating probability at 4 days:

$$\mathbf{P} \times \mathbf{P} \times \mathbf{P} \times \mathbf{P} = \mathbf{P^4} = \begin{bmatrix} 0.95 & 0.05 \\ 0.4 & 0.6 \end{bmatrix}^4 = \begin{bmatrix} 0.889056 & 0.100944 \\ 0.80755 & 0.19245 \end{bmatrix}$$

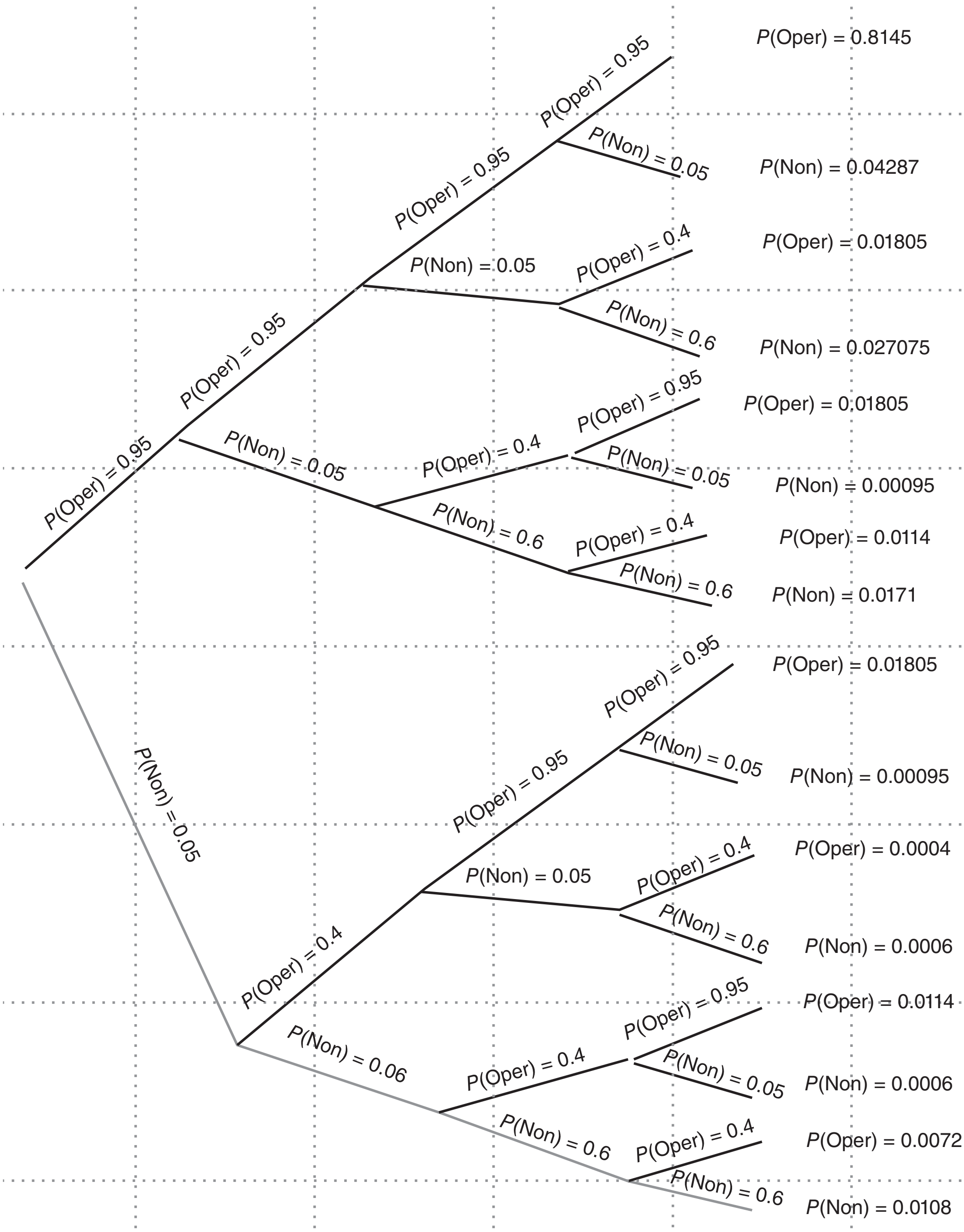


Figure 10.18 Probability tree for aircraft availability.

where

$$\text{"Steady } \textit{state}\text{"} \cong \mathbf{P}^{20} = \begin{bmatrix} 0.8888896 & 0.111110398 \\ 0.88888319 & 0.111116814 \end{bmatrix}$$

That is, in the long run, availability will be 0.89, and conversely, unavailability will be 0.11.

Markov Availability – Advantages and Disadvantages

The Advantages of Markov Availability Analysis

1) The Markov analysis is preferred by most maintenance specialists to test the performance of small running systems with components that show a great level of dependency on each other. With a small and updated Markov diagram, it is possible to analyze the transition between states and the degree with which this transition is happening. The other advantage that you will find with using this analysis is that reliance on past state results is not all that important in determining how the future states will behave.
2) The Markovian process being integrated into computer software allows for easy and quick typing of commands to generate fast solutions where large and complicated Markov diagrams are in use.

The Disadvantages of Markov Availability Analysis

1) The downside of the Markovian process is that it only fits small models, and the diagrams get complex when trying to analyze dependency in larger systems. It becomes completely impractical to evaluate the diagrams manually, which is why it prompts the use of computer software.
2) The Markovian analysis is ideal for weighing dependency in situations such as evaluating components in warm or cold standby, or analyzing spares with short on-site stocks. When analyzing bigger models, these difficulties can be alleviated through combining more quantitative models.

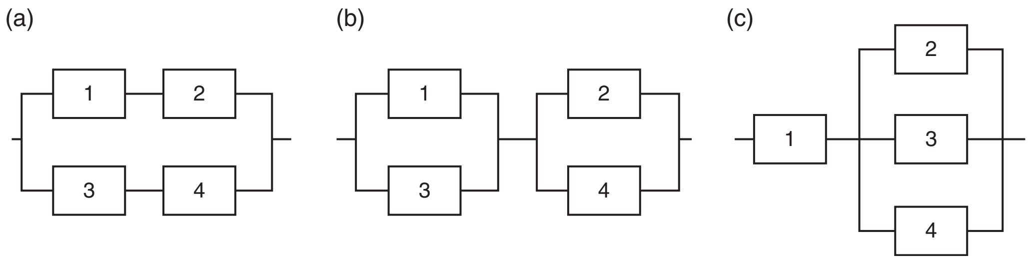
Bibliography

Barlow, R.E. and Proschan, F. (1965). *Mathematical Theory of Reliability*. New York: Wiley.
Feller, W. (1968). *An Introduction to Probability Theory and its Applications. Wiley* .
Green, A.E. and Bourne, A.J. (1972). *Reliability Technology*. New York: Wiley.
Grinstead, C.M. and Snell, J.L. (1997). *Introduction to Probability*. American Mathematical Society.
Henley, E.J. and Kumamoto, H. (1981). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.
Kemeny, J.G. and Snell, J.L. (1960). *Finite Markov Chains*. Van Nostrand.
McCormick, N.J. (1981). *Reliability and Risk Analysis*. New York: Academic Press.
Sandler, G.H. (1963). *System Reliability Engineering*. Englewood Cliffs, NJ: Prentice-Hall.

Exercises

10.1 Two stamping machines operate in parallel positions on an assembly line, each with the same MTTF at the rated speed. If one fails, the other takes up the load by doubling its operating speed. When this happens, however, the failure rate also doubles. Assuming no repair, how many MTTF for a machine at the rated speed will elapse before the system reliability drops below (a) 0.99, (b) 0.95, and (c) 0.90?

10.2 Enumerate the 16 possible states of a four-component system by writing a table similar to Table 10.1. For the following configurations, which are the failed states?



10.3 Consider a system consisting of two identical units in an active parallel configuration. The units cannot be repaired. Moreover, because they share loads, the failure rate $\lambda*$ of the remaining unit is substantially larger than the unit failure rates when both are operating.

a) Find an approximation for the system reliability for a short period of time (i.e. $\lambda t \ll 1$ and $\lambda * t \ll 1$).
b) How large must the ratio of $\lambda*/\lambda$ become before the MTTF of the system is no greater than that for a single unit with failure rate λ?

10.4 Repeat Exercise 10.1 for the standby configurations shown in Figure 10.14.

10.5 For the idealized standby system for which the reliability is given by Eq. (10.52),

a) Calculate the MTTF in terms of λ.
b) Plot the time-dependent failure rate $\lambda(t)$, and compare your results to the active parallel system depicted in Figure 9.2b.

10.6 Verify Eqs. (10.42) through (10.45).

10.7 Calculate the variance for the time-to-failure for two identical units, each with a failure rate λ, placed in standby parallel configuration, and compare your results to the variance of the same two units placed in active parallel configuration. (Ignore switching failures and failures in the standby mode.)

10.8 Derive Eq. (10.52) assuming that $\lambda_b = \lambda_a$ from the beginning.

10.9 Under a specified load, the failure rate of a turbogenerator is decreased by 30% if the load is shared by two such generators. A designer must decide whether to put two such generators in active or standby parallel configuration. Assuming that there are no switching failures or failures in the standby mode,

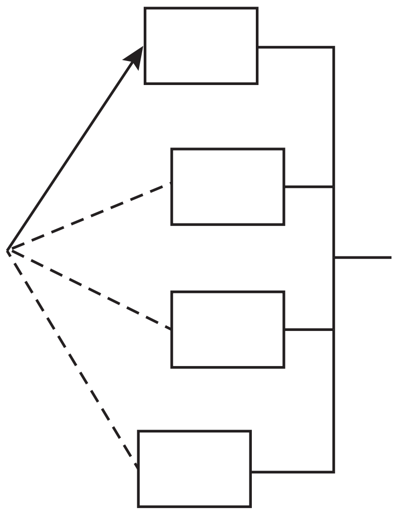
a) Which system will yield the larger MTTF?
b) What is the ratio of MTTF for the two systems?

10.10 Show that Eq. (10.64) reduces to Eq. (10.52) as $\lambda^+ \to 0$.

10.11 Consider the following configuration consisting of four identical units with failure rate λ and with negligible switching and standby failure rates. There is no repair.

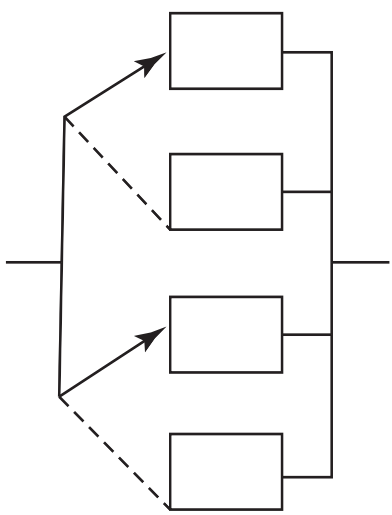
a) Show that the reliability can be expressed in terms of the Poisson distribution discussed in Chapter 3.

b) Evaluate the reliability in the rare-event approximation for small λt.
c) Compare the result from b to the rare-event approximation for four identical units in active parallel configuration, as developed in Chapter 3, and evaluate the reliabilities for $\lambda t = 0.1$.



10.12 Verify Eq. (10.68).

10.13 For the following system, assume unit failure rates λ, no repair, and no switching or standby failures.



a) Calculate the reliability.
b) Approximate the result by the rare-event approximation for small λt, and compare your result to that for four units in an active parallel configuration.

10.14 Consider a standby system in which there is a switching failure probability p and a failure rate in the standby mode of λ_b^+.

a) Draw the transition diagram.
b) Write the Markov equations.
c) Solve for the system reliability.
d) Reduce the reliability to the situation in which the units are identical, $\lambda_a = \lambda_b = \lambda, \quad \lambda_b^+ = \lambda$

10.15 A design team is attempting to optimize the reliability of a navigation device. The choices for the rate gyroscopes are (a) a hot-standby system consisting of two gyroscopes and (b) a 2/3 voting system consisting of three gyroscopes. The mission time is 20 hour, and the gyroscope failure rate is 3×10^{-5}/hour. What is the greatest probability of switching failure in the hot-standby system for which mission reliability is greater than that of the $\frac{2}{3}$ system? Assume that failures in logic on the 2/3 system can be neglected. (*Hint*: Assume rare-event approximations for the gyroscope failures.)

10.16 Derive Eq. (10.72).

10.17 (a) Find the asymptotic availability for a standby system with two repair crews; the Markov matrix is given by Eq. (10.108). Assume that $\lambda_a = \lambda_b = 0.01$/hour and $v = 0.5$/hour.

(b) Evaluate the asymptotic availability for a standby system for the same data, except that there is only one repair crew. The Markov matrix is given by Eq. (10.96).

10.18 Derive Eqs. (10.82) and (10.83).

10.19 A system has an asymptotic availability of 0.93. A second redundant system is added, but only the original repair crew is retained. Assuming that all failures are revealed, estimate the asymptotic availability.

10.20 Derive Eqs. (10.103) through (10.105).

10.21 Assume that the units in Exercise 10.11 all have failure and repair rates λ and v. A single crew repairs the most recently failed unit first.

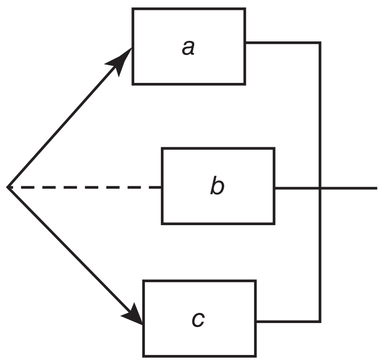
a) Determine the asymptotic availability in terms of v and λ.
b) Approximate your result for the case $\lambda/v \ll 1$.
c) Compare your result to that for the same units in active parallel configuration when $\lambda/v = 0.02$.

10.22 Consider the 2/3 standby configuration shown on the following page. It consists of three identical units; two units are required for operation. If either unit a or c fails, unit b is switched on. Ignore switching failures and repair, but assume failure rate λ and $\lambda*$ in the operating and standby modes.

a) Enumerate the possible system states and draw a transition diagram.
b) Write the Markov equations for the system.

10.23 Two ventilation units are in active parallel configuration. Each has an MTTF of 120 hour. Each is attended by a repair crew, and the MTTR is known to be 8 hour.

a) Calculate the availability, assuming that either unit can provide adequate ventilation.
b) The units are replaced by new models with an MTTF of 200hour. Can the staff be reduced to one repair crew without a net loss of availability? (Assume that the MTTR remains the same.)



10.24 Assume that the units in Exercise 10.22 have identical repair rates v.

a) Enumerate the system states and draw a transition diagram.
b) Write the transition matrix, M, for the Markov equations.
c) Determine the asymptotic value of the system availability.

11

System Safety Analysis

"Human error, lad of imagination, and blind ignorance, The practice of engineering is in large measure a continuing struggle to avoid making mistakes for these reasons."
Source: Samuel C. Horman; The Existential Pleasures of Engineering, (1976)

11.1 Introduction

The discussion of system safety analysis in this chapter presents a different emphasis from the more general reliability considerations considered thus far. While all failures are included in the determination of reliability, our attention now is turned specifically to those that may create safety hazards. The analysis of such hazards is often difficult, for with proper precautions taken in design, manufacture, and operation, failures causing safety problems should occur infrequently. Thus, the small probabilities encountered complicate the collection of data needed for analysis and making improvements. As a result, increased importance is assumed by more qualitative methods as well as by the engineer's understanding of the hazards that may arise. These difficulties notwithstanding the potentially life-threatening nature of the hazards under consideration make safety analysis an indispensable component of reliability engineering.

Safety systems analysis has derived much of its importance from its association with industrial activities that may engender accidents of grave consequences. If we examine, in detail, historic accidents such as the disastrous chemical leak at Bhopal, India, in 1984, and the 1986 destruction of the nuclear reactor at Chernobyl, some of the difficulties in the safety assessment of such systems begin to become apparent. First, the system is likely to have very small probabilities of a catastrophic failure, because it has redundant configurations of critical components. It then follows that the events to be avoided have either never occurred or if they have, only rarely. There are few, if any, statistics on the probabilities of failures of the system as a whole, and reliability testing on the system level is likely to be impossible. Secondly, whatever accidents have occurred have rarely been the result of component failures of a type that would be easy to predict through reliability testing. Rather, the web of events leading to the accident is usually a complex of equipment failures, faulty maintenance, instrumentation and control problems, and human errors.

Safety analysis is essential for the full range of products and systems, from the large technological systems just discussed to small consumer items, for even though the latter may not pose the threat of single catastrophic accidents, their production in large quantities leads to the possibility of many individual incidents, each capable of causing injury or death. Here again, the limitations of

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

standard reliability testing and evaluation procedures are apparent. The primary challenge to the product development personnel is to understand the wide variety of environments and circumstances under which the product will be used and to try to anticipate and protect against faulty installation or maintenance, misuse, inappropriate environments, and other hazards that may not be revealed through standard reliability tests. An additional imperative is to examine not only how the product may fail in a hazardous manner but also how the user may be harmed during normal operation. Adequate protection must be afforded from the rotating blades, electrical filaments, flammable liquids, heated surfaces, and other potential hazardous features that are necessary constituents of many industrial and consumer products.

Even though hazard creation most often involves the intertwined effects of equipment failure and human behavior, analysis is expedited by examining them separately. Thus, in the following section, we build on the discussion in the preceding chapters to focus on those particular aspects of equipment failure most closely related to safety hazards. In Section 11.3, the importance of the human element is emphasized. In that discussion, the primary focus is on the operations of industrial facilities where efforts may be much more effective in reducing human error than they are likely to be in modifying consumer psychology. With the background gained in examining the hazardous aspects of equipment and of human causes, we are prepared in Section 11.4 for an overview of those analytical methods that have been developed to rationalize the discussion of safety analysis. Sections 11.5 then focuses on fault trees. The Chapter end with Section 11.6 - Reliability/Safety Risk Analysis, continuing the introduction to Risk analysis from Chapter 5.

11.2 Product and Equipment Hazards

In examining equipment with safety repercussions, it is useful once again to frame the analysis in terms of the bathtub curve and consider infant mortality, random events, and aging as hazard causes. Most of the materials discussed in earlier chapters regarding these causes remain relevant. Now, however, we must extend the level of analysis to even less probable and therefore possibly more bizarre sets of causes. We also must consider not only product or equipment failures but also potential hazards created in the course of product usage.

Design shortcomings, or variability in the production process, are the most likely causes of early or infant mortality failures. Changes in details late in the design process to facilitate manufacture or construction, which are not thoroughly checked to ensure that a new hazard has not been introduced, may be particularly dangerous. Such a change was implicated, for example in the 1981 collapse of the Kansas City Hyatt Regency walkways that resulted in 114 fatalities. Failure to meet materials specification, improvisation in construction procedures, and unsafe economic choices made in manufacturing processes may all defeat the integrity of the original design and result in weakened systems that are then prone to infant mortality hazards. Faulty installations of hot water heaters, stoves, or other consumer products are also prone to create infant mortality hazards.

Random failures or hazards are characterized by chance occurrences that are independent of product age. In general, they are caused by an environment that is unanticipated or for which the product does not have the strength to withstand. They tend to be brought about because the product is used – or misused – under conditions that were not contemplated in the design or were thought to be so improbable that they were lost in the cost-performance trade-offs. The largest danger in creating a new product is arguably not that there is an inadequate safety margin against a known hazard, but that a potential hazard completely escapes the attention of the design team. Even if a thorough study reveals all significant hazards, however, many decisions must be faced with safety implications.

Governmental bodies, professional organizations, and insurance underwriters' codes of standards provide a basis for assessing the level of potential hazards for many products. Often, such standards must be promulgated by specialized bodies cognizant of unique hazard combinations of particular industries. The safety of food processing equipment, for example is complicated by the conflicting requirements that machinery be readily accessible for cleaning to prevent unsanitary conditions from arising and the need for extensive guard equipment to protect workers from hot surfaces, cutting blades, and other mechanical hazards. While standards and codes of good practice provide a point of departure for the analysis of hazards, new designs and novel applications may be expected to present potentially hazardous conditions that have not been contemplated in the standards. Thus, to make informed safety decisions it is incumbent upon the product development personnel to gain a thorough understanding of the product and its required use.

To understand the difficult trade-offs that must be faced, consider a television monitor. Ventilation slits are required to prevent overheating and to allow the electronics to operate at a reasonable temperature. More and larger ventilation paths will likely improve reliability and prolong the life of the set. However, the designer must also consider unusual locations where ventilation is curtailed, where debris is piled on top or stacked against the monitor, or where other cooling impediments are encountered. Safety analysis then requires not only the determination of the effects of these situations on set life but also whether there is an unacceptable risk of fire. Conversely, if the ventilation slits are made larger to add an extra margin of cooling capacity, then the increased danger that a child will succeed in inserting a kitchen knife or other object through a slit and come into contact with high voltage must be addressed. Thirdly, the magnitude of the hazard created if fluid is spilled or the monitor immersed must be considered to determine whether fluid entering through the ventilation slits will result in a benign failure or an unacceptable risk of electrical shock.

The engineering for safety must go beyond the contemplation of unusual accidents and inadvertent misuse to consider situations where the user behavior compounds potential hazards. From the nineteenth-century captains of Mississippi river boats, who blocked safety valves in order to get more pressure and more performance from their boilers, to present-day motorists, who negate the effects of antilock brakes by driving more aggressively on wet pavements, product users frequently overcome safety features in order to enhance performance at the cost of increased risk. Operational limits exceeded to increase performance, safety guards removed to facilitate maintenance, and warnings ignored as a result of past false alarms are among the plethora of causes of increased risk induced by unintended usage. Such behavior further complicates the already difficult legal and ethical issues raised in determining the extent to which users must be protected from their deliberate unsafe practices.

Product modifications or modernizations likewise may introduce new and unanticipated hazards. Motors modified for racing, aircraft converted from civilian to military or from passenger to cargo use, and robots or machinery devoted to new and novel manufacturing tasks all require careful scrutiny to ensure that the safety integrity of the original design is not compromised. But often, modifications take place years into the product life, when knowledge of the original design calculations has faded, components suppliers have changed, and technology has evolved. An example of particularly ill-conceived design modifications was those made to the steamship *Birkenhead*. In converting this warship to a troop carrier, large passageways were cut through the water-tight bulkheads to provide more light, air, and spaciousness for the troops. But the penetrations not only destroyed the water-tight compartmentalization of the ship but also greatly weakened the bulkheads. Thus, when the ship struck a rock in 1852, it both flooded very rapidly and broke into two, resulting in over 400 fatalities. While engineering safety practices have matured a great deal since that time, it, similar to other historical disasters, serves as a reminder of the potential consequences of ignorance in making ad hoc modifications to the existing systems.

Even after provisions have been made to minimize the dangers of infant mortality or random hazards, there remains the problem of dealing with the aging failures that may be expected to become increasingly pronounced as the product approaches the end of its useful life. Normally, a target life is stipulated as a part of the design process. Assuming that adequate maintenance is provided to replace those components with shorter lives – such as spark plugs, brake linings, and tires on automobiles, for example – failures attributable to aging should not create significant risk within the design life. In relatively few situations, however, can it be guaranteed that a product or system will not continue to be used well beyond its design life. To be sure, in some areas of rapid technological development, such as in microprocessor development, products may become obsolescent and be replaced long before aging effects become important. Likewise, safety-critical systems may be licensed or controlled for removal from service after the number of operating hours for which previous analysis and/or life tests have verified their capability. Military aircraft and nuclear reactor pressure vessels, for example may fall into this category. More often than not, however, the increasing cost of maintenance and recovery from breakdown is weighed against replacement cost in determining at what point a product is retired.

Even where there are strong safety implications, a system can be allowed to operate well beyond its target design life, provided dependable inspection and repair protocols are employed. The knowledge of the aging process that has been gained through the years of operation, however, must provide inspection methods capable of detecting the aging phenomena early enough to repair or take the system out of service before the deterioration reaches a hazardous threshold. Many commercial aircraft, for example have been allowed to operate under such scrutiny beyond the design life originally targeted.

With consumer products, the situation is likely to be quite different, for unless there is a clear and obvious danger, the user is prone to run the product until it fails and then decide whether to replace or repair it. The critical design consideration here is to ensure that the wearout modes are benign. The challenge is simply illustrated with a hot plate, coffee maker, or other appliance with a heating element. Suppose that the design includes a fuse to prevent fire in the event that the heater fails in a dangerous mode. Then, the heater failure better occur before the fuse deterioration becomes a problem. One complicated situation, in fact, was recently in the courts, where a consumer product design was "improved" by incorporating a heater with a longer design life. However, after the new design resulted in a number of fires it was discovered that the melting temperature of the fuse gradually increased with time to the point where by the time the heater finally failed, the fuse was no longer operable.

The foregoing discussion provides only the beginnings for the level of sophistication needed to ferret out the potential hazards that may be brought about by infant mortality, random and aging phenomena, and their interactions. The analytical methods introduced in Section 11.4 provide techniques for more structured analysis. Use of these should reduce the possibility of potentially significant hazards that escape consideration altogether. In addition, the reading of case histories in newspapers and the professional literature over a period of years is invaluable in enhancing one's ability to identify and eliminate potential hazards before they become safety problems.

11.3 Human Error

All engineering is a human endeavor, and in the broadest sense most failures are due to human causes, whether they be ignorance, negligence, or limitations of vigilance, strength, and manual dexterity. Designers may fail to fully understand system characteristics or to anticipate properly the nature and magnitudes of the loading to which a system may be subjected or the environmental conditions under which it must operate. Indeed, much of engineering education is devoted to understanding these and the related phenomena. Similarly, errors committed during manufacture or construction are attributable either to the personnel involved or to the engineers responsible for the setup of the manufacturing process. Quality assurance programs have a central role in detecting and eliminating such errors in manufacture and construction.

We consider here only human errors that are committed after design and manufacture, those that are committed in the operation and maintenance of a system. This is a convenient separation, since design and manufacturing errors, whether they are considered human or not, appear in the as-built system as shortcomings in the reliability of the hardware.

Even with our attention confined to human errors appearing in the operation and maintenance of a system, we find that the uncertainties involved are generally much greater than in the analysis of hardware reliability. There are three categories of uncertainty. First, the natural variability of human performance is considerable. Not only do the capabilities of people differ, but the day-to-day and hour-to-hour performance of any one individual also varies. Second, there is a great deal of uncertainty about how to model probabilistically the variability of human performance, since the interactions with the environment, with stress, and with fellow workers are extremely complex and to a large extent psychological. Third, even when tractable models for limited aspects of human performance can be formulated, the numerical probabilities or model parameters that must be estimated in order to apply them are usually only very approximate, and the range of situations to which they apply is relatively narrow.

It is, nevertheless, necessary to include the effects of human error in the safety analysis of any complex system, for as the consequences of accidents become more serious, and more emphasis is put on reliable hardware and highly redundant configurations, an increasing proportion of the risk is likely to come from human error or more accurately from complex interactions of human shortcomings and equipment problems. Even though accurate predictions of failure probabilities are problematical, a great deal may be gained from studying the characteristics of human reliability and contrasting them with those of hardware. From such study comes an insight into how systems may be designed and operated in order to minimize and mitigate accidents in which the operating and maintenance staff may play an important role.

It has been pointed out (Rasmussen 1982) that increasingly there is a centralization of systems, whether they be larger capacity power and chemical plants, aircraft carrying greater number of passengers, or structures with larger capacities. Since human error in the operation of many such centralized systems may lead to accidents of major consequence to life and property, there has been an increased emphasis on plant automation. There are certainly limitations on such automation, particularly when the uncertainty of how an operator may react to a situation is overridden by the need for human adaptability in dealing with conditions that have not or could not be incorporated into the automated control system. Moreover, automated operation does not tend to eliminate humans from consideration but rather to remove them to tasks of two quite dissimilar varieties, routine tasks of maintaining, testing, and calibrating equipment and protective tasks of watching for plant malfunctions and preventing their accident propagation. These two classes of tasks tend to enter system safety considerations in different ways. When humans err in routine testing, maintenance, and repair work, they may introduce latently risky conditions into the plant. Any errors that they make in taking protective actions under emergency conditions may increase the severity of an accident.

The problems inherent in maximizing human reliability for the two classes of tasks may be viewed graphically in Figure 11.1. Generally, there is an optimum level of psychological stress

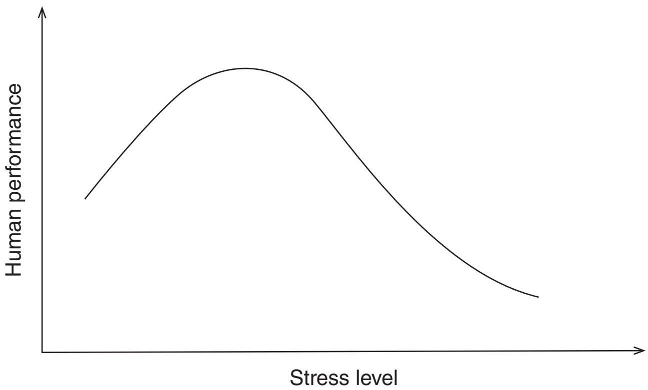


Figure 11.1 The effect of stress level on human performance.

for human performance. When the level is too low, humans are bored and make careless errors; too high a level may cause them to make a number of inappropriate, near-panic responses to a situation. To illustrate, consider the example of flying a commercial airliner. The pilot's monitoring of controls during level, uneventful flight in a highly automated aircraft would fall on the low level of the curve. The principal danger here is carelessness or lack of attention. Normal take-offs and landings are likely to be closer to the optimum stress level for attentive behavior. At the other extreme, pilot reaction to major inflight emergencies, such as onboard fires or power failures, is likely to be degraded by the high stress level present. Because of the quite different factors that come into play, we now consider human reliability and its degradation under the two limiting situations of very routine tasks and tasks performed in emergency situations.

Routine Operations

For purposes of analysis it is useful to classify human errors as random, systematic, or sporadic. These classes may be illustrated by considering the simple example, shown in Figure 11.2, of the ability to hit a target (H.R. Guttmann, unpublished lecture notes, Northwestern University, 1982). Random errors are dispersed about the desired value without bias; that is, they have the true mean value (in x and y), but the variance may be too large. These errors may be corrected if they are attributable to an inappropriate tool or man–machine interface. For example, if it is not possible to read instruments finely enough or to adjust setting precisely enough, such improvements are in order. Similarly, training in the particular task may reduce the dispersion of random errors. Figure 11.2b illustrates systematic errors whose dispersion is sufficiently small, but with a bias departing from the mean value. Such bias may be caused by tools or instruments that are out of calibration, or it may come from incorrect performance of a procedure. In either case, corrective measures may be taken. More subtle psychological factors – such as the desire of an inspector not to miss any faulty parts, and thus declaring a good many faulty even though they are not – may also cause bias errors.

Perhaps sporadic errors, pictured in Figure 11.2c, are the most difficult to deal with, for they rarely show observable patterns. They are committed when the person acts in an extreme or careless way: forgetting to do something altogether, performing an action that was not called for, or reversing the order in which things are done. For example, a meter reader might, in taking a series of meter readings, read a wrong meter. Again, careful design of the man–machine interface can

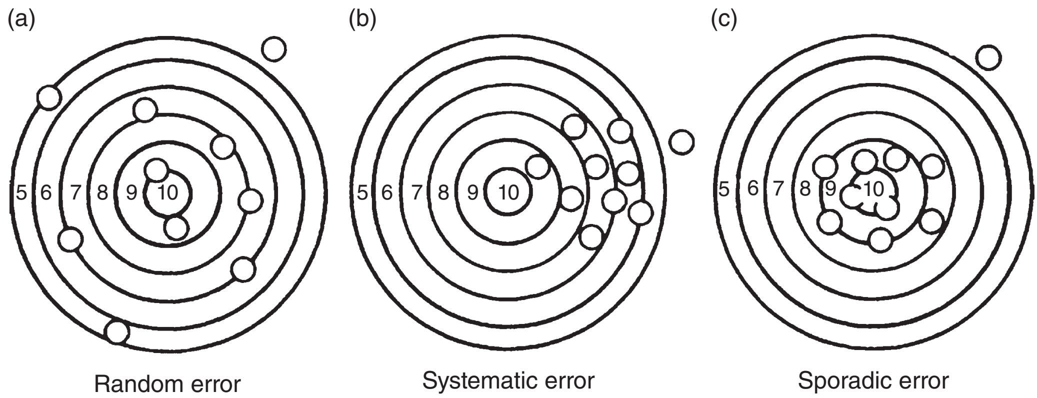


Figure 11.2 Classes of *human error*.

minimize the number of sporadic errors. Color, shape, and other means can be used to differentiate instruments and control and to minimize confusion. Sporadic errors, in particular, are amplified by the carelessness inherent in low-stress situations as well as by the confusion of high-stress situations.

Let us first examine sporadic errors made in routine situations. Certainly, under any circumstances, errors are minimized by a well-designed work environment. Such design would take into account all the standard considerations or human factors engineering: comfortable seating, adequate light, temperature and humidity control, and well-designed control and instrument panels to minimize the possibilities for confusion. The attention span that can be expected for routine tasks is still limited. As indicated in Figure 11.3, attention spans for detailed monitoring tend to deteriorate rapidly after about half an hour, indicating the need for frequent rotation of such duties for optimal performance. The same deterioration may be expected for very repetitive tasks, unless there is careful checking or other intervention to ensure that such deterioration does not take place.

Probably, one of the most important ways in which system reliability is degraded is through the dependencies introduced between redundant components during the course of routine

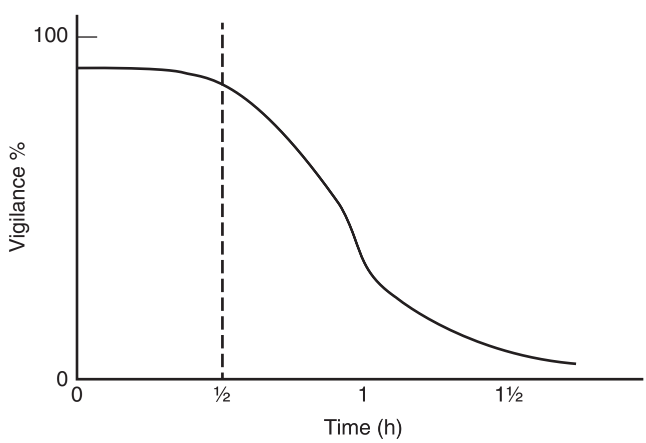


Figure 11.3 Vigilance versus time.

maintenance, testing, and repair. An example is the turning off of both the redundant auxiliary feedwater systems at the Three Mile Island reactor. The point is that if technicians perform a task incorrectly on one piece of equipment, they are likely to do it incorrectly on all like pieces of equipment. This problem may be countered, at least in part, by a variety of techniques. Diversity of equipment is one, for just as the hardware will not be subjected to the same failure modes, the maintenance procedures will also be different. Staggering the times or the personnel doing maintenance on redundant equipment also tends to reduce dependencies, although some smaller degree of dependency may remain through the use of common tools or incorrect training procedures.

Independent checking of procedures also decreases both the probability of failure and the degree of dependency. Even here, however, psychological factors limit effectiveness. When the inspector and the person performing the maintenance have worked with each other for an extended period of time, the inspector may tend to become less careful as he or she grows more confident of the colleague's abilities. Similarly, if two independent checks are to be performed, they are unlikely to be truly independent, for often the very knowledge that a procedure is being checked twice will tend to decrease the care with which it is done.

Reliability is also degraded when operating and maintenance personnel inappropriately modify or make shortcuts in operating and maintenance procedures. Often, operating and maintenance personnel gain an understanding of the system that was not available at the time of design and modify procedures to make them more efficient and safer. The danger is that, without a thorough design review, new loadings and environment degradation may be introduced, and component dependencies may increase inadvertently. For example, in the 1979 crash of the DC-10 in Chicago, it is thought that a modified procedure for removing the engines for inspection and preventive maintenance led to excessive fatigue stresses on the engine support pylon, causing the engine to break off during takeoff.

Although the methodology is not straightforward, data are available on the errors committed in the course of routine tasks. Extensive efforts have been made to develop task analysis and simulation methods (Swain and Guttmann 1980). Failure probabilities are first estimated for rudimentary functions. Then, by combining these factors, we can estimate probabilities that more extensive procedures will engender errors.

Emergency Operations

At the high-stress end of the spectrum shown in Figure 11.1 are the protective tasks that must be performed by operations personnel under emergency conditions to prevent potentially dangerous situations from getting completely out of hand. Here, a well-designed, man–machine interface, clear-cut procedures, and thorough training are critical, for in such situations actions that are not familiar from routine use must be taken quickly, with the knowledge that mistakes may be disastrous. Moreover, since such situations are likely to be caused by subtle combinations of malfunctions, they may be confusing and call for diagnostic and problem-solving ability, not just the skill and rule-based actions exercised for routine tasks.

Under emergency conditions, conflicting information may well confuse operators who then act in ways that further propagate the accident. With proper training and the ability to function under psychological stress, however, they may be able to solve the problem and save the day. For example, the confusion of the operators at the Three Mile Island reactor caused them to turn off the emergency core-cooling system, thus worsening the accident. In contrast, the pilot of a Boeing 767 managed to make use of his earlier experience as an amateur glider pilot and safely land his aircraft after a series of equipment failures and maintenance errors had caused the plane to run out of fuel while in flight over Canada.

There are a number of common responses to emergency situations that must be taken into consideration when designing systems and establishing operating procedures. Perhaps, the most important is the incredulity response. In the rare event of a major accident, it is common for an operator not to believe that an accident is taking place. The operator is more likely to think that there is a problem with the instruments or alarms, causing them to produce spurious signals. At installations that have been subjected to substantial numbers of false alarms, a real one may very well be disbelieved. Systems should be carefully designed to keep spurious alarms to a minimum, and straightforward checks to distinguish accidents from faulty instrument performance should be provided. In some situations it is desirable to mandate that safety actions be taken, even though the operator may feel that faulty instruments are the cause of the problem.

A second common reaction to emergencies is reverting to stereotype. The operator reverts to the stereotypical response of the population of which he or she is a part, even though more recent training has been to the contrary. For example, in the United States, turning a light or other switch "up" means that it is "on." In Europe, however, "down" is "on." Thus, although Americans may be trained to put a particular switch down to turn it on, under the time pressure of an emergency they are likely to revert to the population stereotype and try to put the switch up. The obvious solution to this problem is to take great care in human factors engineering not to violate population stereotypes in the design of instrumentation and control systems. This problem may be aggravated if operators from one culture are transferred to another, or if care is not taken in the use of imported equipment.

Finally, once a mistake is made, such as placing a switch in the wrong position, in a panic an operator is likely to repeat the mistake rather than think through the problem. This reaction, as well as other inappropriate emergency responses, must be considered when deciding the extent to which emergency actions should or can be automated. On the one hand, when there is extreme time pressure, automated protection systems may eliminate the errors discussed. At the same time, such systems do not have the flexibility and problem-solving ability of human operators, and these advantages may be of overwhelming importance, assuming that there is time for the situation to be properly assessed.

In summary, to ensure a high degree of human reliability in emergency situations, control rooms, whether they be aircraft cockpits or chemical plant control installations, must be carefully designed according to good human factors practice. It is also important that the procedures for all anticipated situations are readily understandable, and finally, that operators are drilled at frequent intervals on emergency procedures, preferably with simulators that model the real conditions.

Even though we may characterize human behavior under emergency conditions and suggest actions that will improve human reliability, it is difficult indeed to obtain quantitative data on failure probabilities. As we have indicated, such situations happen only infrequently, and often, they are not well documented. Moreover, it is difficult to obtain a realistic response from simulator experiments when the subjects know that they are in an experiment and not a life-threatening situation.

11.4 Methods of Analysis

Probably, the most important task in eliminating or reducing the probability of accidents is to identify the mechanisms by which they may take place. The ability to make such identifications in turn requires that the analysts have a comprehensive understanding of the system under consideration, both in how it operates and in the limitations of its components. Even the most knowledgeable analysts are in danger of missing critical failure modes, however, unless the analysis is carried out in a very systematic manner. For this reason, a substantial number of formal approaches have been developed for safety analysis. In this section, we introduce three of the most widely used: failure modes and effects analysis, event trees, and fault trees. In later sections, the use of fault trees is developed in more detail.

Failure Modes, Effects, and Criticality Analysis (FMECA)

In Chapter 7, we introduced FMEA, a very valuable qualitative tool in the process of product development. We also alluded to the FMECA which we introduce here as a safety-oriented extension of the FMEA.

To quickly recap, failure mode and effects analysis (FMEA) is a logical, structured analysis of a system, subsystem, piece part, or function. Identified in the analysis are potential failure modes, their causes, and the effects associated with the failure mode's occurrence at the piece part, subsystem, and system levels.

Failure mode, effects, and criticality analysis (FMECA) is an **extension** of the FMEA task, where each failure mode is evaluated for its "**criticality**," i.e. an assessment of the severity of the event at the system level, and the probability of its occurrence – based on DATA and EXPERIENCE.

The FMECA tool was initially utilized starting in the late 1960s where it was used primarily to assess the safety and reliability of system components in the aerospace industry. In the 1980s, FMECA was applied to manufacturing and assembly processes in the automotive industry. And today, FMECAs are being used for the design of products and processes as well as for the design of software and services in virtually all industries.

An FMECA provides a basis for the recognition of failure modes developed from historical "lessons learned" databases of similar equipment and the unacceptable effects that limit the achievement of design requirements. FMECA is performed as early as possible in the design process in order to verify the adequacy of the design, change the design if not adequate, or incorporate appropriate controls. As has been mentioned before, problems discovered during the design phase are much easier and less costly to correct than if they are identified in service.

In addition, FMECA provides:

1) A communication tool between product designers, manufacturing engineers, test engineers, and R&M engineers.
2) A tool for identifying potential single point failure modes of a "critical" nature.
3) A tool for identifying the types of test and testing environments needed to certify whether a design or process is suitable.
4) How changes in design, process, or materials are to be evaluated/certified.

In short, a roadmap of the design.

Criticality

Criticality is a relative measure of the consequences of a failure mode and its frequency of occurrence. Criticality can be based on qualitative judgment or on failure rate data (*quantitative*). Qualitative analysis is used when specific part or item failure rates are not available. Quantitative analysis is used when sufficient failure rate data is available to calculate criticality numbers. In either case, *Criticality Analysis* (CA) is a procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

Qualitative FMECA

1) One very easy CA is to use the FMEA that has already been completed, and for each failure mode:

$$\text{Criticality}_{\text{failure mode } i} = \text{Severity}_{\text{failure mode } i} \times \text{Occurrence}_{\text{failure mode } i} \tag{11.1}$$

This ignores the probability of detection and hence is a conservative estimate of criticality.

2) The next uses a bit more definition from the FMEA (see Chapter 7) and sets up a "criticality matrix." The criticality matrix provides a means of identifying and comparing each failure mode to all other failure modes with respect to severity (notice again that the criticality matrix depends on the completed FMEA with no other data). The matrix can be used as a potential safety summary of the FMEA for a subsystem or system. This information is then passed to the safety group for their use (Figure 11.4).

Quantitative FMECA

A quantitative FMECA uses the following formula (with definitions):

(λ_P)		(α)		(ε)		(t)		
Item Failure Rate	$\times$	Failure Mode Ratio	$\times$	Probability of worst case Failure Effects	$\times$	time	$=$	Criticality
↓		↓		↓		↓		
How often the Parts Fails		The % that fails due to this failure		The % of this failure mode that results in worst case effects		"Mission" time		

(11.2)

The top row of abbreviations is used in Mil-Std-1629A and is hence used by many DOD contractors.

		Number of failure modes by severity				
	Severity	9–10	6–8	4–5	1–3	Total
FMEA occurrence	Catastrophic	High (0)	High (0)	Med (0)	Med (0)	0
	Critical	High (0)	Med (0)	Low (0)	Accept (0)	0
	Marginal	Med (0)	Low (0)	Low (0)	Accept (0)	0
	Minor	Low (0)	Low (0)	Low (0)	Accept (0)	0
	Sum of failure modes by severity	0	0	0	0	0

Figure 11.4 Criticality matrix setup for qualitative FMECA. *Source:* Adapted from FAA-H-8083-2 (2009) and NAVAIR 00-25-403 (2016).

A lot more work in terms of data gathering goes into the quantitative FMECA, but a lot better information is the outcome.

Generally speaking, product lines such as automobiles, aircraft, engines, elevators, air conditioners, and most other systems that have been designed and manufactured by a company over many years have the “Lessons Learned” and design experience and data to put together a quantitative FMECA for a new product, at the beginning stages of design/development and continue to refine it throughout the process.

Now let us go through an example of an FMEA and add the criticality component to amplify what we discussed in the opening paragraphs of this section.

Example 11.1 To illustrate the application of FMECA, we use the failure data from 93 power transformers. This system has three components: winding, bushing, and on-load-tap-changer (OLTC, each with potential failure modes. The failure probabilities of winding, bushing, and OLTC are 68.48%, 18.47%, and 13.04%, respectively.

As background:

A fault in windings can occur due to mechanical damage or in insulation material. Windings are arranged as cylindrical shell around the core, and each strand is wrapped with insulation paper. Based on the research investigation, the major causes of winding failures are due to mechanical damage.

The function of bushings is to isolate the electrical contact between tanks and windings and to connect the windings to the power system outside the transformer. The main failure of bushings in a power transformer is short circuit. The major cause of a short circuit is due to mechanical damage or due to material faults in the insulation.

The tap changer is a voltage-regulating device. It changes the ratio of a transformer by adding or subtracting to and from either the primary or the secondary winding. OLTC generally consists of two switches: the diverter switch and the tap selector. The diverter switch does the entire load making and breaking of currents, while the tap selector preselects the tap to which the diverter switch will transfer the load current.

Source: Data taken from Saraswati et al. (2014).

The FMEA of the power transformer system is shown in Figure 11.5.

First, doing a qualitative FMECA using Eq. (11.1), Figure 11.6.

From this, the design team could look at criticalities = 42, 56, and 35 as design priorities.

Analyzing the same FMEA using the criticality matrix approach in Figure 11.7.

In this case, the addition of the definitions of “High,” “Medium,” “Low,” and “Very Low” has given further importance to working on “short circuit”/”bushing damage” failure mode and “copper sulfide generation”/“fault in isolation material” failure mode.

This criticality matrix is used by safety groups in the same way. An example of how reliability and safety are working together to produce not only a reliable product but a safe one as well producing “customer satisfaction.” !!

Taking this example one step forward, suppose that we have the following power transformer data in Table 11.1.

Using the interval MLE approach from Chapter 5, we produce the following Weibull (Figure 11.8):

Now, you have a customer who is demanding a 15-year warranty. Based on this data and the FMEA, using the probabilities of occurrence from Chapter 5 for FMEA and calculating the failure rate at 15 years:

Item	Function	Potential failure mode	Potential effects of failure	Severity	Potential causes/ mechanisms of failure	Occurrence	Current design controls detection	Detect	R.P.N.	Recommended actions
Winding	Conducts current	Short circuit	*Mechanical damage	6	*Construction fault	3	*Daily visual inspection	8	144	Weekly inspection
				2	*Transformer movement	2	*Vibration monitor	3	12	Weekly inspection
			*Fault in insulation material	4	*Transient overvoltage	6	*Computer voltage recording	3	72	SPC of data on line with warning
				7	*Hotspot	5	*Computer temp recording	3	105	SPC of data on line with warning
				6	*Copper sulfide generation	7	*Sensor detection of copper sulfide buildup	3	126	SPC of data on line with warning
Load-tap-changer (OLTC)	Regulates the voltage level	Cannot change voltage level	*Mechanical damage	8	*Wear	2	*Sensors on voltage at various locations	8	128	SPC on sensor output with warning
Bushing	*Connect windings	Short circuit	*Insulation fault	7	*Dirt	6	*Weekly inspection and sensor placement	5	210	SPC on sensor output with warning
	*Isolate tank and windings	Short circuit	*Bushing damage	8	*Water penetration (leak)	7	*Weekly inspection and sensor placement	3	168	SPC on sensor output with warning
				8	*Careless handling	1	*Weekly inspection	2	16	Weekly inspection

Figure 11.5 FMEA of power transformer system.

Item	Function	Potential failure mode	Potential effects of failure	Severity	Potential causes/ mechanisms of failure	Occurrence	Current design controls detection	Detect	R.P.N.	Recommended actions	Criticality = (severity X occurrence)
Winding	Conducts current	Short circuit	*Mechanical damage	6	*Construction Fault	3	*Daily visual inspection	8	144	Weekly inspection	18
				2	*Transformer movement	2	*Vibration monitor	3	12	Weekly inspection	4
			*Fault in insulation material	4	*Transient\ overvoltage	6	*Computer voltage recording	3	72	SPC of data on line with warning	24
				7	*Hotspot	5	*Computer temp recording	3	105	SPC of data on line with warning	35
				6	*Copper sulfide generation	7	*Sensor detection of copper sulfide buildup	3	126	SPC of data on line with warning	42
Load-tap-changer (OLTC)	Regulates the voltage level	Cannot change voltage level	*Mechanical damage	8	*Wear	2	*Sensors on voltage at various locations	8	128	SPC on sensor output with warning	16
Bushing	*Connect windings	Short circuit	*Insulation fault	7	*Dirt	6	*Weekly inspection and sensor placement	5	210	SPC on sensor output with warning	42
	*Isolate tank and windings	Short circuit	*Bushing damage	8	*Water penetration (leak)	7	*Weekly inspection and sensor placement	3	168	SPC on sensor output with warning	56
				8	*Careless handling	1	*Weekly inspection	2	16	Weekly inspection	8

Figure 11.6 FMECA using Eq. (11.1) approach.

		Number of failure modes by severity				
		9–10	6–8	4–5	1–3	Total
FMEA occurrence	Catastrophic	High (0)	High (2)	Med (0)	Med (0)	2
	Critical	High (0)	Med (2)	Low (1)	Accept (0)	3
	Marginal	Med (0)	Low (1)	Low (0)	Accept (0)	1
	Minor	Low (0)	Low (2)	Low (0)	Accept (1)	3
	Sum of failure modes by severity	0	7	1	1	9

Figure 11.7 FMECA using second qualitative FMECA (criticality matrix) approach. *Source:* Adapted from FAA-H-8083-2 (2009) and NAVAIR 00-25-403 (2016).

Table 11.1 Power transformer failure by year interval data.

Start time (years)	**End time (years)**	**Number of failures**
*	1	5
1	4	13
4	8	18
8	12	6
12	16	19
16	20	8
20	24	4
24	28	5
28	32	10
32	*	5

* Indicates unknown start (or end) time. This dataset was set up for MINITAB.

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} \tag{5.8}$$

So,

$$\lambda(15\ \text{years}) = \frac{1.2}{15.25}\left(\frac{15}{15.25}\right)^{1.2-1} = 0.0784 \text{ failures per year}$$

Converting to failures per 1,000,000 hours:
or

$$\lambda(t) = \frac{0.0784}{(365{*}24)} = 8.95 \times 10^{-6}$$

Using this rate in the FMECA in Figure 11.9, where we multiplied the criticality by time in hours in 15 years = 15∗365∗24.

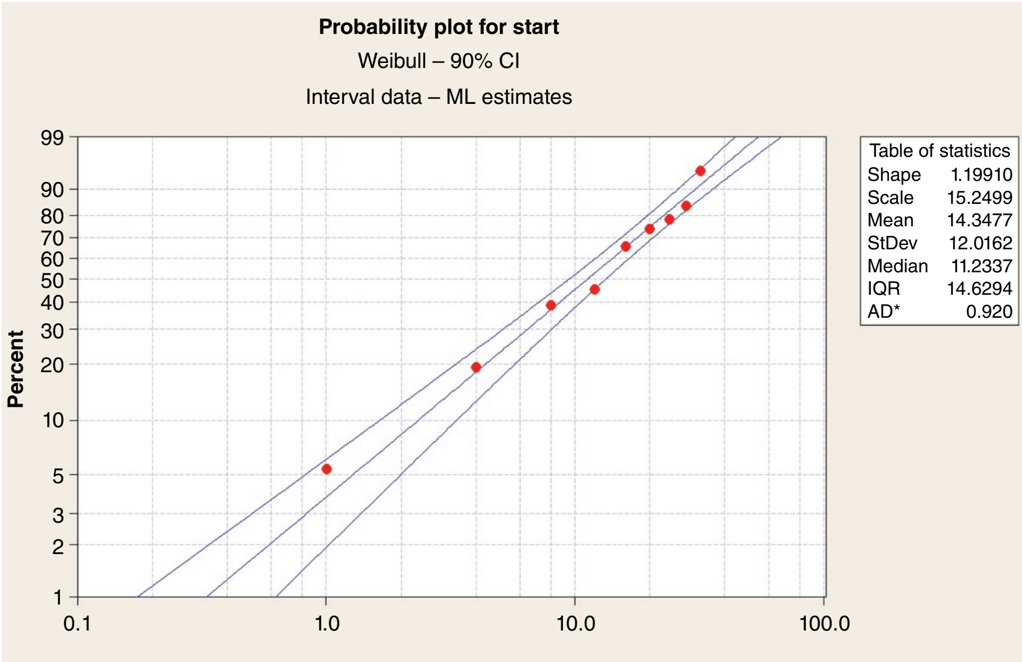


Figure 11.8 Weibull failure distribution of power transformer data.

Here, the short circuit caused by fault in isolation material caused by copper sulfide generation is by far the most safety critical (40,279 criticality). The additional information of the failure distribution and the breakdown of the % failures by group allowed for more insights for the design team.

These approaches to an FMECA will vary from industry to industry, indeed often from company to company within an industry. So, use the information here as a guideline and consult your company's approach not only to FMEA but also FMECA.

If there are no guidelines, consider some of the documents in the Bibliography under "FMEA/FMECA" for a starting point.

Event Trees

In many accident scenarios the initiating event – say, the failure of a component – may have a wide spectrum of results, ranging from inconsequential to catastrophic. The consequences may be determined by how the accident progression is affected by subsequent failure or operation of other components or subsystems, particularly safety or protection devices, and by human errors made in responding to the initiating event. In such situations, an inductive method may be very useful. We begin by asking "what if" the initiating event occurs and then follow each of the possible sequences of events that result from assuming failure or success of the components and humans affected as the accident propagates. After such sequences are defined, we may attempt to attach probabilities to them if such a quantitative estimate is needed.

The event tree is a quantitative technique for such inductive analysis. It begins with a specific initiating event, a particular cause of an accident, and then follows the possible progressions of the accident according to the success or failure of other components or pieces of equipment. Event trees are a particular adaptation of the more general decision-tree formalism that is widely

Item	Function	Potential failure mode	Potential effects of failure	Severity	Potential causes/ mechanisms of failure	Occurrence	Current design controls detection	Detect	R.P.N.	Recommended actions	Responsibility and target completion date
Winding	Conducts current	Short circuit	*Mechanical damage	6	*Construction fault	3	*Daily visual inspection	8	144	Weekly inspection	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.68		Probability 1/15,000			Criticality*15*365*24 53.7	
				2	*TRANSFORMER MOVEMENT	2	*Vibration monitor	3	12	Weekly inspection	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.68		Probability 1/150,000			Criticality*15*365*24 5.4	
			*Fault in insulation material	4	*TRANSIENT OVERVOLTAGE	6	*Computer voltage recording	3	72	SPC of data on line with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.68		Probability 1/80			Criticality*15*365*24 10,069.8	
				7	*Hotspot	5	*Computer temp recording	3	105	SPC of data on line with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.68		Probability 1/400			Criticality*15*365*24 2014.0	
				6	*Copper sulfide generation	7	*Sensor detection of copper sulfide buildup	3	126	SPC of data on line with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.68		Probability 1/20			Criticality*15*365*24 40,279	
Load-tap-changer (OLTC)	Regulates the voltage level	Cannot change voltage level	*Mechanical damage	8	*Wear	2	*Sensors on voltage at various locations	8	128	SPC on sensor output with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.13		Probability 1/150,000			Criticality*15*365*24 1.02	
Bushing	*Connect windings	Short circuit	*Insulation fault	7	*Dirt	6	*Weekly inspection and sensor placement	5	210	SPC on sensor output with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.185		Probability 1/80			Criticality*15*365*24 2720	
	*isolate tank and windings	Short circuit	*Bushing damage	8	* Water penetration (leak)	7	*Weekly inspection and sensor placement	3	168	SPC on sensor output with warning	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.185		Probability 1/20			Criticality*15*365*24 10,878	
				8	*Careless handling	1	*Weekly inspection	2	16	Weekly inspection	
			Failure rate 8.95/1,000,000 h		Failure mode ratio 0.185		Probability 1/1,500,000			Criticality*15*365*24 0.15	

Figure 11.9 Quantitative FMECA of the power transformer.

employed for business and economic analysis. They are quite useful in analyzing the effects of the functioning or failure of safety systems in response to an accident, particularly when events follow with a particular time progression. The following is a very simple application of event-tree analysis.

Suppose that we want to examine the effects of the power failure in a hospital in order to determine the probability of a blackout, along with other likely consequences. For simplicity, we assume that the situations may be analyzed in terms of just three components: (i) the off-site local utility power system that supplies electricity to the hospital; (ii) a diesel generator that supplies emergency power, and (iii) a voltage-monitoring system that monitors the off-site power supply and, in the event of a failure, transmits a signal that starts the diesel generator.

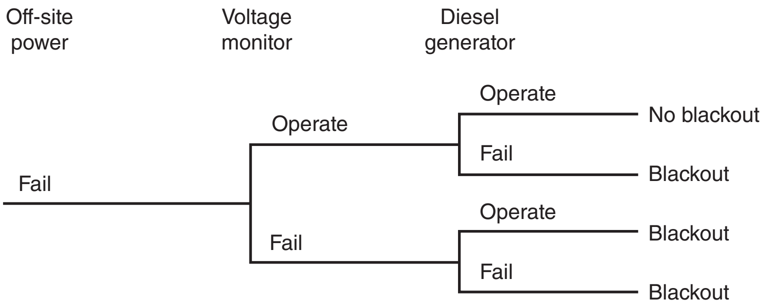


Figure 11.10 Event tree for power failure.

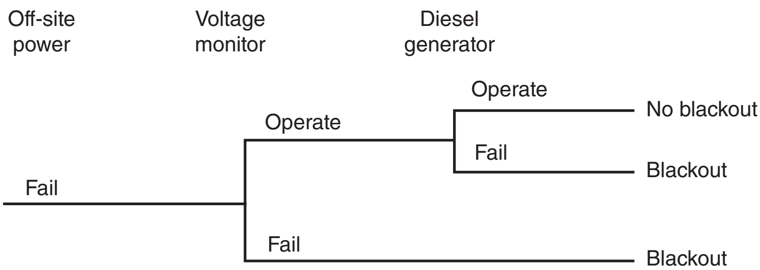


Figure 11.11 Reduced event tree for power failure.

We are concerned with a sequence of three events. The initiating event is the loss of off-site power. The second event is detection of the loss and subsequent functioning of the voltage-monitoring system; and the third event is the start-up and operation of the diesel generator. This sequence is shown in the event tree in Figure 11.10. Note that at each event there is a branch corresponding to whether a system operates or fails. By convention, the upward branches signify successful operation, and the lower branches failure.

Note that for a sequence of N events, there will be 2^N branches of the tree. The number may be reduced, however, by eliminating impossible branches. For example, the generator cannot start unless the voltage monitor functions. Thus, the path is impossible (has a zero probability) and can be pruned from the tree, as in Figure 11.11.

We may follow an event tree from left to right to find the probabilities and consequences of differing sequences of events. The probabilities of the various outcomes are determined by attaching a probability to each event on the tree. In our tree, the probabilities are P_i for the initial event, P_v for the failure of the voltage-monitoring system, and P_g for the failure of the diesel generator. With the assumption that the failures are independent, the probability of a blackout is therefore $P_i\, P_v + P_i(1 - P_v)P_g$.

11.5 Fault Trees

Fault-tree analysis is a deductive methodology for determining the potential causes of accidents, or for system failures more generally, and for estimating the failure probabilities. In its narrowest sense, fault-tree analysis may be looked on as an alternative to the use of reliability block diagrams in determining system reliability in terms of the corresponding components. However, fault-tree analysis differs both in the approach to the problem and in the scope of the analysis.

Fault-tree analysis is centered about determining the causes of an undesired event, referred to as the top event, since fault trees are drawn with it at the top of the tree. We then work downward, dissecting the system in increasing detail to determine the root causes or combinations of causes of the top event. Top events are usually failures of major consequence, engendering serious safety hazards or the potential for significant economic loss.

The analysis yields both qualitative and quantitative information about the system at hand. The construction of the fault tree in itself provides the analyst with a better understanding of the potential sources of failure and thereby a means to rethink the design and operation of a system in order to eliminate many potential hazards. Once completed, the fault tree can be analyzed to determine what combinations of component failures, operational errors, or other faults may cause the top event. Finally, the fault tree may be used to calculate the demand failure probability, unreliability, or unavailability of the system in question. This task of quantitative evaluation is often of primary importance in determining whether a final design is considered to be acceptably safe.

The rudiments of fault-tree analysis may be illustrated with a very simple example. We use the same problem of a hospital power failure treated inductively by event-tree analysis earlier to demonstrate the deductive logic of fault-tree analysis. We begin with blackout as the top event and look for the causes, or combination of causes, that may lead to it. To do this, we construct a fault tree as shown in Figure 11.12. In examining its causes, we see that both the off-site power system *and* the emergency power supply must fail. This is represented by a $\cap$ gate in the fault tree, as shown. Moving down to the second level, we see that the emergency power supply fails if the voltage monitor *or* the diesel generator fails. This is represented by a $\cup$ gate in the fault tree as shown.

We see that the fault tree consists of a structure of OR and gates, with boxes to describe intermediate events. Using the same probabilities as in the event tree, we can determine the probability of a

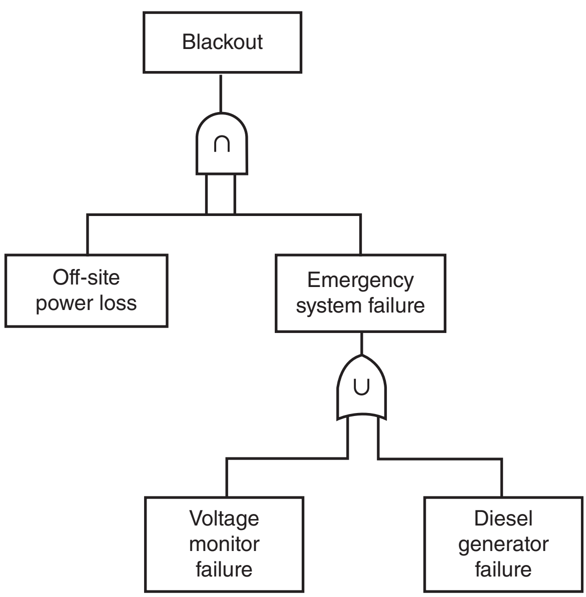


Figure 11.12 Fault tree for blackout.

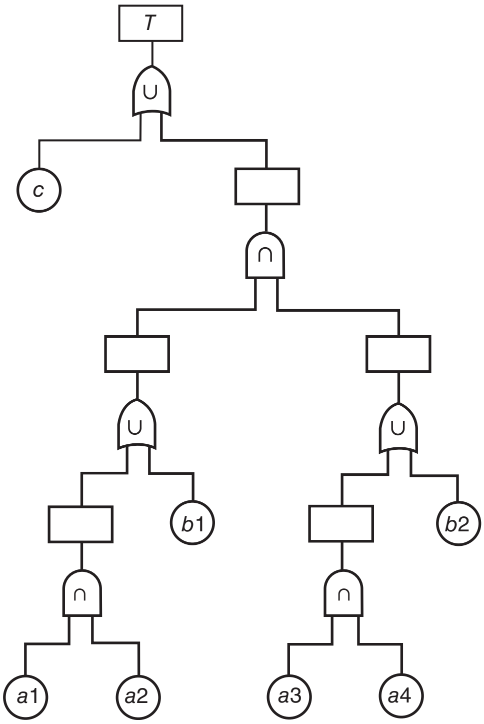


Figure 11.13 Fault tree.

blackout in terms of P_i, P_v, and P_g, the failure probabilities for off-site power, voltage monitor, and diesel generator.

The most straightforward fault trees to draw are those, such as in the preceding example, in which all the significant primary failures are component failures. If a reliability block diagram can be drawn, a fault tree can also be drawn. This can be seen in an additional example.

Consider the system shown in Figure 3.17. We may look at the system as consisting of an upper subsystem ($a1$, $a2$, and $b1$) and a lower subsystem ($a3$, $a4$, and $b2$), in addition to component c. For a system to fail, either component c must fail or the upper and lower subsystems must fail. Proceeding downward, for the upper subsystem to fail, either component $b1$ must fail or both $a1$ and $a2$ must fail. Treating the lower subsystem analogously, we obtain the tree shown in Figure 11.13.

Example 11.2 Construct a reliability block diagram corresponding to the fault tree in Figure 11.12.

Solution:
The reliability block diagram having the same logic and failure probability as the fault tree of Figure 11.12 is depicted in Figure 11.14.

Fault-Tree Construction

Of the methods discussed in the preceding section, fault-tree analysis has been the most thoroughly developed and is finding increased use for system safety analysis in a wide variety of applications. It is particularly well suited to situations in which tracing a failure to its root causes requires

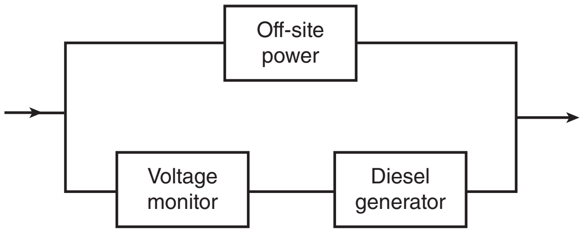


Figure 11.14 Reliability block diagram for electrical power.

dissecting the system into subsystems, components, and parts to get at the level where failure data are available. For example, in the afore-treated hospital blackout, we may not have the test data that is required to determine P_v for the voltage monitor or P_g for the diesel generator. We must then delve more deeply and examine the components of these devices; we may need to construct the probability that the voltage monitor will fail from the failure rates of its components.

It may be argued that such dissection can also be done by subdividing the blocks appearing in reliability block diagrams. Although this is true, there are some important differences. Reliability block diagrams are success oriented; that is, all failures are lumped together to obtain the probability that a system will fail. In most reliability studies, we are interested only in knowing the reliability (i.e. the probability that the system does not fail). Conversely, in fault-tree analysis we are often interested only in a particular undesirable event (i.e. a failure that leads to a safety hazard) and in calculating the probability that it will happen. Hence, failures that do not cause the safety hazard defined by the top event are excluded from consideration.

The difference between reliability analysis and safety analysis may be illustrated by the example of a hot-water heater. In reliability analysis – carried out with a reliability block diagram – failure of any kind will cause failure of the system to supply hot water. Most of these failures have no safety implications: The heater unit fails to turn on, the tank develops a leak, and so on. In safety analysis – using a fault tree – we would be interested in a particular safety hazard such as the explosion of the tank. The other failures listed would not be included in the fault-tree construction.

Because of the increasing importance of fault-tree analysis, the remainder of this chapter is devoted to it. In this section, we discuss the construction of fault trees by first giving the standardized nomenclature. Then, following a brief discussion of fault classifications, we supply several illustrative examples. In Sections 11.6 and 11.7, fault trees are evaluated. In qualitative evaluation, the fault tree is reduced to a logical expression, giving the top event in terms of combinations of primary-failure events. In quantitative evaluation, the probability of the top event is expressed in terms of the probabilities of the primary-failure events.

Nomenclature

As we have seen, the fault tree is made up of events, expressed as boxes, and gates. Two types of gates appear, the OR and the AND gate. The OR gate as indicated in Figure 11.15a is used to show that the output event occurs only if one or more of the input events occur. There may be any number of input events of an OR gate. The AND gate as indicated in Figure 11.15b is used to show that the output fault occurs only if all the input faults occur. There may be any number of input faults to an AND gate.

Generally, OR and gates are distinguished by their shape. In free-hand drawings, however, it may be desirable to put the $\cup$ and $\cap$ A symbols on the gates. Or the so-called engineering notation, in

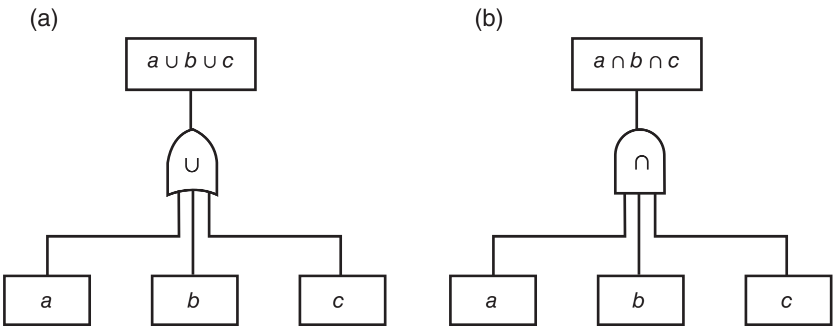


Figure 11.15 Fault-tree gates: (a) OR and (b) AND.

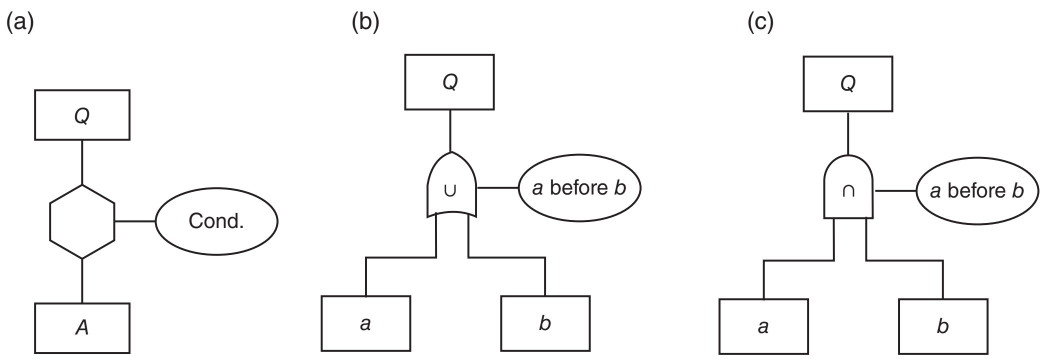


Figure 11.16 Fault-tree conditional gates.

which OR is represented by a "+" and by "·," may be used. Obviously, if these notations are included, the care with which the shape of the gate is drawn becomes of secondary importance.

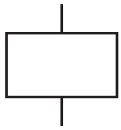
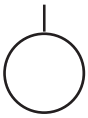
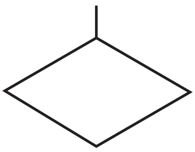
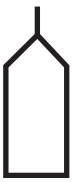
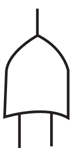
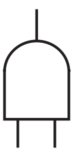
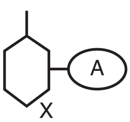
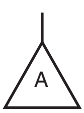
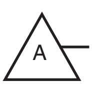
In addition to the AND OR gates, the INHIBIT gate shown in Figure 11.16a is also widely used. It is a special case of the AND gate. The output is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The condition that must exist is indicated conventionally by an ellipse, which is located to the right of the gate. In other words, the output happens only if the input occurs under the conditions specified within the ellipse. The ellipse may also be used to indicate conditions on OR AND gates. This is shown in Figure 11.16b and c.

The rectangular boxes in the foregoing figures indicate top or intermediate events; they appear as outputs of gates. Shape also distinguishes different types of primary or input events appearing at the bottom of the fault tree. The primary events of a fault tree are events that, for one of a number of reasons, are not developed further. They are events for which probabilities must be provided if the fault tree is to be evaluated quantitatively (i.e. if the probability of the top event is to be calculated).

In general, four different types of primary events are distinguished. These make up part of the list of symbols in Table 11.2. The circle describes a basic event. This is a basic initiating fault event that requires no further development. The circle indicates that the appropriate resolution of the fault tree has been reached.

The undeveloped event is indicated by a diamond. It refers to a specific fault event, although it is not further developed, either because the event is of insufficient consequence or because information relevant to the event is unavailable. In contrast, the external event, signified by a house-shaped

Table 11.2 Fault-tree symbols commonly used.

Symbol	**Name**	**Description**
	Rectangle	Fault event; it is usually the result of the logical combination of other events
	Circle	Independent primary fault event
	Diamond	Fault event not fully developed, for its causes are not known; it is only an assumed primary fault event
	House	Normally occurring basic event; it is not a fault event
	OR gate	The union operation of events, i.e. the output event occurs if one or more of the inputs occur
	AND gate	The intersection operation of events, i.e. the output event occurs if and only if all the inputs occur
	INHIBIT gate	Output exists when *X* exists, and condition *A* is present; this gate functions somewhat like an AND gate and is used for a secondary fault event *X*
 	Triangle-in Triangle-out	Triangle symbols provide a tool to avoid repeating sections of a fault tree or to transfer the tree construction from one sheet to the next. The triangle-in appears at the bottom of a tree and represents the branch of the tree (in this case *A*) shown at another location in the Fault Tree. The triangle-out appears at the top of a tree and denotes that the tree *A* is a subtree to one shown someplace else

Source: Adapted from Roberts et al. (1981).

figure, indicates an event that is normally expected to occur. Thus, house symbol displays are not of themselves faults.

The last symbols in Table 11.2 are the triangles indicating transfers into and out of the fault tree. These are used when more than one page is required to draw a fault tree. A transfer-in triangle indicates that the input to a gate is developed on another page. A transfer-out triangle at the top of a tree indicates that it is the input to a gate appearing on another page.

In fault-tree construction, a distinction is made between a fault and a failure. The word *failure* is reserved for basic events such as a burned-out bearing in a pump or a short circuit in an amplifier. The word *fault* is more all-encompassing. Thus, if a valve closes when it should not, this may be considered a valve fault. However, if the valve fault is due to a spurious signal from the shorted amplifier, it is not a valve failure. Thus, all failures are faults, but not all faults are failures.

Fault Classification

The dissection of a system to determine what combinations of primary failures may lead to the top event is central to the construction of a fault tree. This dissection is likely to proceed most smoothly when the system can be divided into subsystems, components, or parts in order to associate the faults with discrete pieces of the system. Even then, a great deal of attention must be given to the component interactions, particularly common-mode failures. Beyond decomposing the system into components, however, we must also examine which components are more likely to fail and study with care the various modes by which component failure may occur.

In the material already covered, we have examined several ways of classifying failures that are very useful for fault-tree construction. Distinguishing between hardware faults and human error is essential, as is the classification of hardware failures into early, random, and aging, each with its own characteristics and causes. In what follows, we discuss briefly two additional classifications. The division of failures into primary, secondary, and command faults is particularly useful in determining the logical structure of a fault tree. The classification of components as passive or active is important in determining which ones are likely to make larger contributions to system failure.

Primary, Secondary, and Command Faults

Failures may be usefully classified as primary, secondary, and command faults (Roberts et al. 1981). A primary fault by definition occurs in an environment and under a loading for which the component is qualified. Thus, a pressure vessel's bursting at less than the design pressure is classified as a primary fault. Primary faults are most often caused by defective design, manufacture, or construction and are therefore most closely correlated to wear-in failures. Primary faults may also be caused by excessive or unanticipated wear, or they may occur when the system is not properly maintained and parts are not replaced on time.

Secondary faults occur in an environment or under loading for which the component is not qualified. For example, if a pressure vessel fails through excessive pressure for which it was not designed, it has a secondary fault. As indicated by the name, the basic failure is not of the vessel but in the excessive loading or adverse environment. Such failures often occur randomly and are characterized by constant failure rates.

Although a component fails when it has primary and secondary faults, it operates correctly when it has a command fault, but at the wrong time or place. Thus, our pressure vessel might lose pressure through the unwanted opening of a relief valve, even though there is no excessive pressure. If the valve opens through an erroneous signal, it has a command fault. For command failures, we must look beyond the component failure to find the source of the erroneous command.

Passive and Active Faults

Components may be designated as either passive or active. Passive components include things such as pipes, cables, bearings, welds, and bolts. They function in a more or less static manner, often acting as transmitters of energy, such as a buss bar or cable, or of fluids such as piping. Transmitters of mechanical loads, such as structural members, beams, and columns, and connectors, such as welds, bolts, and other fasteners, are also passive components. A passive component may usually be thought of as a mechanism for transmitting the output of one active component to the input of another. In the broadest sense, the quantity transmitted may be an electric signal, a fluid, mechanical loading, or any number of other quantities.

Active components contribute to the system function in a dynamic manner, altering in some way the system's behavior. For example, pumps and valves modify fluid flow; relays, switches, amplifiers, rectifiers, and computer chips modify electric signals; and motors, clutches, and other machinery modify the transmission of mechanical loading.

Our primary reason for distinguishing between active and passive components is that failure rates are normally much higher for active components than for passive components, often by two or three orders of magnitude. The terms *active* and *passive* refer to the primary function of the component. Indeed, an active component may have many passive parts that are prone to failure. For example, a pump and its function are active, but the pump housing is considered passive, even though a housing rupture is one mode by which the pump may fail. In fact, one of the reasons that active components have higher failure rates than passive ones is that they tend to be made up of many nonredundant parts, both active and passive.

Fault Tree Examples

We present here four examples of rather simple systems and ones that are, moreover, readily understandable without specialized knowledge. This is consistent with the philosophy that one should not attempt to construct a fault tree until the design and function of the system is thoroughly understood. The first example is a demand failure, the failure of a motor to start, and the second is the failure of a continuously operating system. The third involves both start-up and operation; in the fourth, the top event is a catastrophic failure, and its causes involve faulty procedures and operator actions as well as equipment failures.

Examples 11.3 Draw a fault tree for the motor circuit shown in Figure 11.16. The top event for the fault-tree analysis is simply failure of the motor to operate (Figure 11.17).

Solution:
The fault tree is shown in Figure 11.18. Note that failures are distinguished as primary and secondary. For primary failures, we would expect data to be available to determine the failure probabilities.

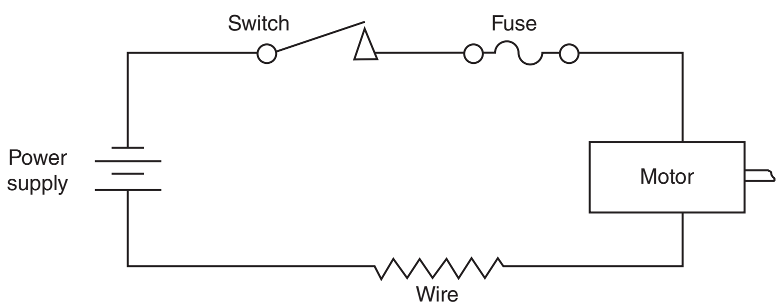


Figure 11.17 Electric motor circuit. *Source:* Fussel (1976).

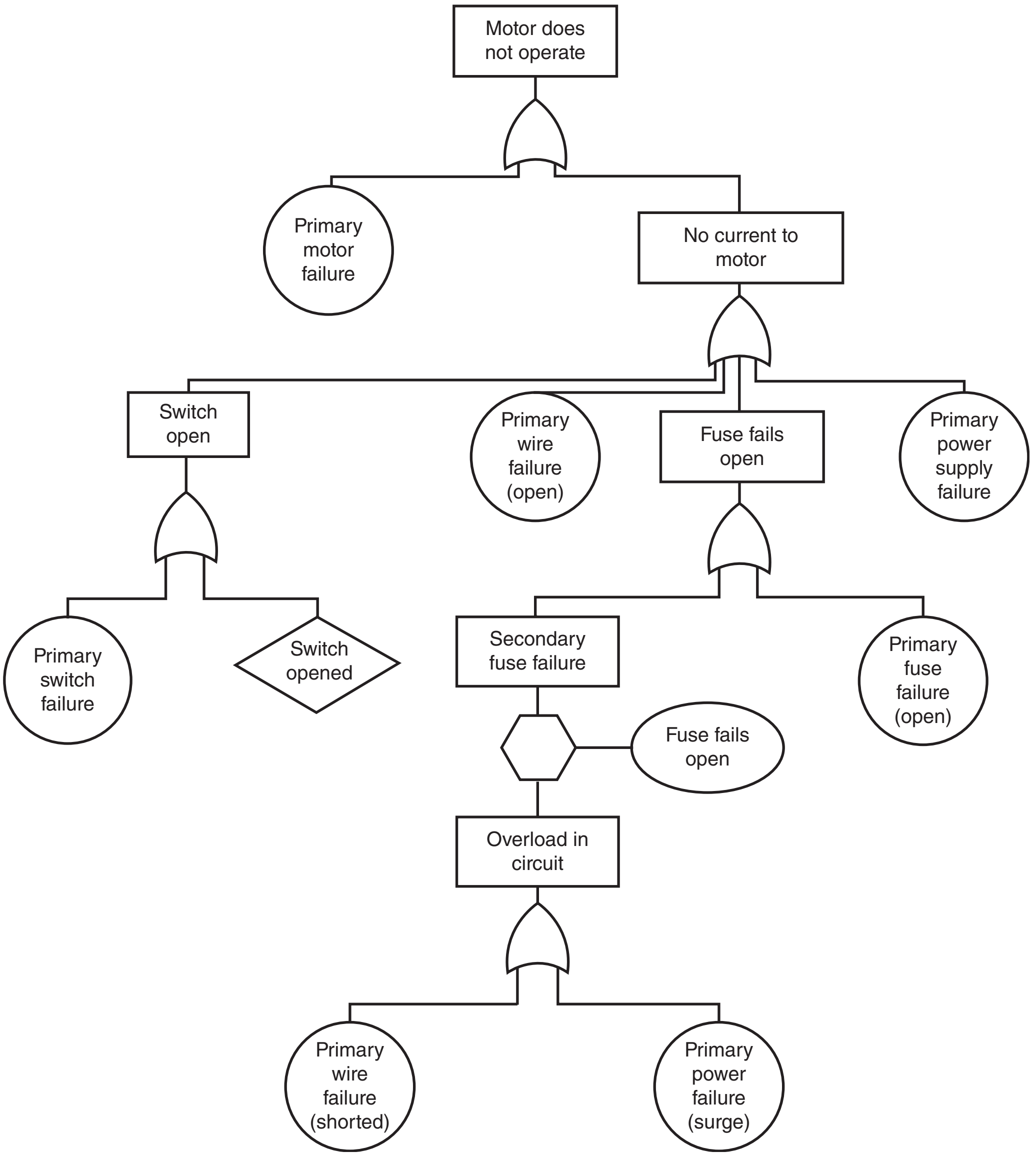


Figure 11.18 Fault tree for electric motor circuit. *Source:* Fussel (1976), reprinted by permission.

If not, further dissection of the component into its parts might be necessary. The secondary faults are either command faults, such as no current to the motor, or excessive loading, such as an overload in the circuits. For these, we must delve deeper to locate the causes of the faults.

Source: Adapted from Fussel (1976).

Examples 11.4 Draw a fault tree for the coolant supply system pictured in Figure 11.19. Here, the top event is loss of minimum flow to a heat exchanger.

Solution:
The fault tree is shown in Figure 11.20. Not all of the faults at the bottom of the tree are primary failures. Thus, it may be desirable to develop some of the faults, such as loss of the pump inlet supply, further. Conversely, the faults may be considered too insignificant to be traced further, or data may be available even though they are not primary failures.

Source: Adapted from Burgess (1970).

Example 11.5 Consider the sump pump system shown in Figure 11.21. Redundance is provided by a battery-driven backup system that is activated when the utility power supply fails. Draw a fault tree for the flooding of a basement protected by this system.

Solution:
The fault tree is shown in Figure 11.22. The tree accounts for the fact that flooding can occur if the rate of inflow from the storm exceeds the pump capacity. Moreover, flooding can occur from storms within the system's capacity if there are malfunctions of both pumps and the inflow is large enough to fill the sump. Primary pump failures may be caused either by the failure of the pump itself or by loss of ac power. Similarly, the second pump may malfunction or it may be lost through failure of the battery. The battery fails only if all three events at the bottom of the tree take place.

Source: Adapted from Ang and Tang (1984).

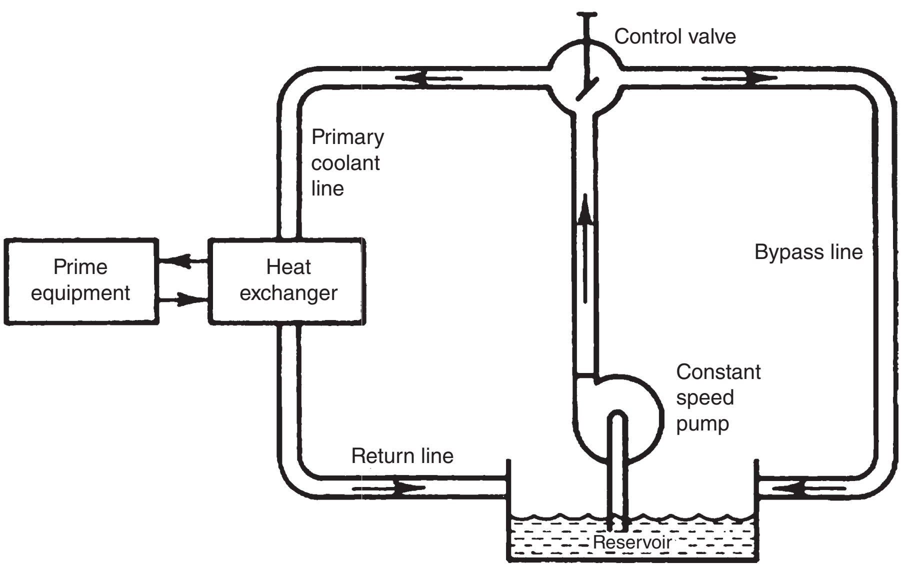


Figure 11.19 Coolant supply system. *Source:* Reprinted from *Machine Design,* © 1984, by Penton/IPC, Cleveland, OH.

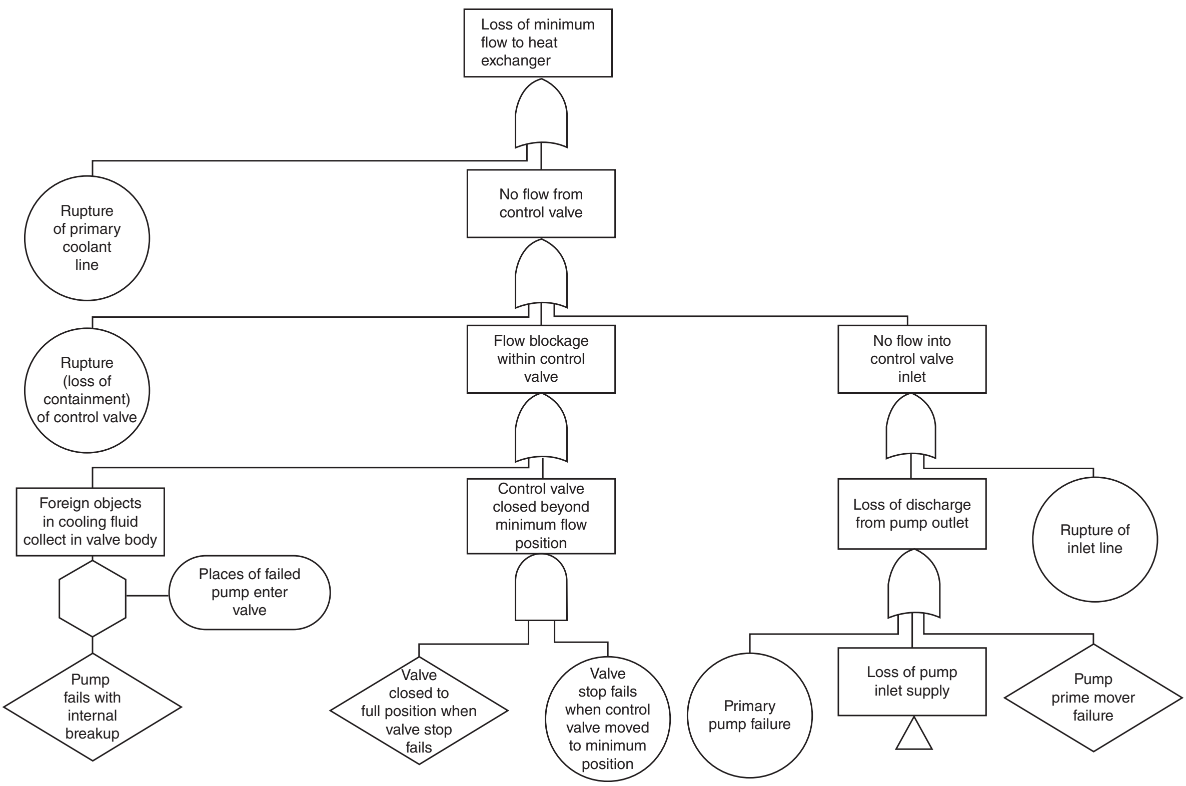


Figure 11.20 Fault tree for coolant supply system. *Source:* Reprinted from *Machine Design*, © 1984, by Penton/IPC, Cleveland, OH.

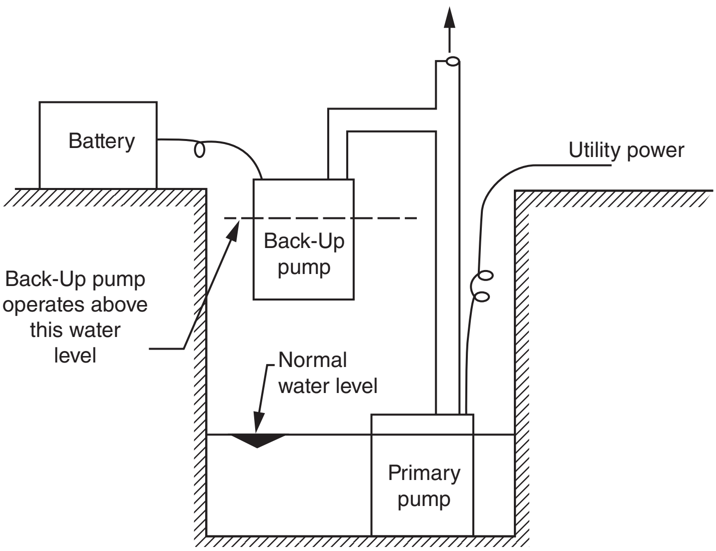


Figure 11.21 Sump pump system. *Source:* Ang and Tang (1984). Copyright © 1984, by John Wiley & Sons, New York. Reprinted by permission.

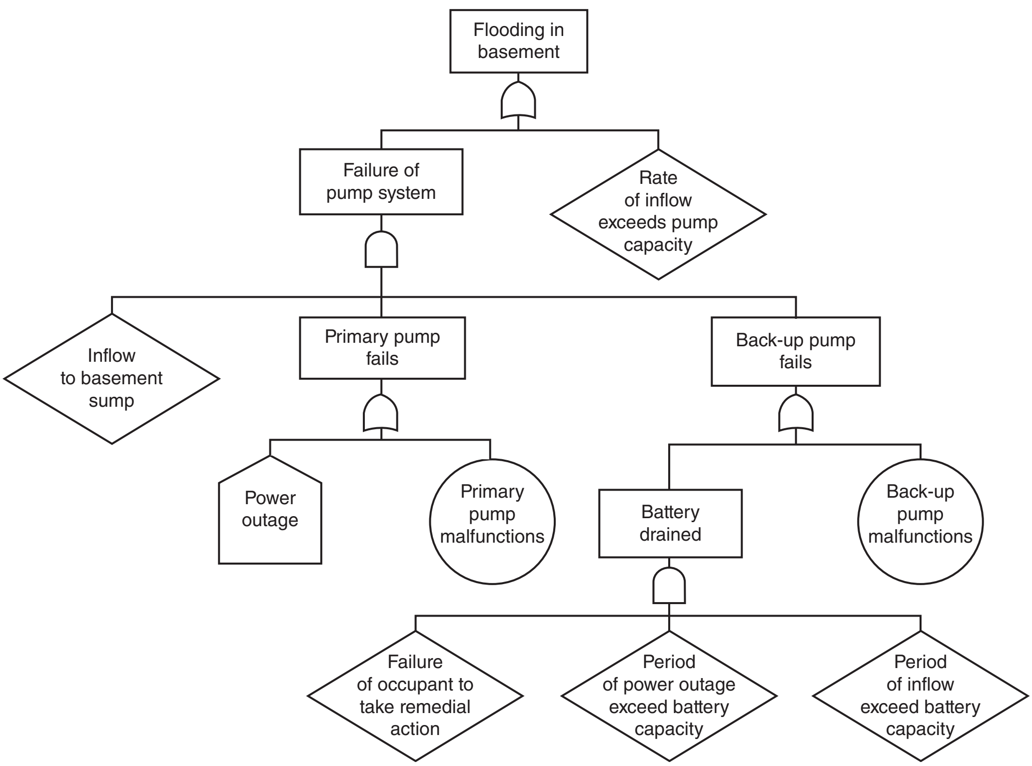


Figure 11.22 Fault tree for basement flooding. *Source:* Ang and Tang (1984). Copyright © 1984, by John Wiley & Sons, New York. Reprinted by permission.

Example 11.6 The final example that we consider is the hot gas manifold and heat exchanger on the SSME shown with other modules/subsystems of the SSME in Figure 11.23. The top event in both subsystems is "engine fire." This situation has the added complication that operator errors (mishandling, installation errors, and welding errors) as well as equipment failures may lead to the top event. Before a fault tree can be drawn, the procedure by which the system is operated must be specified. The SSME is started 6.6 seconds before the solid rocket boosters (SRBs) are ignited; this assures that all three SSMEs are working before the SRBs are ignited (being solid rockets they cannot be turned off after being ignited – think "controlled burn fire cracker."). The flight is off! Now the possible top event that must be studied is "engine fire."

Solution:
In thinking through a fault tree for both of these subsystems you can refer to the FMEA (if one is completed – see Table 7.2), or, as is often the case early in a design, the safety and reliability group representatives form a team to produce a fault tree. See Figures 11.24a and 11.24b for the fault trees the team produced. Notice in the hot gas manifold that the second tier is "duct rupture" and "joint leaks." Under "duct rupture," the engineering team had experience with "cracks" being the cause of "duct rupture" and breaking down "cracks" further into five possible causes (again based on engineering experience). In the case of "joint leaks," there were two possible causes: "loose bolts" and "seal damage. Notice that "installation error" could have caused either of these, whereas "contamination" could have caused "seal damage" by itself. After some experience is obtained through testing, the actual data can be used to attach a probability of occurrence to the bottom events.

Source: Adapted from Henley and Kumamoto (1981a).

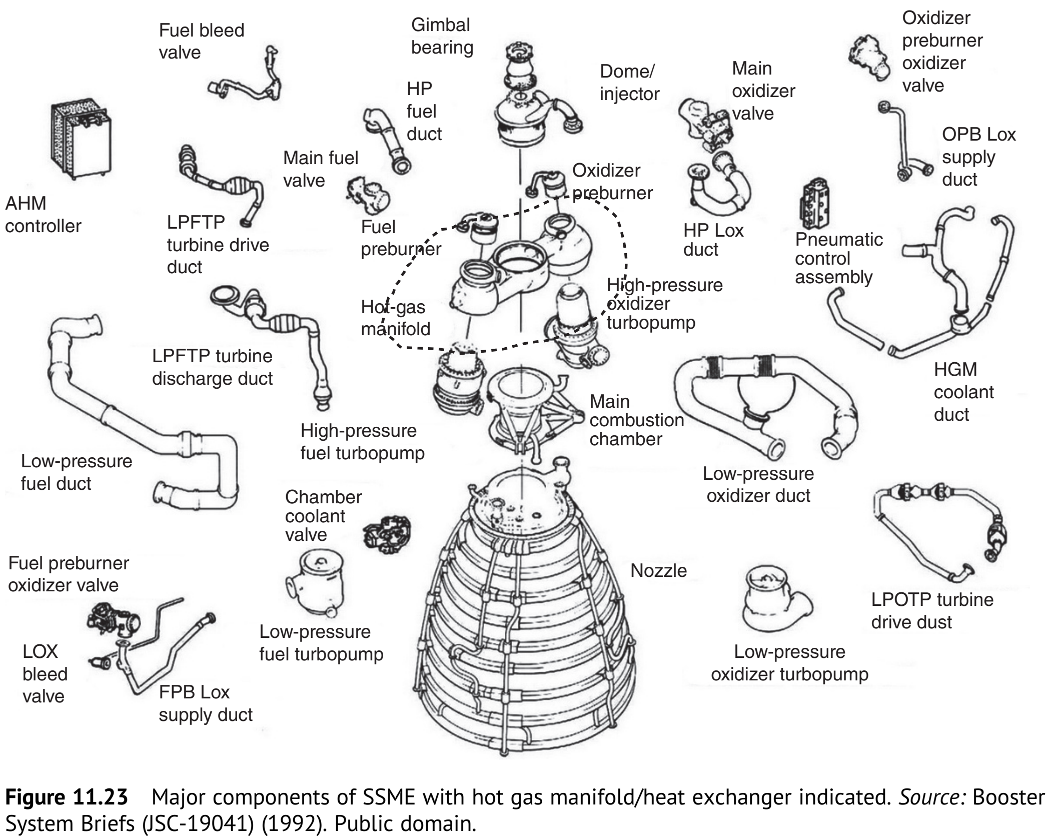


Figure 11.23 Major components of SSME with hot gas manifold/heat exchanger indicated. *Source:* Booster System Briefs (JSC-19041) (1992). Public domain.

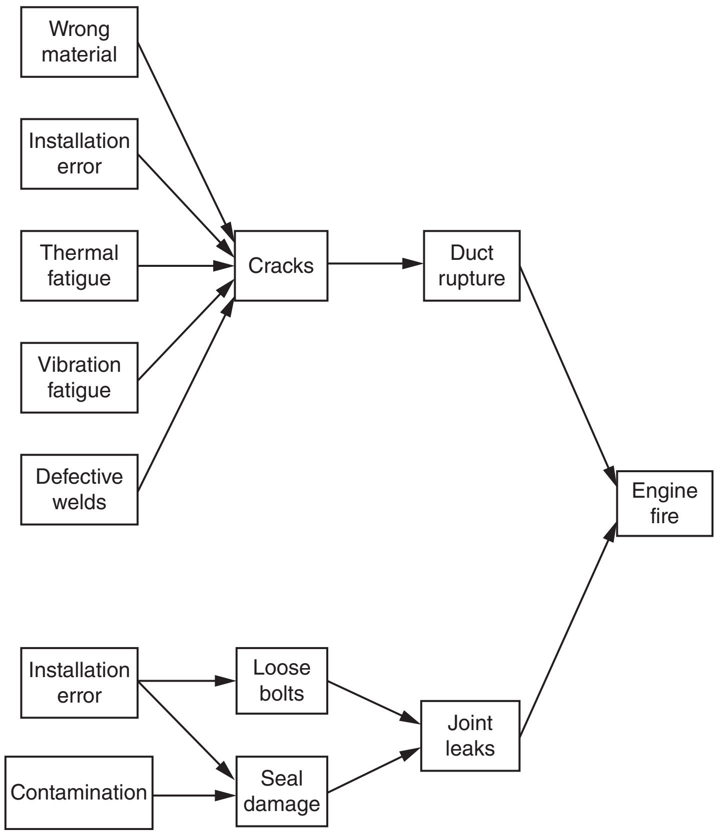


Figure 11.24a Hot gas manifold fault tree. *Source:* Booster System Briefs (JSC-19041) (1992). Public domain.

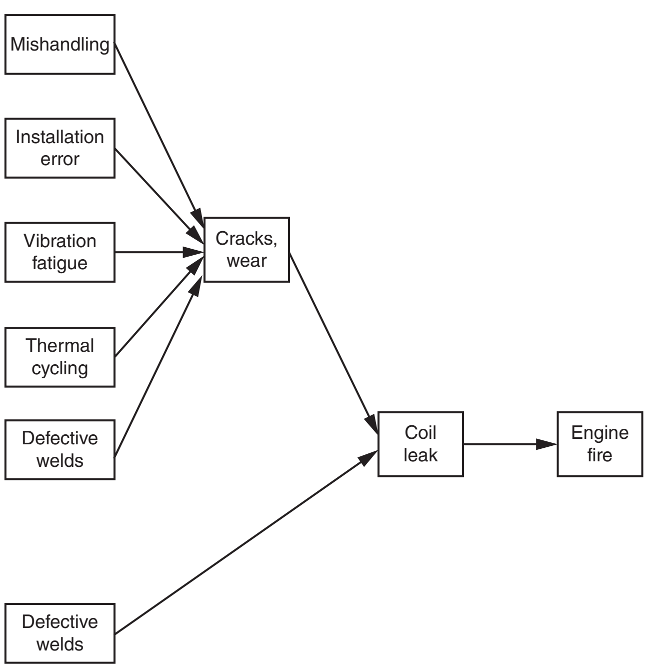


Figure 11.24b Heat exchanger fault tree. *Source:* Booster System Briefs (JSC-19041) (1992). Public domain.

Looking at the heat exchanger fault tree you find immediately that "coil leak" is the cause and notice that "defective welds" is a possible cause of both the "coil leak" and the "cracks, wear" side of the "coil leak." It is obvious from looking at both fault trees that human error was given utmost attention in the fabrication of these two subsystems.

The foregoing examples give some idea of the problems inherent in drawing fault trees. The reader should consult more advanced literature for fault-tree constructions for more complex configurations, keeping in mind that the construction of a valid fault tree for any real system (as opposed to textbook examples) is necessarily a learning experience for the analyst. As the tree is drawn, more and more knowledge must be gained about the details of the system's components, its failure modes, the operating and maintenance procedures, and the environment in which the system is to be located.

Direct Evaluation of Fault Trees

The evaluation of a fault tree proceeds in two steps. First, a logical expression is constructed for the top event in terms of combinations (i.e. unions and intersections) of the basic events. This is referred to as qualitative analysis. Second, this expression is used to give the probability of the top event in terms of the probabilities of the primary events. This is referred to as quantitative analysis. Thus, knowing the probabilities of the primary events, we can calculate the probability of the top event. In these steps the rules of Boolean algebra contained in Table 11.3 are very useful. They allow us to simplify the logical expression for the fault tree and thus also to streamline the formula, giving the probability of the top event in terms of the primary-failure probabilities.

In this section, we first illustrate the two most straightforward methods for obtaining a logical expression for the top event, top-down, and bottom-up evaluation. We then demonstrate how the resulting expression can be reduced in a way that greatly simplifies the relation between the probabilities of top and basic events. Finally, we discuss briefly the most common forms that the primary-failure probabilities take and demonstrate the quantitative evaluation of a fault tree.

The so-named direct methods discussed in this section become unwieldy for very large fault trees with many components. For large trees, the evaluation procedure must usually be cast in the form of a computer algorithm. These algorithms make extensive use of an alternative evaluation procedure in which the problem is recast in the form of so-called minimum cut sets, both because the technique is well suited to computer use and because additional insights are gained concerning the failure modes of the system. We define cut sets and discuss their use in the following section.

Qualitative Evaluation

Suppose that we are to evaluate the fault tree shown in Figure 11.25. In this tree we have signified the primary failures by uppercase letters A through C. Note that the same primary failure may occur

Table 11.3 Boolean logic.

A	B	$A \cap B$	$A \cup B$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	1	1

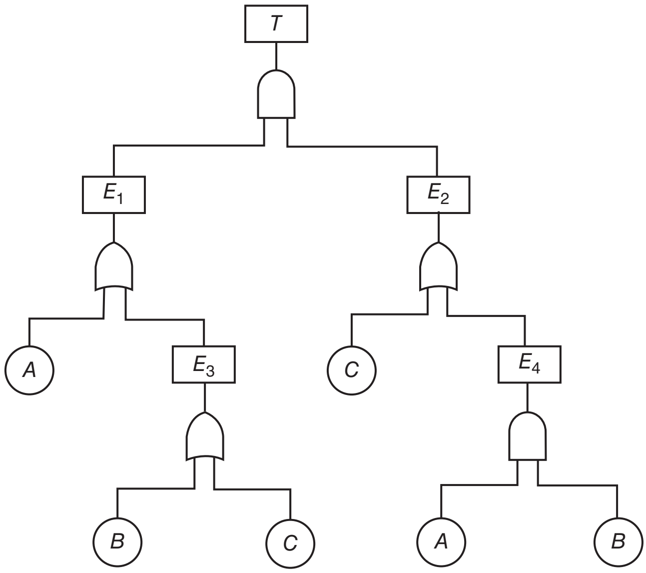


Figure 11.25 Example of a fault tree.

in more than one branch of the tree. This is typical of systems with m/N redundancy of the type discussed in Chapter 3. The intermediate events are indicated by E_i, and the top event by T.

Top Down

To evaluate the tree from the top down, we begin at the top event and work our way downward through the levels of the tree, replacing the gates with the corresponding OR AND symbol. Thus, we have

$$T = E_1 \cap E_2 \tag{11.3}$$

at the highest level of the tree, and

$$E_1 = A \cup E_3; \quad E_2 = C \cup E_4 \tag{11.4}$$

at the intermediate level. Substituting Eq. (11.4) into Eq. (11.3), we then obtain

$$T = (A \cup E_3) \cap (C \cup E_4) \tag{11.5}$$

Proceeding downward to the lowest level, we have

$$E_3 = B \cup C; \quad E_4 = A \cap B \tag{11.6}$$

Substituting these expressions into Eq. (11.5), we obtain as our final result

$$T = [A \cup s(B \cup C)] \cap [C \cup (A \cap B)] \tag{11.7}$$

Bottom Up

Conversely, to evaluate this same tree from the bottom up, we first write the expressions for the gates at the bottom of the fault tree as

$$E_3 = B \cup C; \quad E_4 = A \cap B \tag{11.8}$$

Then, proceeding upward to the intermediate level, we have

$$E_1 = A \cup E_3; \quad E_2 = C \cup E_4 \tag{11.9}$$

Hence, we may substitute Eq. (11.8) into Eq. (11.9) to obtain

$$E_1 = A \cup (B \cup C) \tag{11.10}$$

and

$$E_2 = C \cup (A \cap sB) \tag{11.11}$$

We now move to the highest level of the fault tree and express the AND gate appearing there as

$$T = E_1 \cap E_2 \tag{11.12}$$

Then, substituting Eqs. (11.10) and (11.11) into Eq. (11.12), we obtain the final form:

$$T = [A \cup (B \cup C)] \cap [C \cup (A \cap B)] \tag{11.13}$$

The two results, Eqs. (11.7) and (11.13), which we have obtained with the two evaluation procedures, are not surprisingly the same.

Logical Reduction

For most fault trees, particularly those with one or more primary failures occurring in more than one branch of the tree, the rules of Boolean algebra contained in Table 2.4 may be used to simplify the logical expression for T, the top event. In our example, Eq. (11.13) can be simplified by first applying the associative and then the commutative law to write $A \cup (B \cup C) = (A \cup B) \cup C = C \cup (A \cup B)$. Then, we have

$$T = [C \cup (A \cup B)] \cap [C \cup (A \cap B)] \tag{11.14}$$

We then apply the distributive law with $X \equiv C$, $Y \equiv A \cup$ B, and Z $\equiv A \cap B$ to obtain

$$T = C \cup [(A \cup B) \cap (A \cap B)] \tag{11.15}$$

From the associative law, we can eliminate the parenthesis on the right. Then, since $A \cap B = B \cap A$, we have

$$T = C \cup [(A \cup B) \cap B \cap A] \tag{11.16}$$

Now, from the absorption law $(A \cup B) \cap B = B$. Hence,

$$T = C \cup (B \cap A). \tag{11.17}$$

This expression tells us that for the fault tree under consideration the failure of the top system is caused by the failure of C or by the failure of both A and B. We then refer to $M_1 = C$ and $M_2 = A \cap B$ as the two failure modes leading to the top event. The reduced fault tree can be drawn to represent the system as shown in Figure 11.26.

Quantitative Evaluation

Having obtained, in its simplest form, the logical expression for the top event in terms of the primary failures, we are prepared to evaluate the probability that the top event will occur. The evaluation may be divided into two tasks. First, we must use the logical expression and the rules

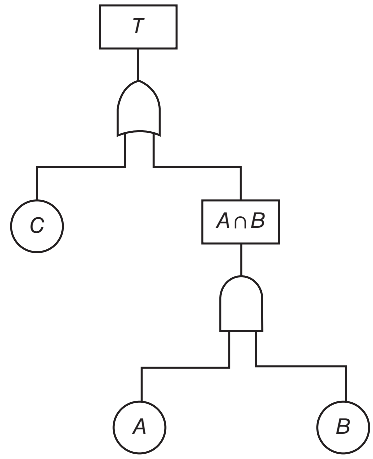


Figure 11.26 Fault-tree equivalent to Figure 11.25.

developed in Chapter 2 for combining probabilities to express the probability of the top event in terms of the probabilities of the primary failures. Second, we must evaluate the primary-failure probabilities in terms of the data available for component unavailabilities, component unavailability, and demand-failure probabilities.

Probability Relationships

To illustrate the quantitative evaluation, we again use the fault tree that reduces to Eq. (11.17). Since the top event is the union of C with $B \cap A$, we use Eq. (2.6) to obtain

$$P\{T\} = P\{C\} + P\{B \cap A\} - P\{A \cap B \cap C\} \tag{11.18}$$

thus expressing the top events in terms of the intersections of the basic events. If the basic events are known to be independent, the intersections may be replaced by the products of basic-event probabilities. Thus, in our example,

$$P\{T\} = P\{C\} + P\{A\}P\{B\} - P\{A\}P\{B\}P\{C\} \tag{11.19}$$

If there are known dependencies between events, however, we must determine expression for $P\{A \cap B\}$, $P\{A \cap B \cap C\}$, or both through more sophisticated treatments such as the Markov models discussed in Chapter 10. Alternatively, we may be able to apply the ξ-factor treatment of Chapter 3 for common-mode failures (see Eq. (3.117) and (3.118) for definitions).

Even where independent failures can be assumed, a problem arises when larger trees with many different component failures are considered. Instead of three terms as in Eq. (11.19), there may be hundreds of terms of vastly different magnitudes. A systematic way is needed for making reasonable approximations without evaluating all the terms. Since the failure probabilities are rarely known to more than two or three places of accuracy, often only a few of the terms are of significance. For example, suppose that in Eq. (11.19) the probabilities of A, B, and C are ~ 10^{-2}, 10^{-4}, and ~ 10^{-6}, respectively. Then, the first two terms in Eq. (11.19) are each of the order of 10^{-6}; in comparison, the last term is of the order of 10^{-12} and may therefore be neglected.

One approach that is used in rough calculations for larger trees is to approximate the basic equation for $P\{X \cup Y\}$ by assuming that both events are improbable. Then, instead of using Eq. (2.6), we may approximate

$$P\{X \cup Y\} \approx P\{X\} + P\{Y\} \tag{11.20}$$

which leads to a conservative (i.e. pessimistic) approximation for the system failure. For our simple example, we have, instead of Eq. (11.19), the approximation

$$P\{T\} \approx P\{C\} + P\{A\}P\{B\} \tag{11.21}$$

The combination of this form of the rare-event approximation and the assumption of independence,

$$P\{X \cap Y\} = P\{X\}P\{Y\} \tag{11.22}$$

often allows a very rough estimate of the top-event probability. We simply perform a bottom-up evaluation, multiplying probabilities at AND gates and adding them at OR gates. Care must be exercised in using this technique, for it is applicable only to trees in which basic events are not repeated – since repeated events are not independent – or to trees that have been logically reduced to a form in that primary failures appear only once. Thus, we may not evaluate the tree as it appears in Figure 11.25 in this way, but we may evaluate the reduced form in Figure 11.26. More systematic techniques for truncating the prohibitively long probability expressions that arise from large fault trees are an integral part of the minimum cut-set formulation considered in the following section.

Primary-Failure Data

In our discussions we have described fault trees in terms of failure probabilities without specifying the particular types of failure represented either by the top event or by the primary-failure data. In fact, there are three types of top events and, correspondingly, three types of basic events frequently used in conjunction with fault trees. They are (i) the failure on demand, (ii) the unreliability for some fixed period of time t, and (iii) the unavailability at some time.

When failures on demand are the basic events, a value of p is needed. For the unreliability or unavailability, it is often possible to use the following approximations to simplify the form of the data, since the probabilities of failure are expected to be quite small. If we assume a constant failure rate, the unreliability is

$$\widetilde{R} \cong \lambda t \tag{11.23}$$

Similarly, the most common unavailability is the asymptotic value for a system with constant failure and repair rates λ and ν. From Eq. (9.56), we have

$$\widetilde{A}(\infty) = 1 - \frac{\nu}{\nu + \lambda} \tag{11.24}$$

But, since in the usual case $\nu \gg \lambda$, we may approximate this by

$$\widetilde{A}(\infty) \approx \lambda/\nu \tag{11.25}$$

Often, demand failures, unreliabilities, and unavailabilities will be mixed in a single fault tree. Consider, for example a very simple fault tree for the failure of a light to go on when the switch is flipped. We assume that the top event, T, is the failure on demand for the light to go on, which is due to

X = bulb burned out,
Y = switch fails to make contact,
Z = power failure to house.

Therefore, $T = X \cup Y \cup Z$. In this case, X might be considered an unreliability of the bulb, with the time being that since it was originally installed; Y would be a demand failure, assuming that the cause was a random failure of the switch to make contact; and Z would be the unavailability of power to the circuit. Of course, the tree can be drawn in more depth. Is the random demand failure the only significant reason (a demand failure) for the switch not to make contact, or is there a significant probability that the switch is corroded open (an unreliability)?

Fault-Tree Evaluation by Cut Sets

The direct evaluation procedures just discussed allow us to assess fault trees with relatively few branches and basic events. When larger trees are considered, both evaluation and interpretation of the results become more difficult, and digital computer codes are invariably employed. Such codes are usually formulated in terms of the minimum cut-set methodology discussed in this section. There are at least two reasons for this. First, the techniques lend themselves well to the computer algorithms, and second, from them a good deal of intermediate information can be obtained concerning the combination of component failures that are pertinent to improvements in system design and operations.

The discussion that follows is conveniently divided into qualitative and quantitative analysis. In qualitative analysis, information about the logical structure of the tree is used to locate weak points and evaluate and improve system design. In quantitative analysis, the same objectives are taken further by studying the probabilities of component failures in relation to system design.

Qualitative Analysis

In these subsections, we first introduce the idea of minimum cut sets and relate it to the qualitative evaluation of fault trees. We then discuss briefly how the minimum cut sets are determined for large fault trees. Finally, we discuss their use in locating system weak points, particularly possibilities for common-mode failures.

Minimum Cut-Set Formulation

A minimum cut set is defined as the smallest combination of primary failures which, if they all occur, will cause the top event to occur. It is, therefore, a combination (i.e. intersection) of primary failures sufficient to cause the top event. It is the smallest combination in that all the failures must take place for the top event to occur. If even one of the failures in the minimum cut set does not happen, the top event will not take place.

The terms minimum cut set and failure mode are sometimes used interchangeably. However, there is a subtle difference that we observe hereafter. In reliability calculations, a failure mode is a combination of component or other failures that cause a system to fail, regardless of the consequences of the failure. A minimum cut set is usually more restrictive, for it is the minimum combination of failures that causes the top event as defined for a particular fault tree. If the top event is defined broadly as system failure, the two are indeed interchangeable. Usually, however, the top event encompasses only the particular subset of system failures that bring about a particular safety hazard.

The origin for using the term cut set may be illustrated graphically using the reduced fault tree in Figure 11.26. The reliability block diagram corresponding to the tree is shown in Figure 11.27. The idea of a cut set comes originally from the use of such diagrams for electric apparatus, where the signal enters at the left and leaves at the right. Thus, a minimum cut set is the minimum number of

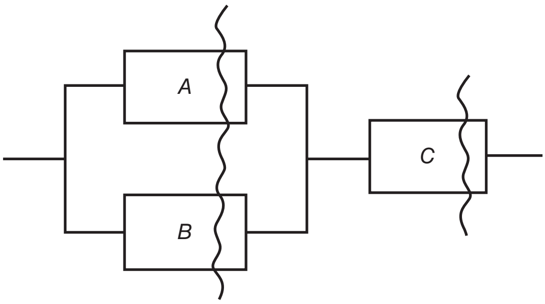


Figure 11.27 Minimum cut sets on a reliability block diagram.

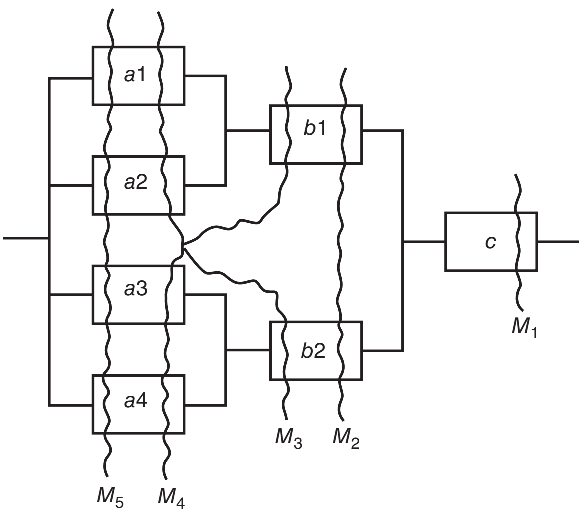


Figure 11.28 Minimum cut sets on a reliability block diagram of a seven-component system.

components that must be cut to prevent the signal flow. There are two minimum cut sets, M_1, consisting of components A and B, and M_2, consisting of component C.

For a slightly more complicated example, consider the redundant system of Figure 3.16, for which the equivalent fault tree appears in Figure 11.13. In this system, there are five cut sets, as indicated in the reliability block diagram of Figure 11.28.

For larger systems, particularly those in which the primary failures appear more than once in the fault tree, the simple geometrical interpretation becomes problematical. However, the primary characteristics of the concept remain valid. It permits the logical structure of the fault tree to be represented in a systematic way that is amenable to interpretation in terms of the behavior of the minimum cut sets.

Suppose that the minimum cut sets of a system can be found. The top event, system failure, may then be expressed as the union of these sets. Thus, if there are N minimum cut sets,

$$T = M_1 \cup M_2 \cup \cdots \cup M_N \tag{11.26}$$

Each minimum cut set then consists of the intersection of the minimum number of primary failures required to cause the top event. For example, the minimum cut sets for the system shown in Figures 11.13 and 11.28 are

$$M_1 = C \qquad M_3 = a1 \cap a2 \cap b2$$
$$M_2 = b1 \cap b2 \quad M_4 = a3 \cap a4 \cap b1 \tag{11.27}$$
$$M_5 = a1 \cap a2 \cap a3 \cap a4$$

Before proceeding, it should be pointed out that there are other cut sets that will cause the top event, but they are not minimum cut sets. These need not be considered, however, because they do not enter the logic of the fault tree. By the rules of Boolean algebra contained in Table 2.4, they are absorbed into the minimum cut sets. This can be illustrated using the configuration of Figure 11.28 again. Suppose that we examine the cut set $M_0 = b1 \cap c$, which will certainly cause system failure, but it is not a minimum cut set. If we include it in the expression for the top event, we have

$$T = M_0 \cup M_1 \cup M_2 \cup \cdots \cup M_N \tag{11.28}$$

Now, suppose that we consider $M_0 \cup M_1$. From the absorption law of Table 2.4, however, we see that

$$M_0 \cup M_1 = (b1 \cap c) \cup c = c \tag{11.29}$$

Thus, the nonminimum cut set is eliminated from the expression for the top event. Because of this property, minimum cut sets are often referred to simply as cut sets, with the minimum implied.

Since we are able to write the top event in terms of minimum cut sets as in Eq. (11.26), we may express the fault tree in the standardized form shown in Figure 11.29. In this, X_{mn} is the nth element of the mth minimum cut set. Note from our example that the same primary failures may often be expected to occur in more than one of the minimum cut sets. Thus, the minimum cut sets are not generally independent of one another.

Cut-Set Determination

In order to utilize the cut-set formulations, we must express the top event as the union of minimum cut sets, as in Eq. (11.26). For small fault trees this can be done by hand, using the rules of Table 2.4, just as we reduced the top-event expression for T given by Eq. (11.13) to the two-cut-set expression given by Eq. (11.17). For larger trees, containing perhaps 20 or more primary failures, this

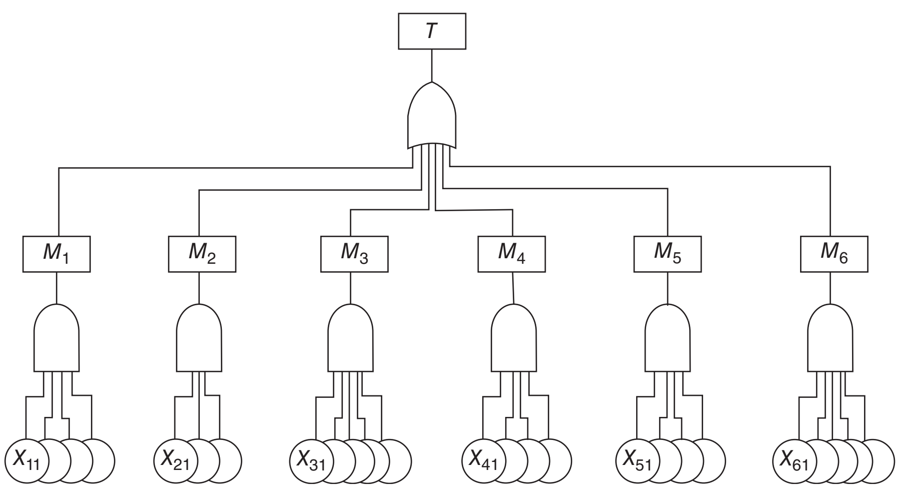


Figure 11.29 Generalized minimum cut-set representation of a fault tree.

procedure becomes intractable, and we must resort to digital computer evaluation. Even then, the task may be prodigious, for a larger tree with a great deal of redundancy may have a million or more minimum cut sets.

The computer codes for determining the cut sets (McCormick 1981) do not typically apply the rules of Boolean algebra to reduce the expression for the top set to the form of Eq. (11.26). Rather, a search is performed for the minimum cut sets; in this, a failure is represented by 1, and a success by 0. Then, each expression for the top event is evaluated using the outcome shown in Table 11.3 for the union and intersection of the events. A number of different procedures may be used to find the cut sets. In exhaustive searches, all single failures are first examined, and then all combinations of two primary failures, and so on. In general, there are 2^N, where N is the number of primary failures that must be examined. Other methods involve the use of random number generators in Monte Carlo simulation to locate the minimum cut sets.

When millions of minimum cut sets are possible, the search procedures are often truncated, for cut sets requiring many primary failures to take place are so improbable that they will not significantly affect the overall probability of the top event. Moreover, simulation methods must be terminated after a finite number of trials.

Cut-Set Interpretations

Knowing the minimum cut sets for a particular fault tree can provide valuable insight concerning potential weak points of complex systems, even when it is not possible to calculate the probability that either a particular cut set or the top event will occur. Three qualitative considerations, in particular, may be very useful: the ranking of the minimal cut sets by the number of primary failures required, the importance of particular component failures to the occurrence of the minimum cut sets, and the susceptibility of particular cut sets to common-mode failures.

Minimum cut sets are normally categorized as singlets, doublets, triplets, and so on, according to the number of primary failures in the cut set. Emphasis is then put on eliminating cut sets corresponding to small numbers of failures, for ordinarily these may be expected to make the largest contributions to system failure. In fact, the common design criterion that no single component failure should cause system failure is equivalent to saying that all singlets must be removed from the fault tree for which the top event is system failure. Indeed, if component failure probabilities are small and independent, then provided that they are of the same order of magnitude, doublets will occur much less frequently than singlets, triplets much less frequently than doublets, and so on.

A second application of cut-set information is in assessing qualitatively the importance of a particular component. Suppose that we wish to evaluate the effect on the system of improving the reliability of a particular component, or conversely, to ask whether, if a particular component fails, the system-wide effect will be considerable. If the component appears in one or more of the low-order cut sets, say singlets or doublets, its reliability is likely to have a pronounced effect. On the other hand, if it appears only in minimum cut sets requiring several independent failures, its importance to system failure is likely to be small.

These arguments can rank minimum cut-set and component importance, assuming that the primary failures are independent. If they are not, that is if they are susceptible to common-mode failure, the ranking of cut-set importance may be changed. If five of the failures in a minimum cut set with six failures, for example can occur as the result of a common cause, the probability of the cut sets occurring is more comparable to that of a doublet.

Extensive analysis is often carried out to determine the susceptibility of minimum cut sets to common-cause failures. In an industrial plant one cause might be fire. If the plant is divided into several fire-resistant compartments, the analysis might proceed as follows. All the primary failures of equipment located in one of the compartments that could be caused by fire are listed. Then, these components would be eliminated from the minimum cut sets (i.e. they would be assumed to fail). The resulting cut sets would then indicate how many failures – if any – in addition to those caused by the fire would be required for the top event to happen. Such analysis is critical for determining the layout of the plant that will best protect it from a variety of sources of damage: fire, flooding, collision, earthquake, and so on.

Quantitative Analysis

With the minimum cut sets determined, we may use probability data for the primary failures and proceed with quantitative analysis. This normally includes both an estimate of the probability of the top events occurring and quantitative measures of the importance of components and cut sets to the top event. Finally, studies of uncertainty about the top events happening, because the probability data for the primary failures are uncertain, are often needed to assess the precision of the results.

Top-Event Probability

To determine the probability of the top event, we must calculate

$$P\{T\} = P\{M_1 \cup M_2 \cup \cdots \cup M_N\} \tag{11.30}$$

As indicated in Section 2.26, the union can always be eliminated from a probability expression by writing it as a sum of terms, each one of which is the probability of an intersection of events. Here, the intersections are the minimum cut sets. Probability theory provides the expansion of Eq. (11.30) in the following form:

$$\begin{aligned} P\{T\} = & \sum_{i=1}^{N} P\{M_i\} - \sum_{i=2}^{N}\sum_{j=1}^{i-1} P\{M_i \cap M_j\} \\ & + \sum_{i=3}^{N}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} P\{M_i \cap M_j \cap M_k\} - \cdots \\ & + (-1)^{N-1} P\{M_1 \cap M_2 \cap \cdots \cap M_N\} \end{aligned} \tag{11.31}$$

This is sometimes referred to as the inclusion–exclusion principle.

The first task in evaluating this expression is to evaluate the probabilities of the individual minimum cut sets. Suppose that we let X_{im} represent the mth basic event in minimum cut set i. Then,

$$P\{M_i\} = P\{X_{i1} \cap X_{i2} \cap X_{i3} \cap \cdots P\{X_{iM}\} \tag{11.32}$$

If it may be proved that the primary failures in a given cut set are independent, we may write

$$P\{M_i\} = P\{X_{i1}\}P\{X_{i2}\}\cdots P\{X_{iM}\} \tag{11.33}$$

If they are not, a Markov model or some other procedure must be used to relate $P\{M_i\}$ to the properties of the primary failures.

The second task is to evaluate the intersections of the cut-set probabilities. If the cut sets are independent of one another, we have simply

$$P\{M_i \cap M_j\} = P\{M_i\}P\{M_j\} \tag{11.34}$$

$$P\{M_i \cap M_j \cap M_K\} = P\{M_i\}P\{M_j\}P\{M_k\} \tag{11.35}$$

and so on. More often than not, however, these conditions are not valid, for in a system with redundant components, a given component is likely to appear in more than one minimum cut set: If the same primary failure appears in two minimum cut sets, they cannot be independent of one another. Thus, an important point is to be made. Even if the primary events are independent of one another, the minimum cut sets are unlikely to be. For example, in the fault trees of Figures 11.13 and 11.28 the minimum cut sets $M_1 = c$ and $M_2 = b1 \cap b2$ will be independent of one another if the primary failures of components $b1$ and $b2$ are independent of c. In this system, however, M_2 and M_3 will be dependent even if all the primary failures are independent because they contain the failure of component $b2$.

Although minimum cut sets may be dependent, calculation of their intersections is greatly simplified if the primary failures are all independent of one another, for then the dependencies are due only to the primary failures that appear in more than one minimum cut set. To evaluate the intersection of minimum cut sets, simply take the product of probabilities that appear in one or more of the minimal cut sets:

$$P\{M_i \cap M_j\} = P\{X_{1ij}\}P\{X_{2ij}\}\cdots P\{X_{Nij}\} \tag{11.36}$$

where X_{1ij}, X_{2ij}, ..., X_{Nij} is the list of the failures that appear in M_i, M_j, or both.

That the foregoing procedure is correct is illustrated by a simple example. Suppose that we have two minimal cut sets $M_1 = A \cap B$ and $M_2 = B \cap C$, where the primary failures are independent. We then have

$$M_1 \cap M_2 = (A \cap B) \cap (B \cap C) = A \cap B \cap B \cap C \tag{11.37}$$

but $B \cap B = B$. Thus,

$$P\{M_1 \cap M_2\} = P\{A \cap B \cap C\} = P\{A\}P\{B\}P\{C\} \tag{11.38}$$

In the general notation of Eq. (11.36), we would have

$$X_{112} = A, \quad X_{212} = B, \quad X_{312} = C \tag{11.39}$$

With the assumption of independent primary failures, the series in Eq. (11.31) may in principle be evaluated exactly. When there are thousands or even millions of minimum cut sets to be considered, however, the task may be both prohibitive and unwarranted, for many of the terms in the series are likely to be completely negligible compared to the leading one or two terms.

The true answer may be bracketed by taking successive terms, and it is rarely necessary to evaluate more than the first two or three terms. If $P\{T\}$ is the exact value, it may be shown that (Vesely 1970)

$$P_1\{T\} \equiv \sum_{i=1}^{N} P\{M_i\} > P\{T\} \tag{11.40}$$

$$P_2\{T\} \equiv P_1\{T\} - \sum_{i=2}^{N}\sum_{j=1}^{i-1} P\{M_i \cap M_j\} < P\{T\} \tag{11.41}$$

$$P_3\{T\} \equiv P_2\{T\} + \sum_{i=3}^{N}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} P\{M_i \cap M_j \cap M_k\} > P\{T\} \tag{11.42}$$

and so on, with $P_4\{T\} < P\{T\}$.

Often, the first-order approximation $P_1\{T\}$ gives a result that is both reasonable and pessimistic. The second-order approximation might be evaluated to check the accuracy of the first. And rarely would more than the third-order approximation be used.

Even taking only a few terms in Eq. (11.40) may be difficult, and wasteful, if a million or more minimum cut sets are present. Thus, as mentioned in the preceding subsection, we often truncate the number of minimum cut sets to include only those that contain fewer than some specified number of primary failures. If all the failure probabilities are small, say <0.1, the cut-set probabilities should go down by more than an order of magnitude as we go from singlets to doublets, doublets to triplets, and so on.

Importance

As in qualitative analysis, it is not only the probability of the top event that normally concerns the analyst. The relative importance of single components and of particular minimum cut sets must be known if designs are to be optimized and operating procedures revised.

Two measures of importance ((Henley and Kumamoto 1981a, Chapter 10) are particularly simple but useful in system analysis. In order to know which cut sets are the most likely to cause the top event, the cut-set importance is defined as

$$I_{M_i} = \frac{P\{M_i\}}{P\{T\}} \tag{11.43}$$

for the minimum cut set i. Generally, we would also like to determine the relative importance of different primary failures in contributing to the top event. To accomplish this, the simplest measure is to add the probabilities of all the minimum cut sets to which the primary failure contributes. Thus, the importance of component X_i is

$$I_{X_i} = \frac{1}{P\{T\}} \sum_{X_i \in M_l} P\{M_l\} \tag{11.44}$$

Other more sophisticated measures of importance have also found applications.

Uncertainty

What we have obtained thus far are point or best estimates of the top event's probability. However, there are likely to be substantial uncertainties in the basic parameters – the component failure rates, demand failures, and other data – that are input to the probability estimates. Given these considerable uncertainties, it would be very questionable to accept point estimates without an accompanying interval estimate by which to judge the precision of the results. To this end, the component failure rates and other data may themselves be represented as random variables with a mean or best-estimate value and a variance to represent the uncertainty. The lognormal distribution has been very popular for representing failure data in this manner. For small fault trees, a number of analytical techniques may be applied to determine the sensitivity of the results to the data uncertainty. For larger trees, the Monte Carlo method has found extensive use (Henley and Kumamoto 1981a, Chapter 11).

11.6 Reliability/Safety Risk Analysis

In Section 5.4 of Chapter 5, we discussed Weibull Risk analysis and illustrated risk analysis with several rather simple examples. Those examples were based on one failure distribution and predicting how many of that failure mode would fail over a future time. We now move on to two additional items:

1) Calculating the safety "incident" from the predicted reliability failures for a single failure distribution.
2) Predicting the safety impact on a system of various independent variables and their effect on a design limit. We cover examples of the calculation of failures and safety incidents for such phenomenon as maximum bending stress, low cycle fatigue (LCF) life, etc.

Example 11.7 Calculating safety "incidents" from a reliability failure.
A safety incident is often simply a "factor" (or probability) of the predicted failures of a reliability failure mode. Using Example 5.18 Bearing Cage Fractures on a twin engine fighter aircraft. A 1000-hour inspection was chosen by the project management. The reason in this case was due to the 0.05 probability of a Bearing Cage fracture causing an unbalance in the engine turbine rotor, which when combined with the probability of that causing a turbine part to penetrate the other engine with probability 0.25 would give a predicted number of safety incidents > 1.

Recall the 1000-hour inspection projection of Bearing Cage Fracture incidents:

"Therefore, assuming a 1000-hour inspection makes a bearing "good as new" in terms of cage fracture, there is a total expectation of failure for each bearing by 4000 hours of $0.013 + 0.013 + 0.013 + 0.013 = 0.052$. For 1703 bearings that have an inspection every 1000 hours and run to 4000 hours that would mean $0.052 \times 1703 = 89$ failed bearings."

The projected safety incidents:

$$\begin{aligned}&\text{Projected safety incidents (with 1000 hour inspection)}\\&\quad = \text{Projected number of bearing cage fractures}\\&\qquad \times \text{Probability of high rotor unbalance}\\&\qquad \times \text{Probability of turbine disk parts exiting the nacelle and impacting the other engine.}\\&\quad = 89 \times 0.05 \times 0.25 = 1.1 \text{ safety incidents}\end{aligned}$$

The safety incident in this case might be the loss of an aircraft.

The factors referred to in the above calculation are the result of the engine design and test engineers using previous test experience and the safety engineers analyzing all safety information to see how the design and test factors are corroborated by other data available outside the experience of the engine manufacturer (e.g. government aircraft safety information).

Example 11.8 Calculating a safety incident – simple beam example.
Suppose that we have a beam anchored as illustrated in Figure 11.30.

The parameters for the study are shown in Table 11.4.

The maximum bending stress is the dependent variable of interest, with a yield stress = 2000 psi. In this study,

$$\text{Max bending} = \frac{6^{*}F^{*}L}{B^{*}H^{2}} \tag{11.45}$$

Calculating the mean or nominal max bending = 1638.4 psi.

That gives a

$$\text{Margin} = 1 - \frac{\text{Performance}}{\text{Requirement}} = \frac{1638.4}{2000} = \sim 18\% > 10\% \text{.......good design?} \tag{11.46}$$

Source: Shigley and Mitchell (1983).

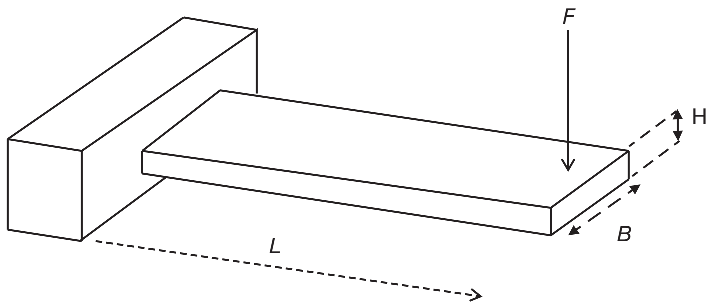


Figure 11.30 Beam with length (L), width (B), height(H), and force (F).

Table 11.4 Parameter means.

L	40 in
B	3.75 in
H	0.625 in
F	10 lbs

Table 11.5 Max bending parameter means and std deviation.

Parameter	Mean	Std dev
L	40	0.2
B	3.75	0.015
H	0.625	0.01
F	10	1

Now, suppose that we take into consideration the possible variation in each of the parameters (Table 11.5):

(And assume that each parameter follows a normal distribution.)

Assume that a normal distribution makes the calculation of the overall variation easier from an analytical perspective.

Let us first go back to what we know about probability and the normal distribution:

- Most values in a normal distribution will fall within ±three standard deviations ($\pm 3\sigma$) of the mean. If we assume that the "worst-case" is 3σ away from the mean value:

  $\mathbf{F + 3 * \sigma_F = 13}$

  $\mathbf{L + 3 * \sigma_L = 40.6}$

  $\mathbf{B - 3 * \sigma_B = 3.3}$

  $\mathbf{H - 3 * \sigma_H = 0.595}$

- The probability of this happening for *any single one* of these – (see normal table at 3σ) **= 0.00135.**
- The probability of this happening for ***ALL*** of these –
  = $(0.00135)^4 = 3.3 \times 10^{-12}$

But this is "worst case," a more reasonable (and accurate) answer can be calculated analytically since we have assumed normality for each of the parameters using the Taylor series expansion. We are also assuming no correlation between parameters.

$$\text{Mean of the max bending stress} = \frac{6^*\mathrm{F_{Mean}}^*\mathrm{L_{Mean}}}{\mathrm{B_{Mean}}^*\mathrm{H_{Mean}}^2} = \frac{6^*10^*40}{3.75^*0.625^2} = 1638.4\ \text{ksi}$$

$$\begin{aligned}
\sigma_{\mathrm{Max}}^2 &= \left(\frac{\partial Max}{\partial F}\right)^2\sigma_{\mathrm{F}}^2 + \left(\frac{\partial Max}{\partial L}\right)^2\sigma_{\mathrm{L}}^2 + \left(\frac{\partial Max}{\partial B}\right)^2\sigma_{\mathrm{B}}^2 + \left(\frac{\partial Max}{\partial H}\right)^2\sigma_{\mathrm{H}}^2\\
&= \left(\frac{6^*\mathrm{L_{Mean}}}{\mathrm{B_{Mean}}^*\mathrm{H_{Mean}}^2}\right)^2\sigma_{\mathrm{F}}^2 + \left(\frac{6^*\mathrm{F_{Mean}}}{\mathrm{B_{Mean}}^*\mathrm{H_{Mean}}^2}\right)^2\sigma_{\mathrm{L}}^2 + \left(-\frac{6^*\mathrm{F_{Mean}}^*\mathrm{L_{Mean}}}{\mathrm{B_{Mean}}^{2*}\mathrm{H_{Mean}}^2}\right)^2\sigma_{\mathrm{B}}^2 + \left(-2^*\frac{6^*\mathrm{F_{Mean}}^*\mathrm{L_{Mean}}}{\mathrm{B_{Mean}}^*\mathrm{H_{Mean}}^3}\right)^2\sigma_{\mathrm{H}}^2\\
&= \left(\frac{6^*40}{3.75^*0.625^2}\right)^2 1 + \left(\frac{6^*10}{3.75^*0.625^2}\right)^2 0.04 + \left(-\frac{6^*10^*40}{3.75^{2*}0.625^2}\right)^2 0.015^2 + \left(-2^*\frac{6^*10^*40}{3.75^*0.625^3}\right)^2 0.01^2\\
&= 26772.10 + 67.11 + 42.95 + 2748.78 = 29{,}630.94\\
\sigma_{\mathrm{Max}} &= \sqrt{29{,}630.94} = 172\ \text{psi}
\end{aligned} \tag{11.47}$$

In addition, using the above summarized in a table, we can easily calculate the contribution of each parameter to max bending:

With a mean = 1638.4 psi, standard deviation = 172 psi, the probability of exceeding the 2000 psi yield stress :

$$\text{Probability of} > 2000\ \text{psi} = 1 - \mathrm{P}\left(\frac{2000 - \mu_{\text{Max bend}}}{\sigma_{\text{Max bend}}}\right) = 1 - \mathrm{P}\left(\frac{2000 - 1638.4}{172}\right)$$
$$= 1 - Z(2.1) = 1 - 0.982 = 0.018$$

Therefore, when considering the variability in parameters that calculate max bending, the yield stress of 2000 psi will be exceeded ~2% of the time.

This contrasts with the assumption of "worst case" being a probability **= 3.3×10^{-12}**.

Conclusion: Assuming Worst Case can be Misleading

Another Approach: Monte Carlo Simulation

Using Eq. (11.45) along with the definitions of the normally distributed parameter means and standard deviations in Table 11.6, a Monte Carlo simulation can be completed using any number of software packages (e.g. EXCEL™, MATLAB™, MINITAB®, Oracle Crystal Ball, and @Risk). See Rubenstein and Kroese (2016) or Sobol (1994) for background on Monte Carlo simulation.

Using EXCEL™ to do this Monte Carlo simulation (assuming 10,000 iterations), we obtain the histogram of max bending in Figure 11.31 The histogram shows 216 instances of max bending > yield stress as opposed to 180 predicted by statistical solution above. However, we only did 10,000 iterations, and increasing it to 100,000 or 1 million would get the Monte Carlo estimate closer to the analytical.

Using a tool such as a crystal ball for 1,000,000 iterations (takes <30 seconds on a desktop PC) gives the same answer as analytical with ≪1% error.

So, why bother with a Monte Carlo simulation? Well, in truth very few dimensions in the "real world" of manufacturing are normally distributed. In addition, there are interactions of parameters that often have to be considered in an engineering model.

To emphasize that point,

Table 11.6 Calculation details of total variance in max bending with breakdown of % of total variance.

Parameter	X	σ	σ^2	$\partial Y/\partial X$	$(\partial Y/\partial X)^2$	$(\partial Y/\partial X)^2 * \sigma^2$	% of Total variance
F	10	1	1.00000	163.6218	26,772.10	26772.10	90.4
L	40	0.2	0.04000	40.9603	1677.75	67.11	0.2
B	3.75	0.015	0.000225	436.9083	190,888.89	42.95	0.1
H	0.625	0.01	0.00010	5242.8809	27,487,800.00	2748.78	9.3
					Total variance=	29,630.94	

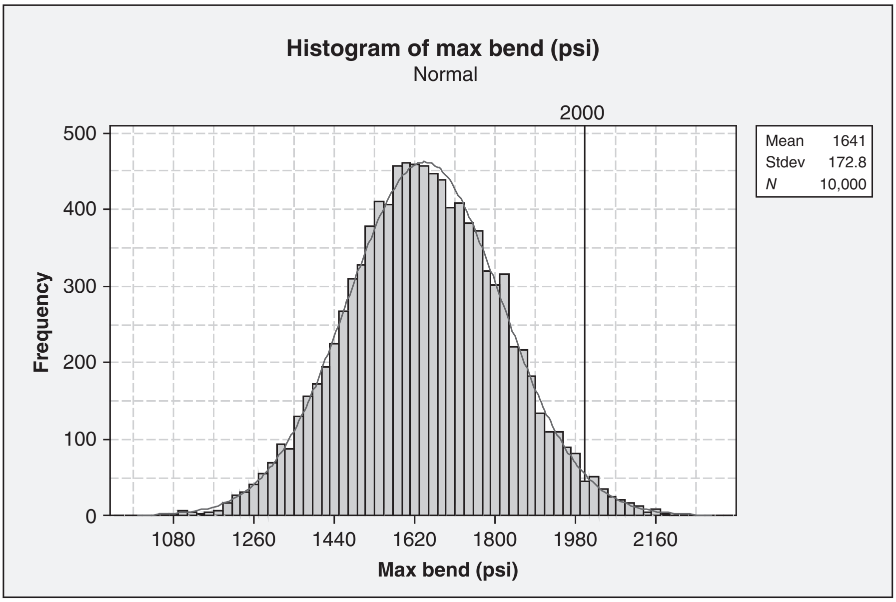


Figure 11.31 Histogram of max bending using EXEL with 10,000 iterations.

Example 11.9 Modeling variation in LCF life

Low cycle fatigue life of a turbine rotor part depends on stress and metal temperature. The relationship is shown in Figure 11.32. It goes without saying that turbine engine rotor parts are critical parts in a turbofan/turbojet engine, and a failure of a rotor part is a safety concern.

Continuing, stress and metal temperature again depend on various other parameters. Stress depends on spacer thickness, load, and speed, while metal temperature depends on chamber temperature, cooling temperature, and inlet temperature.

This particular rotor part has a nominal stress = 50 ksi and a nominal metal temperature = 1242°F.

The overall engineering models for the study:

$$\text{Mean life} = f(\text{stress, metal temperature}) + \text{Std error of materials curve} \tag{11.48}$$

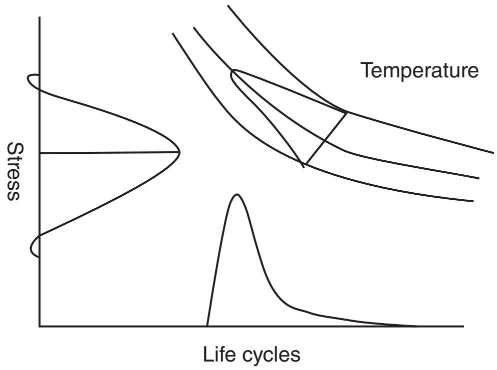


Figure 11.32 Overall view of LCF fatigue life calculation of a turbine rotor part.

$$\text{Stress} = f(\text{thickness, load, speed}) \text{ all acting independently on stress} \tag{11.49}$$

$$\text{Metal temperature} = f(\text{inlet temperature, chamber temperature, cooling temperature}) \text{ all acting independently on metal temparature} \tag{11.50}$$

The variables affecting stress: spacer thickness, load on the rotor, and speed of rotor.

The variables affecting metal temperature: cooling temperature of rotor, chamber temperature, and inlet temperature.

Distributions of primary parameters in Table 11.7.

The relationships of these variables to stress and metal temperature follow:

Engineering relationships affecting stress (Figures 11.33–11.35):

where Δ stress = random stress adder-50 ksi in all cases because the parameters are independent of each other.

Therefore,

$$\text{Total stress} = 50 + \sum_{i=1}^{3} (\text{Delta stress})_i \tag{11.51}$$

Likewise, for engineering relationships affecting metal temperature (Figure 11.36):

Where ΔMetal Temp = random temperature adder-1242°F in all cases because the parameters are independent of each other.

Therefore,

$$\text{Total Metal Temp} = 1242 + \sum_{i=1}^{3} (\text{Delta Metal Temp})_i \tag{11.52}$$

Table 11.7 Distributions of primary parameters affecting stress and metal temperature.

Spacer thickness	Uniform	Min = 0.9 in	Max = 1.1 in	
Load	Normal	Mean = 10,800 lbs	Std dev = 1200	
Speed	Normal	Mean = 9905 rpm	Std dev = 42	
Cooling temp	Triangular	Lower = 700°F	Midpt = 750°F	Upper = 900°F
Chamber temp	Normal	Mean = 1038°F	Std dev = 23°F	
Inlet temp	Triangular	Lower = 1816°F	Midpt = 1975°F	Upper = 2040°F

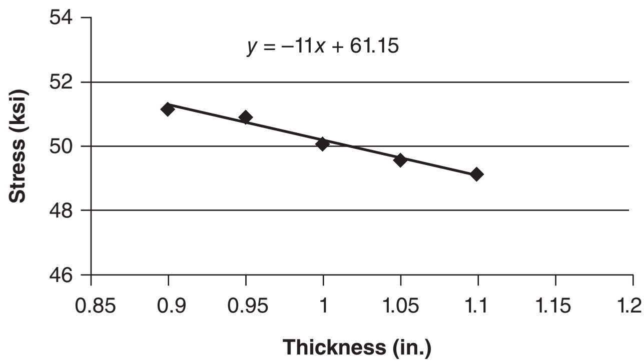


Figure 11.33 Relationship of stress to spacer thickness

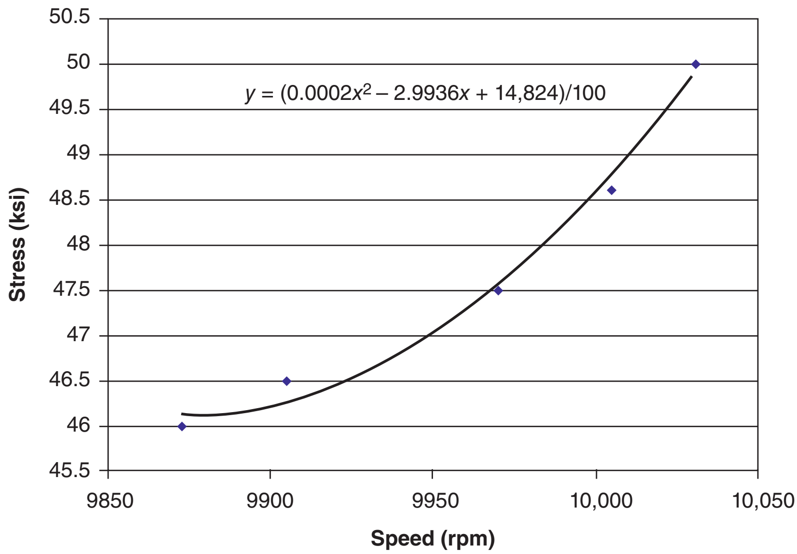


Figure 11.34 Relationship of stress to rotor speed.

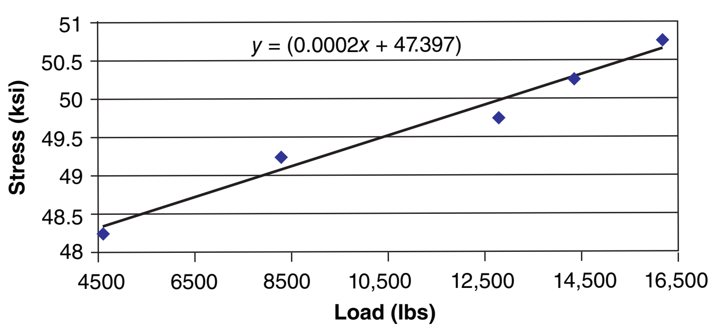


Figure 11.35 Relationship of stress to load.

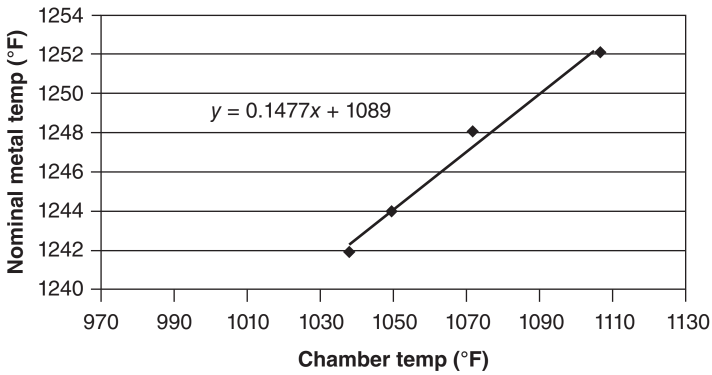


Figure 11.36 Relationship of metal temperature to chamber temperature.

One remaining item is needed. The materials equation for Waspaloy:

$$\begin{aligned}\text{Ln Life (cycles)} &= 5.0184753 - (9.729248^{*}\ \ln\ \text{Stress})\\ &+ (18.052402^{*}\ \ln\ \text{Temp}) - (3.947019^{*}(\ln\ \text{Temp})2)\\ &- (2.256088^{*}(\ln\ \text{Temp} - 2.79896)^{*}(\ln\ \text{Stress} - 1.98977))\end{aligned} \tag{11.53}$$

The standard error of estimate or root mean square error is 0.3249 ln cycles.

Simulation outline:

For each iteration (10,000 or more):

1) Pick a random spacer thickness: uniform (0.9, 1.1)
   Use the equation in Figure 11.33 and choose a Δstress thickness = (stress from equation) – 50
2) Pick a random rotor speed: normal (9905, 42)
   Use the equation in Figure 11.34 and choose a Δstress speed = (stress from equation) – 50
3) Pick a random load: normal (10, 800, 1200)
   Use the equation in Figure 11.35 and choose a Δstress load = (stress from equation) – 50
4) Pick a random chamber temp: normal (1038, 23)
   Use the equation in Figure 11.36 and choose a Δmetal temp = (metal temp from equation) – 1242
5) Pick a random cooling temp: triangular (700, 750, 800)
   Use the equation in Figure 11.37 and choose a Δmetal temp = (metal temp from equation) – 1242

Note: Triangular distribution is used when there are no data on the actual parameter, but the design and thermo engineers believe they know the min, mean, and max values, so the distribution in this case would look like (Figure 11.39):

6) Pick a random inlet temp: triangular (1816, 1975, 2040)
   Use the equation in Figure 11.38 and choose a Δmetal temp = (metal temp from equation) – 1242
   Then, using Eq. (11.3), expanded with Eq. (11.51) and Eq. (11.52):

$$\text{Log LCF life}_{\text{iteration}} = f(\text{total stress, total metal temperature}) + \text{normal}(0,\ 0.3249)$$

Continue this for the number of iterations chosen, saving the LCF life for each iteration.

Figures are the histogram of an average life for 100 averages of 1000 (Figure 11.40) and a Weibull fit to the data (Figure 11.41).

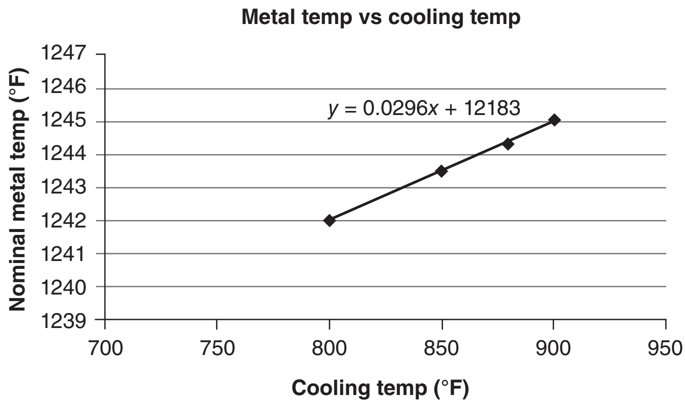


Figure 11.37 Relationship of metal temperature to cooling temperature (°F).

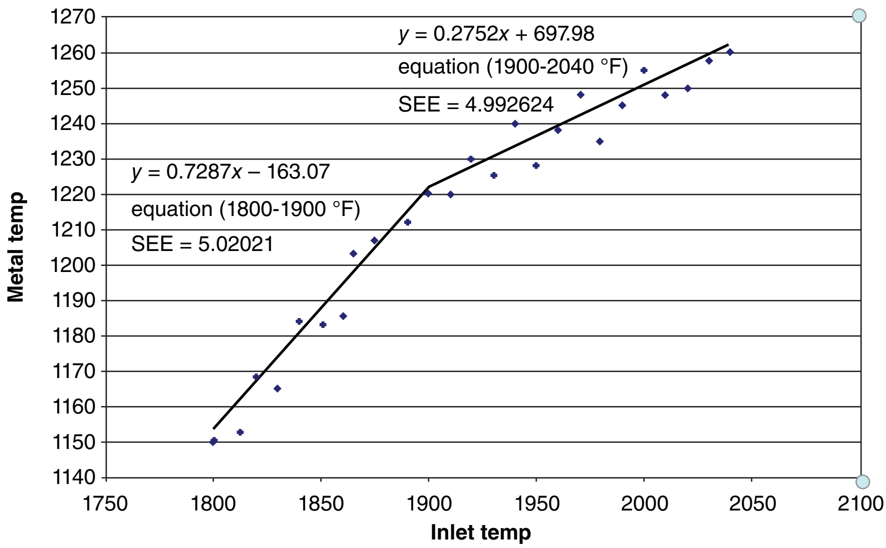
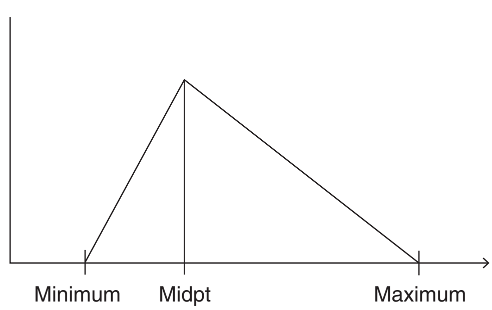


Figure 11.38 Relationship of metal temperature to inlet temperature (°F).

Figure 11.39 Triangular distribution.



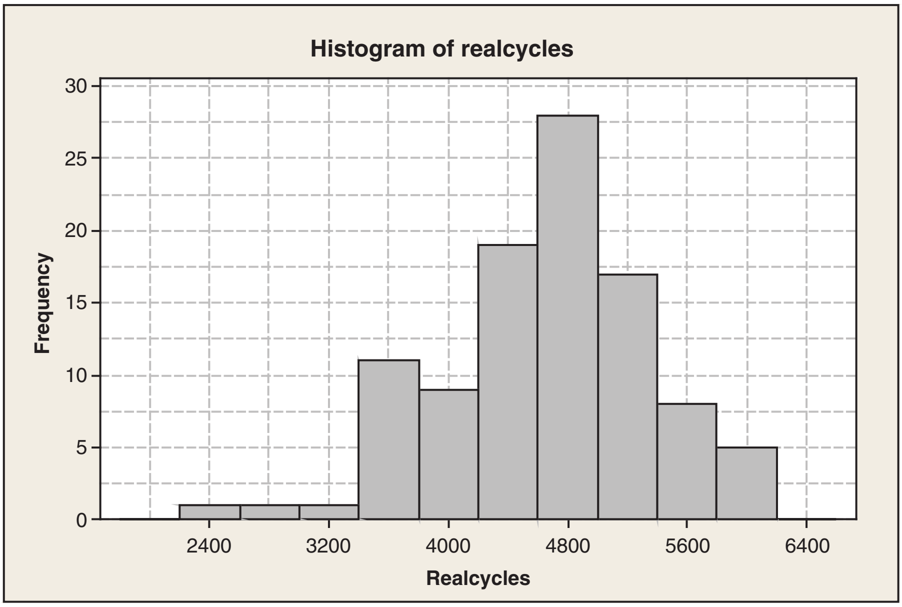


Figure 11.40 Histogram of sample Monte Carlo run of 100 averages of 1000.

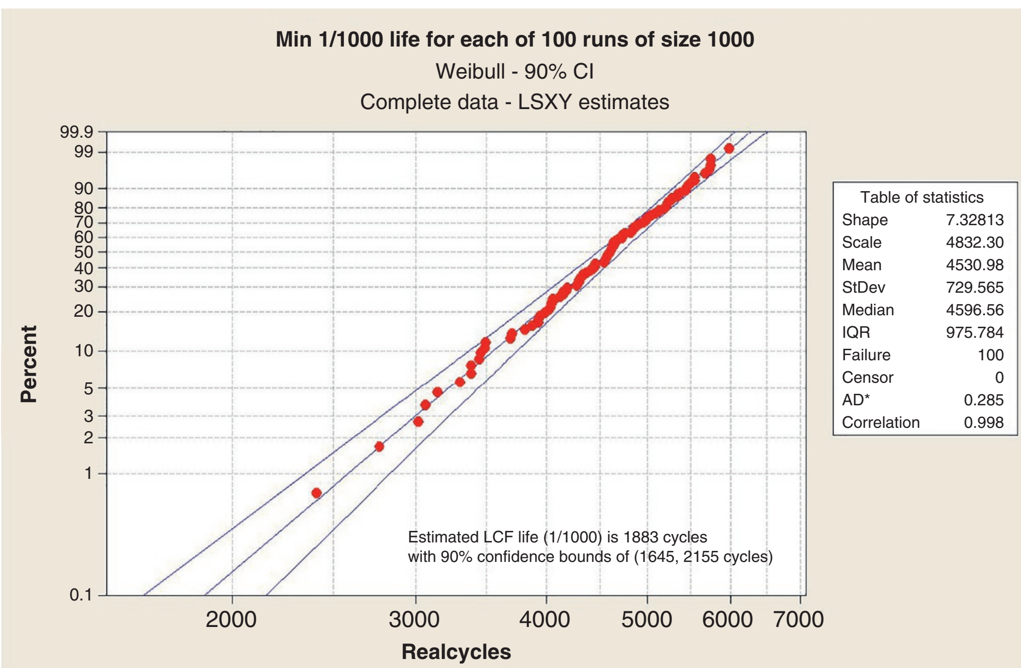


Figure 11.41 Probability plot of sample Monte Carlo run of 100 averages of 1000.

Bibliography

Ang, A.H.-S. and Tang, W.H. (1984). *Probability Concepts in Engineering Planning and Design*, vol. **2**. New York: Wiley.

Booster System Briefs (JSC-19041) (1992). *Systems Division, Guidance and Propulsion Systems Branch*. Houston, TX: NASA Johnson Space Flight Center.

Brockley, D. (ed.) (1992). *Engineering Safety*. London: McGraw-Hill.

Burgess, J.A. (1970). Spotting trouble before it happens. *Machine Design* **42** (23): 150.

Fussel, J.B. (1976). *Generic Techniques in System Reliability Assessment* (ed. E.J. Henley and J.W. Lynn). Leyden, Holland: Nordhoff.

Green, A.E. (1983). *Safety Systems Analysis*. New York: Wiley.

Henley, E.J. and Kumamoto, H. (1981a). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.

Henley, E.J. and Kumamoto, H. (1981b). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall, Chapter 10.

Henley, E.J. and Kumamoto, H. (1981c). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall, Chapter 11.

Henley, E.J. and Kumamoto, H. (1992). *Probabilistic Risk Assessment*. New York: IEEE Press.

Henley, E.J. and Lynn, J.W. (ed.) (1976). *Generic Techniques in System Reliability Assessment*. Leyden, Holland: Nordhoff.

McCormick, E.J. (1976). *Human Factors in Engineering Design*. New York: McGraw-Hill.

McCormick, N.J. (1981). *Reliability and Risk Analysis*. New York: Academic Press.

NUREG/CR (1983). *PRA Procedures Guide*, vol. **1**. U.S. Nuclear Regulatory Commission, NUREG/CR-2300.

Rasmussen, J. (1982). Human factors in high risk technology. In: *High Risk Technology* (ed. A.E. Green). New York: Wiley.

Roberts, H.R., Vesley, W.E., Haast, D.F., and Goldberg, F.F. (1981). *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission, NUREG-0492.

Rubenstein & Kroese (2016). *Simulation and the Monte Carlo Method*, 3ee. Wiley.

Shigley, J.E. and Mitchell, L.D. (1983). *Mechanical Engineering DesignMcGraw-Hill*, 4ee, 268–269.

Sobol, I.M. (1994). *A Primer for the Monte Carlo Method*. CRC Press.

Swain, A.D. and Guttmann, H.R. (1980). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. U.S. Nuclear Regulatory Commission, NUREG/CR-1287.

Vesely, W.E. (1970). Time Dependent Methodology for Fault Tree Evaluation. *Nucl. Eng. Design* **13**.

Henley, E.J. and Kumamoto, H. (1981d). *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.

FMEA/FMECA

FAA-H-8083-2 (2009). *Risk Management Handbook*. U.S. Department of Transportation, Federal Aviation Administration.

FMECA (2012). *Applied R&M Manual for Defence Systems Part C - R&M Related Techniques,* Chapter 33, Version 1. FMECA.

Mil-Std-1629A (1980) Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 24 November .

NAVAIR 00-25-403 (2016). *The Naval Aviation Reliability-Centered Maintenance Process* (ed. 1 June.).

Reliability Analysis Center (1993). *Failure Mode, Effects and Criticality Analysis (FMECA)*. Griffiss AFB, NY: Rome Laboratory, AD-A278 508.

D. Saraswati, I. Anne Marie and A. Witonohadi (2014). *Power transformer failures evaluation using failure mode effect and criticality analysis (FMECA) method, Asian Journal of Engineering and Technology, 2 (6)*, December, ISSN: 2321-2462.

Stamatis, D.H. (1995). *Failure Modes and Effect Analysis*. Milwaukee, WI: ASQC Quality Press.

Exercises

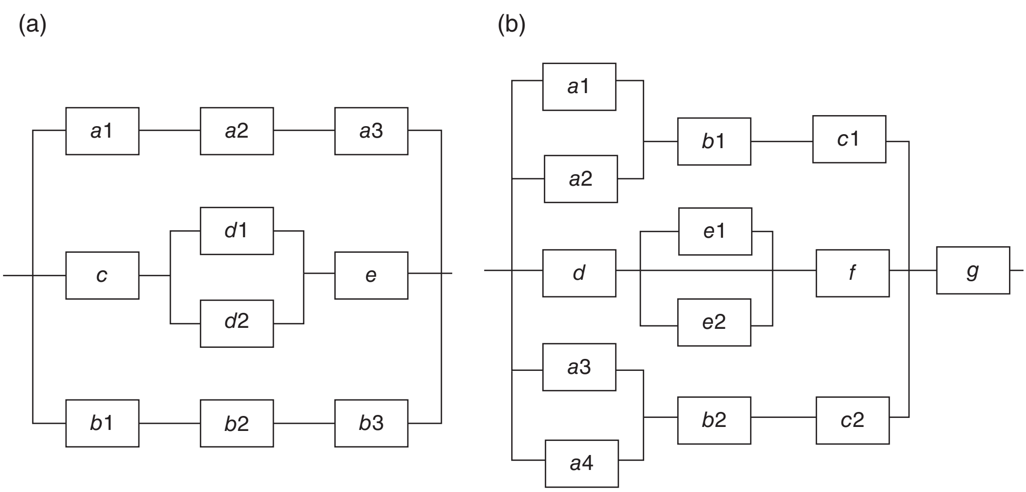
11.1 Classify each of the failures in Figure 11.15 as (a) passive, (b) active, or (c) either.

11.2 Make a list of six population stereotypical responses.

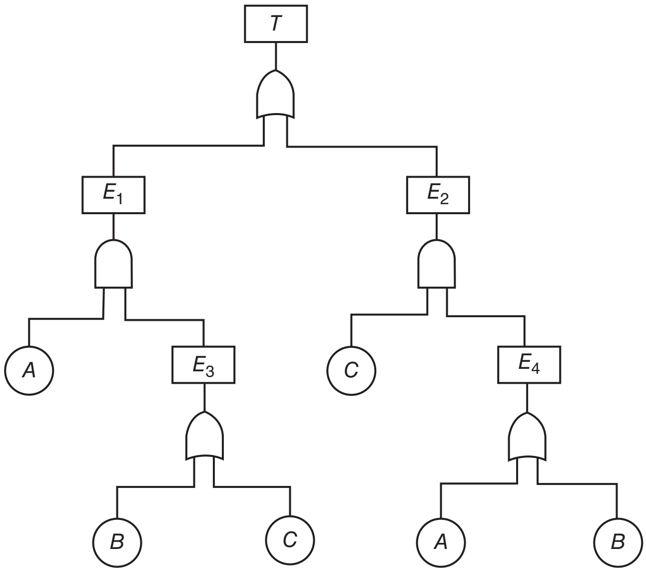
11.3 Suppose that a system consists of two subsystems in parallel. Each has a mission reliability of 0.9.

a) Draw a fault tree for mission failure, and calculate the probability of the top event.
b) Assume that there are common-mode failures described by the ξ-factor method (Chapter 3) with $\xi = 0.1$. Redraw the fault tree to take this into account, and recalculate the top event.

11.4 Find the fault tree for system failure for the following configurations.

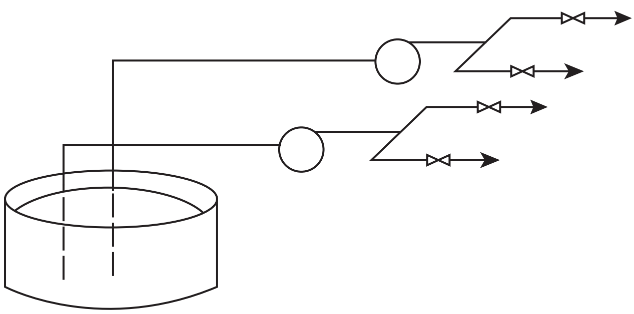


11.5 Find the minimum cut sets of the following fault tree.



11.6 Draw a fault tree corresponding to the reliability block diagram in Exercise 3.68.

11.7 The following system is designed to deliver emergency cooling to a nuclear reactor.



In the event of an accident, the protection system delivers an actuation signal to the two identical pumps and the four identical valves. The pumps then start up, the valves open, and the liquid coolant is delivered to the reactor. The following failure probabilities are found to be significant:

$p_{ps} = 10^{-5}$ the probability that the protection system will not deliver a signal to the pump and valve actuators.

$pp = 2 \times 10^{-2}$ the probability that a pump will fail to start when the actuation signal is received.

$p_v = 10^{-1}$ the probability that a valve will fail to open when the actuation signal is received.

$p_r = 0.5 \times 10^{-5}$ the probability that the reservoir will be empty at the time of the accident.

a) Draw a fault tree for the failure of the system to deliver any coolant to the primary system in the event of an accident.
b) Evaluate the probability that such a failure will take place in the event of an accident.

11.8 Construct a fault tree for which the top event is your failure to arrive on time for the final exam of a reliability engineering course. Include only the primary failures that you think have probabilities large enough to significantly affect the result.

11.9 Suppose that a fault tree has three minimum cut sets. The basic failures are independent and do not appear in more than one cut set. Assume that $P\{M_1\} = 0.03$, $P\{M_2\} = 0.12$, and $P\{M_3\} = 0.005$. Estimate $P\{T\}$ by the three successive estimates given in Eqs. (11.38), (11.39), and (11.40).

11.10 Develop a logical expression for the fault trees in Figure 11.13 in terms of the nine root causes. Find the minimum cut sets.

11.11 Suppose that for the fault tree given in Figure 11.21 $P\{\mathrm{A}\} = 0.15$, $\mathrm{P}\{B\} = 0.20$, and $P\{C\} = 0.05$.
a) Calculate the cut-set importances.
b) Calculate the component importances.
(Assume independent failures.)

11.12 The logical expression for a fault tree is given by

$$T = A \cap (B \cup C) \cap [D \cup (E \cap F \cap G)]$$

a) Construct the corresponding fault tree.
b) Find the minimum cut sets.
c) Construct an equivalent reliability block diagram.

11.13 From the reliability block diagram shown in Figure 11.23, draw a fault tree for system failure in minimum cut-set form. Assume that the failure probabilities for component types *a*, *b*, and *c* are, respectively, 0.1, 0.02, and 0.005. Assuming independent failures, calculate
a) $P\{T\}$, the probability of the top event;
b) the importance of components $a1$, $b1$, and c;
c) the importance of each of the five minimum cut sets.

11.14 Construct the fault trees for system failure for the low- and high-level redundant systems shown in Figure 3.15. Then, find the minimum cut sets.

11.15 In an FMECA, the item is a critical electrical component with mission time of 72 hours, an item failure rate λp of 10 per 106 hours. The failure mode of the component is due to an overstress voltage condition. The failure mode ratio, α, is 0.50, and the failure effect probability, ε, is 1.00. Calculate an estimate of criticality of this failure mode.

11.16 Fault tree provides graphical representation of all known events and/or combination of events which can lead to the undesired event being evaluated. A fault tree can support a failure mode effect and criticality analysis (FMECA) in identification of potential failure modes. Check off all those items that a fault tree can detect and those an FMECA can detect/calculate:

	FTA	FMECA
Multiple failure description		
Analyzing single point failures		
Avoiding analysis of noncritical failures		
Identifying external influences		
Identifying critical characteristics		
Providing a format for validation plans		

11.17 Below is a "late to work" FMEA. Calculate a ***qualitative*** criticality for each failure mode: any surprises?

Item			**Sever**	**Potential**	**Occur**		**Detec**		
Function	Potential Failure Modes	Potential Effect(s) of Failure		Cause(s) Mechanisms of Failure		Current Controls		R. P. N.	Criticality
Wake-up	Alarm	Late to work	6	Wrong time set	4	more than one alarm	5	120	
Getting dressed	No clean clothes/ wrinkled	Delayed	7	Forgot to check clothes	4	Check the night before	1	28	
Getting ready	Kids	Late to work	6	They ***are*** kids	10	Time-outs	5	300	
Breakfast	Nothing available	Hungry/ delayed/ angry	8	No time to make it/no groceries	3	Cafeteria fast food	1	24	
Drive	Weather	Late to work	6	God	5	N/A	10	300	
Drive	Traffic/ lights	Late to work	5	DMV	4	N/A	10	200	
Drive	Accident	Late to work	10	Sleepy, cell phone, inattentive	3	Coffee	4	120	
Drive	No gas	Late to work	8	Forgot to check or to expense	4	Check the night before	1	32	
Drive	No ID badge	Late to work	6	Misplaced	4	One location	1	24	
Drive	Flat tire	Late to work	8	Wear	2	Check pressure/ daily	1	16	
Drive	No keys	Late to work	8	Misplaced	1	One location	1	8	

Appendix A

Useful Mathematical Relationships

A.1 Integrals

Definite Integrals

$$\int_0^\infty e^{-ax}dx = \frac{1}{a}, \quad a > 0$$

$$\int_0^\infty x^n e^{-ax}dx = \frac{n!}{a^{n+1}}, \quad n = \text{integer} \geq 0, a > 0$$

$$\int_0^\infty e^{-a^2x^2}dx = \frac{\sqrt{\pi}}{2a}, \quad a > 0$$

$$\int_0^\infty xe^{-x^2}dx = \frac{1}{2}$$

$$\int_0^\infty x^2 e^{-x^2}dx = \frac{\sqrt{\pi}}{4}$$

$$\int_0^\infty x^{2n} e^{-ax^2}dx = \frac{1\cdot3\cdot5\cdots(2n-1)}{2^{n+1}a^n}\sqrt{\pi/a}, \quad n = \text{integer} > 0, a > 0$$

Integration by Parts

$$\int_a^b f(x)\frac{d}{dx}g(x)dx = f(b)g(b) - f(a)g(a) - \int_a^b g(x)\frac{d}{dx}f(x)dx$$

Derivative of an Integral

$$\frac{d}{dc}\int_p^q f(x,c)\,dx = \int_p^q \frac{\partial}{\partial c}f(x,c)dx + f(q,c)\frac{dq}{dc} - f(p,c)\frac{dp}{dc}$$

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

A.2 Expansions

Integer Series

$$1 + 2 + 3 + \cdots + n = \frac{n}{2}(n + 1)$$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n}{6}\left(2n^2 + 3n + 1\right)$$

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2}{4}(n + 1)^2$$

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Binomial Expansion

$$(p + q)^N = \sum_{n=0}^{N} C_n^N p^n q^{N-n}$$

$$_N C_n = C_n^N = \frac{N!}{(N - n)!n!}$$

Geometric Progression

$$\frac{1 - p^n}{1 - p} = 1 + p + p^2 + p^3 + \cdots + p^{n-1}$$

Infinite Series

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \quad x^2 < \infty .$$

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots, \quad x^2 < 1$$

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + x^4 + \cdots, \quad x^2 < 1$$

$$\frac{1}{(1 - x^2)} = 1 + 2x + 3x^2 + 4x^3 + \cdots, \quad x^2 < 1$$

$$\frac{1 + x}{(1 - x^2)^3} = 1 + 2^2x + 3^2x^2 + 4^2x^3 + \cdots, \quad x^2 < 1$$

A.3 Solution of First-order Linear Differential Equation

$$\frac{d}{dx}y(x) + \alpha(x)y(x) = S(x)$$

Note that

$$\frac{d}{dx}y(x)\exp\left[\int_{x_0}^{x}\alpha(x')dx'\right] = \left[\frac{d}{dx}y(x) + \alpha(x)y(x)\right]\exp\left[\int_{x_0}^{x}\alpha(x')dx'\right]$$

Thus, multiplying by the integrating factor $\exp\left[\int_{x_0}^{x}\alpha(x')dx'\right]$, we have

$$\frac{d}{dx}y(x)\exp\left[\int_{x_0}^{x}\alpha(x')dx'\right] = S(x)\exp\left[\int_{x_0}^{x}\alpha(x')dx'\right]$$

Integrating between x_0 and x, we have

$$y(x) = y(x_0)\exp\left[-\int_{x_0}^{x}\alpha(x')dx'\right] + \int_{x_0}^{x}dx'S(x')\exp\left[-\int_{x'}^{x}\alpha(x'')dx''\right]$$

If α is constant, then

$$y(x) = y(x_0)\exp\left[-\alpha(x-x_0)\right] + \int_{x_0}^{x}dx'S(x')\exp\left[-\alpha(x-x')\right]$$

Appendix B

Binomial Failure Probability Charts

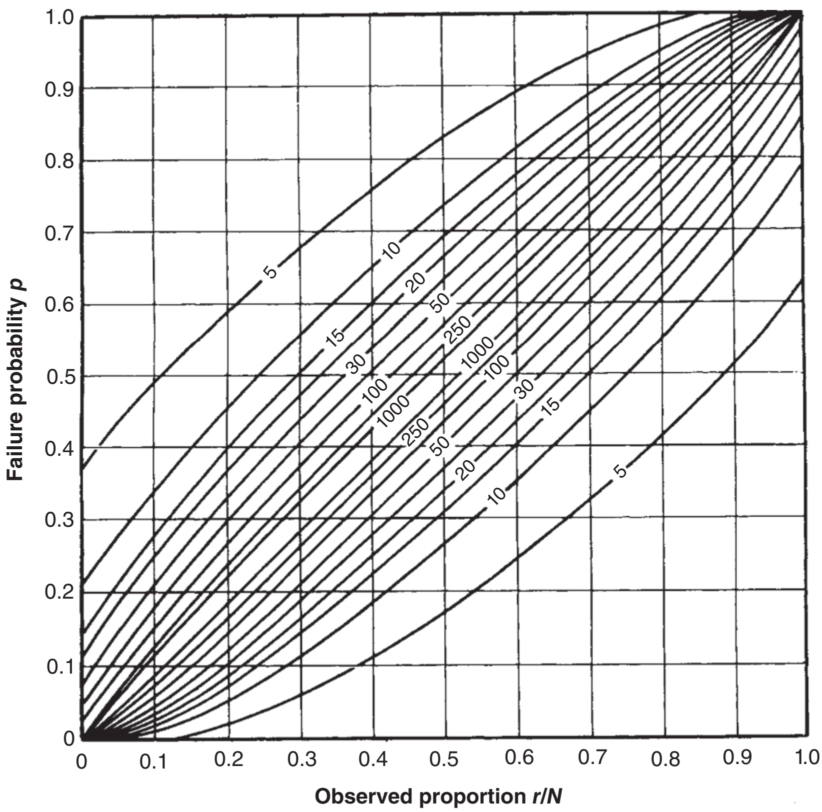


Figure B.1 An 80% confidence interval for binomial failure probability. *Source:* W.J. Dixon and F.J. Massey, Jr., Introduction to Statistical Analysis, 2nd ed., © 1957, with permission from McGraw-Hill Book Company, New York.

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

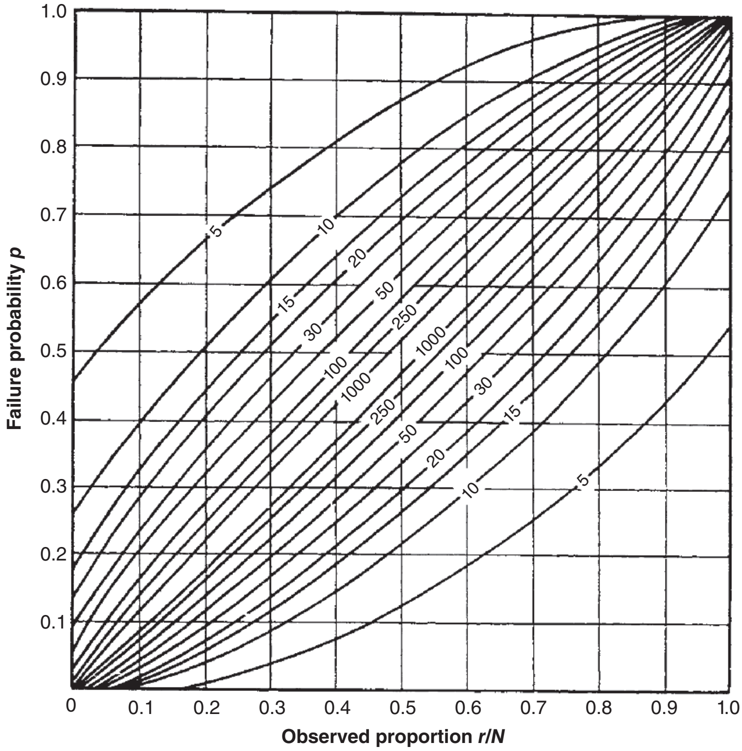


Figure B.2 A 90% confidence interval for binomial failure probability. *Source:* W.J. Dixon and F.J. Massey, Jr., Introduction to Statistical Analysis, 2nd ed., © 1957, with permission from McGraw-Hill Book Company, New York.

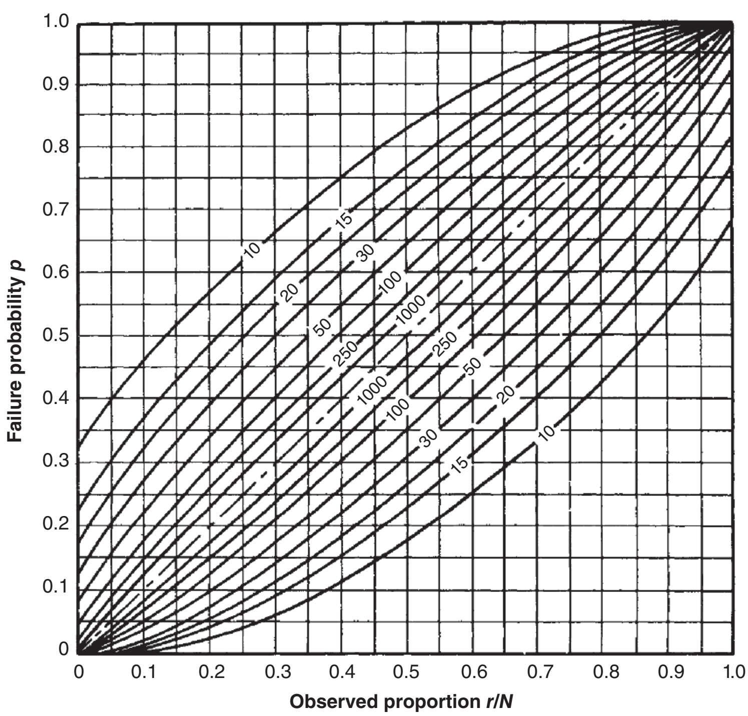


Figure B.3 A 95% confidence interval for binomial failure probability. *Source:* E. S. Pearson and C. J. Clopper, "The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial," Biometrika, 26, 404 (1934). With permission of Biometrika.

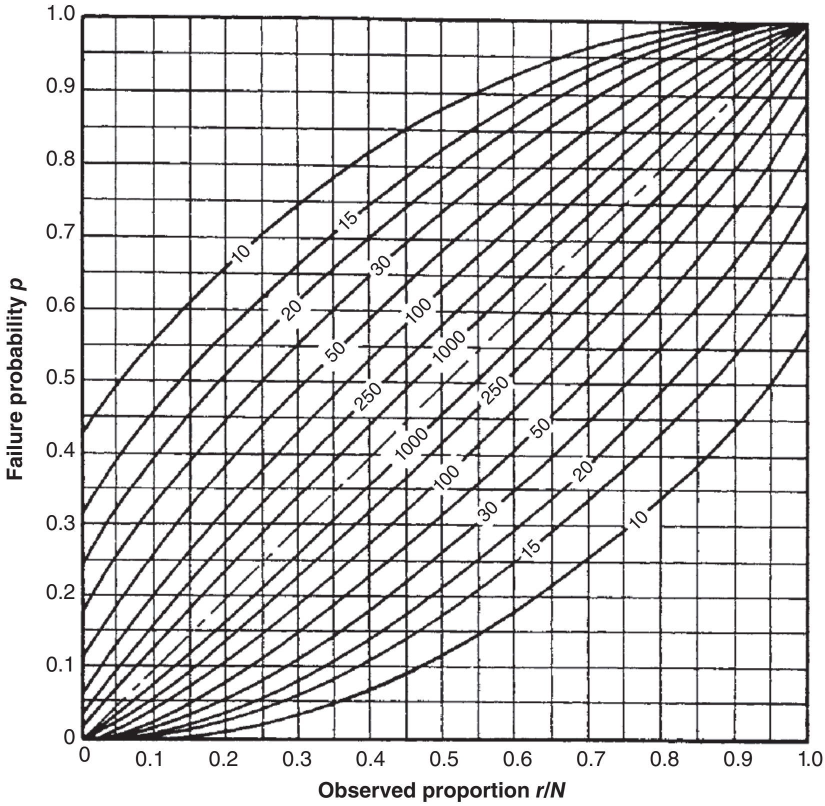


Figure B.4 A 99% confidence interval for binomial failure probability. *Source:* E. S. Pearson and C. J. Clopper, "The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial," Biometrika, 26, 404 (1934). With permission of Biometrika.

Appendix C

Φ(*z*): Standard Normal CDF

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

z	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
− .0	0.5000	0.4960	0.4920	0.4880	0.4840	0.4801	0.4761	0.4721	0.4681	0.4641
− .1	0.4602	0.4562	0.4522	0.4483	0.4443	0.4404	0.4364	0.4325	0.4286	0.4247
− .2	0.4207	0.4168	0.4129	0.4090	0.4052	0.4013	0.3974	0.3936	0.3897	0.3859
− .3	0.3821	0.3783	0.3745	0.3707	0.3669	0.3632	0.3594	0.3557	0.3520	0.3483
− .4	0.3446	0.3409	0.3372	0.3336	0.3300	0.3264	0.3228	0.3192	0.3156	0.3121
− .5	0.3085	0.3050	0.3015	0.2981	0.2946	0.2912	0.2877	0.2343	0.2810	0.2776
− .6	0.2743	0.2709	0.2676	0.2643	0.2611	0.2578	0.2546	0.2514	0.2483	0.2451
− .7	0.2420	0.2389	0.2358	0.2327	0.2297	0.2266	0.2236	0.2206	0.2177	0.2148
− .8	0.2119	0.2090	0.2061	0.2033	0.2005	0.1977	0.1949	0.1922	0.1894	0.1867
− .9	0.1841	0.1814	0.1788	0.1762	0.1736	0.1711	0.1685	0.1660	0.1635	0.1611
−1.0	0.1587	0.1562	0.1539	0.1515	0.1492	0.1469	0.1446	0.1423	0.1401	0.1379
−1.1	0.1357	0.1335	0.1314	0.1292	0.1271	0.1251	0.1230	0.1210	0.1190	0.1170
−1.2	0.1131	0.1131	0.1113	0.1093	0.1075	0.1056	0.1038	0.1020	0.1003	0.09853
−1.3	0.09680	0.09510	0.09342	0.09176	0.09012	0.08851	0.08691	0.08534	0.08379	0.08226
−1.4	0.08076	0.07927	0.07780	0.07636	0.07493	0.07353	0.07215	0.07078	0.06944	0.06811
−1.5	0.06681	0.06552	0.06426	0.06301	0.06178	0.06057	0.05938	0.05821	0.05705	0.05592
−1.6	0.05480	0.05370	0.05262	0.05155	0.05050	0.04947	0.04846	0.04746	0.04648	0.04551
−1.7	0.04457	0.04363	0.04272	0.04182	0.04093	0.04006	0.03920	0.03836	0.03754	0.03673
−1.8	0.03593	0.03515	0.03438	0.03362	0.03288	0.03216	0.03144	0.03074	0.03005	0.02938
−1.9	0.02872	0.02807	0.02743	0.02680	0.02619	0.02559	0.02500	0.02442	0.02385	0.02330
−2.0	0.02275	0.02222	0.02169	0.02118	0.02068	0.02018	0.01970	0.01923	0.01876	0.01831
−2.1	0.01786	0.01743	0.01700	0.01659	0.01618	0.01578	0.01539	0.01500	0.01463	0.01426
−2.2	0.01390	0.01355	0.01321	0.01287	0.01255	0.01222	0.01191	0.01160	0.01130	0.01101
−2.3	0.01072	0.01044	0.01017	$0.0^{2}9903$	$0.0^{2}9642$	$0.0^{2}9387$	$0.0^{2}9137$	$0.0^{2}8894$	$0.0^{2}8656$	$0.0^{2}8424$
−2.4	$0.0^{2}8198$	$0.0^{2}7976$	$0.0^{2}7760$	$0.0^{2}7549$	$0.0^{2}7344$	$0.0^{2}7143$	$0.0^{2}6947$	$0.0^{2}6756$	$0.0^{2}6569$	$0.0^{2}6387$
−2.5	$0.0^{2}6210$	$0.0^{2}6037$	$0.0^{2}5868$	$0.0^{2}5703$	$0.0^{2}5543$	$0.0^{2}5386$	$0.0^{2}5234$	$0.0^{2}5085$	$0.0^{2}4940$	$0.0^{2}4799$
−2.6	$0.0^{2}4661$	$0.0^{2}4527$	$0.0^{2}4396$	$0.0^{2}4269$	$0.0^{2}4145$	$0.0^{2}4025$	$0.0^{2}3907$	$0.0^{2}3793$	$0.0^{2}3681$	$0.0^{2}3573$
−2.7	$0.0^{2}3467$	$0.0^{2}3364$	$0.0^{2}3264$	$0.0^{2}3167$	$0.0^{2}3072$	$0.0^{2}2980$	$0.0^{2}2890$	$0.0^{2}2803$	$0.0^{2}2718$	$0.0^{2}2635$
−2.8	$0.0^{2}2555$	$0.0^{2}2477$	$0.0^{2}2401$	$0.0^{2}2327$	$0.0^{2}2256$	$0.0^{2}2186$	$0.0^{2}2118$	$0.0^{2}2052$	$0.0^{2}1988$	$0.0^{2}1926$
−2.9	$0.0^{2}1866$	$0.0^{2}1807$	$0.0^{2}1750$	$0.0^{2}1695$	$0.0^{2}1641$	$0.0^{2}1589$	$0.0^{2}1538$	$0.0^{2}1489$	$0.0^{2}1441$	$0.0^{2}1395$
−3.0	$0.0^{2}1350$	$0.0^{2}1306$	$0.0^{2}1264$	$0.0^{2}1223$	$0.0^{2}1183$	$0.0^{2}1144$	$0.0^{2}1107$	$0.0^{2}1070$	$0.0^{2}1035$	$0.0^{2}1001$
−3.1	$0.0^{3}9676$	$0.0^{3}9354$	$0.0^{3}9043$	$0.0^{3}8740$	$0.0^{3}8447$	$0.0^{3}8164$	$0.0^{3}7888$	$0.0^{3}7622$	$0.0^{3}7364$	$0.0^{3}7114$
−3.2	$0.0^{3}6871$	$0.0^{3}6637$	$0.0^{3}6410$	$0.0^{3}6190$	$0.0^{3}5976$	$0.0^{3}5770$	$0.0^{3}5571$	$0.0^{3}5377$	$0.0^{3}5190$	$0.0^{3}5009$
−3.3	$0.0^{3}4834$	$0.0^{3}4663$	$0.0^{3}4501$	$0.0^{3}4342$	$0.0^{3}4189$	$0.0^{3}4041$	$0.0^{3}3897$	$0.0^{3}3758$	$0.0^{3}3624$	$0.0^{3}3495$
−3.4	$0.0^{3}3369$	$0.0^{3}3248$	$0.0^{3}3131$	$0.0^{3}3018$	$0.0^{3}2909$	$0.0^{3}2803$	$0.0^{3}2701$	$0.0^{3}2602$	$0.0^{3}2507$	$0.0^{3}2415$
−3.5	$0.0^{3}2326$	$0.0^{3}2241$	$0.0^{3}2158$	$0.0^{3}2078$	$0.0^{3}2001$	$0.0^{3}1926$	$0.0^{3}1854$	$0.0^{3}1785$	$0.0^{3}1718$	$0.0^{3}1653$

−3.6	$0.0^{3}1591$	$0.0^{3}1531$	$0.0^{3}1473$	$0.0^{3}1417$	$0.0^{3}1363$	$0.0^{3}1311$	$0.0^{3}1261$	$0.0^{3}1213$	$0.0^{3}1166$	$0.0^{3}1121$
−3.7	$0.0^{3}1078$	$0.0^{3}1036$	$0.0^{4}9961$	$0.0^{4}9574$	$0.0^{4}9201$	$0.0^{4}8842$	$0.0^{4}8496$	$0.0^{4}8162$	$0.0^{4}7841$	$0.0^{4}7532$
−3.8	$0.0^{4}7235$	$0.0^{4}6948$	$0.0^{4}6673$	$0.0^{4}6407$	$0.0^{4}6152$	$0.0^{4}5906$	$0.0^{4}5669$	$0.0^{4}5442$	$0.0^{4}5223$	$0.0^{4}5012$
−3.9	$0.0^{4}4810$	$0.0^{4}4615$	$0.0^{4}4427$	$0.0^{4}4247$	$0.0^{4}4074$	$0.0^{4}3908$	$0.0^{4}3747$	$0.0^{4}3594$	$0.0^{4}3446$	$0.0^{4}3304$
−4.0	$0.0^{4}3167$	$0.0^{4}3036$	$0.0^{4}2910$	$0.0^{4}2789$	$0.0^{4}2673$	$0.0^{4}2561$	$0.0^{4}2454$	$0.0^{4}2351$	$0.0^{4}2242$	$0.0^{4}2157$
−4.1	$0.0^{4}2066$	$0.0^{4}1978$	$0.0^{4}1894$	$0.0^{4}1814$	$0.0^{4}1737$	$0.0^{4}1662$	$0.0^{4}1591$	$0.0^{4}1523$	$0.0^{4}1458$	$0.0^{4}1395$
−4.2	$0.0^{4}1335$	$0.0^{4}1277$	$0.0^{4}1222$	$0.0^{4}1168$	$0.0^{4}1118$	$0.0^{4}1069$	$0.0^{4}1022$	$0.0^{5}9774$	$0.0^{5}9345$	$0.0^{5}8934$
−4.3	$0.0^{5}8540$	$0.0^{5}8163$	$0.0^{5}7801$	$0.0^{5}7455$	$0.0^{5}7124$	$0.0^{5}6807$	$0.0^{5}6503$	$0.0^{5}6212$	$0.0^{5}5934$	$0.0^{5}5668$
−4.4	$0.0^{5}5413$	$0.0^{5}5169$	$0.0^{5}4935$	$0.0^{5}4712$	$0.0^{5}4498$	$0.0^{5}4294$	$0.0^{5}4098$	$0.0^{5}3911$	$0.0^{5}3732$	$0.0^{5}3561$
−4.5	$0.0^{5}3398$	$0.0^{5}3241$	$0.0^{5}3092$	$0.0^{5}2949$	$0.0^{5}2813$	$0.0^{5}2682$	$0.0^{5}2558$	$0.0^{5}2439$	$0.0^{5}2325$	$0.0^{5}2216$
−4.6	$0.0^{5}2112$	$0.0^{5}2013$	$0.0^{5}1919$	$0.0^{5}1828$	$0.0^{5}1742$	$0.0^{5}1660$	$0.0^{5}1581$	$0.0^{5}1506$	$0.0^{5}1434$	$0.0^{5}1366$
−4.7	$0.0^{5}1301$	$0.0^{5}1239$	$0.0^{5}1179$	$0.0^{5}1123$	$0.0^{5}1069$	$0.0^{5}1017$	$0.0^{6}9680$	$0.0^{6}9211$	$0.0^{6}8765$	$0.0^{6}8339$
−4.8	$0.0^{6}7933$	$0.0^{6}7547$	$0.0^{6}7178$	$0.0^{6}6827$	$0.0^{6}6492$	$0.0^{6}6173$	$0.0^{6}5869$	$0.0^{6}5580$	$0.0^{6}5304$	$0.0^{6}5042$
−4.9	$0.0^{6}4792$	$0.0^{6}4554$	$0.0^{6}4327$	$0.0^{6}4111$	$0.0^{6}3906$	$0.0^{6}3711$	$0.0^{6}3525$	$0.0^{6}3348$	$0.0^{6}3179$	$0.0^{6}3019$
0.0	0.5000	0.5040	0.5080	0.5120	0.5160	0.5199	0.5239	0.5279	0.5319	0.5359
0.1	0.5398	0.5438	0.5478	0.5517	0.5557	0.5596	0.5636	0.5675	0.5714	0.5753
0.2	0.5793	0.5832	0.5871	0.5910	0.5948	0.5987	0.6026	0.6064	0.6103	0.6141
0.3	0.6179	0.6217	0.6255	0.6293	0.6331	0.6368	0.6406	0.6443	0.6480	0.6517
0.4	0.6554	0.6591	0.6628	0.6664	0.6700	0.6736	0.6772	0.6808	0.6844	0.6879
0.5	0.6915	0.6950	0.6985	0.7019	0.7054	0.7088	0.7123	0.7157	0.7190	0.7224
0.6	0.7257	0.7291	0.7324	0.7359	0.7389	0.7422	0.7454	0.7486	0.7517	0.7549
0.7	0.7580	0.7611	0.7642	0.7673	0.7703	0.7734	0.7764	0.7794	0.7823	0.7852
0.8	0.7881	0.7910	0.7939	0.7967	0.7995	0.8023	0.8051	0.8078	0.8106	0.8133
0.9	0.8159	0.8186	0.8212	0.8238	0.8264	0.8289	0.8315	0.8340	0.8365	0.8389
1.0	0.8413	0.8438	0.8461	0.8485	0.8508	0.8531	0.8554	0.8577	0.8599	0.8621
1.1	0.8643	0.8665	0.8686	0.8708	0.8729	0.8749	0.8770	0.8790	0.8810	0.8830
1.2	0.8849	0.8869	0.8888	0.8907	0.8925	0.8944	0.8962	0.8980	0.8997	0.90147
1.3	0.90320	0.90490	0.90658	0.90824	0.90988	0.91149	0.91309	0.91466	0.91621	0.91774
1.4	0.91924	0.92073	0.92220	0.92364	0.92507	0.92647	0.92785	0.92922	0.93056	0.93189
1.5	0.93319	0.93448	0.93574	0.93699	0.93822	0.93943	0.94062	0.94179	0.94295	0.94408
1.6	0.94520	0.94630	0.94738	0.94845	0.94950	0.95053	0.95154	0.95254	0.95352	0.95449
1.7	0.95543	0.95637	0.95728	0.95818	0.95907	0.95994	0.96080	0.96164	0.96246	0.96327
1.8	0.96407	0.96485	0.96562	0.96638	0.96712	0.96784	0.96856	0.96926	0.96995	0.97062

(*Continued*)

z	**0.00**	**0.01**	**0.02**	**0.03**	**0.04**	**0.05**	**0.06**	**0.07**	**0.08**	**0.09**
1.9	0.97128	0.97193	0.97257	0.97320	0.97381	0.97441	0.97500	0.97558	0.97615	0.97670
2.0	0.97725	0.97778	0.97831	0.97882	0.97932	0.97982	0.98030	0.98077	0.98124	0.98169
2.1	0.98214	0.98257	0.98300	0.98341	0.98382	0.98422	0.98461	0.98500	0.98537	0.98574
2.2	0.98610	0.98645	0.98679	0.98713	0.98745	0.98778	0.98809	0.98840	0.98870	0.98899
2.3	0.98928	0.98956	0.98983	$0.9^{2}0097$	$0.9^{2}0358$	$0.9^{2}0613$	$0.9^{2}0863$	$0.9^{2}1106$	$0.9^{2}1344$	$0.9^{2}1576$
2.4	$0.9^{2}1802$	$0.9^{2}2024$	$0.9^{2}2240$	$0.9^{2}2451$	$0.9^{2}2656$	$0.9^{2}2857$	$0.9^{2}3053$	$0.9^{2}3244$	$0.9^{2}3431$	$0.9^{2}3613$
2.5	$0.9^{2}3790$	$0.9^{2}3963$	$0.9^{2}4132$	$0.9^{2}4297$	$0.9^{2}4457$	$0.9^{2}4614$	$0.9^{2}4766$	$0.9^{2}4915$	$0.0^{2}5060$	$0.0^{2}5201$
2.6	$0.9^{2}5339$	$0.9^{2}5473$	$0.9^{2}5604$	$0.9^{2}5731$	$0.9^{2}5855$	$0.9^{2}5975$	$0.9^{2}6093$	$0.9^{2}6207$	$0.0^{2}6319$	$0.0^{2}6427$
2.7	$0.9^{2}6533$	$0.9^{2}6636$	$0.9^{2}6736$	$0.9^{2}6833$	$0.9^{2}6928$	$0.9^{2}7020$	$0.9^{2}7110$	$0.9^{2}7197$	$0.0^{2}7282$	$0.0^{2}7365$
2.8	$0.9^{2}7445$	$0.9^{2}7523$	$0.9^{2}7599$	$0.9^{2}7673$	$0.9^{2}7744$	$0.9^{2}7814$	$0.9^{2}7882$	$0.9^{2}7948$	$0.0^{2}8012$	$0.0^{2}8074$
2.9	$0.9^{2}8134$	$0.9^{2}8193$	$0.9^{2}8250$	$0.9^{2}8305$	$0.9^{2}8359$	$0.9^{2}8411$	$0.9^{2}8462$	$0.0^{2}8511$	$0.0^{2}8559$	$0.0^{2}8605$
30	$0.9^{2}8650$	$0.9^{2}8694$	$0.9^{2}8736$	$0.9^{2}8777$	$0.9^{2}8817$	$0.9^{2}8856$	$0.9^{2}8893$	$0.9^{2}8930$	$0.9^{2}8965$	$0.9^{2}8999$
3.1	$0.9^{3}0324$	$0.9^{3}0646$	$0.9^{3}0957$	$0.9^{3}1260$	$0.9^{3}1553$	$0.9^{3}1836$	$0.9^{3}2112$	$0.9^{3}2378$	$0.9^{3}2636$	$0.9^{3}2886$
3.2	$0.9^{3}3129$	$0.9^{3}3363$	$0.9^{3}3590$	$0.9^{3}3810$	$0.9^{3}4024$	$0.9^{3}4230$	$0.9^{3}4429$	$0.9^{3}4623$	$0.9^{3}4810$	$0.9^{3}4991$
3.3	$0.9^{3}5166$	$0.9^{3}5335$	$0.9^{3}5499$	$0.9^{3}5658$	$0.9^{3}5811$	$0.9^{3}5959$	$0.9^{3}6103$	$0.9^{3}6242$	$0.9^{3}6376$	$0.9^{3}6505$
3.4	$0.9^{3}6631$	$0.9^{3}6752$	$0.9^{3}6869$	$0.9^{3}6982$	$0.9^{3}7091$	$0.9^{3}7197$	$0.9^{3}7299$	$0.9^{3}7398$	$0.9^{3}7493$	$0.9^{3}7585$
3.5	$0.9^{3}7674$	$0.9^{3}7759$	$0.9^{3}7842$	$0.9^{3}7922$	$0.9^{3}7999$	$0.9^{3}8074$	$0.9^{3}8146$	$0.9^{3}8215$	$0.9^{3}8282$	$0.9^{3}8347$
3.6	$0.9^{3}8409$	$0.9^{3}8469$	$0.9^{3}8527$	$0.9^{3}8583$	$0.9^{3}8637$	$0.9^{3}8689$	$0.9^{3}8739$	$0.9^{3}8787$	$0.9^{3}8834$	$0.9^{3}8879$
3.7	$0.9^{3}8922$	$0.9^{3}8964$	$0.9^{4}0039$	$0.9^{4}0426$	$0.9^{4}0799$	$0.9^{4}1158$	$0.9^{4}1504$	$0.9^{4}1838$	$0.9^{4}2159$	$0.9^{4}2468$
3.8	$0.9^{4}2765$	$0.9^{4}3052$	$0.9^{4}3327$	$0.9^{4}3593$	$0.9^{4}3848$	$0.9^{4}4094$	$0.9^{4}4331$	$0.9^{4}4558$	$0.9^{4}4777$	$0.9^{4}4988$
3.9	$0.9^{4}5190$	$0.9^{4}5385$	$0.9^{4}5573$	$0.9^{4}5753$	$0.9^{4}5926$	$0.9^{4}6092$	$0.9^{4}6253$	$0.9^{4}6406$	$0.9^{4}6554$	$0.9^{4}6696$
4.0	$0.9^{4}6833$	$0.9^{4}6964$	$0.9^{4}7090$	$0.9^{4}7211$	$0.9^{4}7327$	$0.9^{4}7439$	$0.9^{4}7546$	$0.9^{4}7649$	$0.9^{4}7748$	$0.9^{4}7843$
4.1	$0.9^{4}7934$	$0.9^{4}8022$	$0.9^{4}8106$	$0.9^{4}8186$	$0.9^{4}8263$	$0.9^{4}8338$	$0.9^{4}8409$	$0.9^{4}8477$	$0.9^{4}8542$	$0.9^{4}8605$
4.2	$0.9^{4}8665$	$0.9^{4}8723$	$0.9^{4}8778$	$0.9^{4}8832$	$0.9^{4}8882$	$0.9^{4}8931$	$0.9^{4}8978$	$0.9^{5}0226$	$0.9^{5}0655$	$0.9^{5}1066$
4.3	$0.9^{5}1460$	$0.9^{5}1837$	$0.9^{5}2199$	$0.9^{5}2545$	$0.9^{5}2876$	$0.9^{5}3193$	$0.9^{5}3497$	$0.9^{5}3788$	$0.9^{5}4066$	$0.9^{5}4332$
4.4	$0.9^{5}4587$	$0.9^{5}4831$	$0.9^{5}5065$	$0.9^{5}5288$	$0.9^{5}5502$	$0.9^{5}5706$	$0.9^{5}5902$	$0.9^{5}6089$	$0.9^{5}6268$	$0.9^{5}6439$
4.5	$0.9^{5}6602$	$0.9^{5}6759$	$0.9^{5}6908$	$0.9^{5}7051$	$0.9^{5}7187$	$0.9^{5}7318$	$0.9^{5}7442$	$0.9^{5}7561$	$0.9^{5}7675$	$0.9^{5}7784$
4.6	$0.9^{5}7888$	$0.9^{5}7987$	$0.9^{5}8081$	$0.9^{5}8172$	$0.9^{5}8258$	$0.9^{5}8340$	$0.9^{5}8419$	$0.9^{5}8494$	$0.9^{5}8566$	$0.9^{5}8634$
4.7	$0.9^{5}8699$	$0.9^{5}8761$	$0.9^{5}8821$	$0.9^{5}8877$	$0.9^{5}8931$	$0.9^{5}8983$	$0.9^{5}0320$	$0.9^{6}0789$	$0.9^{6}1235$	$0.9^{6}1661$
4.8	$0.9^{6}2067$	$0.9^{6}2453$	$0.9^{6}2822$	$0.9^{6}3173$	$0.9^{6}3508$	$0.9^{6}3827$	$0.9^{6}4131$	$0.9^{6}4420$	$0.9^{6}4696$	$0.9^{6}4958$
4.9	$0.9^{5}5208$	$0.9^{5}5446$	$0.9^{5}5673$	$0.9^{5}5889$	$0.9^{5}6094$	$0.9^{5}6289$	$0.9^{5}6475$	$0.9^{5}6652$	$0.9^{5}6821$	$0.9^{5}6981$

Source: A. Hald, Statistical Tables and Formulas, Wiley, New York, 1952. Table II. Reproduced by permission.

Appendix D

Nonparametric Methods and Probability Plotting

D.1 Introduction

Reliability engineering relies on explaining and predicting results based on a set of data. A set of reliability data will almost always be a sample (in the case of failures) of varying sizes, along with a usually larger set of unfailed units, whose times must be included if available.

As we remember from elementary statistics, if we are told that data are from a normal distribution (see Chapter 4 for a refresher), the distribution is described with the mean (μ) and standard deviation (σ).

Probability plotting has the advantage of providing both parameter estimates and a visual representation of how well the distribution describes the data.

Another example of "A picture is worth a thousand words."

In the usual case, however, we will be presented with the actual data. If the data is failure data, e.g. lab test, test stand tests, field failures, we need to first decide what distribution will fit the data. Is it normally distributed, Weibull, lognormal, or something else?

If you have no previous history with regard to the failure mode on previous systems, or if this is a new failure mode you have not seen before, you need to use "nonparametric methods" to look at the data first.

D.2 Nonparametric Methods for Probability Plotting

Nonparametric methods allow us to gain perspective as to the nature of the distribution from which data has been drawn without selecting one particular distribution. When there is a sufficient number of data points, the representation of the distribution by a histogram or with sample statistics can be quite helpful. In many situations, however, the amount of data is insufficient to construct a realistic histogram. It is then useful to approximate the cumulative distribution function (CDF) by the technique plotting the median rank – a term that is defined below.

Boxplots and Histograms

Boxplot

Looking at a set of (new) data as in Table D.1, one of the first things to do might be a boxplot. A boxplot (sometimes called a "box and whisker" plot), will give you an overall view of the data and point out any unusually high or low datapoints (see Figure D.1a).

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

Table D.1 Data are the cycles to failure of aluminum test coupons.

A	B	C	D	E	F	G
1115	865	1015	885	1594	1000	1416
1310	2130	845	1223	2023	1820	1560
1540	1421	1674	375	1315	1940	1055
1502	1109	1016	2265	1269	1120	1764
1258	1481	1102	1910	1260	910	1330
1315	1567	1605	1018	1888	1730	1608
1085	1883	706	1452	1782	1102	1535
798	1203	2215	1890	1522	1578	1781
1020	1270	785	2100	1792	758	1750
1501	1238	990	1468	1512	1750	1642

Source: Data from Montgomery & Runger (2011).

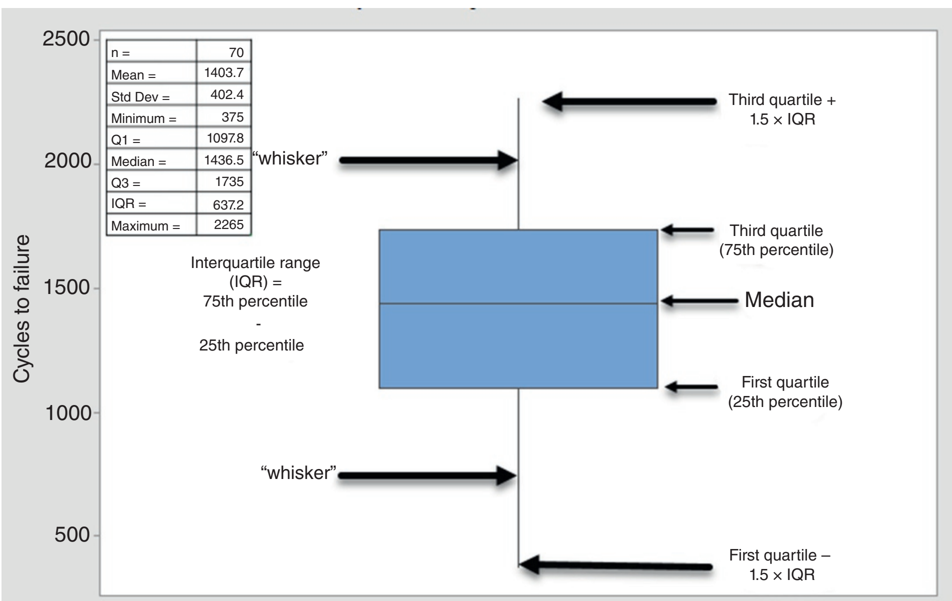


Figure D.1a Boxplot of cycles to failure of aluminum test coupons.

The boxplot of this data shows that the distributions of these 70 cycles to failure are approximately symmetrical around the median. The maximum = third quartile + 1.5 × IQR, and the minimum = first quartile − 1.5 × IQR. Since no points lie above or below those, there are no unusual points in the dataset (some books use the word "outlier" for points that are above the third quartile + 1.5 × IQR, and less than the first quartile − 1.5 × IQR). In short, the boxplot gives you a "5000-foot" view of your data.

Histogram

Histograms have been used in data analysis since Pearson (1895) first described them.

The purpose of a histogram is to assess the probability distribution of a given set of data by depicting the frequencies of occurrence in a certain range or interval of values by breaking down the data in a "bars" of data between the smallest and largest values in the data.

MINITAB® histograms in Figure D.1b illustrate what the Aluminum cycles to failure data may look like if you choose several different intervals between the smallest and the largest.

The MINITAB plots in Figure D.2 illustrate the cycles to failure data from Table D.1 data using the statistically best interval size as well as fitting a normal "bell shape" to the histogram in Figure D.2. Most statistical software will use the "best" number of intervals when producing a histogram.

The normal "bell-shaped " curve does not seem to fit well. As mentioned in Chapters 4 and 5, the Weibull and lognormal are the 1–2 choices for failure distributions. More about this will be discussed later.

Example D.1 Calculate the mean, variance, range, skewness, and kurtosis of the Aluminum test coupon data given in Table D.1

Solution:

These four quantities are commonly included as spread-sheet formulae. The data in Table D.1 are already in spread-sheet format. Using Excel™, we simply calculate the four sample quantities with the standard formulae as follows:

$$\begin{aligned}
&\text{Mean}: && \hat{\mu} = \text{AVERAGE}\,(\text{A1}:\text{G10}) = 1403.7 \\
&\text{Variance}: && \hat{\sigma}^2 = \text{VAR}\,(\text{A1}:\text{G10}) \quad = 161913.9 \\
&\text{Skewness}: && \widehat{s_k} = \text{SKEW}\,(\text{A1}:\text{G10}) \quad = -0.03 \\
&\text{Kurtosis}: && \widehat{k_u} = \text{KURT}(\text{A1}:\text{G10}) \quad = -0.44
\end{aligned}$$

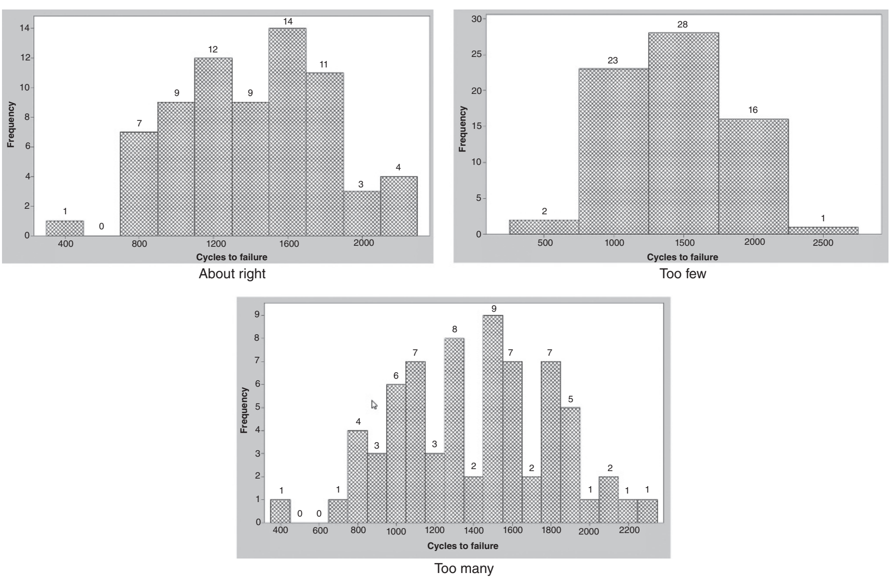


Figure D.1b Effect of the number of intervals chosen on the shape of data.

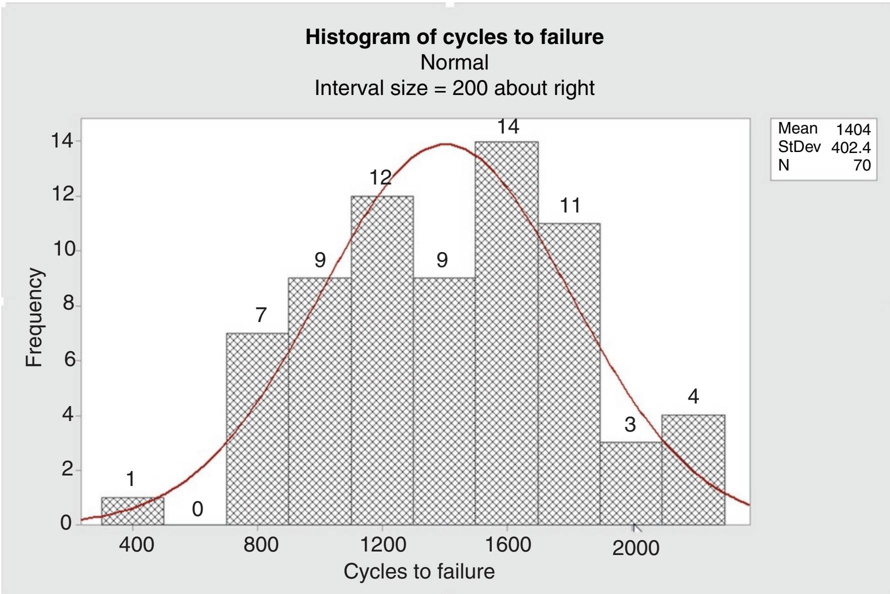


Figure D.2 MINITAB histogram of aluminum test coupon cycles to failure with normal distribution fit.

Note that in applying the formulae to data in Table D.1, all the data in the rectangle with column A row 1 on the upper left and column G row 10 on the lower right are included.

Rank Statistics

Often, the number of data points is too small to construct a histogram with enough resolution to be helpful. Such situations occur frequently in reliability engineering, particularly when an expensive piece of equipment must be tested to failure for each data point. Under such circumstances, rank statistics provide a powerful graphical technique for viewing the cumulative distribution function (i.e. the CDF). They also serve as a basis for the probability plotting taken up in the following section.

To employ this technique, we first take the samplings of the random variable and rank them; that is, list them in ascending order. We then approximate the CDF at each value of x_i. With a large number N of data points, the CDF could reasonably be approximated by

$$\hat{F}(x_i) = \frac{i}{N}, \quad i = 1, 2, 3, \ldots, N \tag{D.1}$$

where $F(0) = 0$ if the variable is defined only for $x > 0$.

If N is not a large number, say less than 15 or 20, there are some shortcomings in using Eq. (D.1). In particular, we find that $F(x) = 1$ for values of x greater than x_N. If a much larger set of data were obtained, say $10N$ values, it is highly likely that several of the samples would have larger values than x_N. Therefore, Eq. (D.1) may seriously overestimate $F(x)$. The estimate is improved by arguing that if a very large sample were to be obtained, roughly equal numbers of events would occur in each of the intervals between the x_i, and the number of samples larger than x_N would probably be about equal to the number within one interval. From this argument, we may estimate the CDF as

$$\hat{F}(x_i) = \frac{i}{N+1}, \quad i = 1, 2, 3, \ldots, N \tag{D.2}$$

This quantity can be derived from more rigorously statistical arguments; it is known in the statistical literature as the *mean rank*. Other statistical arguments may be used to obtain slightly different approximations for $F(x)$. One of the more widely used is the *median rank* or

$$\hat{F}(x_i) = \frac{i - 0.3}{N + 0.4}, \quad i = 1, 2, 3, \ldots, N \tag{D.3}$$

In practice, the randomness and limited amounts of data introduce more uncertainty than the particular form that is used to estimate F. For large values of N, they yield nearly identical results for $F(x)$ after the first few samples. For the most part, using Eq. (D.3) is a reasonable compromise between computational ease and accuracy.

Example D.2 The following are the times to failure for 14, 6-volt flashlight bulbs operated at 12.6 volts to accelerate the rate the failure: 72, 82, 97, 103, 113, 117, 126, 127, 127, 139, 154, 159, 199, and 207 minutes. Make a plot of $F(t)$, where t is the time to failure.

Solution:
Table D.2 contains the necessary calculations. Each of the aforementioned ranking equations (D.1, D.2, and D.3) are used in order to compare the results.

The combined scatterplot of $F(t)$ for each of the ranks (Figure D.3) shows what was noted earlier that the differences in ranking equation are not significant when compared to each other.

D.3 Parametric Methods

If we know what distribution best describes the data:

1) We can describe the data based on two (or three) parameters; e.g. normal (μ, σ), Weibull (β, η) or (β, η, t_0), lognormal.
2) We can then *extrapolate* to find the (say 1/1000) probability of failure of a part or the chances of a remote event such as an earthquake over 7.0 on the Richter scale.
3) We can then find confidence bounds on the parameters and compare the current set of data to another (Base A vs Base B, or Vendor A vs Vendor B, Airplane A vs Airplane B, etc.)
4) In terms of reliability/safety, we can better predict the future occurrences of the failure mode and put it in terms of safety implications.
5) The distributional parameters can lead to the knowledge of the type of failure mode we are observing.

So, with relatively small sample sizes it yields estimates of the distribution parameters and provides both a graphical picture and a quantitative estimate of how well the distribution fits the data. It can be used with success whether the sample sizes are small or large, particularly in this age of computer speed and large memory sizes.

Basically, the method consists of transforming the equation for the CDF to a form that can be plotted as

$$y = ax + b. \tag{D.4}$$

Table D.2 Spreadsheet for Weibull probability plot of flashlight bulb data in Example D.2.

Row	A	B (t)	C (i/N)	D ($i/(N+1)$)	E ($(i-0.3)/(N+0.4)$)	F LN (t)	G using C	H using D	I using E
2	1	72	0.07142857	0.066666667	0.048611111	4.2767	−2.602232166	−2.673752092	−2.999090431
3	2	82	0.14285714	0.133333333	0.118055556	4.4067	−1.869824714	−1.944205697	−2.074444344
4	3	97	0.21428571	0.2	0.1875	4.5747	−1.422286137	−1.499939987	−1.571952527
5	4	103	0.28571429	0.266666667	0.256944444	4.6347	−1.08923964	−1.170683338	−1.214075448
6	5	113	0.35714286	0.333333333	0.326388889	4.7274	−0.816823857	−0.902720456	−0.928610507
7	6	117	0.42857143	0.4	0.395833333	4.7622	−0.580504824	−0.671726992	−0.685367162
8	7	126	0.5	0.466666667	0.465277778	4.8363	−0.366512921	−0.464246379	−0.468392324
9	8	127	0.57142857	0.533333333	0.534722222	4.8442	−0.165702981	−0.271624945	−0.267721706
10	9	127	0.64285714	0.6	0.604166667	4.8442	0.029189236	−0.087421572	−0.076058454
11	10	139	0.71428571	0.666666667	0.673611111	4.9345	0.225351487	0.094047828	0.113030157
12	11	154	0.78571429	0.733333333	0.743055556	5.037	0.432071362	0.278961034	0.306672154
13	12	159	0.85714286	0.8	0.8125	5.0689	0.665729811	0.475884995	0.515201894
14	13	199	0.92857143	0.866666667	0.881944444	5.2933	0.970421781	0.700571065	0.75921576
15	14	207	1	0.933333333	0.951388889	5.3327	(Division by 0) so set = 1	0.996228893	1.106548431

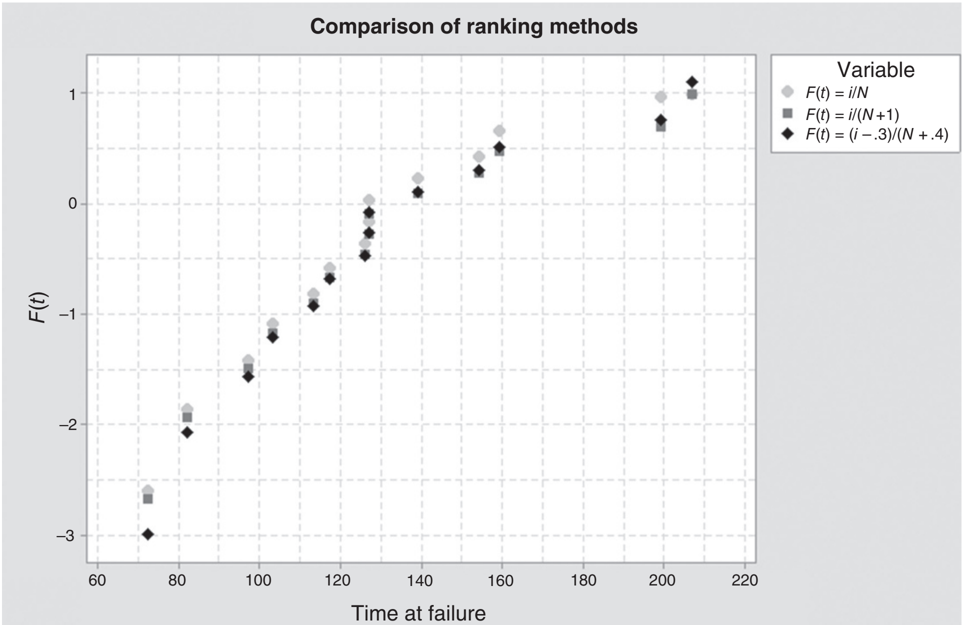


Figure D.3 Comparison of the three ranking methods.

The "median rank" is used to estimate the CDF at each data point in the resulting nonlinear plot. A straight line is then constructed through the data, and the distribution parameters are determined in terms of the slope and intercept.

$$\hat{F}(t_i) = \frac{i - 0.3}{N + 0.4}, \quad i = 1, 2, 3, \ldots, N \text{ datapoints} \tag{D.5}$$

Example D.3 Exponential Distribution

The procedure is best illustrated with a simple example. PROSCHAN (1963) reported on the times between failures of the air-conditioning equipment in 10 Boeing 720 aircraft. Suppose that we want to fit the exponential distribution to Aircraft 7 of these times between air-conditioning failure t_i:

$$F(t) = 1 - e^{-\lambda t}, \quad 0 \le t \le \infty$$

We can rearrange this equation by first solving for $1/(1 - F)$ and then taking the natural logarithm to obtain

$$\text{Ln}\left[\frac{1}{1 - F(t)}\right] = \lambda\, t \tag{D.6}$$

We can approximate $F(x_i)$ using the Median rank equation (D.2) and plot the resulting on semi-log paper versus the corresponding x_i.

The data should fall roughly along a straight line if they were obtained by sampling an exponential distribution. Comparing Eqs. (D.4) and (D.6), we see that $\lambda = a$ can be estimated from the slope of the line. More simply, we note that the left side of Eq. (D.6) is equal to 1 when $1/(1 - F) = e =$

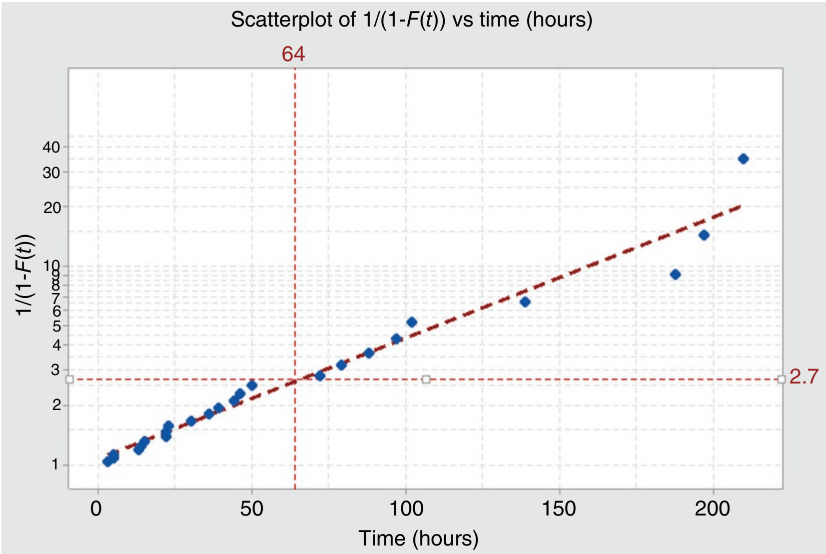


Figure D.4 Graphical estimate of the failure time cumulative distribution.

2.72, and thus at that point $\lambda = t$. Since the exponential is a one-parameter distribution, b, the y intercept is not utilized.

The plot in Figure D.4 is difficult to use since the y-axis is not in cumulative probability. The same data can be used to produce a true probability plot in MINITAB, again assuming that the exponential distribution fits the times (t) in Table D.3.The y-axis of the plot in Figure D.5 is cumulative probability, which can be read directly.

Weibull Distribution Plotting

Weibull plots based on ranked regression use the methodology described in this section. Weibull plots based on maximum likelihood estimated β and η use the same plotting positions as the ranked regression Weibull, but the best fit line is based on the MLE β and η.

"The Weibull plot method" (rank regression) uses Weibull paper to illustrate how well the estimated β and η fits the data. This method uses regression analysis (line fitting) to calculate the Weibull parameters β and η.

What makes the Weibull plot method work is a bit of algebraic manipulation of the Weibull CDF: The CDF with respect to time is given by

$$F(t) = 1 - \exp\left[-(t/\eta)^{\beta}\right], \quad 0 \leq t \leq \infty \tag{D.7}$$

The distribution is put in a form for probability plotting by first solving for $1/(1 - F)$,

$$\frac{1}{1 - F(t)} = \exp\,(t/\eta)^{\beta} \tag{D.8}$$

Table D.3 Spreadsheet for exponential probability plot of air-conditioning data.

A	B	C	D
i	t (time in hours)	$F(t) = (i - 0.3)/(N + 0.4)$	$1/(1 - F(t))$
1	3	0.0287	1.029535865
2	5	0.0697	1.074889868
3	5	0.1107	1.124423963
4	13	0.1516	1.178743961
5	14	0.1926	1.23857868
6	15	0.2336	1.304812834
7	22	0.2746	1.378531073
8	22	0.3156	1.461077844
9	23	0.3566	1.554140127
10	30	0.3975	1.659863946
11	36	0.4385	1.781021898
12	39	0.4795	1.921259843
13	44	0.5205	2.085470085
14	46	0.5615	2.280373832
15	50	0.6025	2.515463918
16	72	0.6434	2.804597701
17	79	0.6844	3.168831169
18	88	0.7254	3.641791045
19	97	0.7664	4.280701754
20	102	0.8074	5.191489362
21	139	0.8484	6.594594595
22	188	0.8893	9.037037037
23	197	0.9303	14.35294118
24	210	0.9713	34.85714286

and then taking the logarithm twice to obtain

$$\ln\ln\left[\frac{1}{1-F(t)}\right] = \beta \ln t - \beta \ln \eta \tag{D.9}$$

This can be cast into the form of Eq. (D.1) if we define

$$y = \ln \ln \left[\frac{1}{1-F(t)}\right] \tag{D.10}$$

and

$$x = \ln t \tag{D.11}$$

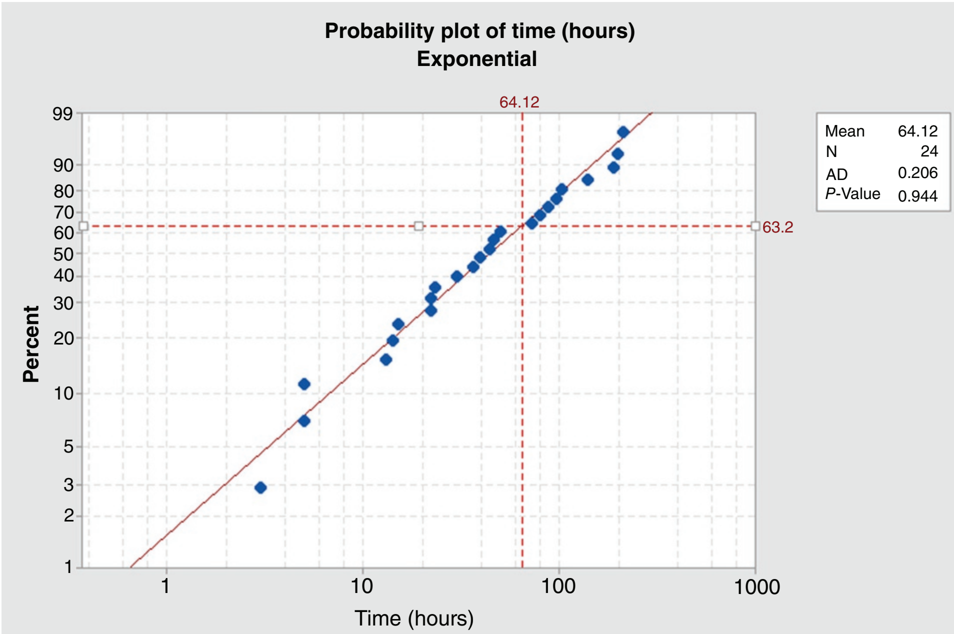


Figure D.5 MINITAB exponential probability plot of air-conditioner failure data.

We find that the shape parameter is equal to the slope

$$\beta = a \tag{D.12}$$

whereas the scale parameter is estimated in terms of the slope and the intercept by

$$\hat{\eta} = \exp\left(-b/a\right) \tag{D.13}$$

The procedure is best illustrated by providing a detailed solution of an example problem

Example D.4 Use probability plotting to fit the flashlight bulb failure times given in Table D.4 to a two-parameter Weibull distribution. What are the shape and scale parameters?

Solution:
The ranks of the failures, the failure times, and the estimates of $F(t_i)$ are already given in columns A, B, and C of Table D.5.

In column D, we tabulate $\ln(t_i)$, and in column E, $\ln(\ln(l/(1-F)))$. Then, we plot column E versus column D and calculate a, b, and r^2. The results are shown in Figure D.6. Since $a = 3.71$ and $b = -18.46$, we have from Eqs. (D.12) and (D.13): $\beta = 3.71$ and $\eta = \exp(+18.46/3.71) = 145$ minutes. A MINITAB Weibull probability plot is presented in Figure D.7. Once again, the plot can be read directly since the scales are transformed.

Table D.4 Flash bulb lab failures in flashes.

72	82	97	103	113
117	126	127	127	139
154	159	199	207	

Table D.5 Spreadsheet for Weibull probability plot of flashlight bulb data.

A	B	C	D	E
i	t	$F(t) = (i - 0.3)/(N + 0.4)$	$x = \text{LN}(t)$	$y = \text{LN}(\text{LN}(1/(1 - F)))$
1	72	0.0486	4.2767	−2.999090431
2	82	0.1181	4.4067	−2.074444344
3	97	0.1875	4.5747	−1.571952527
4	103	0.2569	4.6347	−1.214075448
5	113	0.3264	4.7274	−0.928610507
6	117	0.3958	4.7622	−0.685367162
7	126	0.4653	4.8363	−0.468392324
8	127	0.5347	4.8442	−0.267721706
9	127	0.6042	4.8442	−0.076058454
10	139	0.6736	4.9345	0.113030157
11	154	0.7431	5.037	0.306672154
12	159	0.8125	5.0689	0.515201894
13	199	0.8819	5.2933	0.75921576
14	207	0.9514	5.3327	1.106548431

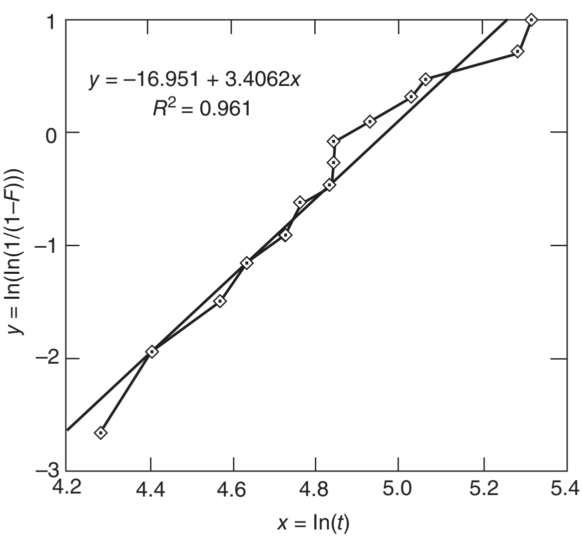


Figure D.6 Weibull scatterplot of flash bulb failure data.

Extreme-Value Distribution Plotting

The procedure for treating extreme-value distributions is quite similar to that employed for Weibull distributions. For example, with the smallest extreme-value distribution, the CDF is given by

$$F(x) = 1 - \exp\left[-e^{(x-\mu)/\Theta}\right], \quad -\infty < x < \infty \tag{D.14}$$

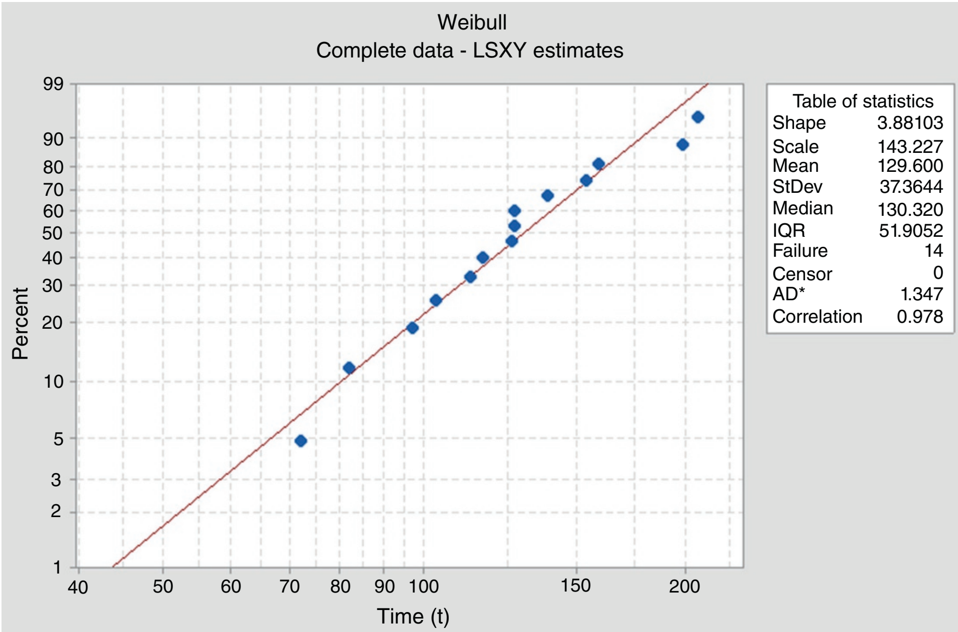


Figure D.7 Weibull probability plot of flash bulb failure data.

If we solve for $1/(1-F)$, and take the natural logarithm twice, we obtain

$$\ln\ \ln\left[\frac{1}{1-F(x)}\right] = \frac{1}{\Theta}x - \frac{\mu}{\Theta} \tag{D.15}$$

Thus, we can make a linear plot with

$$y = \ln\ \ln\left[\frac{1}{1-F(x)}\right] \tag{D.16}$$

The scale parameter is estimated in terms of the slope as

$$\hat{\Theta} = 1/a \tag{D.17}$$

and the location parameter as

$$\hat{\mu} = -b/a \tag{D.18}$$

respectively. Likewise, for the largest extreme-value CDF, given by

$$F(x) = \exp\left[-e^{(x-\mu)/\Theta}\right], \quad -\infty < x < \infty \tag{D.19}$$

an analogous procedure can be used to determine the rectified equation

$$\ln\ \ln\left[\frac{1}{F(x)}\right] = -\frac{1}{\Theta}x + \frac{\mu}{\Theta} \tag{D.20}$$

where the distribution parameters may be estimated in terms of the slope and intercept to be

$$\hat{\Theta} = -1/a \tag{D.21}$$

and

$$\hat{\mu} = -b/a. \tag{D.22}$$

Example D.5 Determine whether the failure data in Example D.4 can be fitted more accurately with a minimum extreme-value distribution than with a Weibull distribution. Estimate the parameters in each case. Employ spread-sheet slope, intercept, and R-squared formulae.

Solution:
The necessary values of y_i and x_i, respectively, are already tabulated in Table D.5, columns E and B, for the minimum extreme-value distribution, and in columns E and D for the Weibull distribution. Thus, for the extreme-value distribution, using Excel™, we obtain

$$r^2 = \text{RSQ}(\text{E2 : E15, B2 : B15}) = 0.87$$
$$a = \text{SLOPE}(\text{E2 : E15, B2 : B15}) = 0.027$$
$$b = \text{INTERCEPT}(\text{E2 : E15, B2 : B15}) = -4.07$$

Thus, from Eqs. (D.17) and (D.18), the extreme-value parameters are

$$\hat{\Theta} = 1/a = 1/a = 36.8 \text{ minutes}, \quad \text{and } \hat{\mu} = -b/a = 4.07/0.027 = 149.8 \text{ minutes}$$

For the Weibull distribution

$$r^2 = \text{RSQ}(\text{E2 : E15, D2 : D15}) = 0.96$$
$$b = \text{INTERCEPT}(\text{E2 : E15, D2 : D15}) = -18.46$$
$$a = \text{SLOPE}(\text{E2 : E15}, D5 : \text{D15}) \ = 3.71$$

Not surprisingly, these are the same values exhibited in Figure D.3. From Eqs. (D.12) and (D.13), the Weibull parameters are $\beta = a = 3.71$; $\eta = \exp(-b/a) = \exp(18.46/3.71) = 144$ minutes. The resulting value of $r^2 = 0.87$ for the extreme-value distribution is substantially smaller than that of 0.96 obtained with the Weibull distribution. Therefore, the extreme-value fit is poorer.

Note that in comparing the smallest extreme-value probability plot (Figure D.8) with the Weibull plot (Figure D.7), the Weibull plot "looks" better! That is, your "eyeball" is a good discerner of fit.

Lognormal Distribution Plotting

Probability plotting with the normal and lognormal distributions is very similar. From Eq. (4.69), we may write the CDF for the lognormal distribution as

$$F(t) = \Phi\left[\frac{1}{\omega}\ln(t/t_0)\right] \tag{D.23}$$

We invert the standard normal distribution to obtain

$$\Phi^{-1}(F) = \frac{1}{\omega}\ln t - \frac{1}{\omega}\ln t_0 \tag{D.24}$$

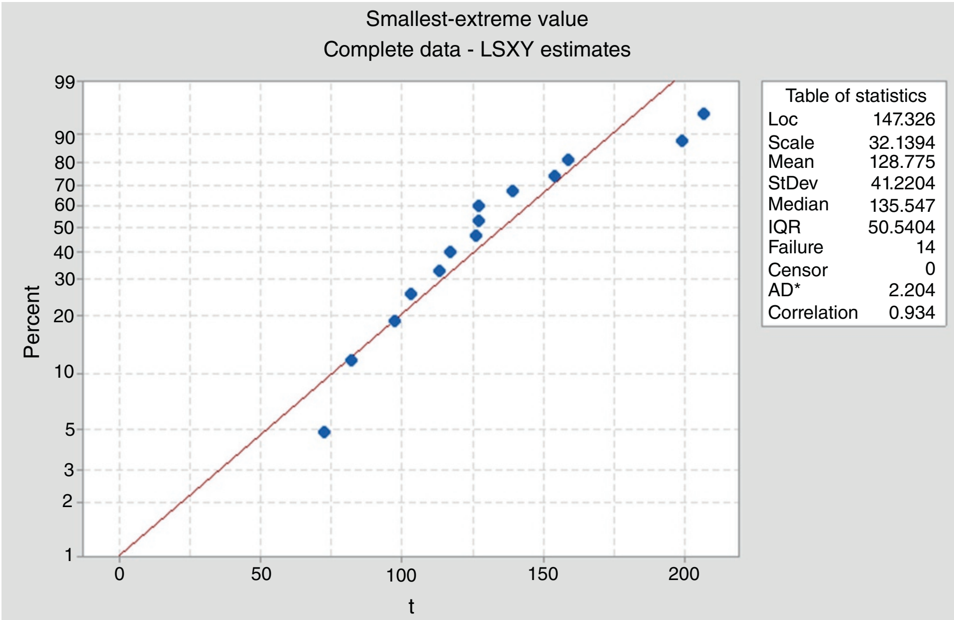


Figure D.8 Smallest extreme probability plot of flash bulb data.

The required linear equation is obtained by once again taking

$$y = \Phi^{-1}(F) \tag{D.25}$$

but with $x = \ln t$. The estimates for the lognormal parameters are

$$\hat{\omega} = 1/a \tag{D.26}$$

and

$$\hat{t}_0 = \exp(-b/a) \tag{D.27}$$

Example D.7 The fatigue lives of 20 specimens, measured in thousands of stress cycles, are found in Table D.6.

Use probability plotting to fit a lognormal distribution to the data and estimate the parameters and the goodness of fit.

Solution:

The calculations are made in Table D.6.

The data rank and the failure times are tabulated in columns A and B, and the natural logarithms of the failure times are tabulated in column C. In column D, the estimates of $F(x_i) = i/(N+1)$ are tabulated. In column E, we tabulate $y_i = \Phi^{-1}(F_i)$ from Eq. (D.27). In Figure D.9, we have plotted column E versus column C and used least-squares fit to obtain the best straight line through the data. From Eqs. (D.26) and (D.27), we find the parameters to be $\hat{\omega} = 1/a = 1/1.01 = 0.99$ and $\hat{t}_0 = \exp(-b/a) = \exp(3.22/1.01) = 24.2$ thousand cycles.(Note that this is the median of the distribution – Using Eq. (4.59), the mean of the lognormal data is 39.7 KSI.)

The corresponding MINITAB Lognormal Probability is in Figure D.10. The fit is quite good with $r^2 = (0.966)^2 = 0.933$.

Table D.6 Spreadsheet for normal probability plot of resistor data in Example D.6.

A	B	C	D	E
i	x_i (#1)	x_i (#2)	$F(x_i)$	y_i
1	48.47	47.67	0.0323	−1.85
2	48.49	47.7	0.0645	−1.52
3	48.66	48	0.0968	−1.3
4	48.84	48.41	0.129	−1.13
5	49.14	48.42	0.1613	−0.99
6	49.27	48.44	0.1935	−0.86
7	49.29	48.64	0.2258	−0.75
8	49.3	48.65	0.2581	−0.65
9	49.32	48.68	0.2903	−0.55
10	49.39	48.85	0.3226	−0.46
11	49.43	49.17	0.3548	−0.37
12	49.49	49.72	0.3871	−0.29
13	49.52	49.85	0.4194	−0.2
14	49.54	49.87	0.4516	−0.12
15	49.69	50.07	0.4839	−0.04
16	49.75	50.75	0.5161	0.04
17	49.78	50.6	0.5484	0.12
18	49.93	50.63	0.5806	0.2
19	49.96	50.9	0.6129	0.29
20	50.03	51.02	0.6452	0.37
21	50.06	51.05	0.6774	0.46
22	50.07	51.28	0.7097	0.55
23	50.09	51.33	0.7419	0.65
24	50.42	51.38	0.7742	0.75
25	50.44	51.43	0.8065	0.86
26	50.57	51.6	0.8387	0.99
27	50.7	51.7	0.871	1.13
28	50.77	51.74	0.9032	1.3
29	50.87	52.06	0.9355	1.52
30	51.87	52.33	0.9677	1.85

D.4 Goodness of Fit

The forgoing examples illustrate some of the uses of probability plotting in the analysis of quality and reliability data. They also serve as a basis for the extensive use of these methods made in Chapter 8 for the analysis of failure data. With the computations carried out quite simply on a

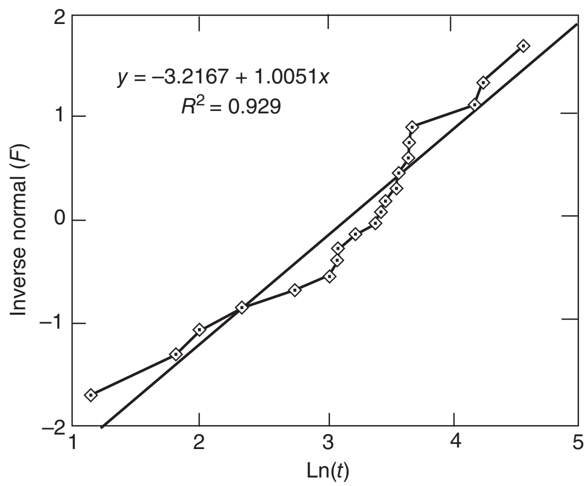


Figure D.9 Lognormal scatterplot of failure times.

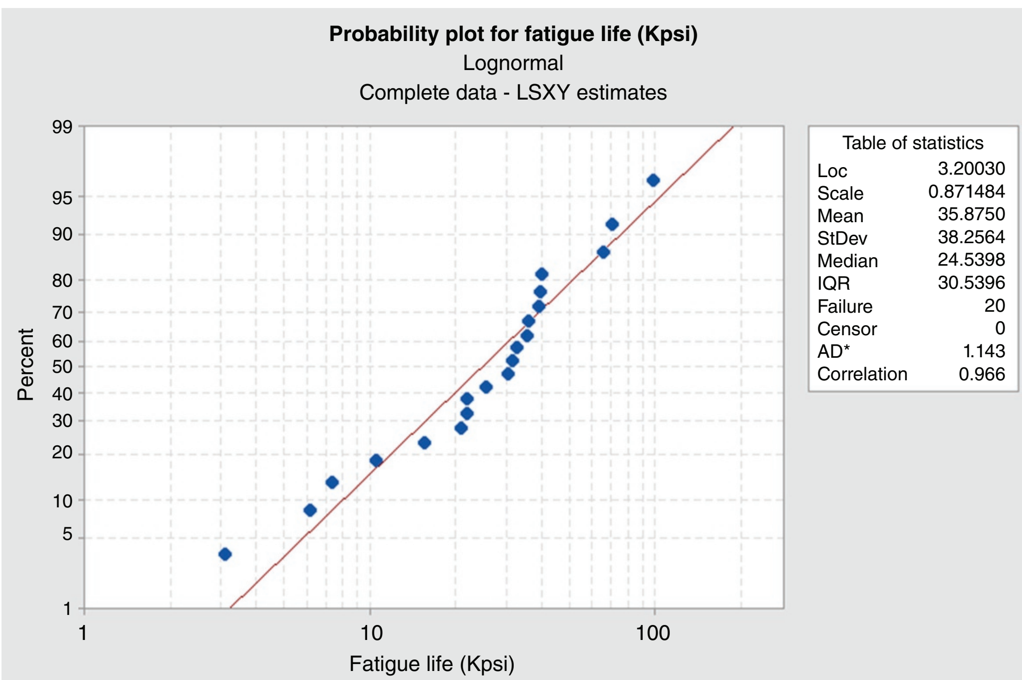


Figure D.10 MINITAB lognormal probability plot of failure times.

spread sheet or other software, one is not limited to a single analysis. Frequently, it may be advisable to try to fit more than one distribution to the data to determine the best fit. Comparison of the values of r^2 is the most objective criterion for this purpose. Other valuable information is obtained from visual inspection of the graph. Outliers may be eliminated, and if the data tends to fall along a curve instead of a straight line it may provide a clue as to what other distribution should be tried.

For example, if normally distributed data is used to make an exponential probability plot, the data will fall along a curve that is concave upward. With some experience, such visual patterns become recognizable, allowing one to estimate which other distribution may be more appropriate.

More formal methods for assessing the goodness of fit exist. These establish a quantitative measure of confidence that the data may be fit to a particular distribution. The most accessible of these are the chi-squared test, which is applicable when enough data is available to construct a histogram, and the Kolmogorov–Smirnov (or K-S) test, which is applicable to ungrouped data. These tests are presented in elementary statistics texts but are not directly applicable to the analysis of much reliability data. In their standard form they assume not only that a distribution has been chosen, but that the parameters are known; they establish only the level of confidence to which a specific distribution with known parameters fits a given set of data. In contrast, in probability plotting, we are attempting both to estimate distribution parameters *and* establish how well the data fit the resulting distribution.

Aside from the simple comparison of r^2 values obtained from probability plotting, establishing goodness of fit from estimated parameters requires the use of more advanced maximum likelihood, moment, or other techniques and often involves a significant amount of computation. Such techniques are treated in advanced statistical texts and increasingly incorporated into statistical software packages. The use of these techniques is often justified to maximize the utility of the reliability data. They are, however, beyond the scope of what can be included in an introductory reliability text of reasonable length. Instead, we focus next on an elementary treatment of confidence levels of estimated parameters.

Example D.8 Picking the right distribution for your data

The following data were obtained from a test of 11 motors with some suspended tests (Table D.7)

A) Analyze the data parametrically (using lognormal, exponential, and Weibull distribution) with MINITAB (Figures D.11–D.13).
B) Which distribution fits the data best?

Table D.7 Spreadsheet for probability plots of data in Example D.8.

Failure #	Failure time	C(ensor)/F(ailure)	Reverse rank	Adjusted rank*	$P(F)$	$R = 1 - F$
1	31.7	F	11	1	0.061	0.939
2	42.1	F	10	2	0.149	0.851
3	61.9	F	9	2.1	0.158	0.842
4	69.1	C	8			
5	81.2	F	7	3.338	0.266	0.734
6	89.1	F	6	4.575	0.375	0.625
7	92.1	C	5			
8	101	F	4	6.06	0.505	0.495
9	103	F	3	7.545	0.636	0.364
10	108	F	2	9.03	0.766	0.234
11	125	C	1			

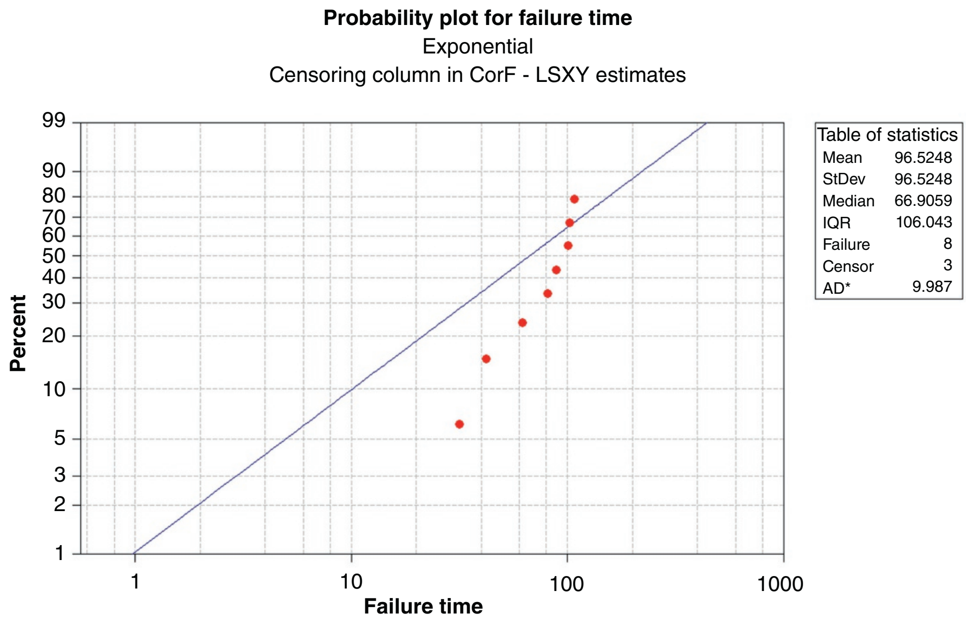


Figure D.11 Using MINITAB to plot the data as an e**xponential distribution.**

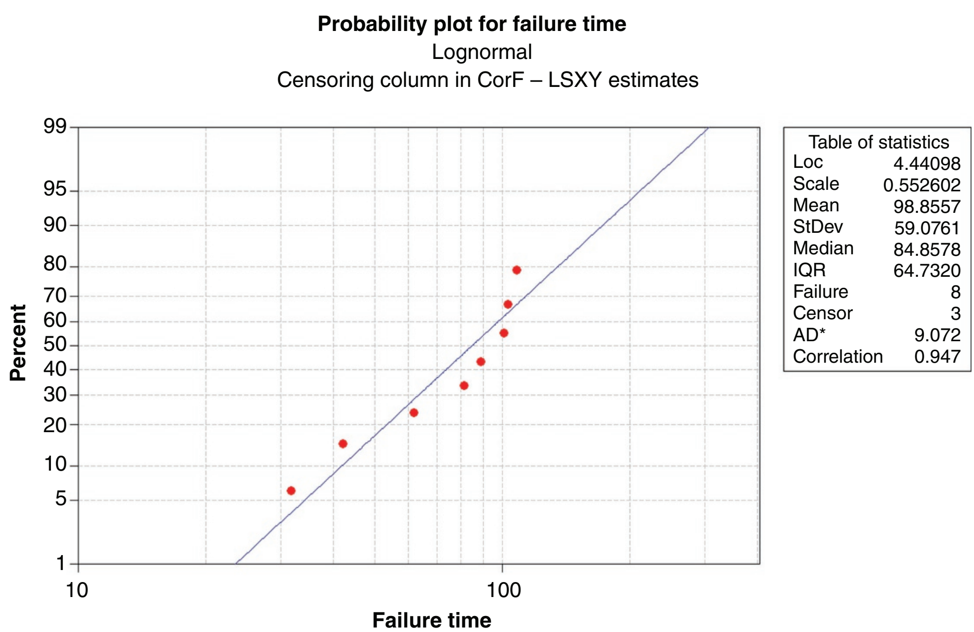


Figure D.12 Using MINITAB to plot the data as a l**ognormal distribution.**

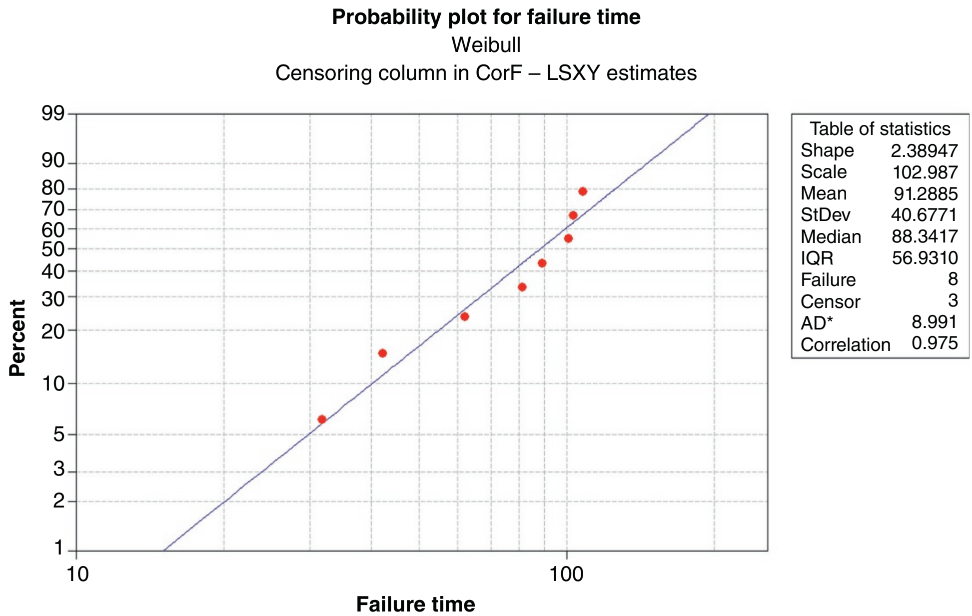


Figure D.13 Using MINITAB to plot the data as a Weibull distribution.

Example D.9 Continuing Example D.8, using the above three distributions, none fit the data very well; however, using knowledge gained in Chapter 5, you can plot the data as a three-parameter Weibull with the following results (Figure D.14):

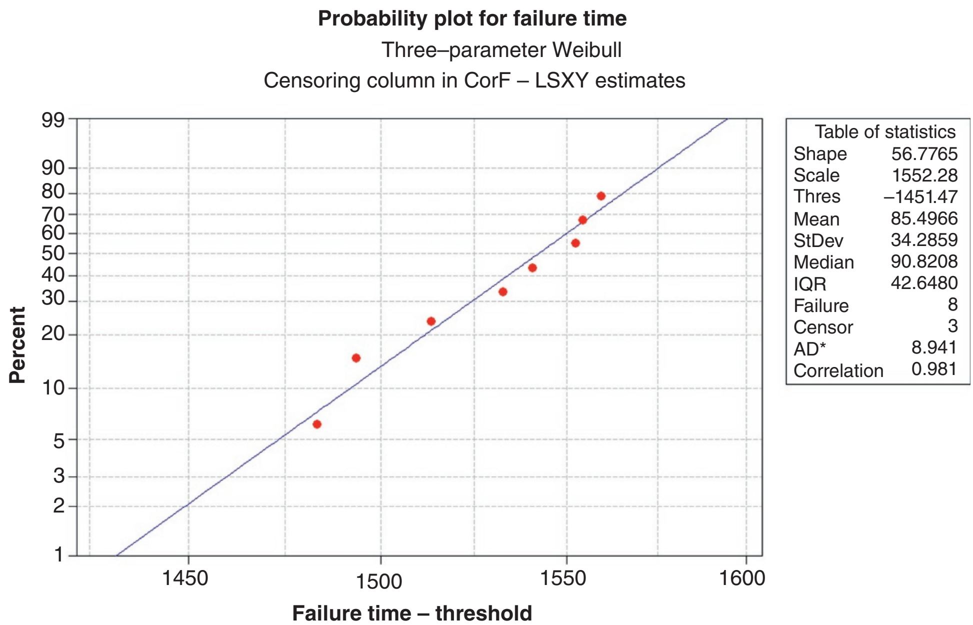


Figure D.14 Using MINITAB to plot the data as a three-parameter Weibull distribution.

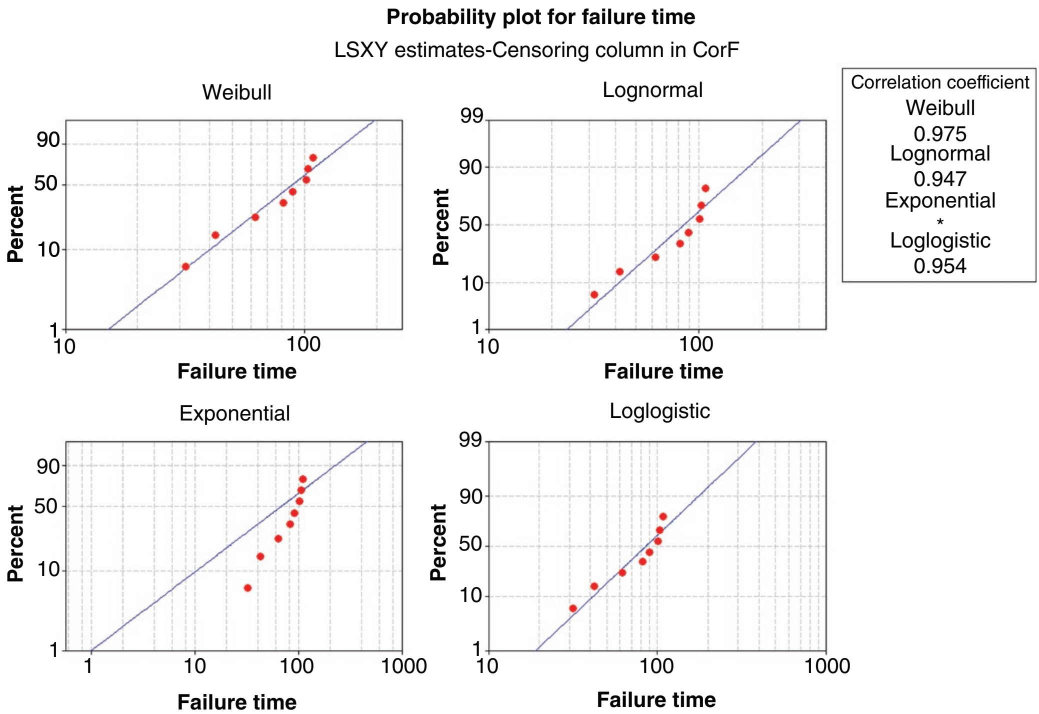


Figure D.15 Using MINITAB to plot the data on the first sheet of distributional plots.

This is a more reasonable fit to the data, but let's go one step further and use a MINITAB shortcut to find the best distribution for this data; thus checking on our result above.

Using the "distribution ID plot" option under "distributional analysis" to compare 11 different distributions available in MINITAB (Figures D.15–D.17).

The smallest Anderson–Darling is given by t**he smallest extreme-value distribution.**

Comparing the three-parameter Weibull to the smallest extreme value (Table D.8).

When comparing distributional fits the lowest AD or the highest Correlation (if an LSXY fit is being done) indicates the better distributional fit. However, always look at the plot of the data on the recommended distribution for your "eyeball" decision as well as to make sure that the distribution makes engineering sense – as in this case).So, let's make sure we've chosen the correct distribution. Doing a smallest extreme-value plot (Figure D.18).

So, the smallest extreme-value distribution is **not suitable since it projects TTF's < 0**.

Hence, three-parameter Weibull is the best fit.

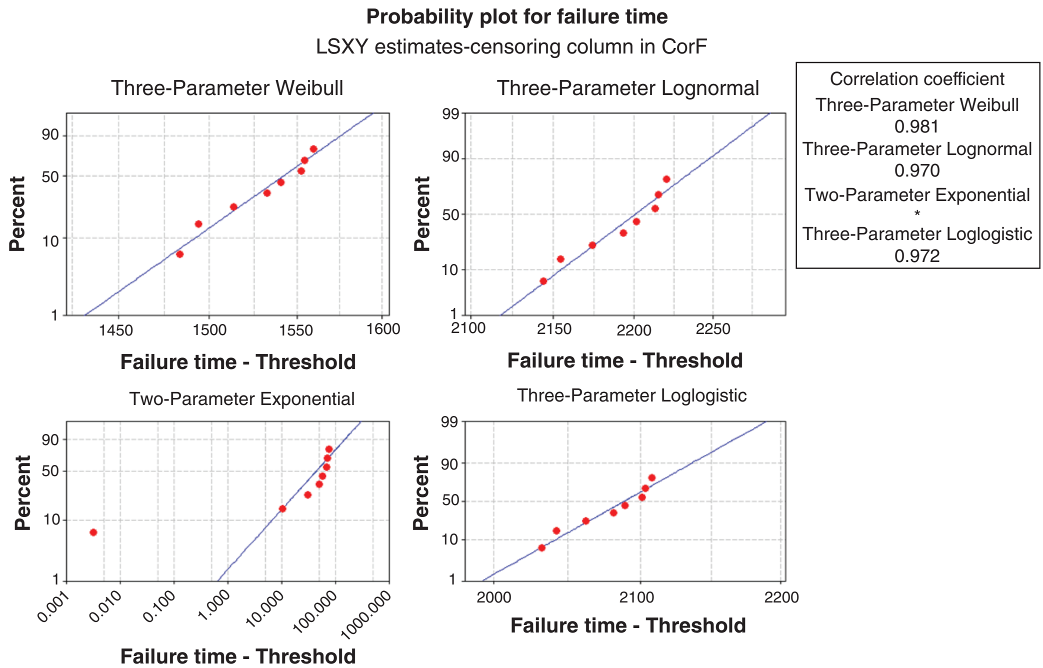


Figure D.16 Using MINITAB to plot the data on the second sheet of distributional plots.

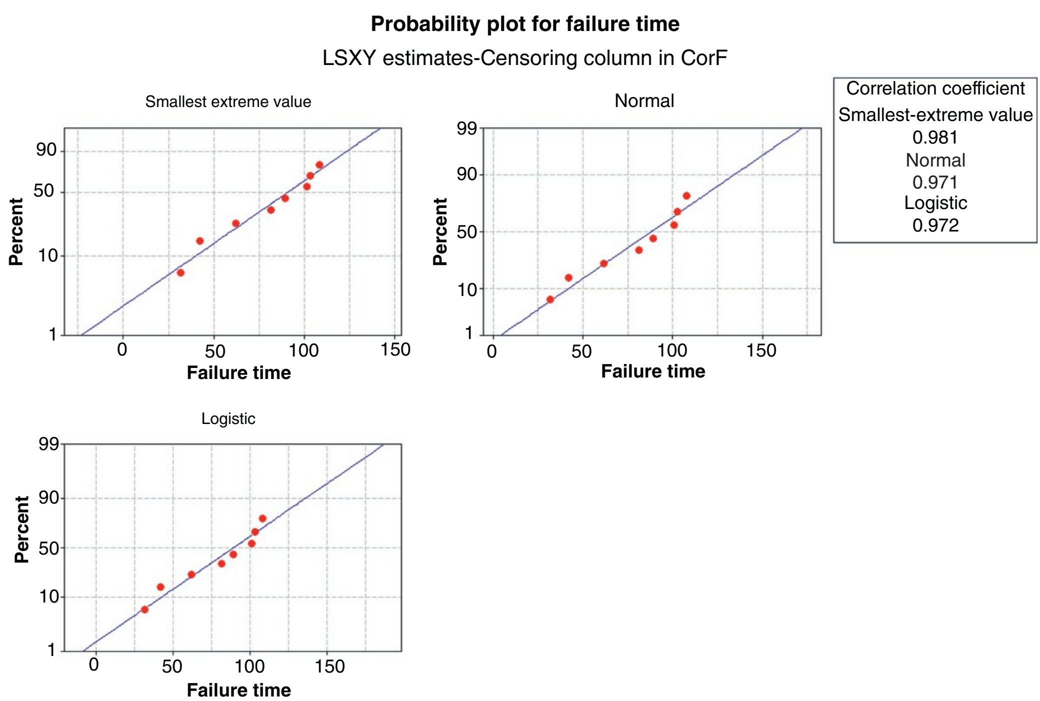


Figure D.17 Using MINITAB to plot the data on the third sheet of distributional plots.

Table D.8 Goodness-of-Fit for 11 distributions available

Distribution	Anderson–Darling(adj)	Correlation coefficient
Weibull	8.991	0.975
Lognormal	9.072	0.947
Exponential	9.987	*
Loglogistic	9.063	0.954
Three-parameter Weibull	8.941	0.981
Three-parameter lognormal	8.983	0.970
Two-parameter exponential	10.054	*
Three-parameter loglogistic	8.983	0.972
Smallest extreme value	8.940	0.981
Normal	8.983	0.971
Logistic	8.983	0.972

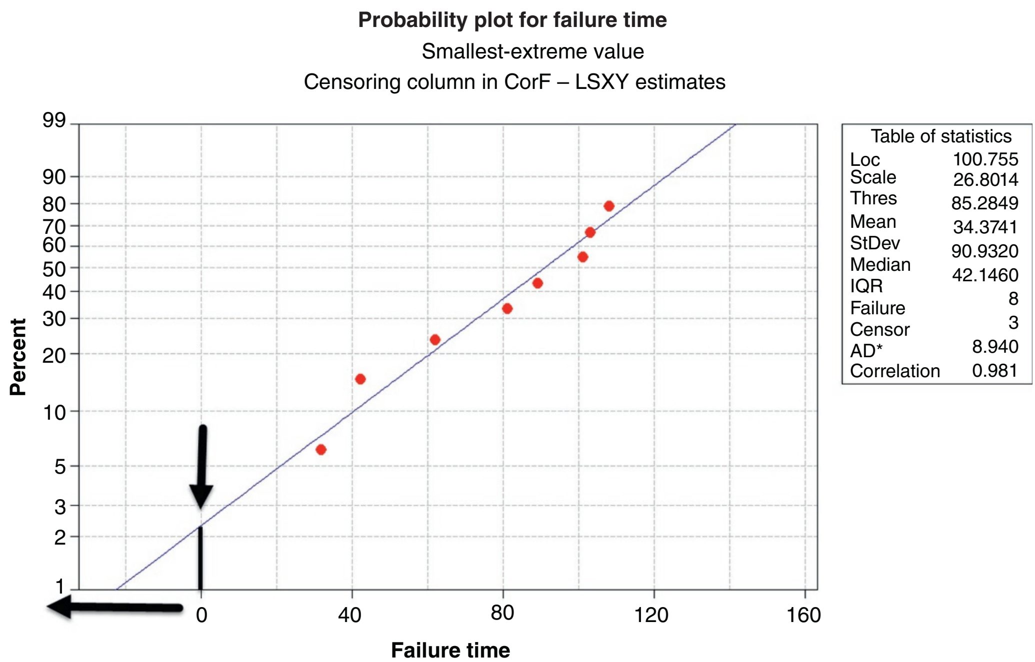


Figure D.18 Using MINITAB to plot the data on more detailed smallest extreme-value plot.

Bibliography

Pearson, K. (1895). Contributions to the mathematical theory of evolution. II. Skew variation in homogeneous material. *Philosophical Transactions of the Royal Society A - Mathematical Physical and Engineering Sciences* **186**: 343–414.

PROSCHAN (1963). Properties of probability distributions with monotone hazard rate. *Annals of Mathematical Statistics* **34** (2): 375–389.

Montgomery & Runger (2011). *Applied Statistics and Probability for Engineers*, 5the, 201. Wiley.

3rd Ed Answers to Odd – Numbered Exercises

Chapter 2 Probability and Discrete Distributions

2.1 (a) $P(X \cap Y) = 0.18 \neq 0$; therefore, not mutually exclusive.
(b) $P\{X|Y\} = 0.409 \neq P\{X\}$; therefore, X and Y not independent
(c) 0.409
(d) 0.5625

2.3 (a) 0.5, (b) 0.25, (c) 0.625, (d) 0.5.

2.5 (a) 0.7225, (b) 0.0225.

2.7 P (no damage in 10 K landings) = 0.9048.

2.9 (a) $P\{X\} = 0.04$, (b) $P\{X_1/X_2\} = 0.25$.

2.11 (a) $C = 1/14$, (b) $F(1) = 1/14$, $F(2) = 5/14$, $F(3) = 1$, (c) $\mu \approx 2.57$, $\sigma = 0.623$.

2.13 $\mu \approx 55/36$, $\sigma^2 \approx 1.97$.

2.15 (a) 10, (b) 36, (c) 792, (d) 20.

2.17 0.0702.

2.19 $P_{\mathrm{NEW}} = 0.0036$.

2.21 (a) 0.058, (b) 6.6×10^{-5}, (c) 0.058.

2.23 (a) 0.594, (b) 0.0166.

2.25 (a) 0.353, (b) 3.0.

2.27 0.0803.

2.29 (a) $1 - 1.2 \times 10^{-6}$, (b) 0.851.

2.31 230 consecutive starts.

2.33 (Binomial: 0.009476) (Poisson: 0.0142).

2.35 90% bounds (on $\mu = Np = 14$) approx. (8.8, 20) or $(p_L, p_U) = (0.088, 0.20)$.
95% bounds (on $\mu = Np = 14$) approx. (7.7, 22) or $(p_L, p_U) = (0.07, 0.22)$.

2.37 $P(TSL) = 0.21$

$P(W \cap TSL) = 0.064$

$$P(W \mid TSL) = \frac{P(W \cap TSL)}{P(TSL)} = \frac{0.064}{0.21} \approx 0.3 \neq 0.4$$

2.39 (a) 0.61, (b) 0.54.

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

Chapter 3 Exponential Distribution and Reliability Basics

3.1 (a) $R(t) = \dfrac{16}{(t+4)^2}$, (b) $\lambda(t) = \dfrac{2}{(t+4)}$, (c) Four years.

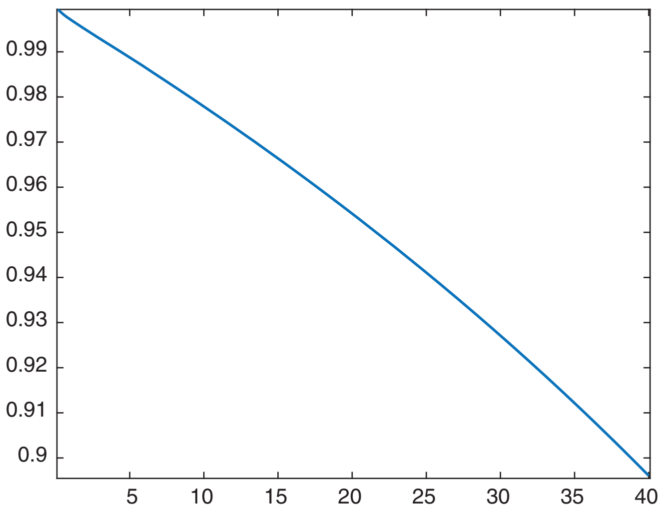
3.3 (a) 129.9 hours, (b) 256.5 hours, (c) 154.6 hours.

3.5 (a) 0.9656, (b) 0.9802, (c) 0.9729, (d) 0.99.

3.7 (a) 0.5034, (b) 0.6202.

3.9 (a) $R(t) = \left[e^{-0.001\left[\left(t - e^{-2t} + 40e^{\frac{t}{40}}\right) - 39\right]}\right]$,

(b)



3.11 $\lambda = 0.1054$/year.

3.13

(a) $f(t) = \begin{cases} 2at, & t < \dfrac{1}{\sqrt{a}} \\ 0 & t > \dfrac{1}{\sqrt{a}} \end{cases}$

(b) $\lambda(t) = \dfrac{-\dfrac{dR(t)}{dt}}{R(t)} \rightarrow f(t) = \begin{cases} \dfrac{2at}{1 - at^2} & t < \dfrac{1}{\sqrt{a}} \\ 0 & t > \dfrac{1}{\sqrt{a}} \end{cases}$

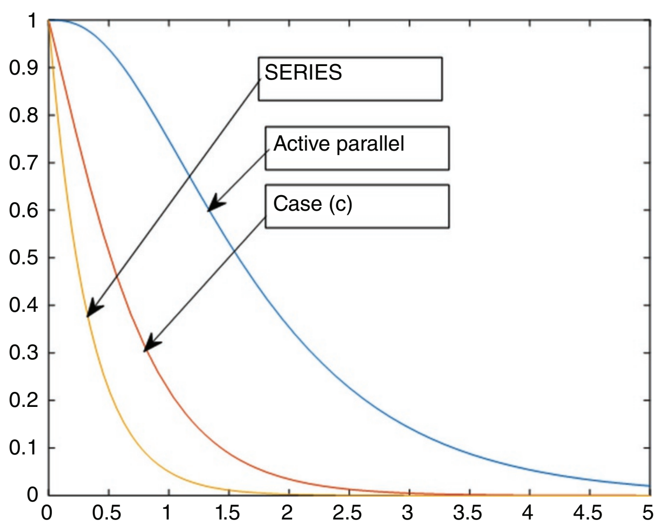
(c) $\text{MTTF} = \int_0^{\frac{1}{\sqrt{a}}} (1 - at^2)\,dt = \left[t - a\dfrac{t^3}{3}\right]_0^{\frac{1}{\sqrt{a}}} = \dfrac{1}{\sqrt{a}} - a\dfrac{1}{3a^{\frac{3}{2}}} = \dfrac{2}{3\sqrt{a}}$

3.15 (a) $P(\text{failure in month 2}) = \int_1^2 \frac{1}{2}e^{-\frac{1}{2}t} = -\left[e^{-\frac{1}{2}t}\right]_1^2 = e^{-\frac{1}{2}} - e^{-1} = 0.2387$, (b) 0.3935, and (c) 3.22 months.

3.17 (a) 0.328, (b) 0.7427.

3.19 $\lambda = (p_0 + p_c)c/\bar{t} + (1-c)\lambda_c + c\lambda_0$
3.21 $\lambda = 5.76 \times 10^{-4}$ per day.
3.23 (a) P(parts exhaustion) = 0.5777, (b) P(parts exhaustion) = 0.3528.
3.25 (a) $f(t) = \frac{1}{9}\left(e^{-\frac{t}{3}} + e^{-\frac{t}{6}}\right)$, (b) $\lambda(t) = \frac{1 + e^{\frac{t}{6}}}{3 + 6e^{\frac{t}{6}}}$, (c) $\lambda(0) = 2/9$ per month, (d) decreases, (e) $\lambda(\infty) = 1/6$ per month.
3.27 (a) Reliability (design life) $= e^{-\frac{1}{T}T}$. (b) 0.9098, (c) $\lambda = \frac{1}{2T}$
3.29 (a) $R(t) = 0.905$, (b) $R(t) = 0.9275$.
3.31 (a) $\boldsymbol{\mu}$ = NF = 1.813.
3.33 (a) 0.0513 per year, (b) 0.9975, (c) 0.9923.
3.35 $\zeta = 1/3$.
3.37 Design life = 1.066 months.
3.39 (a) 0.99, (b) 0.9728.
3.41 $R_S(t) = 0.6288$.
3.43 (a) $R_s = R^3 = e^{-3\lambda t}$
(b) $R_a = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$
(c) $R_c = 2e^{-2\lambda t} - e^{-3\lambda t}$

(d)

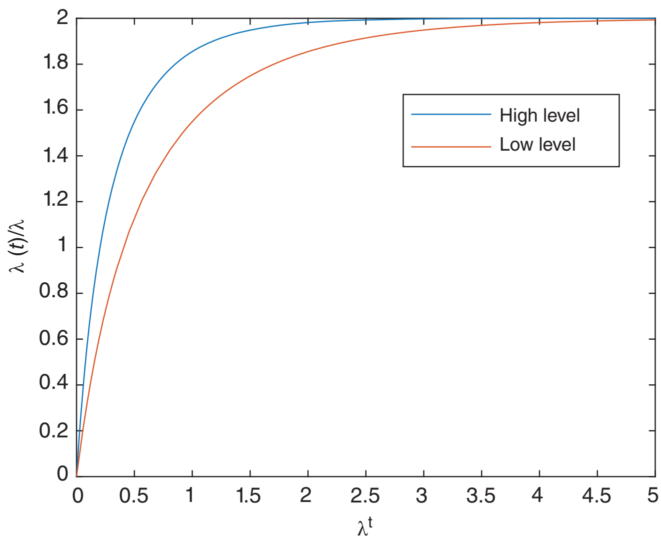


3.45 (a) 30 days, (b) 27.32 days, (c) 27.27 days.
3.47 $\text{MTTF}_{\text{sys}} = 1.293$.
3.49 (a) For $N = 2$, Max failure probability = 0.02241, (b) for $N = 3$, Max failure probability = 0.1376.
3.51 (a) $R_{HL} = 0.9938$, (b) $R_{LL} = 0.996$, (c) $R = 0.9798$.

3.53 (a) $\lambda_{HL}(t) = -\frac{1}{R_{HL}}\frac{d}{dt}\text{R}_{\text{HL}} = 4\lambda\frac{e^{-2\lambda t} - e^{-4\lambda t}}{2e^{-2\lambda t} - e^{-4\lambda t}} = 4\lambda\frac{1 - e^{-2\lambda t}}{2 - e^{-2\lambda t}}$

(b) $\lambda_{LL}(t) = -\frac{1}{R_{LL}}\frac{d}{dt}\text{R}_{\text{LL}} = 4\lambda\frac{2 - 3e^{-\lambda t} + e^{-2\lambda t}}{4 - 4e^{-\lambda t} + e^{-2\lambda t}}$

(c)



3.55 $R = 3.195 \times 10^{-8}$.

3.57 (a) $\dfrac{\text{MTTF}_{HL}}{\text{MTTF}_0} = \dfrac{\dfrac{3}{4\lambda}}{\dfrac{1}{2\lambda}} = \dfrac{3}{2}$, (b) $\dfrac{\text{MTTF}_{LL}}{\text{MTTF}_0} = \dfrac{\dfrac{11}{12\lambda}}{\dfrac{1}{2\lambda}} = \dfrac{11}{6}$

3.59

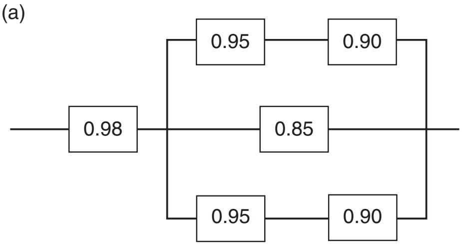
Arrows indicate choices other factors could enter in the decision (e.g. part supplies).

A	B	C	R(SYS)	Cost($)
1	1	1	0.332166	5200
2	2	2	0.722937	10400
3	3	3	0.893915	15600
4	4	4	0.959133	20800
5	5	5	0.983966	26000
6	6	6	0.993604	31200
7	7	7	0.997416	36400
7	6	6	0.993624	32400
6	7	6	0.996785	33600
6	6	7	0.994213	32800
5	7	6	0.996668	32400
6	7	5	0.994814	32000
5	7	5	0.994697	30800
4	7	6	0.995977	31200
6	7	4	0.988457	30400
5	7	4	0.988340	29200
4	7	5	0.994007	29600
4	8	5	0.995340	32000
5	8	4	0.989665	31600

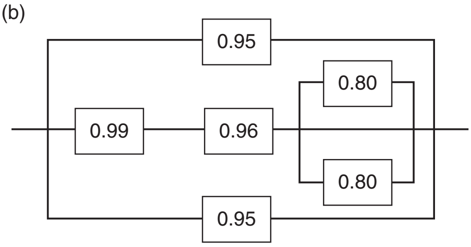
3.61 (a) $R_{HL} = 0.9867$, (b) $R_{LL} = 0.9952$.

3.63 **Calculate the reliabilities of the following systems:**

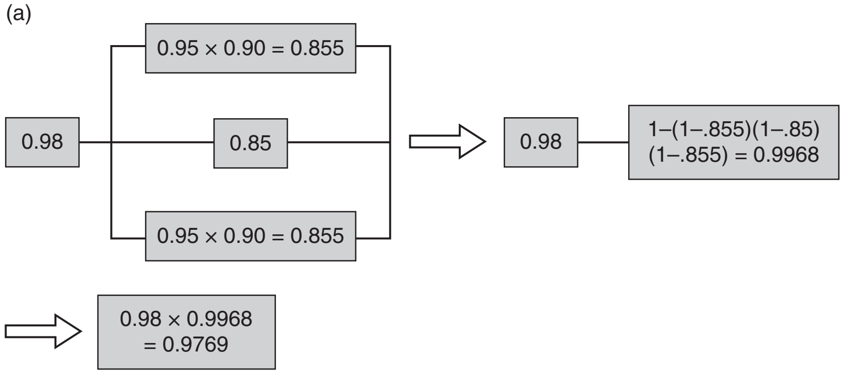
(a)



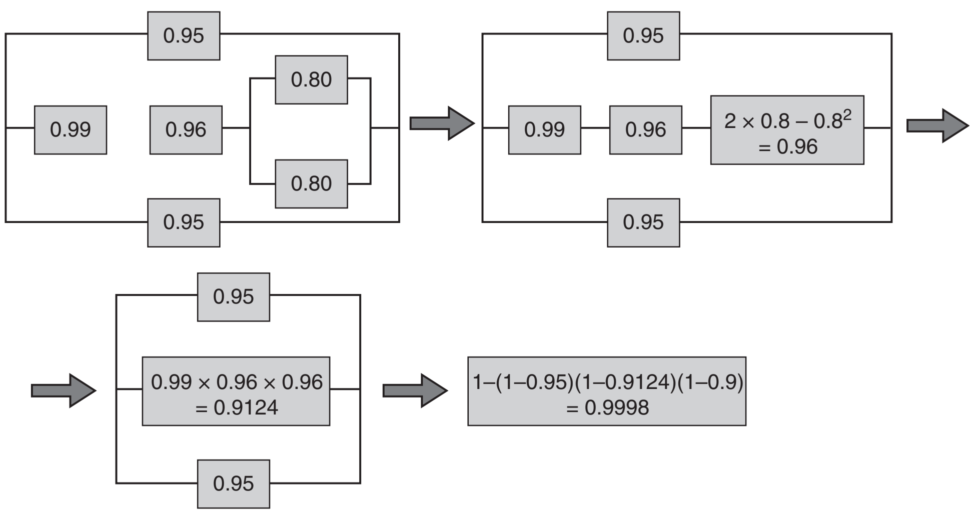
(b)



(a)



(b)



3.65 System reliability $+ \ = R^5 - R^4 - 3R^2 + 4R^2$

$$R = 1 - \lambda t \rightarrow \text{System Reliability} = 1 - (\lambda t)^2 - 3(\lambda t)^3 + 4(\lambda t)^4 + (\lambda t)^5 \approx 1 - (\lambda t)^2$$

3.67 (a) $\boldsymbol{R^+ = 0.99025, R = 0.81225, R = 0.97245,}$

(b) $1 - R_X = 1 - 0.8 = 0.2, \quad R_X = 0.8$

$$R^- = (0.99)(2x0.72) - 0.72^2)(0.99) = 0.90326$$
$$R^+ = (0.99)\left(2x0.9 - 0.9^2\right)(0.99) = 0.970299$$
$$R = R^-(1 - R_X) + R^+(R_X) = 0.9569$$

3.69 (a) $F(1) = 0.09$, (b) $F(5) = 0.7127$, so $R(5) = 0.2873$, (c) Nine months.

Chapter 4 Continuous Distributions – Part 1 Normal and Related Distributions

4.1 (a) $b = 6$, (b) $\mu = 0.5$, (c) $\sigma^2 = 0.05$, and $\sigma = 0.2236$.

4.3 (a) $a = 2b^2$, $b = 3000$; therefore, $a = 18 \times 10^6$, (b) $F(2000) = 0.64$, (c) warranty should be 77.94 or ~78 hours.

4.5 (a) $f(x) = 0.04 \times e^{-0.2x}$, (b) $\mu = 10$, $\sigma^2 = 50$, (c) expected value $(e^{-x}) = 0.0278$.

4.7 (a) $\mu = 1$ μm, (b) $P\{x > 1.5 \text{ μm}\} = 0.8009$, (c) Mean value of accepted flaw size = 0.7202 μm.

4.9 (a) $(x) = \dfrac{1 - e^{-\frac{x}{\gamma}}}{1 - e^{-\frac{\tau}{\gamma}}}$, (b) $P\left\{x > \dfrac{\tau}{2}\right\} = 0.168$.

4.11 If τ_0 is required to keep the pipe from failing, Success $\equiv \tau_0 < \tau - x$, Failure $= \tau_0 > \tau - x$, or $x > \tau - \tau_0$ i.e. the random variable must be less than, or equal to, the total length minus the minimum holding length the pipe to hold

(a)

$$1 - \varepsilon = \int_0^{\tau - \tau_0} f(x)dx \text{ or } \varepsilon = \int_{\tau - \tau_0}^{\tau} \frac{1}{\gamma}\frac{e^{-x/\gamma}}{1 - e^{-\tau/\gamma}}dx = \left(\frac{1}{1 - e^{-\tau/\gamma}}\right)\left[e^{-(\tau_0 - \tau/\gamma)} - e^{-\tau/\gamma}\right]$$

$$= \frac{e^{-\tau/\gamma}}{1 - e^{-\tau/\gamma}}\left[e^{+\tau_0/\gamma} - 1\right] = \frac{1}{e^{+\tau_0/\gamma} - 1}\left[e^{+\tau_0/\gamma} - 1\right]$$

$$\frac{1}{\varepsilon}\left[e^{+\tau_0/\gamma} - 1\right] + 1 = e^{+\tau/\gamma}$$

$$\gamma\left(\ln\left(1 + \frac{1}{\varepsilon}\left[e^{+\tau_0/\gamma} - 1\right]\right)\right) = \tau$$

$$\gamma = 6.25 \text{ mm}, \tau_0 = 4 \text{ cm} = 40 \text{ mm}, \varepsilon = 0.1\% \text{ or } 10^{-3}$$

(b) $\tau = \gamma\left(\ln\left(1 + \dfrac{1}{\varepsilon}\left[e^{+\tau_0/\gamma} - 1\right]\right)\right) = 6.25 \ln\left(1 + \dfrac{1}{10^{-3}}\left[e^{+40/6.25} - 1\right]\right) = 83.2$ mm

(c) For $\gamma = 6.25$ mm, $\tau_0 = 4$ cm $= 40$ mm, $\varepsilon = 0.01\,\%$ or 10^{-4}

$$\tau = 97.6 \text{ mm}$$

(d) For $\tau_0 >> \gamma$, $\tau_0/\gamma >> 1$, $\varepsilon << 1$ and $1/\varepsilon >> 1$

4.13 $sk = \frac{1}{\left(\overline{x}^2 - \overline{x}^{1^2}\right)^{3/2}}\left(\overline{x}^3 - 3\overline{x}^2\overline{x}^1 + 2\overline{x}^{1^3}\right)$

4.15 (a) $fy(y) = \frac{1}{B(b-a)}\left(\frac{y-a}{b-a}\right)^{r-1}\left(\frac{b-y}{b-a}\right)^{t-r-1}$

(b) $\mu y = a + (b-a)\frac{r}{t}$

4.17 (a) 0.8943, (b) 1043.1 lb, (c) 21.5 lb.

4.19 7.44 hours.

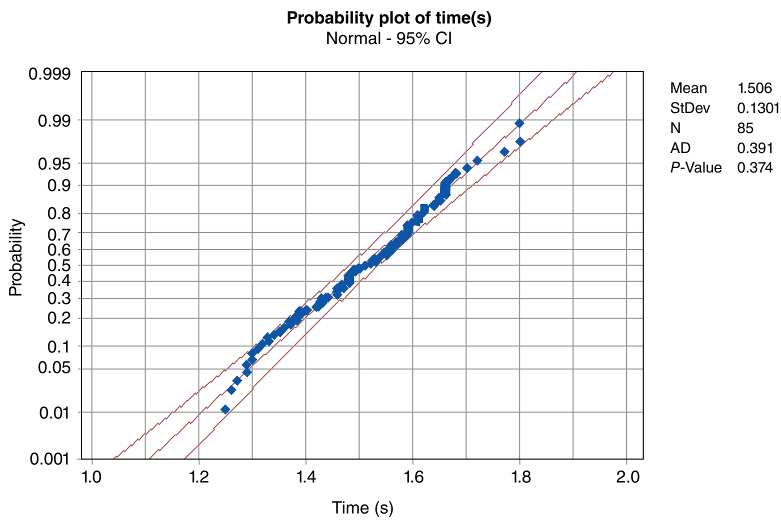
4.21 $\mu_d = 6$ kips, $\sigma_d = 0.4$ kips, $\mu_i = 9.2$ kips, $\sigma_l = 1.2$ kips; $\mu_w = 4.6$ kips, $\sigma_w = 1.1$ kips

$\mu_{\text{total}} = \mu_d + \mu_l + \mu_w = 6 + 9.2 + 4.6 = 19.8$ kips

$$\sigma_d = \sqrt{\sigma_d{}^2 + \sigma_l{}^2 + \sigma_w{}^2} = \sqrt{0.4^2 + 1.2^2 + 1.1^2} = 1.676 \text{ kips}$$

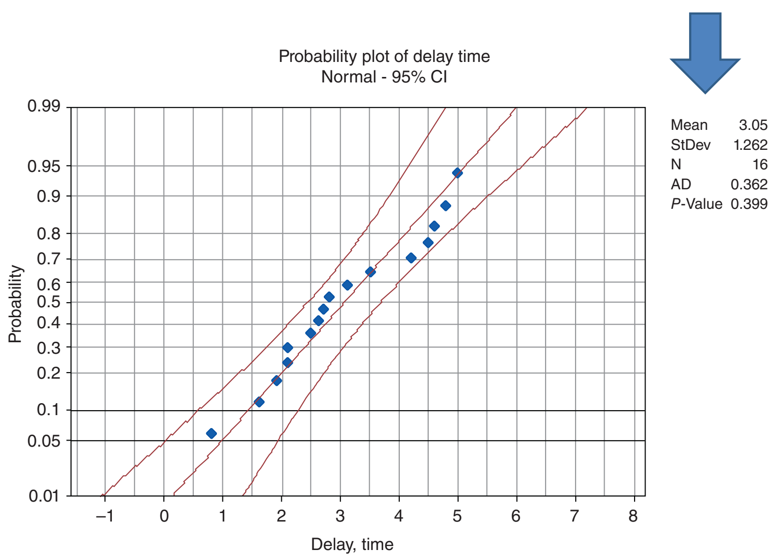
4.23 $f(t) - 0.5$.

4.25 (a) (MINITAB)

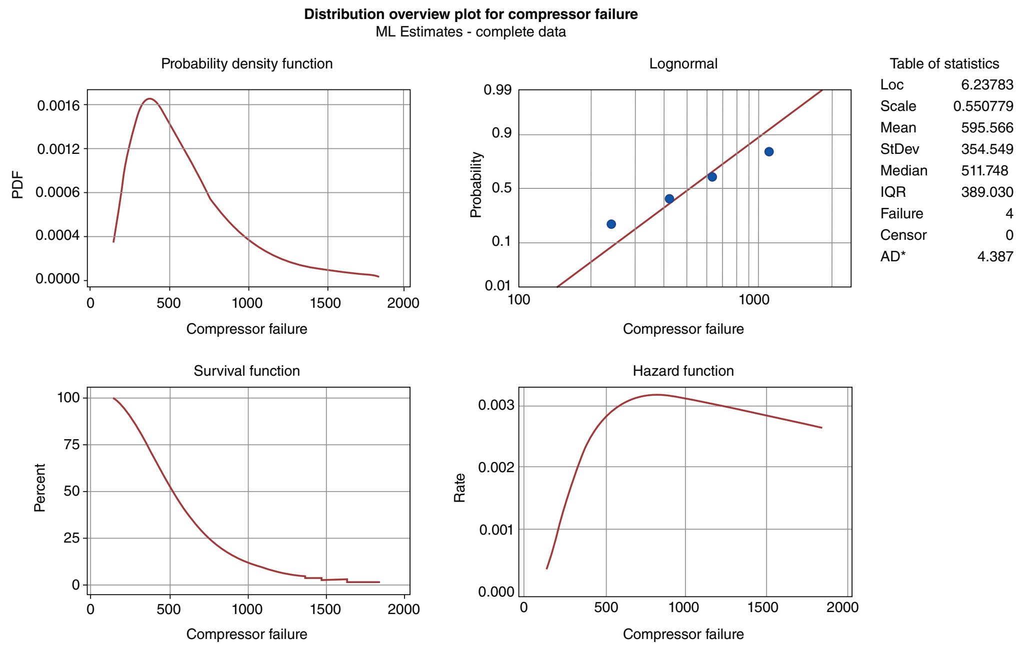


(b) Low AD value accompanied by a p value bigger than the significance level (assumed as 0.05) indicated that the deviation from normal distribution is insignificant.

4.27

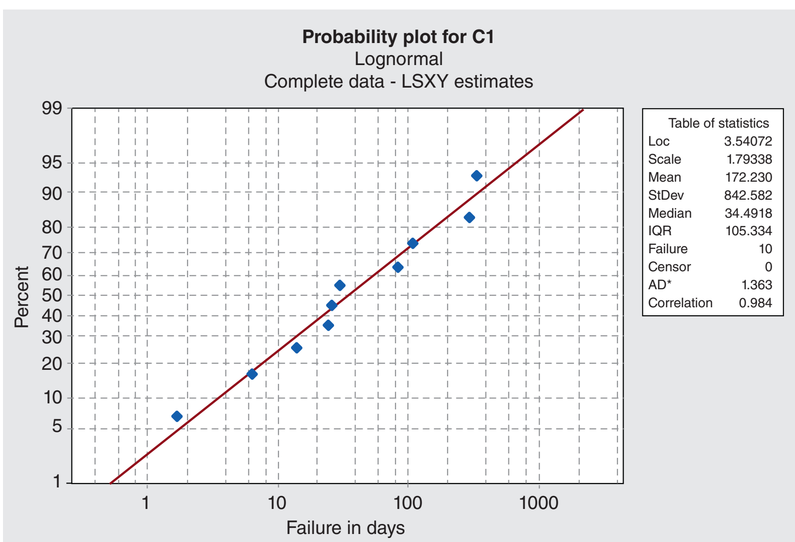


4.29 (a)



(b) Estimate the median time to failure.... 511.

4.31 (a)



Last column is mean percentile/lower bound

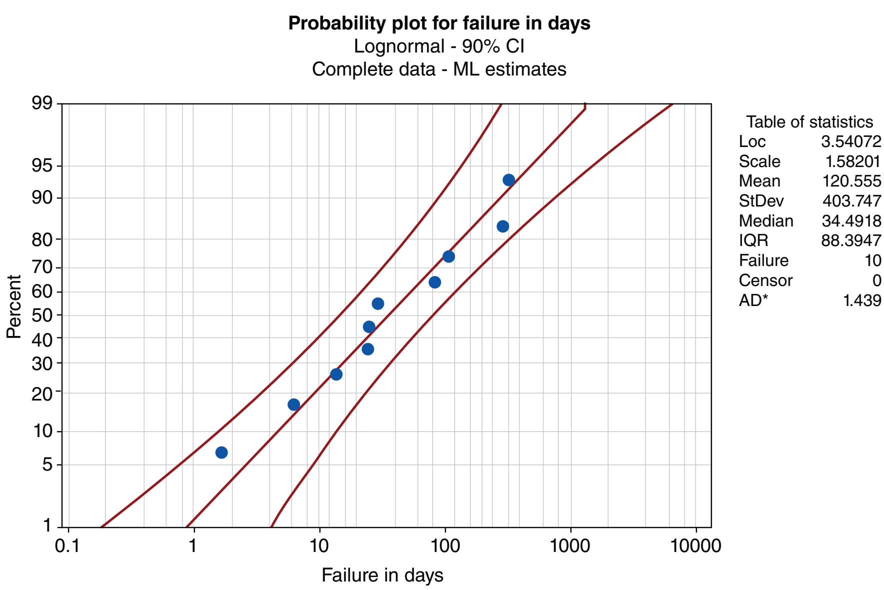
Factor goes from 4.87 at 1% and 99% percentile to 2.27 at 50%.

An illustration of how confidence bounds spread at the extremes (see plot after table).

(b) Table of percentiles

Percent	Percentile	Standard error	90.0% Normal CI		Factor
			Lower	Upper	
1	0.869712	0.837597	0.178403	4.23983	4.874985
2	1.33865	1.18082	0.313718	5.71208	4.267049
3	1.75994	1.46503	0.447560	6.92062	3.932305
4	2.16217	1.72135	0.583684	8.00943	3.704359
5	2.55625	1.96157	0.723498	9.03167	3.533182
6	2.94777	2.19163	0.867722	10.0139	3.397136
7	3.34010	2.41511	1.01680	10.9719	3.284913
8	3.73549	2.63432	1.17105	11.9157	3.189864
9	4.13558	2.85094	1.33072	12.8525	3.107776
10	4.54164	3.06620	1.49601	13.7877	3.035835
20	9.10902	5.30295	3.49624	23.7324	2.605376
30	15.0460	8.02799	6.25562	36.1886	2.405197
40	23.1021	11.7414	10.0136	53.2983	2.307072
50	34.4918	17.2554	15.1476	78.5396	2.277047
60	51.4968	26.1728	22.3212	118.807	2.30708
70	79.0697	42.1887	32.8745	190.178	2.405199
80	130.605	76.0336	50.1291	340.275	2.605373
90	261.950	176.850	86.2856	795.240	3.035848
91	287.670	198.311	92.5644	894.016	3.107782
92	318.481	224.598	99.8419	1015.91	3.189853
93	356.182	257.543	108.430	1170.02	3.284903
94	403.588	300.063	118.803	1371.04	3.39712
95	465.402	357.132	131.723	1644.35	3.533187
96	550.227	438.049	148.535	2038.23	3.704359
97	675.979	562.705	171.904	2658.16	3.932305
98	888.718	783.936	208.275	3792.20	4.267041
99	1367.91	1317.39	280.597	6668.51	4.874999

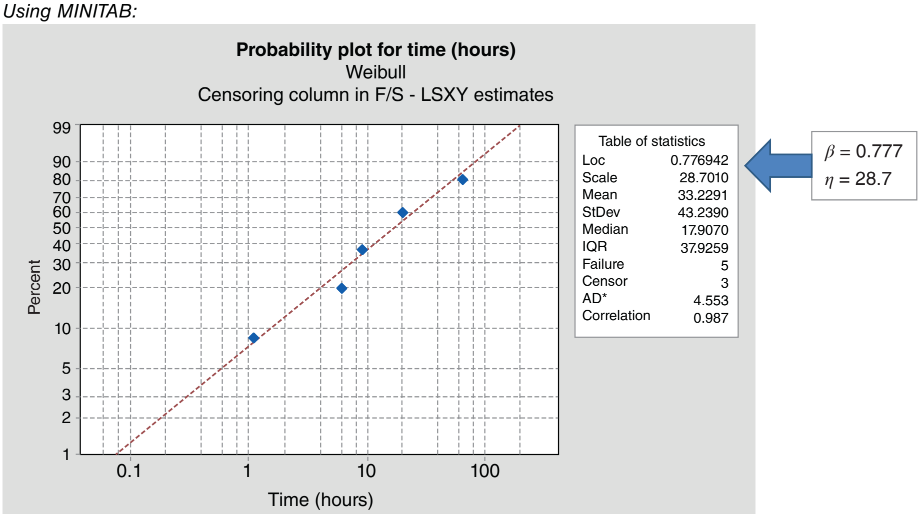
As plotted, with confidence bounds:



Chapter 5 Continuous Distributions – Part 2 Weibull and Extreme Value Distributions

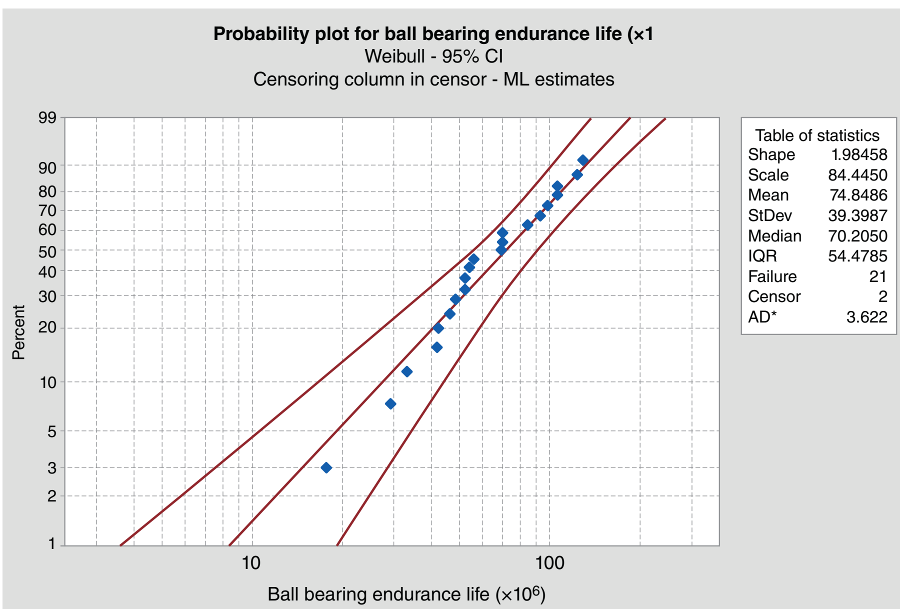
5.1 (a) $F(500) = 0.221$, (b) P(failure in the second 500 hours|successfully finished the first 500 hours) = 0.528.

5.3 (a) *Using MINITAB:*



(b) Infant mortality, (c) low time failures.

5.5 (a)



(b) $\beta = 1.98$ seems about right for bearing fatigue.

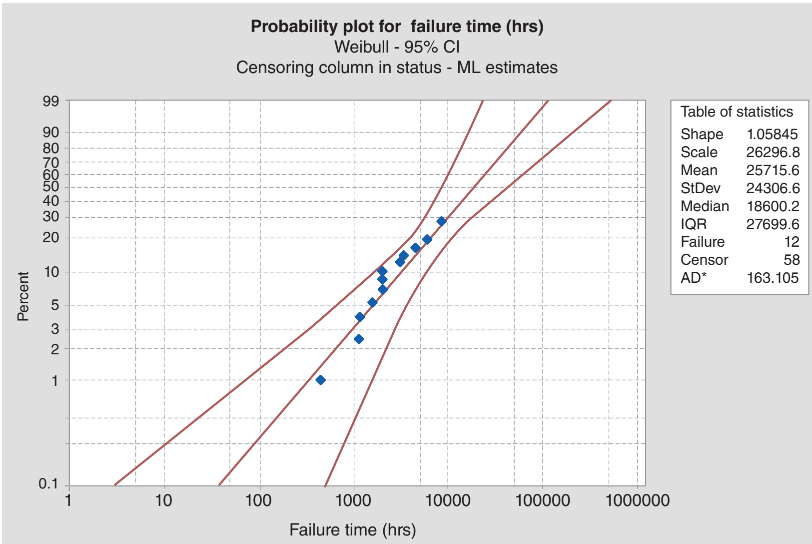
5.7

Parameter estimates

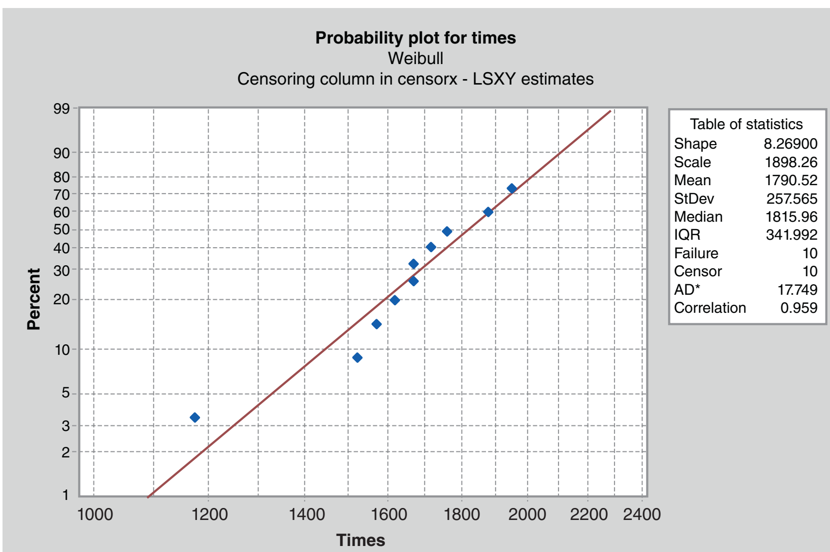
Parameter	Estimate	Standard Error	95.0% Normal CI Lower	Upper
Shape	1.05845	0.268251	0.644082	1.73939
Scale	26296.8	12251.4	10552.1	65534.4

Table of cumulative failure probabilities

Time	Probability	95.0% Normal CI Lower	Upper
8000	0.247067	0.145906	0.399873



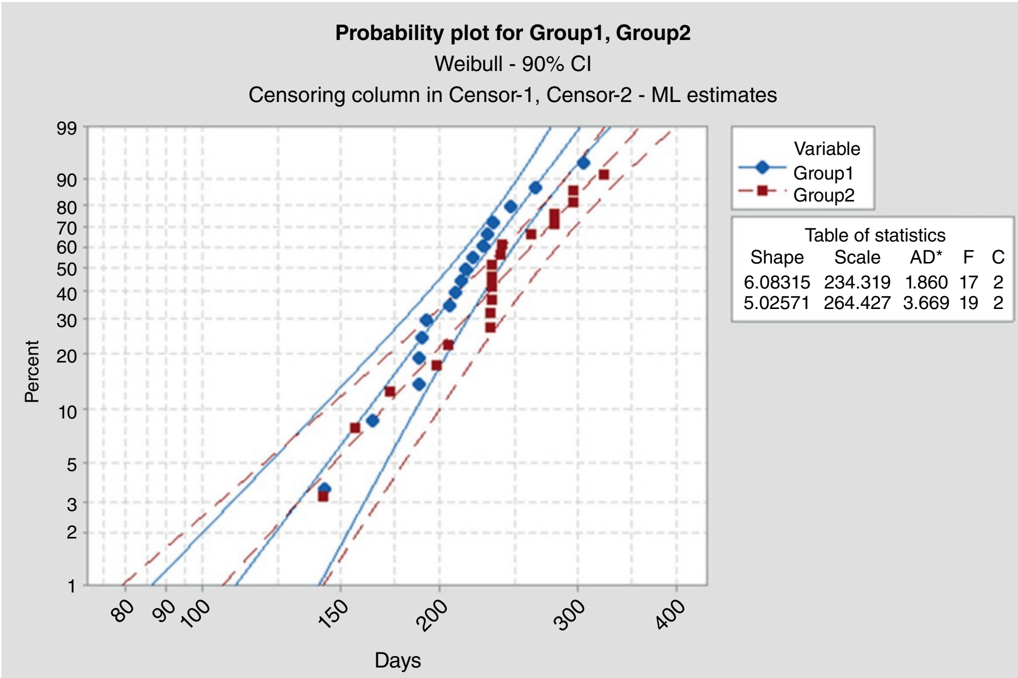
5.9 (a)



(b) $\beta = 8.269$

(c) Since $\beta = 8.269$, this is a (rapid) wearout mode.

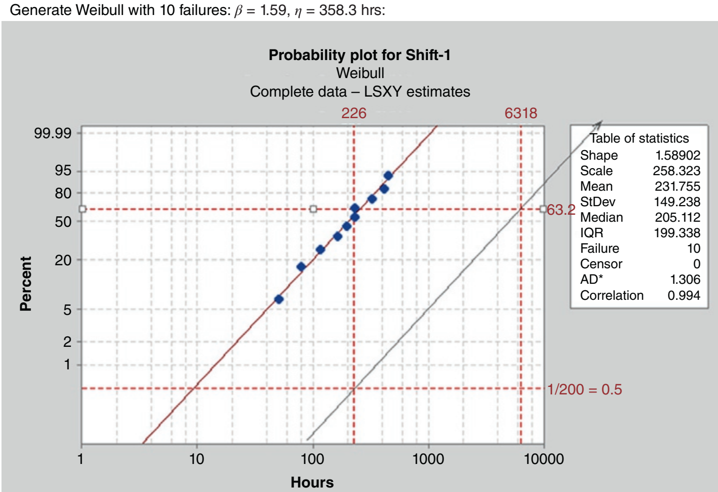
5.11



The overlap of the 90% confidence bounds and the 0.10 probalility level indicates No significant difference in the Treatments.

5.13

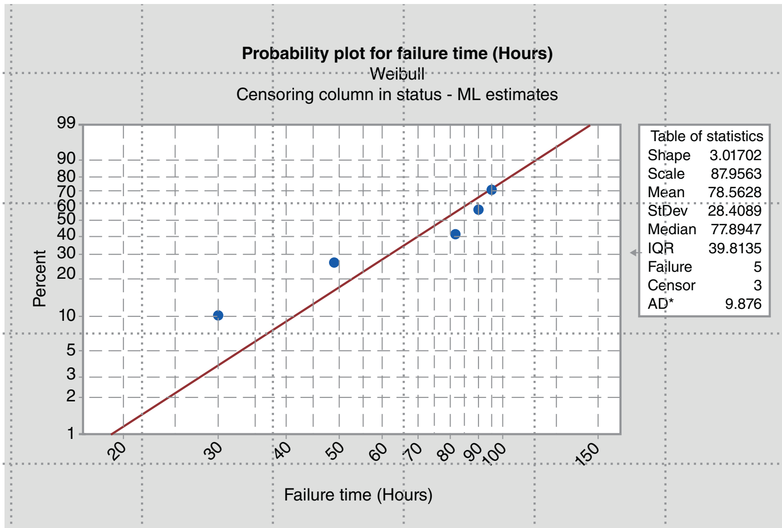
Generate Weibull with 10 failures: β = 1.59, η = 358.3 hrs:



Then, MTTF = Σ failure times/10 =2261/10 = 226 hours
Calculating η(shifted):

$$0.005 = 1 - e^{-\left(\frac{226}{\eta}\right)^{1.59}} \rightarrow \eta = 6318\, hours,$$

5.15 (a, b) 7.44 events over the next five months



5.17 (a) 0.3679, (b) 0.5, (c) 0.1587, (d) 0.456.

5.19 (a) Design life for reliability of (0.9) = 3.36 years.

(b) Design life for reliability of (0.99) = 2.01 years.

5.21 8×10^6 cycles

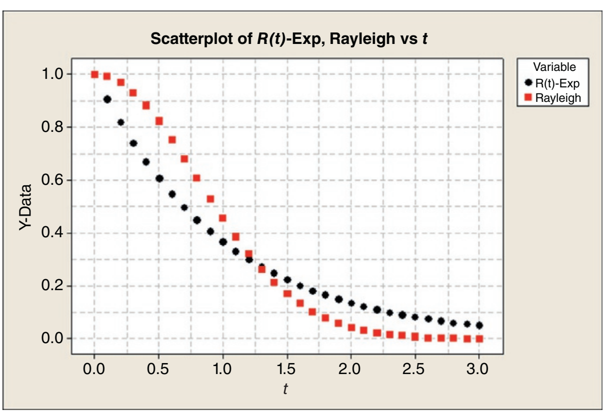
5.23 (a) $\exp\left(-\lambda_0 t_{DL}\right) = \exp\left(-\frac{t_{DL}^2}{\eta^2}\right)$

where DL = design life

Then, $-\lambda_0 t_{DL} = -\frac{t_{DL}^2}{\eta^2}$, so $\eta^2\lambda_0 = t_{DL}$ and from Exercise 5.22 $\eta = \frac{2}{\lambda_0\sqrt{\pi}}$

So, $\frac{4}{{\lambda_0}^2\pi}\lambda_0 = t_{DL} \Rightarrow \frac{4}{\lambda_0\pi} = t_{DL}$

(b)



5.25

$$R(t) = e^{-(t/\eta)^2} \Rightarrow -\frac{dR}{dt} = \frac{2t}{\eta^2}e^{-(t/\eta)^2}$$

$$R_s(t) = R(t) - \int_0^t R(t-t')\frac{d}{dt}R(t')dt'$$

$$R_s(t) = R(t) + \int_0^t e^{-\frac{(t-t')^2}{\eta^2}}\frac{2t'}{\eta^2}e^{-(t'/\eta)^2}dt'$$

$$= R_s(t) = R(t) + \frac{2}{\eta^2}\int_0^t t' \exp\left[\left(-t^2 + 2tt' - 2t'^2\right)/\eta^2\right]dt' \quad \left(-t^2 + 2tt' - 2t'^2\right)$$

$$= -2\left(t'^2 - tt' + \frac{1}{2}t^2\right) = -2\left(t'^2 - tt' + \frac{1}{4}t^2 + \frac{1}{4}t^2\right)$$

$$= -2\left(t' - \frac{1}{2}t\right)^2 - \frac{1}{2}t^2$$

Let

$$x = \frac{\sqrt{2}}{\eta}(t' - t/2) \Rightarrow \text{then} : dx = \frac{\sqrt{2}}{\eta}dt' \text{ and } t' = \frac{\eta}{\sqrt{2}}x + \frac{t}{2}$$

Then

$$\frac{2}{\eta^2}\int_0^t t'\mathrm{e}^{-2(t'-1/2t)^2/\eta^2}dt' = \int_{-t\frac{\sqrt{2}}{2\eta}}^{t\frac{\sqrt{2}}{2\eta}}\left(x + \frac{\sqrt{2}t}{2\eta}\right)e^{-x^2}dx$$

$$= 0 + \frac{\sqrt{2}t}{\eta}\int_0^{t\frac{\sqrt{2}}{2\eta}} e^{-x^2}dx = \frac{\sqrt{2\pi}t}{\eta}erf\left(\frac{\sqrt{2}t}{2\eta}\right)$$

Therefore,

$$R_s(t) = \left[1 + \frac{\sqrt{2\pi}t}{\eta}erf\left(\frac{t}{\sqrt{2}\eta}\right)\right]e^{-(t/\eta)^2}$$

5.27 1.293 MTTF.

5.29 (a) $\beta_1 = 7, \beta_2 = 7, \ \eta_1 = 8$ lbs

N = flaws in 1″, $2N$ = flaws in 2″

$$\eta' = N^{-\frac{1}{\beta}}\eta, \ \eta_1 = N^{-\frac{1}{\beta}}\eta, \ \ \eta_2 = (2N)^{-\frac{1}{\beta}}\eta$$

$$\text{So, } \eta_2 = 2^{-\frac{1}{\beta}}N^{-\frac{1}{\beta}}\eta = 2^{-\frac{1}{\beta}}\eta_1$$

$$\eta_2 = 2^{-\frac{1}{\beta}}8 = 7.25 \ \text{lbs}$$

(b) $0.01 = F(x) = 1 - e^{-\left(\frac{x}{8}\right)7}$

So, for 1″ : $e^{-\left(\frac{x}{8}\right)7} = 0.99 \Rightarrow x = 4.15$ lbs

for 2″ : $F(4.15) = 1 - e^{-\left(\frac{4.15}{7.25}\right)7} = 0.0199 \Rightarrow 2\%$ fail

5.31 $F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^2}$

B10 at one year: $F(1) = 0.1 = 1 - e^{-\left(\frac{1}{\eta}\right)^2} \Rightarrow e^{-\left(\frac{1}{\eta}\right)^2} = 0.9 \Rightarrow \eta = 3.08$ years

$R(t) = e^{-\left(\frac{t}{\eta}\right)^2}$, assume independent bearings

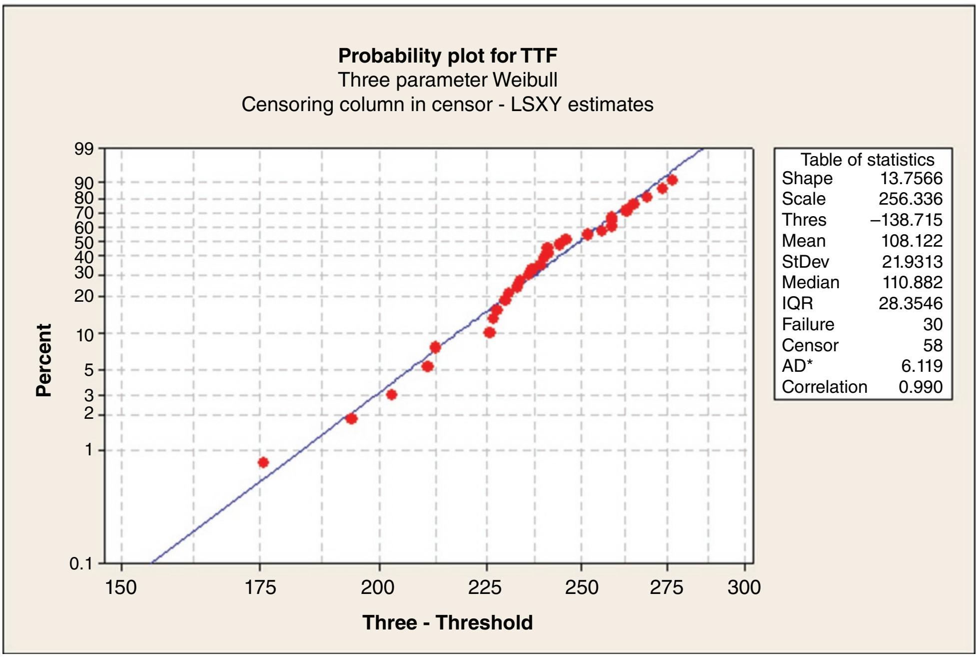
Then, $R_{sys}(t) = (R(t))^{12} = e^{-12\left(\frac{1}{\eta}\right)^2}$

For system B10: $R_{sys}(t) = 0.90 = e^{-12\left(\frac{1}{\eta}\right)^2}$

$$-\ln(0.9) = 12\left(\frac{t}{3.08}\right)^2 \Rightarrow t = 0.289 \text{ years}$$

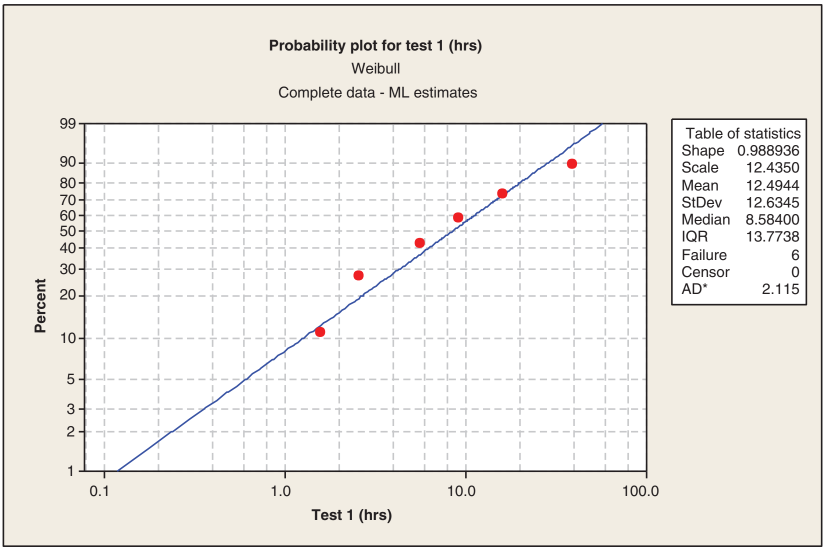
5.33 Using Table 5.5 of Chapter 5, the β for this ratio is =3.5.

5.35

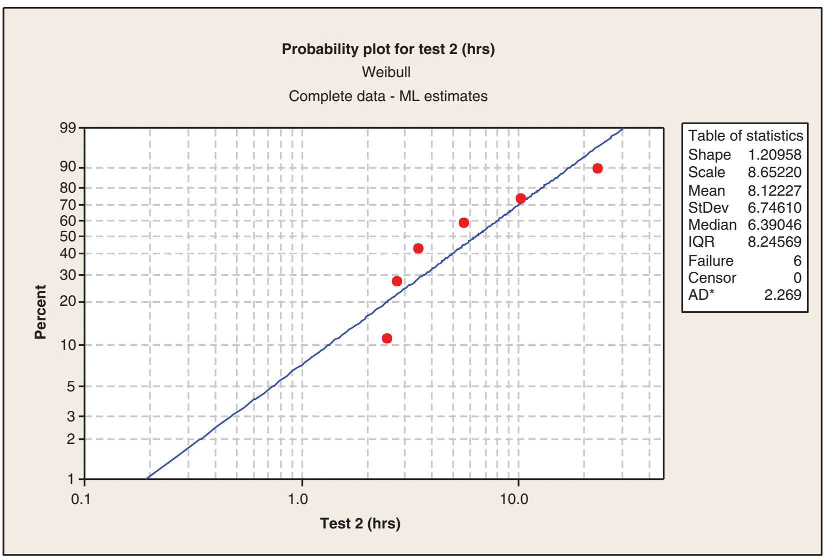


5.37 Ans:

(a)

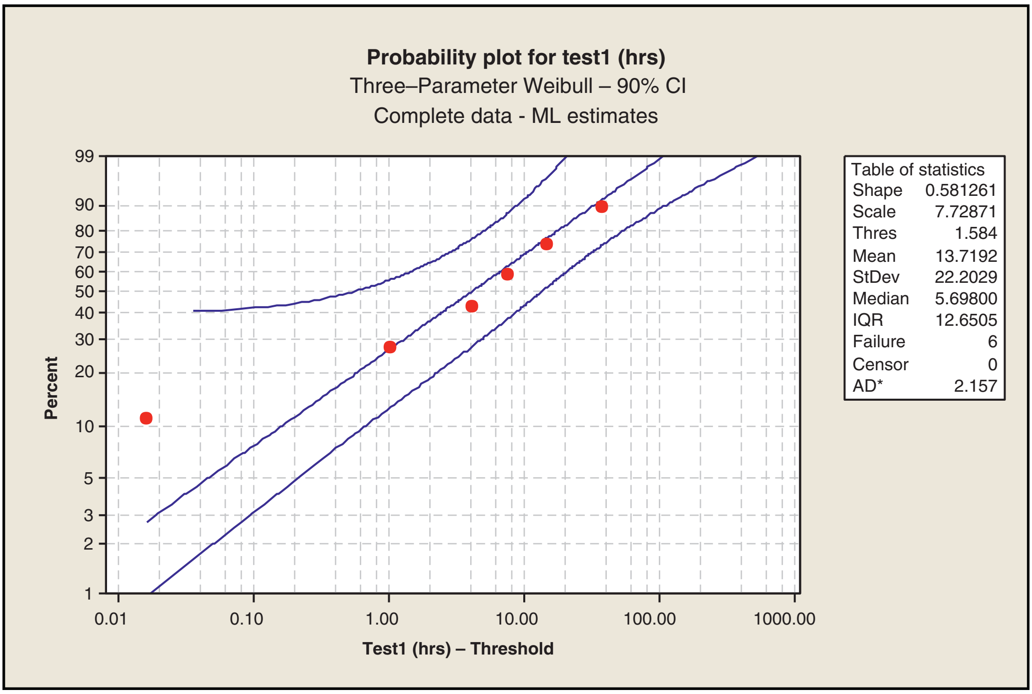


(b)

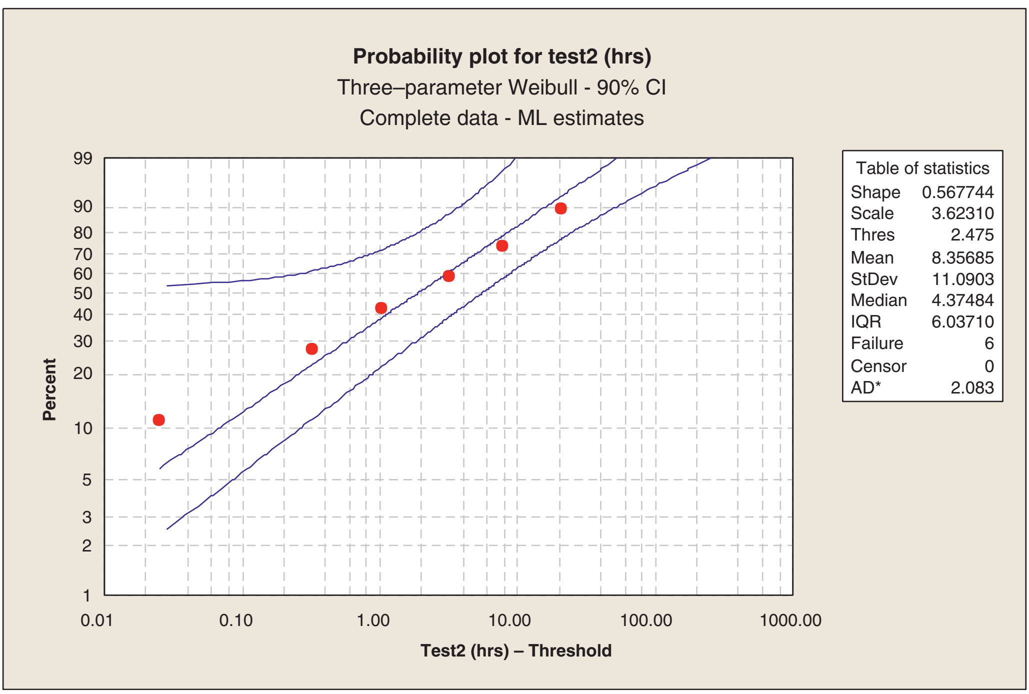


Note: both sets of data need a t_0 correction:

(a)


Probability plot for test1 (hrs)
Three–Parameter Weibull – 90% CI
Complete data - ML estimates
Percent
99
90
80
70
60
50
40
30
20
10
5
3
2
1
0.01
0.10
1.00
10.00
100.00
1000.00
Test1 (hrs) – Threshold
Table of statistics
Shape 0.581261
Scale 7.72871
Thres 1.584
Mean 13.7192
StDev 22.2029
Median 5.69800
IQR 12.6505
Failure 6
Censor 0
AD* 2.157

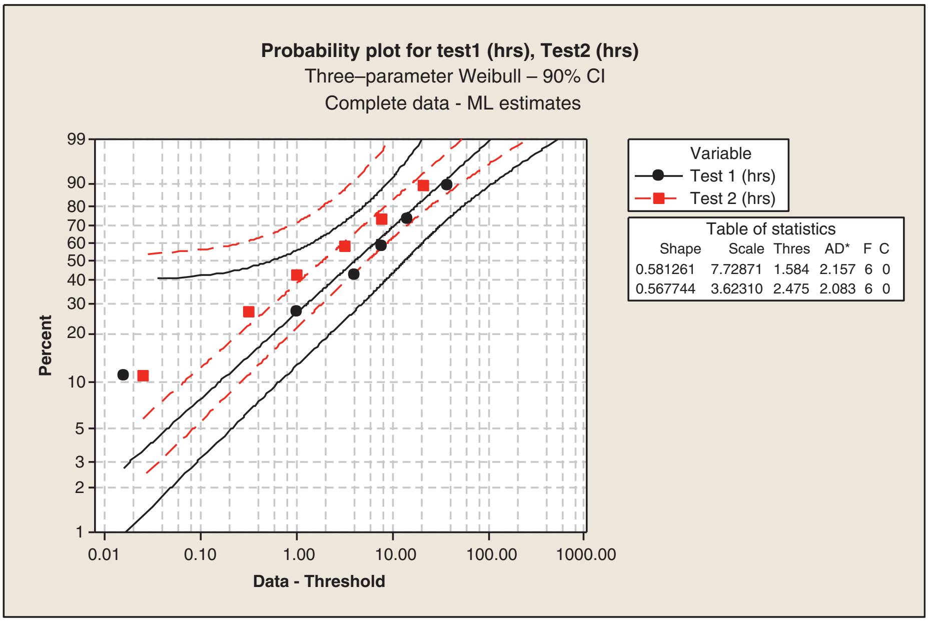
(b)


Probability plot for test2 (hrs)
Three–parameter Weibull - 90% CI
Complete data - ML estimates
Percent
99
90
80
70
60
50
40
30
20
10
5
3
2
1
0.01
0.10
1.00
10.00
100.00
1000.00
Test2 (hrs) – Threshold
Table of statistics
Shape 0.567744
Scale 3.62310
Thres 2.475
Mean 8.35685
StDev 11.0903
Median 4.37484
IQR 6.03710
Failure 6
Censor 0
AD* 2.083

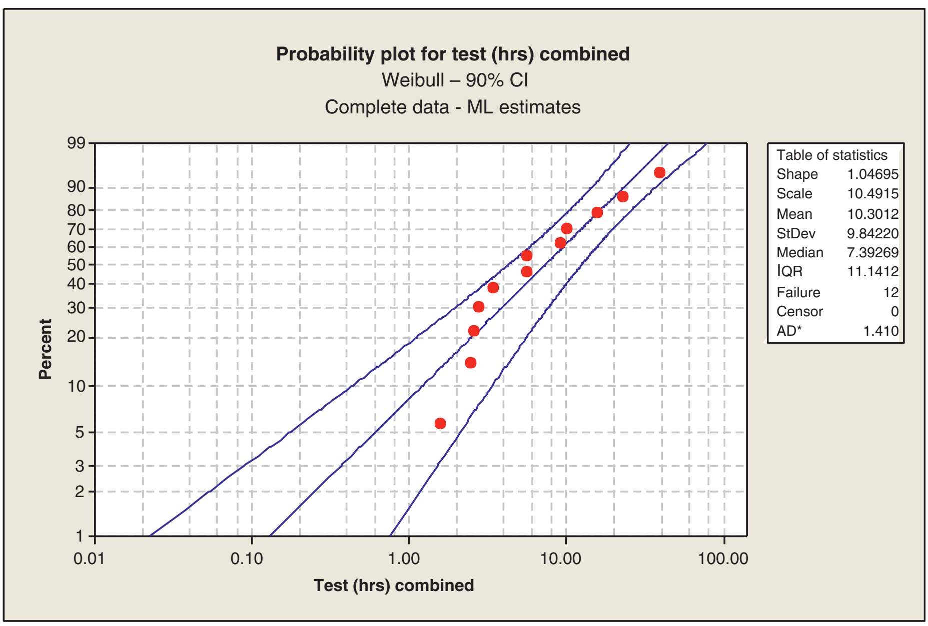
Since Confidence bounds at $p = 0.9$ overlap, there is no statistically significant difference in the two sets of data.

Plotting data as one dataset:

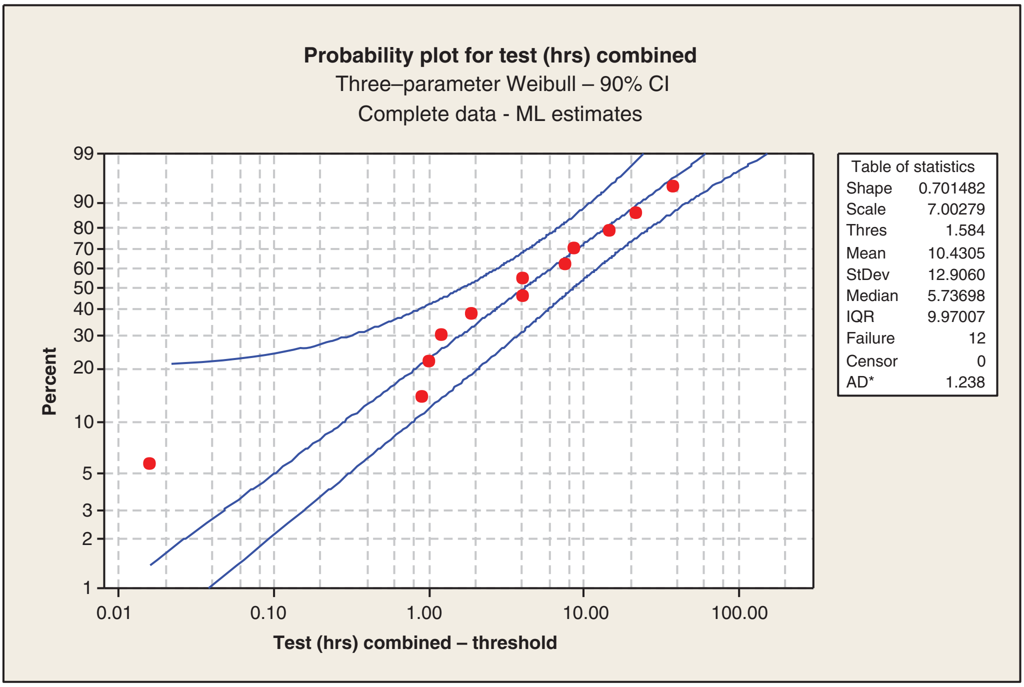
(c)



(d)



Again, the combined data needs a t_0 correction:

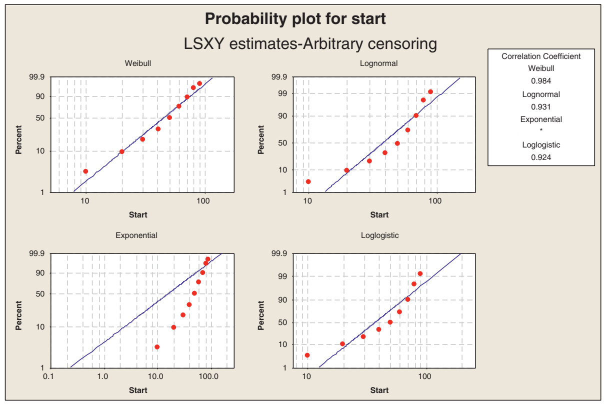


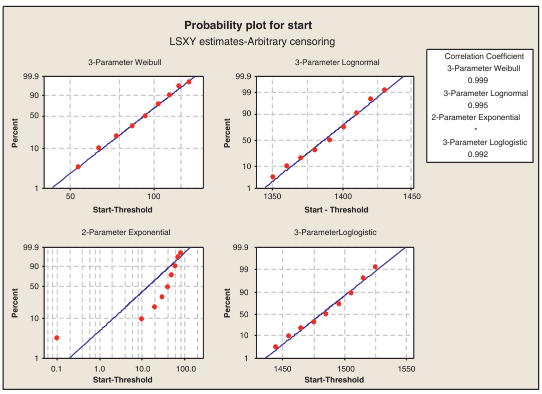
Probability plot for test (hrs) combined
Three–parameter Weibull – 90% CI
Complete data - ML estimates
Percent
99
90
80
70
60
50
40
30
20
10
5
3
2
1
0.01
0.10
1.00
10.00
100.00
Test (hrs) combined – threshold
Table of statistics
Shape 0.701482
Scale 7.00279
Thres 1.584
Mean 10.4305
StDev 12.9060
Median 5.73698
IQR 9.97007
Failure 12
Censor 0
AD* 1.238

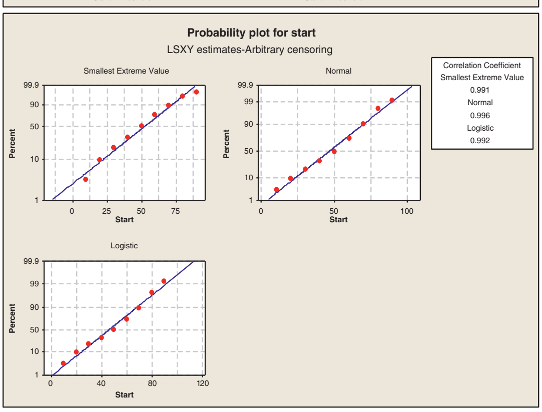
5.39 Ans. Input table for MINITAB:

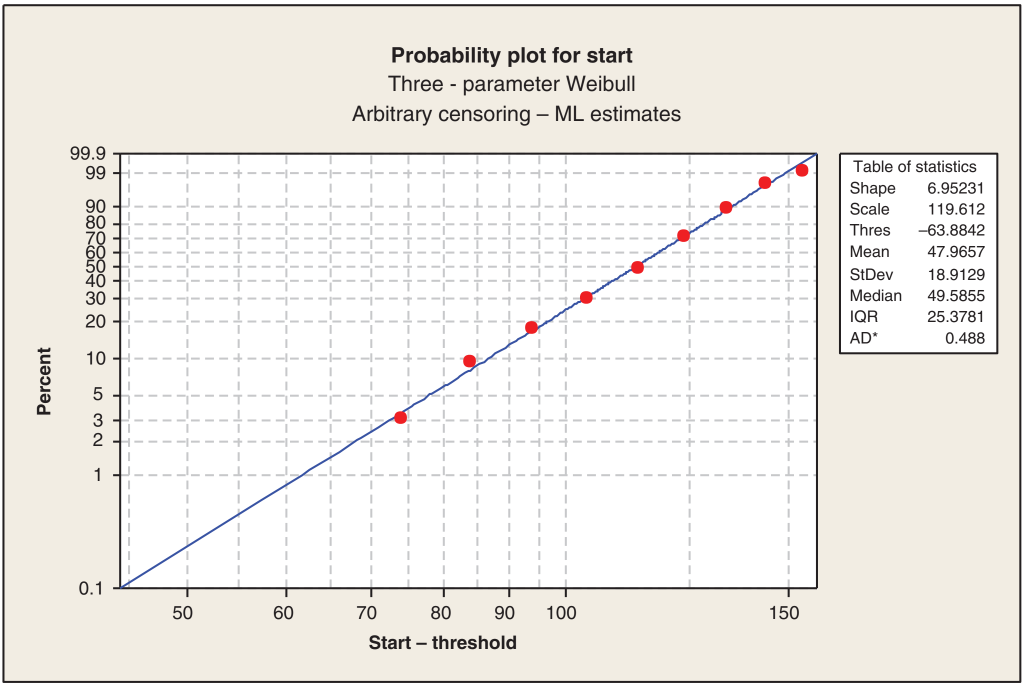
Start	End	Failures
*	10	4
10	20	8
20	30	11
30	40	16
40	50	23
50	60	31
60	70	22
70	80	10
80	90	2
90	100	1

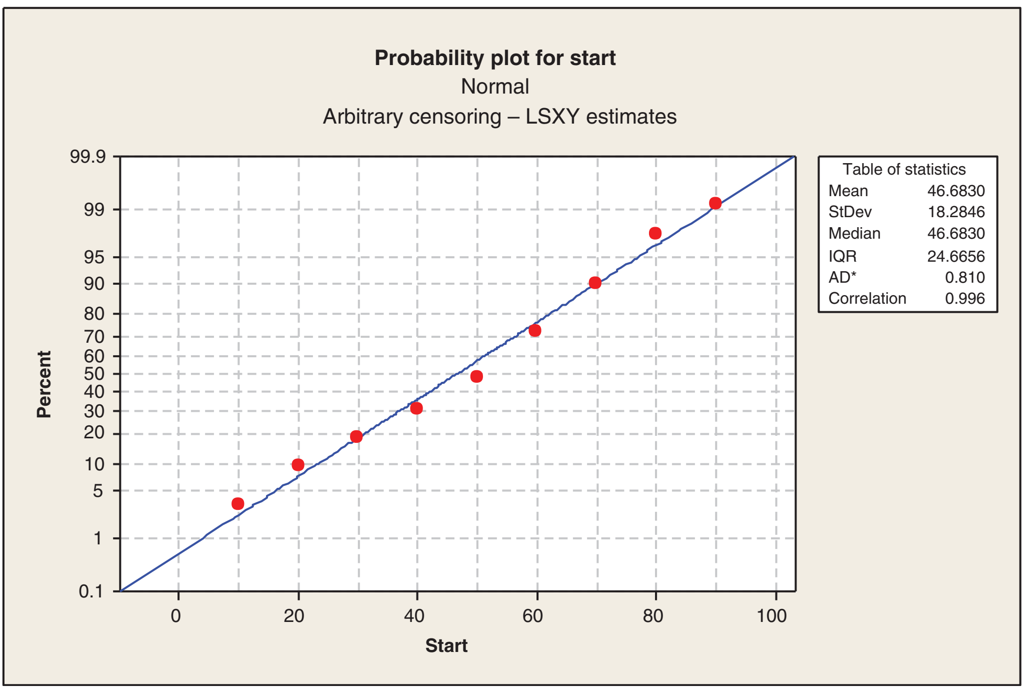
(a)



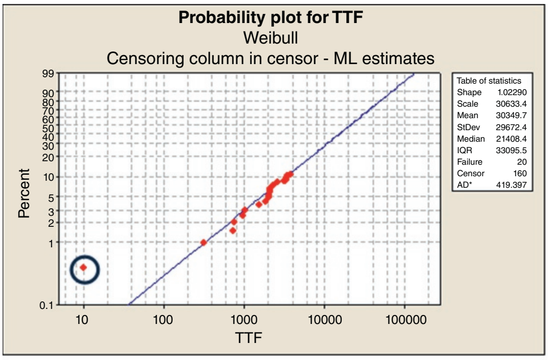





Probability plot for start
Three - parameter Weibull
Arbitrary censoring – ML estimates
Percent
99.9
99
90
80
70
60
50
40
30
20
10
5
3
2
1
0.1
50
60
70
80
90
100
150
Start – threshold
Table of statistics
Shape 6.95231
Scale 119.612
Thres –63.8842
Mean 47.9657
StDev 18.9129
Median 49.5855
IQR 25.3781
AD* 0.488


Probability plot for start
Normal
Arbitrary censoring – LSXY estimates
Percent
99.9
99
95
90
80
70
60
50
40
30
20
10
5
1
0.1
0
20
40
60
80
100
Start
Table of statistics
Mean 46.6830
StDev 18.2846
Median 46.6830
IQR 24.6656
AD* 0.810
Correlation 0.996

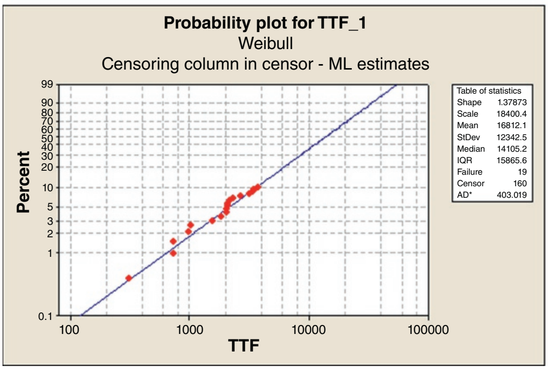
5.41



First failure is an outlier, eliminate and redo plot

Needs a negative t_0?? No.. circled datapoint is an outlier!

Without outlier-- Weibull:



Conditional Risk = (F(8000)–F(4000)/(1–F(4000)) = (0.272–0.115)/(1–0.115) = 0.567

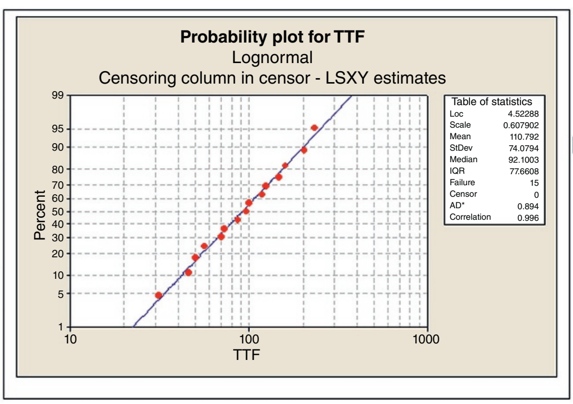
failures between 4000 and 8000 = 0.567*(160) = 91

5.43

Ans.

Input table:

TTF	Freq	Censor
31.4	1	1
45.9	1	1
50.2	1	1
56.4	1	1
70.7	1	1
73.2	1	1
86.6	1	1
96.3	1	1
100.6	1	1
117.9	1	1
124.8	1	1
146.7	1	1
159.5	1	1
205.2	1	1
232.5	1	1



Comparing the two lognormals:

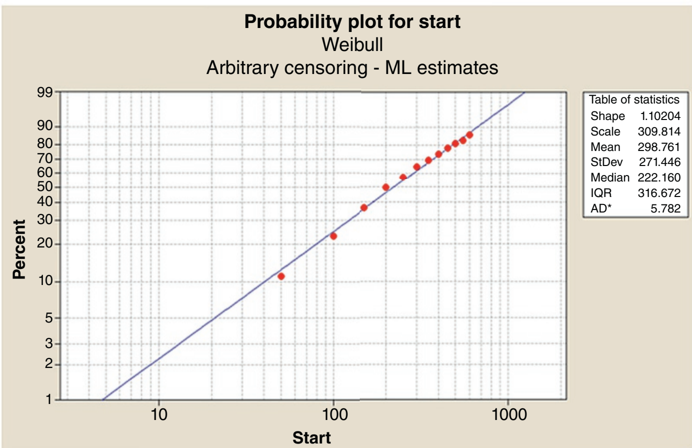
	Exer 6.29 (7 censored)	Exer 6.40 all failed
Loc	4.54	4.52
Scale	0.644	0.608
Mean	83.3	110.8
Correlation	0.993	0.996
AD	51.3	0.894

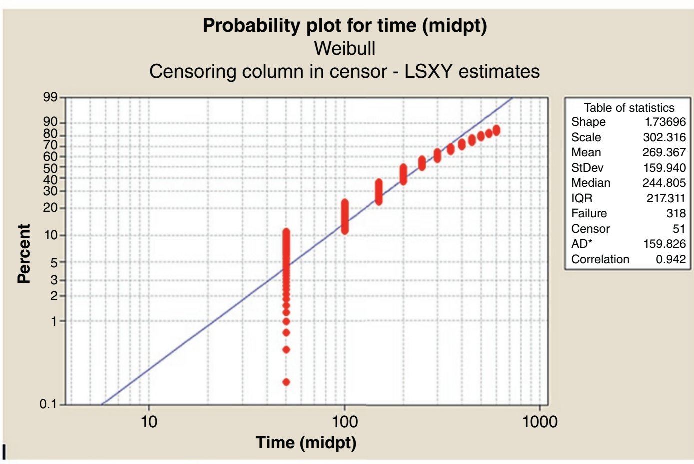
5.45

Ans:Data table:

Start	End	Time interval, hr	Time (midpt)	Freq
*	50	0–50	25	41
50	100	50–100	75	44
100	150	100–150	125	50
150	200	150–200	175	48
200	250	200–250	225	28
250	300	250–300	275	29
300	350	300–350	325	18
350	400	350–400	375	16
400	450	400–450	425	15
450	500	450–500	475	11
500	550	500–550	525	7
550	600	550–600	575	11
600	*		600	51

Weibull plot:

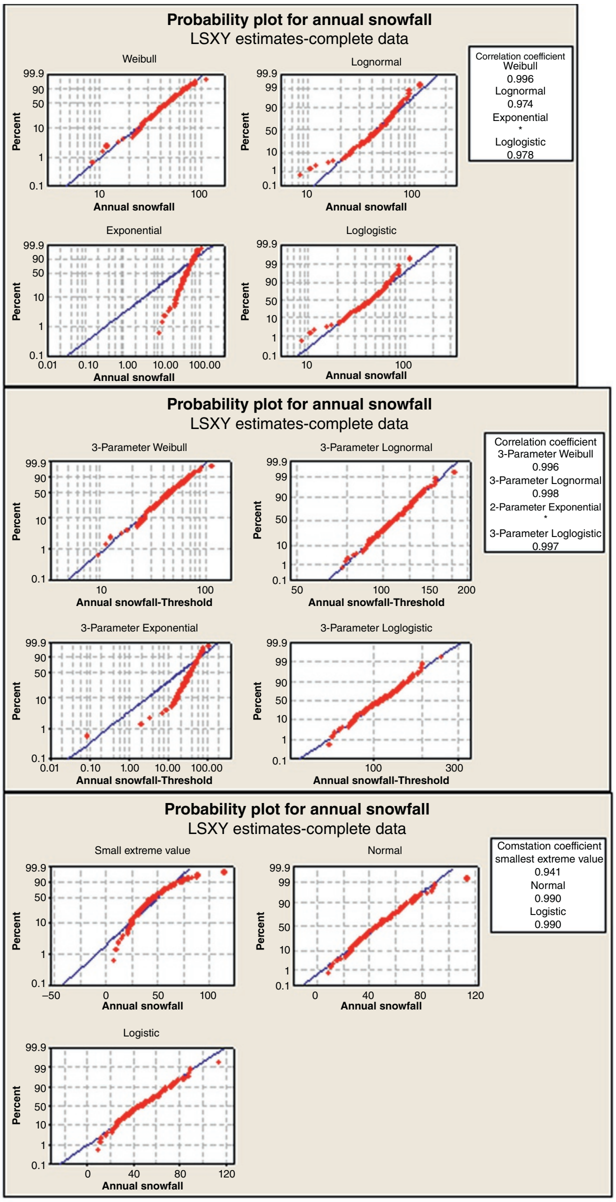




Using the Midpt vaues:AD here is >>AD using Arbitrary censoring.

5.47 (a) ID plots

(a)

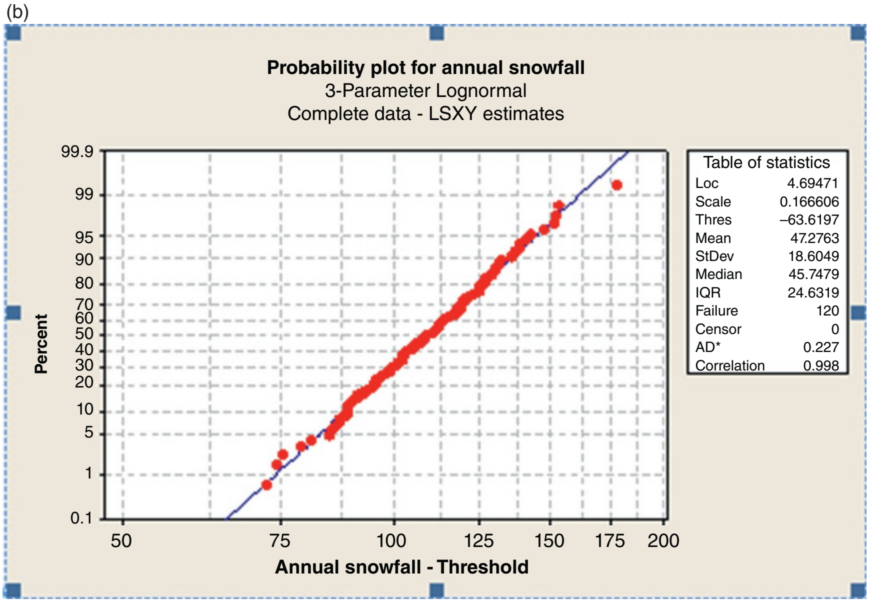


Based on correlation coefficient, three-parameter lognormal is best fit. Doing a two-parameter lognormal plot so we read off 0.01 and 0.99 levels of snowfall: Reading this plot: snowfall of 74” or < will occur with Probability = 0.01: OR the probability of 74” OR MORE will occur with probability 0.99

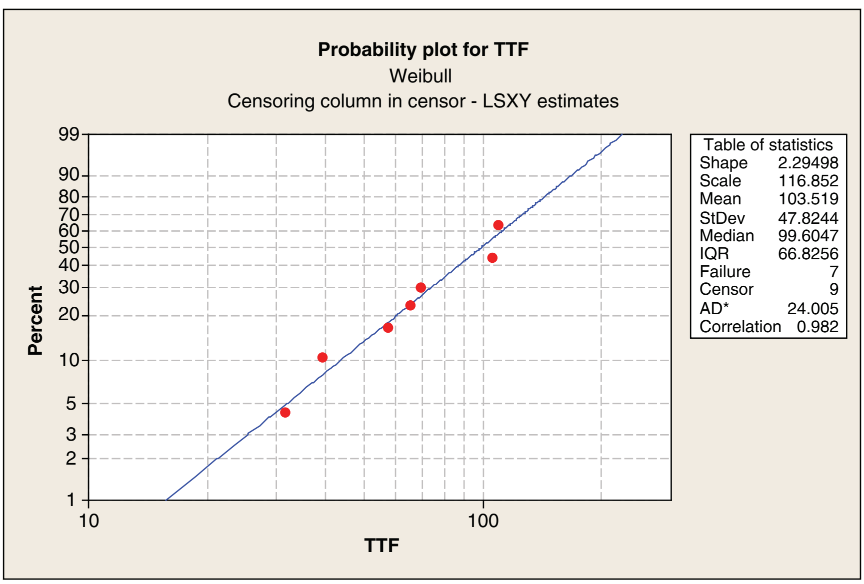
Looking at the three-parameter lognormal:

Probability of 161” OR LESS will occur with probability 0.99; OR the probability of 74” OR MORE will occur with probability 0.99.

(b)



5.49 Consider the following multiply censored data* for the field windings for 16 generators. The times to failure and removal times (in months) are 31.7, 39.2, 57.5, 65.0+, 65.8, 70.0, 75.0+, 75.0+, 87.5+, 86.3+, 94.2 +, 101.7+, 105.8,109.2+ , 110.0, and 130.0+. Make a probability plot of the data. What type of phenomena are we seeing for field windings failures? (NOTE: + indicated a censored value in Nelson's book).



Ans.
$\beta = 2.2$ is indicative of a slow wearout mode.

*From Nelson, *Applied Life Data Analysis*, Wiley, New York, 1982.

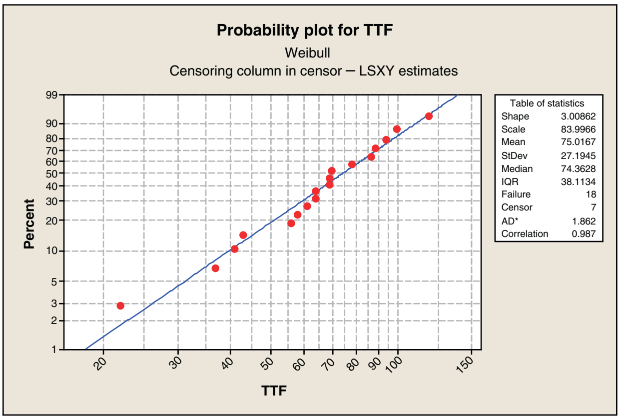
5.51 The following multiply-censored times-to-failure (in hours) have been obtained from a battery-powered motor used in inexpensive consumer products: 22, 37, 41, 43, 56, 57+, 58, 61, 62+, 63+, 64, 64, 65+ , 69, 69, 69+ , 70, 76+, 78, 87, 88+, 89, 94, 100, and 119. (Note + indicates right-censored data.)

(a) Fit the data to a Weibull distribution and estimate the parameters.

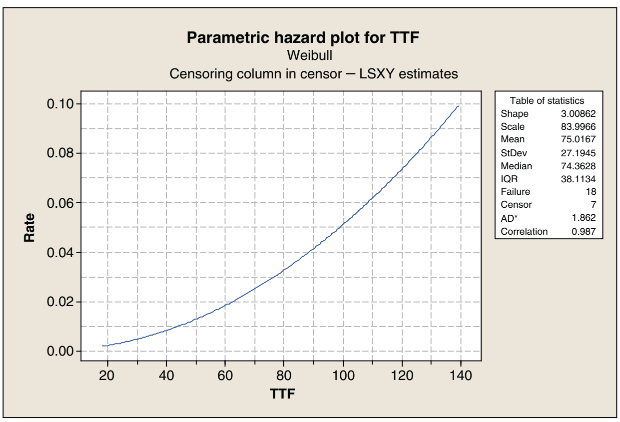
(b) Plot the reliability (survival) and hazard plot for this data

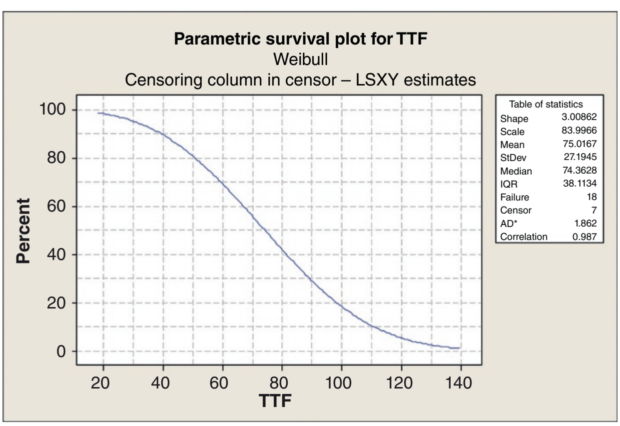
Ans:

(a)



(b)





5.53 Ten units are on test. The units are not replaced when they fail (nonreplacement). One unit fails at $t_1 = 685$ hours, and a second unit fails at $t_2 = 1690$ hours. The test is ended at $t = 2500$ hours with no additional failures.

(a) What is the total accumulated test time?

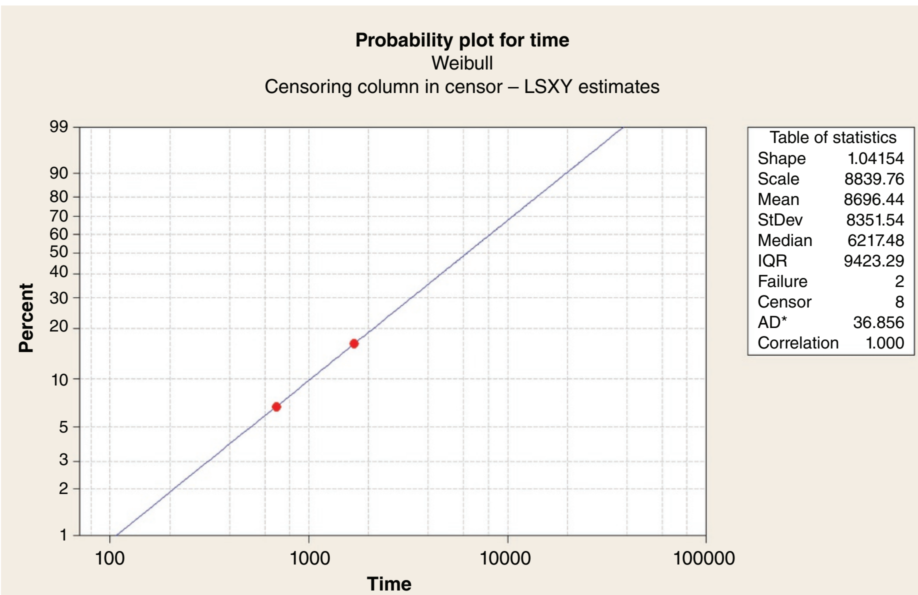
(b) What is the MTTF?

Ans:

(a) $T = 685 + 1690 + (8)(2500) = 22{,}375$ hours

(b) MTTF $= 22375/2 = 11187.5$ hours

And, creating a Weibull plot to check on the (tacit) assumption of exponential:

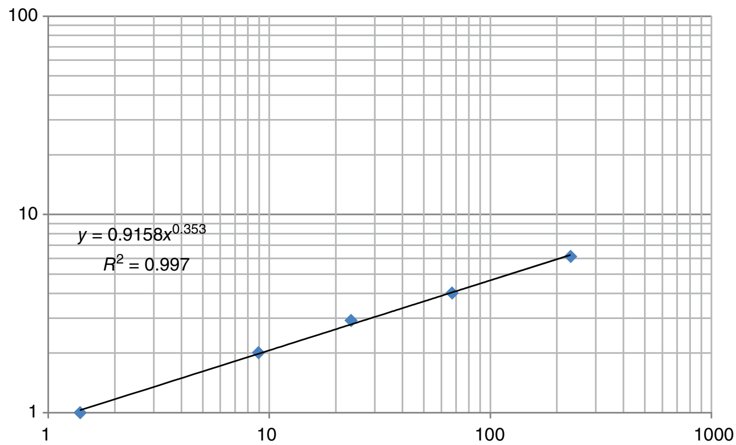


Data input to MINITAB:time	Freq	Censor
685	1	1
1690	1	1
2500	8	0

$\beta = 1.04$ obviously exponential assumption was valid!.

Chapter 6 Reliability Testing

6.1 (a)



(a) $\beta = 0.353$

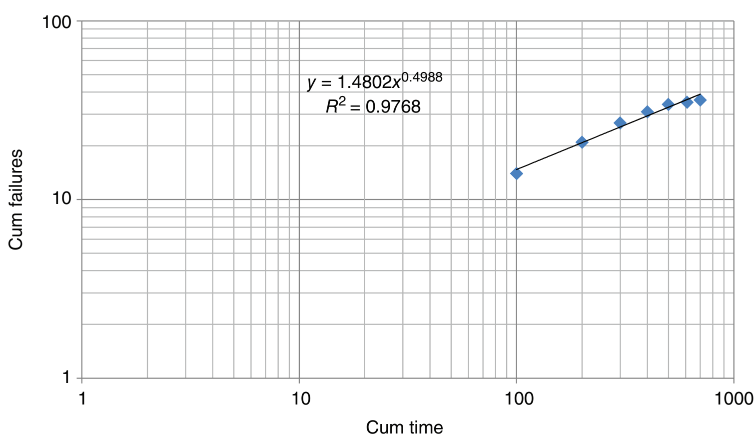
(b) Cumulative failures (1000) $= 0.8158 \times (1000)^{0.353} = 10.5$

Growth slope is <<1.0, hence decreasing failure rate.

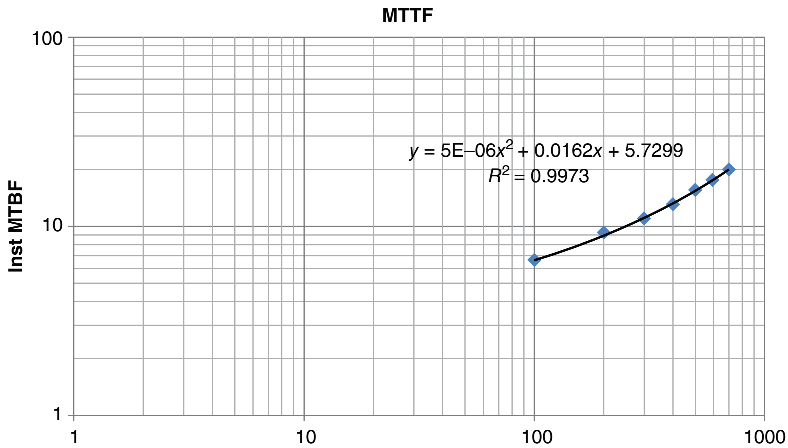
6.3 Data table

T	Cumulative failures	*N*
100	14	14
200	21	7
300	27	6
400	31	4
500	34	3
600	35	1
700	36	1

Reliability Growth plot with fit:



While this plot answered the growth model question, for illustration purposes (talking to the boss), show the instantaneous MTTF plot.



Illustrating that the instantaneous MTBF (newest item with all known fixes) is going up from 7 to ~20 hours. Tell the boss that the test–analyze–fix is working!

6.5

$$R = e^{-\lambda t} \Rightarrow t = \left(\frac{1}{\lambda}\right)\ln\left(\frac{1}{R}\right) = (\text{MTTF})\ln\left(\frac{1}{R}\right) = (20,000)\ln\left(\frac{1}{0.9}\right) = 2107 \ \text{hours}$$

Then,

$$\frac{t}{t_{Acel}} = \left(\frac{V_{Accel}}{V}\right)^3 \Rightarrow V_{Accel} = V\left(\frac{t}{t_{Acel}}\right)^{\frac{1}{3}} = V\left(\frac{2107}{(30)(24)}\right)^{\frac{1}{3}} = V \cdot 1.43$$

6.7 Ans.

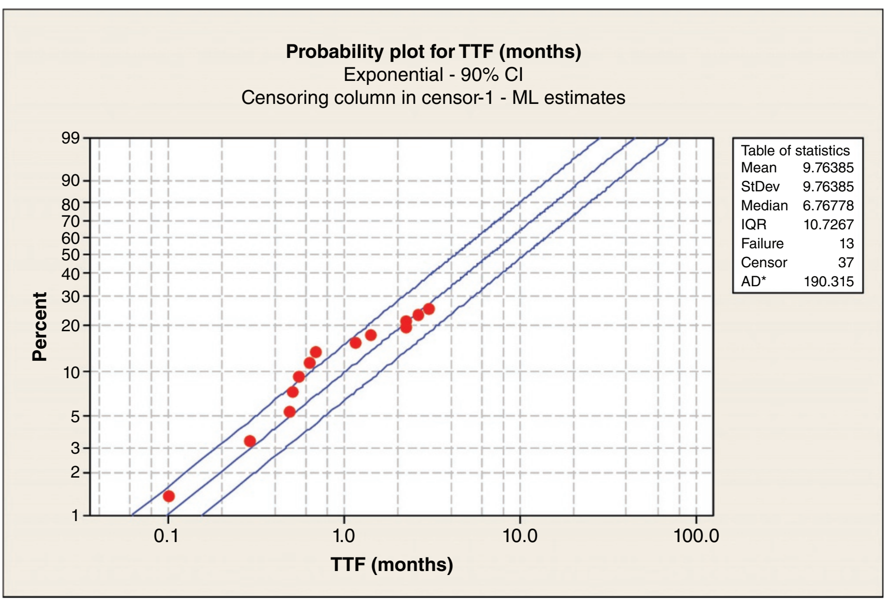


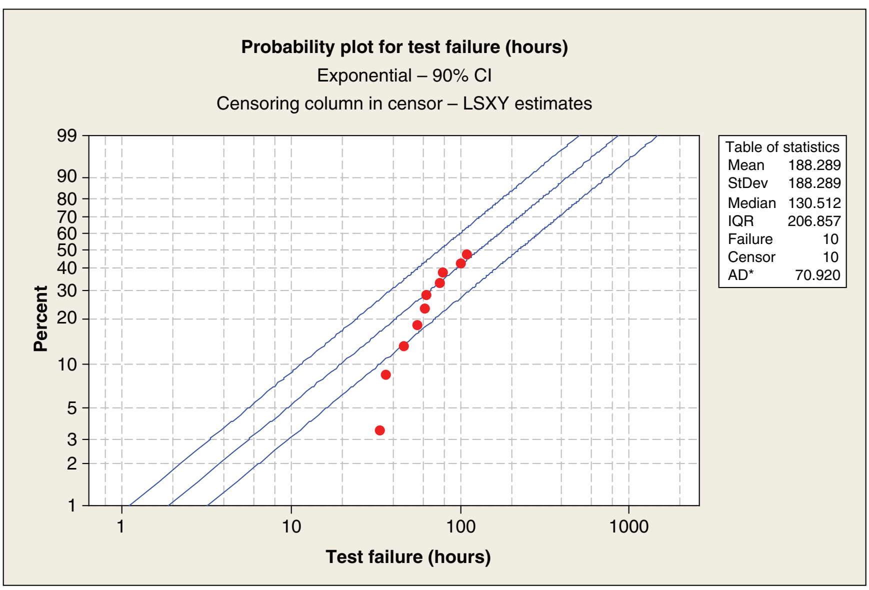
Table in 6.20 becomes

TTF (months)	Freq	Censor-1
0.1	1	1
0.29	1	1
0.49	1	1
0.51	1	1
0.55	1	1
0.63	1	1
0.68	1	1
1.16	1	1
1.4	1	1
2.24	1	1
2.25	1	1
2.64	1	1
2.99	1	1
3	37	0

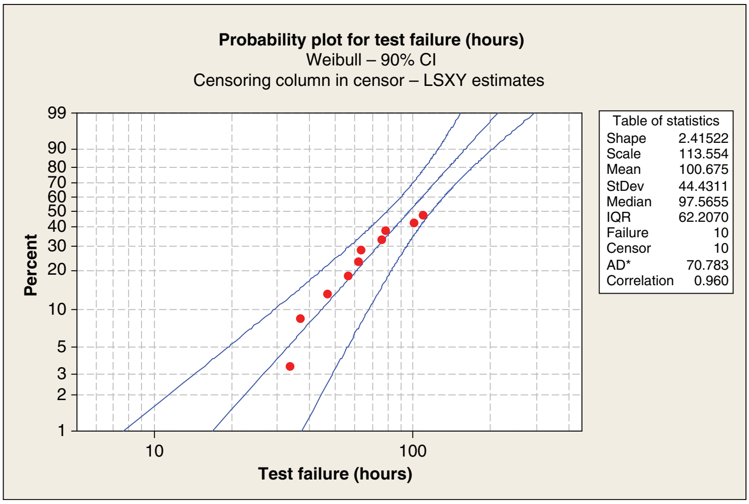
Mean (MTTF) = 9.76.
Table from MINITAB:
Characteristics of distribution

	Standard	90.0%	Normal	CI
	Estimate	Error	Lower	Upper
Mean (MTTF)	9.76385	2.70800	6.18722	15.4080
Standard deviation	9.76385	2.70800	6.18722	15.4080
Median	6.76778	1.87705	4.28865	10.6800

6.9 Ans:



The data are NOT exponential!!
Try Weibull:

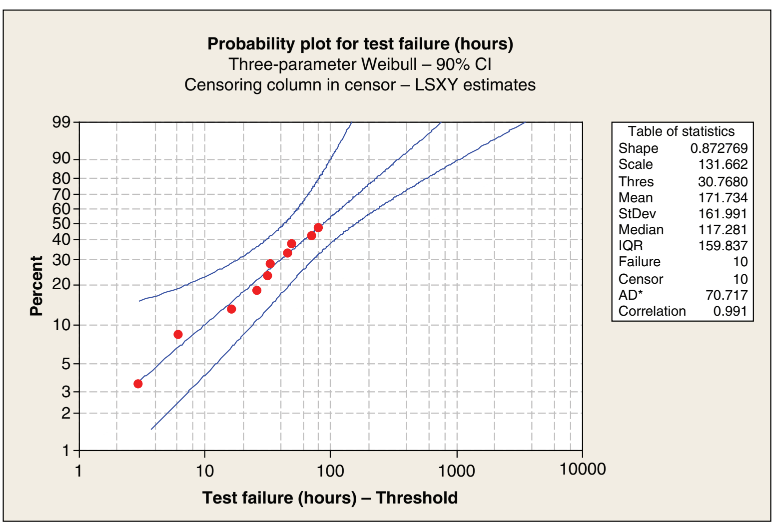


MTTF = 100.68 BUT, the data needs a t_0!!
Parameter estimates

	Standard	90.0%	Normal	CI
Parameter	Estimate	Error	Lower	Upper
Shape	2.41522	0.599575	**1.60554**	**3.63323**
Scale	113.554	13.2048	93.7845	137.490

The t_0 makes the data look like a good fit (note that the correlation went from 0.96 to 0.991).

$$\text{MTTF} = 171.7 + 30.8 = 202.5 \text{ hours}$$



Confidence bounds on parameters and MTTF:
Parameter estimates

Parameter	Standard Estimate	90.0% Error	Normal **Lower**	CI **Upper**
Shape	**0.872769**	**0.303679**	**0.492427**	**1.54688**
Scale	131.662	59.7014	62.4510	277.574
Threshold	30.76800	0	30.7680	30.7680

Characteristics of distribution

	Standard Estimate	**90.0% Error**	**Normal Lower**	**CI Upper**
Mean (MTTF)	**171.734**	**83.9002**	**76.8888**	**383.576**
Standard deviation	161.991	147.156	36.3547	721.810
Median	117.281	33.5726	73.2382	187.809

6.11 Entering Table 6.1 with $\beta = 1.5$ and $n = 20$, factor = 0.2367.
So, factor∗3∗3000 = 0.2367∗9000 = 2130 hours. Testing all 20 bearings for 2130 hours without a failure will assure you of 9000-hour η at 90% confidence.

6.13 Using Table 6.1, note that at 90% confidence you can test 287 pieces, and if they do not fail you have demonstrated 0.992 reliability. Going through Table 6.1 at 90% confidence or more but limiting to 0.9 reliability or more; some of the possibilities from Table 6.1 are highlighted:

Reliability	**Confidence level**					
	90	95	97.5	99	99.5	99.9
0.99999	230258	299572	368887	460515	529830	690773
0.9999	23025	29956	36887	46050	52981	69075
0.999	2302	2995	3688	4603	5296	6905
0.998	1151	1497	1843	2301	2647	3451
0.997	767	998	1228	1533	1764	2300
0.996	575	748	921	1149	1322	1724
0.995	460	598	736	919	1058	1379
0.994	383	498	613	766	881	1148
0.993	328	427	526	656	755	984
0.992	287	373	460	574	660	861
0.991	255	332	409	510	587	765
0.99	230	299	368	459	528	688
0.98	114	149	183	228	263	342
0.97	76	99	122	152	174	227
0.96	57	74	91	113	130	170
0.95	45	59	72	90	104	135

6.15 $AF = \exp\,[EA/K(1/Tu - 1/\text{Ts})]$
$AF = \exp\,[(0.8/8.617\times10^{-5})(1/323 - 1/373)] = 47$

Assuming that the increased temperature did not cause new failure modes, two days of testing at 100 °C is equivalent to about three months of use.

6.17
$$AF = \frac{t_{\text{use}}}{t_{\text{test}}} = \exp\left[\left(\frac{E_a}{kT}\right)\left(\frac{1}{T_{\text{Use}}} - \frac{1}{T_{\text{test}}}\right)\right]$$
$$AF = \exp\left[\left(\frac{0.7\ \text{eV}}{0.00008617eV}\right)\left(\frac{1}{298} - \frac{1}{363}\right)\right] = \exp(4.8813) = 131.8$$

6.19
$$\frac{\lambda}{\lambda_0} = \exp\left(\frac{0.35E}{8.63 \times 10^{-5}}\left(\frac{1}{288} - \frac{1}{303}\right)\right)\exp\left(\frac{0.35E}{8.63 \times 10^{-5}}\left(1.7189 \times 10^{-4}\right)\right) = 2.0$$

- Typically, failure rates change by a factor of 1.2–2.0 for a change in temperature of 15 °C, the higher factor being applied to transistors, and some capacitors and the lower factor being appropriate for resistors.
- In general, failure rates increase exponentially as temperature increases.

6.21 The total unit test time:

$$T = 450 + 800 + (8) \times (1000) = 9250 \text{ hours}$$

The estimate of MTBF:

$$\Theta = T/r = 9150/2 = 4625 \text{ hours}$$

From the χ^2 distribution:

$$\chi^2_{(0.10)\ 6} = 10.645$$

The lower 90% confidence limit:

$$\Theta_{\alpha = 0.10} = (2) \times (9250)/(10.645) = 1740 \text{ hours}$$

6.23 $1 - C = R^N$ (since this is testing with 0 failures)
where C is the confidence level (e.g. 90% confidence = 0.90), R is the reliability, and N is the number of tests without failure.
In this case, $C = 0.60$, $R = 0.90$
$1 - 0.60 = 90^N$
$0.40 = 0.90^N$

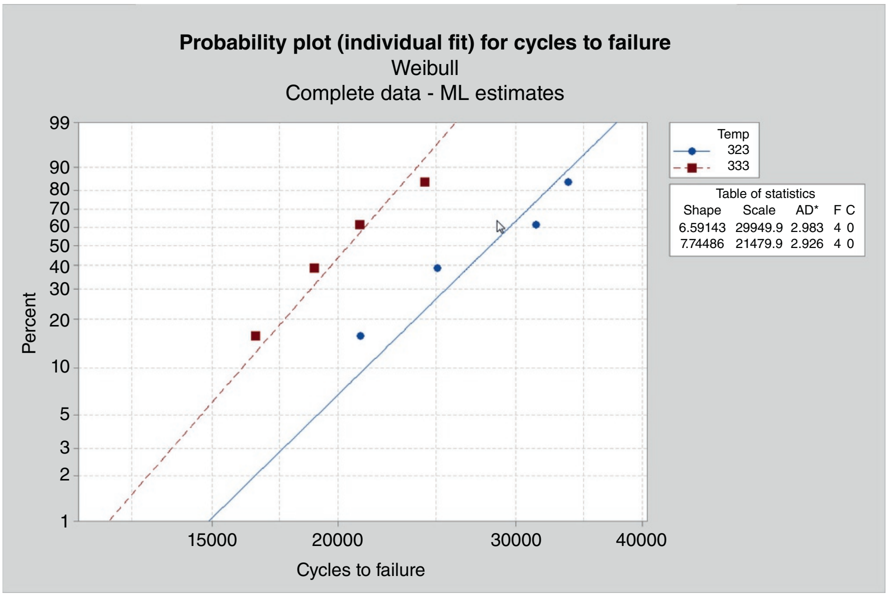
$$N = \frac{\ln(0.40)}{\ln(0.90)} = 8.7 \approx 9$$

6.25 $AF = 8.68$.

6.27 Using MINITAB's accelerated life testing, assuming an Arrhenius relationship:
MINITAB input:

Temp	Cycles to Failure
323	21,045
323	25,077
323	31,407
323	33,812
333	16,551
333	18,935
333	20,996
333	24,363

Plotting both input temperature data together:

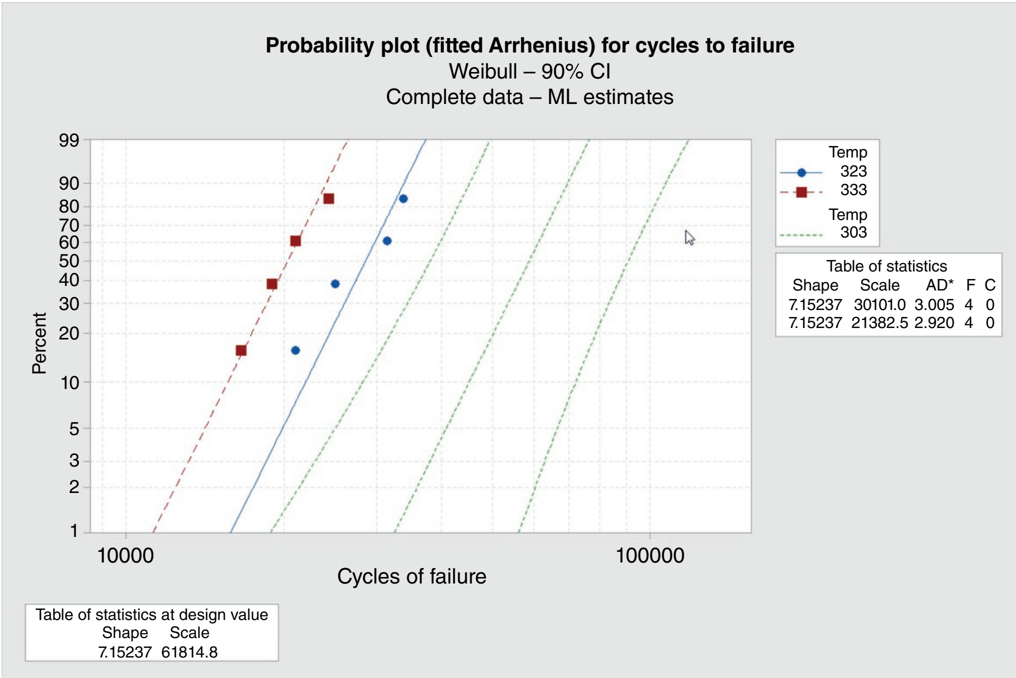


Touching the dashed line (303 °K) will produce:

Temp = 303

Percent	Cycles to Failure	Lower Bound	Upper Bound
1	32491.5	18809.9	56124.6
2	35823.3	21302.8	60241.3
3	37939.9	22891.3	62881.3
4	39525.4	24080.9	64875.6
5	40807.6	25041.5	66500.2
6	41891.9	25852.3	67883.2
7	42836.3	26556.9	69094.9
8	43676.1	27182.1	70178.4
9	44434.7	27745.7	71162.2
10	45128.4	28259.7	72066.1
20	50120.6	31918.7	78702.2
30	53517.3	34358.2	83360.2
40	56273.7	36302.6	87231.4
50	58727.0	38004.6	90748.6
60	61063.9	39599.5	94162.9
70	63440.1	41194.1	97699.6
80	66067.6	42925.0	101687
90	69460.1	45109.3	106956
91	69896.0	45385.8	107643
92	70364.2	45681.8	108383
93	70872.9	46002.2	109190
94	71433.5	46353.7	110083
95	72063.4	46746.9	111090
96	72063.4	46746.9	111090

Using MINITAB's "Accelerated Life Testing" subsection:



So, the expected cycle to failure at B10 and 303 °K is 45,128, with 28,260 lower 90% confidence bound.

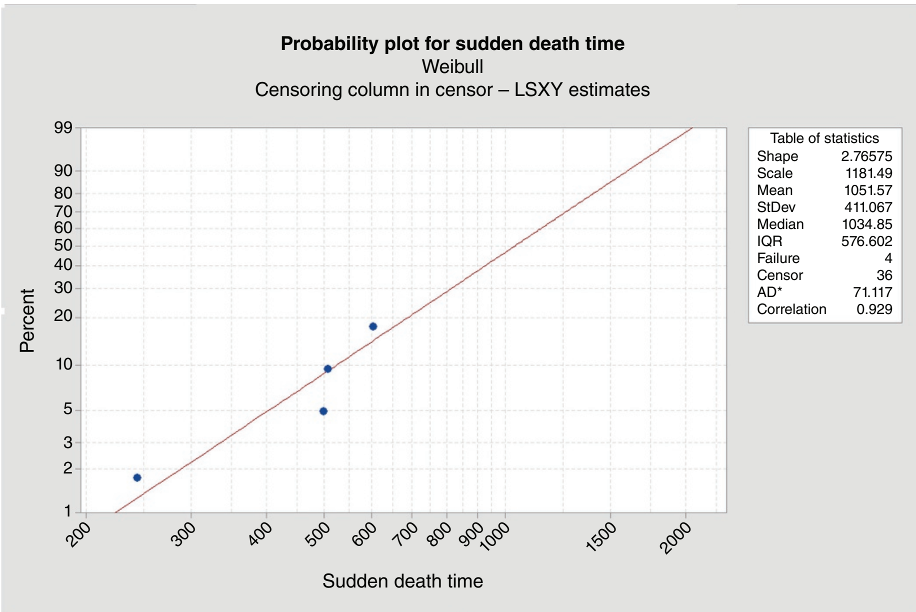
6.29 Using the top portion of Table 6.2 (through $n = 14$):

	Beta									
	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5
N	Infant Mortality	Random	Early Wearout					Old Age Rapid Wearout		
2	1.3255	1.1513	1.0985	1.0730	1.0580	1.0481	1.0411	1.0358	1.0318	1.0286
3	0.5891	0.7675	0.8383	0.8761	0.8996	0.9156	0.9272	0.9360	0.9429	0.9485
4	0.3314	0.5756	0.6920	0.7587	0.8018	0.8319	0.8540	0.8710	0.8845	0.8954
5	0.2121	0.4605	0.5963	0.6786	0.7333	0.7722	0.8013	0.8238	0.8417	0.8563
6	0.1473	0.3838	0.5281	0.6195	0.6818	0.7267	0.7606	0.7871	0.8083	0.8257
7	0.1082	0.3289	0.4765	0.5735	0.6410	0.6903	0.7278	0.7573	0.7811	0.8006
8	0.0828	0.2878	0.4359	0.5365	0.6076	0.6603	0.7006	0.7325	0.7582	0.7795
9	0.0655	0.2558	0.4030	0.5058	0.5797	0.6348	0.6774	0.7112	0.7386	0.7614
10	0.0530	0.2303	0.3757	0.4799	0.5558	0.6129	0.6573	0.6927	0.7216	0.7455
11	0.0438	0.2093	0.3525	0.4575	0.5350	0.5938	0.6397	0.6764	0.7064	0.7314
12	0.0368	0.1919	0.3327	0.4380	0.5167	0.5768	0.6240	0.6618	0.6929	0.7188
13	0.0314	0.1771	0.3154	0.4209	0.5004	0.5616	0.6098	0.6487	0.6807	0.7074
14	0.0271	0.1645	0.3002	0.4055	0.4858	0.5479	0.5971	0.6368	0.6696	0.6970

	Current η = 300	600	
Sample size (units)	η multiplier	Test time per unit	Total time on test
4	0.871	522.6	2090.4
8	0.7325	439.5	3516

Notice that 4 units and less total test time will suffice to show 2× lifesaving.

6.31



6.33 The reliability goal may be stated mathematically as $R(2300) = 0.95$, which means that the reliability of the vane system is 0.95 (95% succeeding, 5% failing) at 2300 cycles. First, convert this reliability goal to a characteristic life goal: substitute $t = 2300$ cycles; $R(t) = 0.95$, and $\beta = 3$ into:

$$\eta = \frac{t}{\left[-\ln\left(R(t)\right]^{\frac{1}{\beta}}\right.} = \frac{2300\text{ cycles}}{[-\ln(0.95]^{\frac{1}{3}}} = 6190.2\text{ cycles}$$

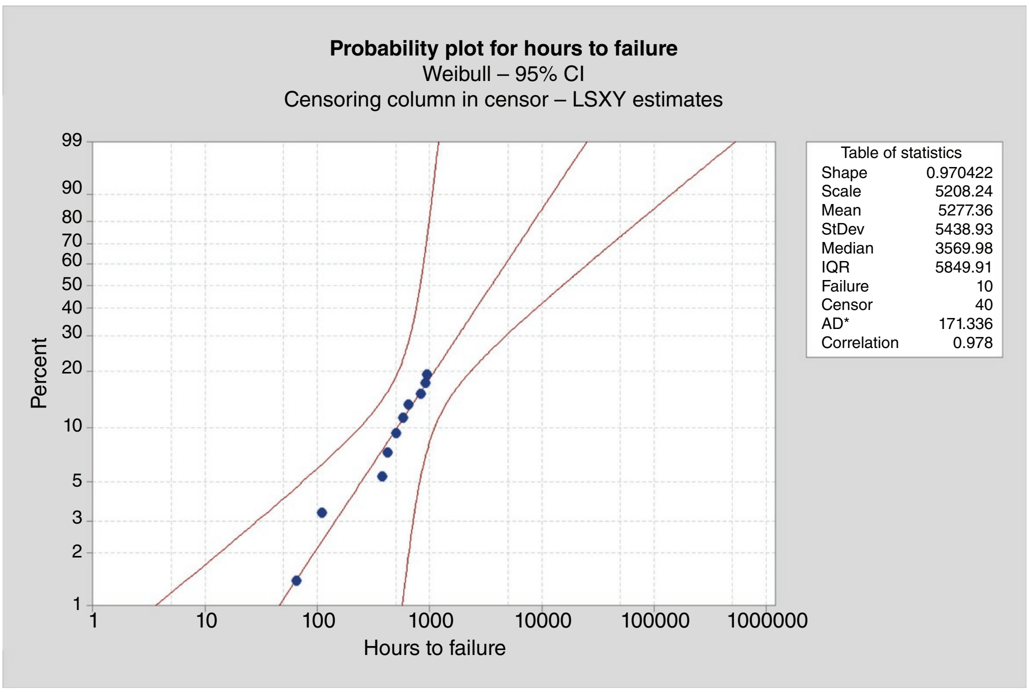
The number of test cycles per turbine was not fixed. The only constraint was that it should not exceed 5000 cycles. The table below shows the number of turbines required, assuming 3000, 4000, and 5000 test cycles accumulated on each as well as the total test cycles required:

Test cycles per turbine	Ratio of test cycles to η	Number of turbines required – Table 6.3	Total test cycles
3000	0.484	22	66,000
4000	0.646	9	36,000
5000	0.808	5	25,000

Therefore, the test plan that satisfies the test requirements and that requires the fewest total test cycles is to test 5 turbines for 5000 cycles each. If all turbines complete the test, with vane erosion within the allowable limits, then no more than 5% of the turbines will be rejected for excessive erosion prior to 2300 cycles, with 90% confidence.

6.35 MINITAB input table:

Hours to failure	Censor	Freq
65	1	1
110	1	1
380	1	1
420	1	1
505	1	1
580	1	1
650	1	1
840	1	1
910	1	1
950	1	1
950	0	40



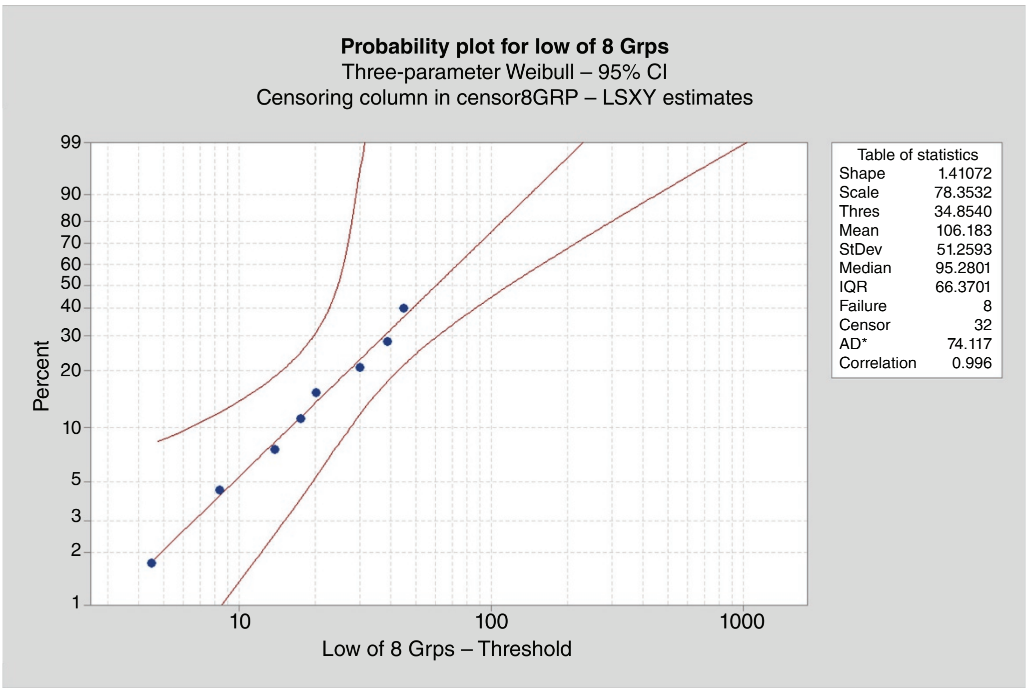
6.36 **MINITAB INPUT TABLE:**

Low of 8 Grps	Censor 8 GRP	Freq 8 Grp
52.28734464	1	1
48.70439991	1	1
43.16654463	1	1
39.31593549	1	1
64.82848045	1	1
79.79845537	1	1
73.44525838	1	1

(*Continued*)

Low of 8 Grps	Censor 8 GRP	Freq 8 Grp
55.05663793	1	1
52.28734464	0	4
48.70439991	0	4
43.16654463	0	4
39.31593549	0	4
64.82848045	0	4
79.79845537	0	4
73.44525838	0	4
55.05663793	0	4

Resulting initial two-parameter Weibull plot:

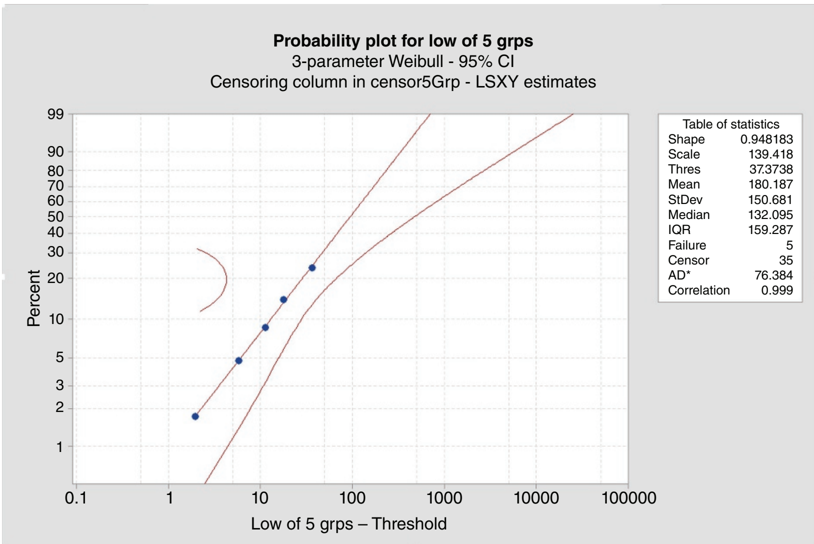


Very good fit. Notice that the slope is close to the same as that in Exercise 6.35.

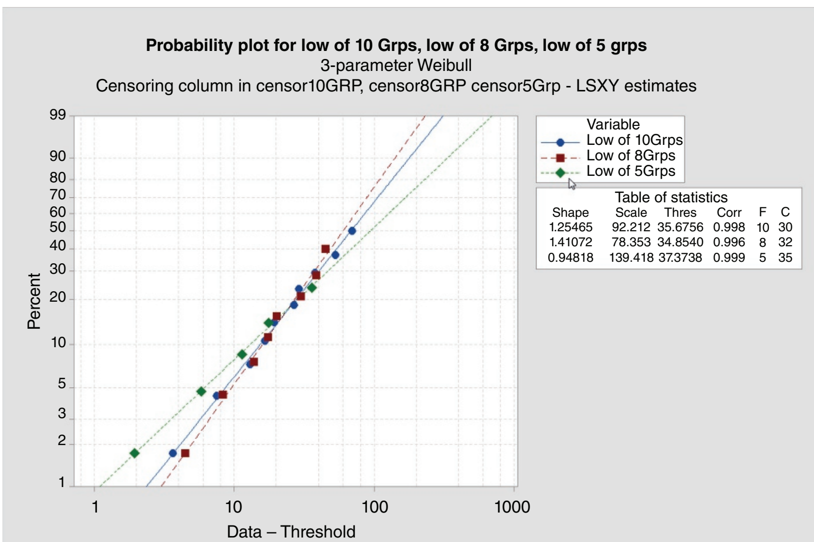
6.37 **MINITAB INPUT TABLE:**

Low of 5 grps	Censor 5 Grp	Freq 5 Grp
48.70439991	1	1
43.16654463	1	1
39.31593549	1	1
73.44525838	1	1
55.05663793	1	1
48.70439991	0	7
43.16654463	0	7
39.31593549	0	7
73.44525838	0	7
55.05663793	0	7

Resulting initial three-parameter Weibull plot:



A Weibull of all three (Exercises 6.35, 6.36, and 6.37) shows that there is no significant difference in results (notice how the confidence bounds and fits are on top of each other).



6.39 Acceleration is 4×, so =2500 hours at 4× cyclic rate in accelerated time is 10,000 hours at normal cycles.
Hence,

$$R(1000) = e^{-\left(\frac{1000}{10000}\right)^{1.7}} = 0.98$$

6.41 From Eq. (6.60), the ratio of use life to accelerated life is

$$\frac{L_{Use}(S)}{L_{Accel}(S)} = e^{\frac{E_A}{K}\left(\frac{1}{T_{Use}} - \frac{1}{T_{Accel}}\right)}$$

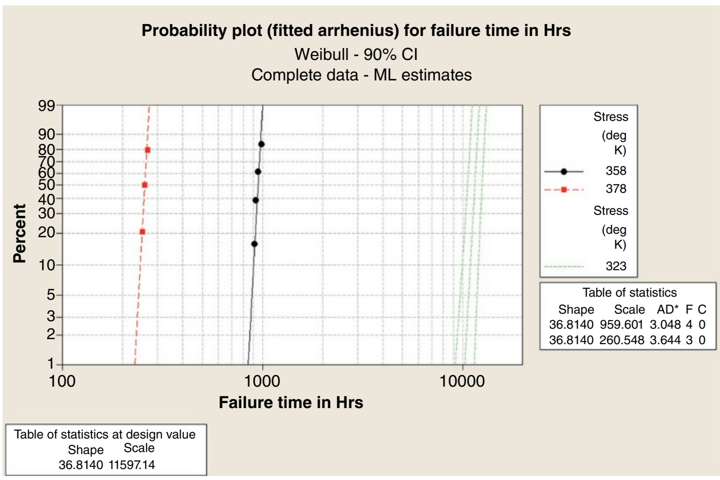
So,

$$L_{Use}(S) = L_{Accel}(S)\left[e^{\frac{E_A}{K}\left(\frac{1}{T_{Use}} - \frac{1}{T_{Accel}}\right)}\right] = 2750\left[e^{\frac{0.5}{8.63\times 10^{-5}}\left(\frac{1}{358} - \frac{1}{423}\right)}\right]$$
$$= 2750[12.02] = 33,064 \text{ hours}$$

And, by Eq. (6.65), $AF = 12.02$

Since, Median Rank(2750) = 0.067, if you wanted to put the use distribution on the same plot as the accelerated plot, you could do that, assuming the same slope.

6.43



The steep slope shows up as very tight confidence bounds.

At 0.9 reliability, the bounds 9950–11962 with a median value = 10,910 hours

Stress (deg K) = 323			
Percent	**Failure time in hours**	**Lower bound**	**Upper bound**
1	10235.1	9172.56	11420.7
2	10431.0	9402.99	11571.5
3	10548.0	9539.03	11663.8
4	10632.3	9636.17	11731.3
5	10698.4	9711.92	11785.1
6	10753.1	9774.11	11830.1
7	10799.7	9826.94	11868.8
8	10840.5	9872.91	11903.0
9	10876.9	9913.64	11933.7
10	10909.7	9950.24	11961.6
20	11134.3	10196.8	12158.1
30	11277.1	10349.1	12288.3
40	11387.7	10464.5	12392.2
50	11482.5	10561.7	12483.5
60	11569.8	10649.6	12569.6

Stress (deg K) = 323			
Percent	**Failure time in hours**	**Lower bound**	**Upper bound**
70	11656.0	10734.7	12656.3
80	11748.2	10824.1	12751.3
90	11863.1	10932.9	12872.4
91	11877.5	10946.4	12887.9
92	11892.9	10960.7	12904.5
93	11909.6	10976.1	12922.4
94	11927.8	10993.0	12942.2
95	11948.2	11011.7	12964.4
96	11971.5	11033.0	12989.9
97	11999.4	11058.3	13020.6
98	12035.1	11090.5	13060.2
99	12088.6	11138.1	13120.1

Chapter 7 Failure Modes and Effects Analysis (FMEA) – Design and Process

7.1

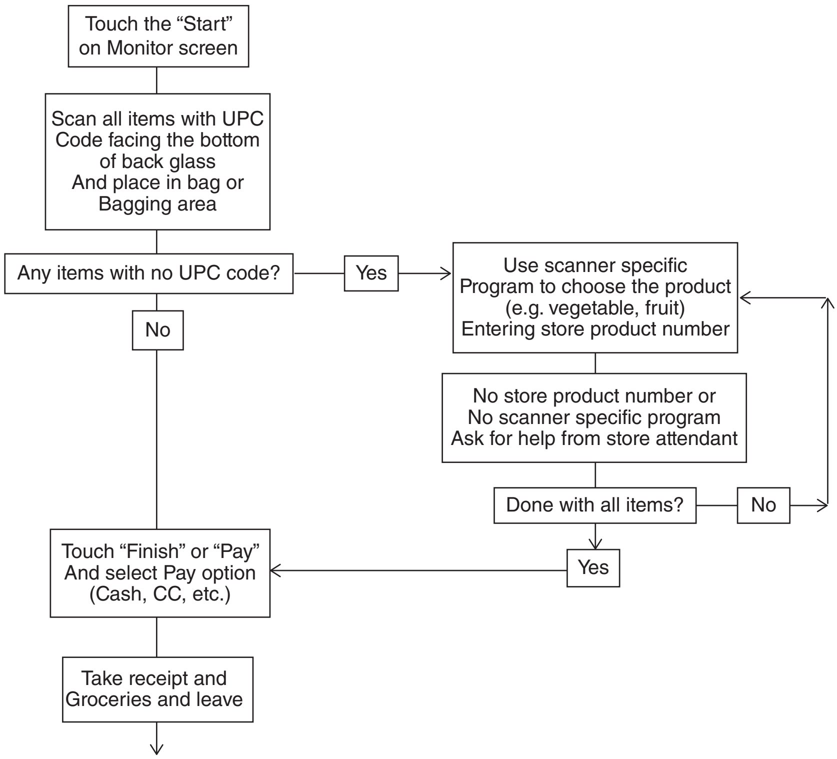
Welding shop
___ Subsystems FMEA Number :
___ Component : Design Responsibility : Big John Prepared by :
Model : Key Date : FMEA Date (Orig.) :
Core Team : Welding

Process step	Potential failure modes	Potential failure effects	Severity	Potential causes	Occurrence	Current controls	Detect	R.P.N.	Recommended actions
Working with Saws	Throwing sparks	Fire	6	Working adjacent to flammable materials	9	Fire extinguisher nearby	9	486	
Argon welding	Exposure to fumes and Toxix gas	Occupational disease	9	Fail to use appropriate protective masks	8	Exhaust hoods	5	360	
Electric welding	Throwing sparks	Burning	5	Nature of the process	6	None	4	120	
	Fall from Height	Injuries	9	Working at height	7	Safety Training	5	315	
Cutting metals	explosion of gas cylinder	Fire & injuries	7	Lack of training & poor maintenance	3	Safety Training	8	168	
CO_2 welding	Flashback flame	Explosion	6	Equipment failure	5	Safety Training	5	150	
Welding	Fire	Fire	5	Fail to separate full and empty cyclinders	3	Safety Training	8	120	
	Collision with obstacles	Injuries	6	Improper layout	3	Safety Training	4	72	
	Collision with forklift	Injuries	6	No warning device	7	Safety Training	4	168	
	Hearing loss	Deafness	6	High noise levels at workplace	8	Wear proper gear	3	144	

7.3

Simple answer:

Better answer:



7.5 ("answer"... will vary according to bicycle studied)

Item and function	Failure mode	Effects of failure	S	Causes of failure	O	Design controls	D	RPN	Recommended actions
Toe Strap Clip: attachment for foot straps	Fracture (snapped)	Foot slips out/ distraction	2	Material not strong enough	7	Shorter than ground clearance to pedal	3	42	Stronger material or method of keeping pedal upright
Crank bearing set allows for pedal rotation	Dirty/ seized	Pedal rotation feels rough or is too hard for user	3	Contamination from dust/dirt, lack of lubrication, not properly preloaded	2	dust caps	4	24	Use better sealed bearing set
Pedal bearing set	Dirty/ seized	Pedal refuses to rotate independently from crank arms/bearings feel rough	3	Contamination from dust/dirt, lack of lubrication, not properly preloaded	2	End caps for pedal housing	4	24	Sealed end caps
Foot grips: provide level and tractive surface to push	Abrasion, yielding	Pedal deforms	1	Impact with ground during operation	1	N/A	1	1	N/A
Crank arm: transfer pedal rotation to crank/ add mechanical advantage	Fracture (casting failure)	Make bike unstable / rapid user weight transfer	8	Unexpected loading	1	N/A	8	64	Inspect at the factory
Chain	Oxidation/ fracture	Cause chain to skip/ rapid user weight transfer/unsatisfactory appearance	8	Damage to chain, rust, lack of lubrication, incorrect tension	8	N/A	4	256	Clear instructions on proper maintenance and easier chain tensioning
Rear hub bearing set	Dirty/ seized	Wheel rotates with resistance/seizes/ bearings feel rough	3	Contamination from dust/dirt, lack of lubrication, not properly preloaded	2	N/A	4	24	Better sealed bearings
Rear axle	Loosening/ yielding	Wheel wobbles/detaches from bike	7	Lack of proper tension/ torque on retaining lock nuts	3	N/A	6	126	Make system more solidly mounted/separate tensioning from wheel fixture

(*Continued*)

Item and function	Failure mode	Effects of failure	S	Causes of failure	O	Design controls	D	RPN	Recommended actions
Rear hub	Fracture	Wheel fails	8	Manufacturing defects/ unexpected loading (potholes)	1	N/A	9	72	Make system more solidly mounted/separate tensioning from wheel fixture
Rear sprocket	Wear/ fatigue	Teeth wear and allow chain slip	6	Wear from excessive use/ lack of lubrication/lack of proper tension	4	N/A	3	72	Strengthen sprocket material/ clear instructions on proper maintenance and easier chain tensioning

7.7

Item	Function	Potential failure mode	Potential effects of failure	SEV	Potential cause of failure	OCC	Current design	DET	RPN	Recommended actions	Actions taken	SEV	OCC	DET	RPN
Chain	Transfers torque from engine to differential sprocket	Insufficient torque	Nonuniform torque transfer	4	Wear due to insufficient lubrication, improper material selection	5	Inspection	5	100	Proper lubrication	Sufficient lubrication with proper use of materials	4	3	3	36
		Link breakage	Insufficient torque jerking	4	Misassembly improper siding, link stretch	4	Inspection	5	80	Proper installation	Proper installation proper siding with strong linkage	4	3	3	36
		Fatigue	Variation in torque transfer	4	Cyclic tensile load on the tight side of the chain due to applied torque and centrifugal force	4	Inspection	4	64	Test the chain performance at an ultimate tensile load for an appropriate amount of time	An appropriate factor of safety for the projected load to be	4	3	3	36

Item	Function	Potential failure mode	Potential effects of failure	SEV	Potential cause of failure	OCC	Current design	DET	RPN	Recommended actions	Actions taken	SEV	OCC	DET	RPN
											considered in design				
Sprocket	Transfers torque from chain to differential	Nonuniform torque transfer	Differential will not receive the uniform torque	5	Wear	4	Inspection	4	80	Light weight sprocket with proper material that can resist wear	Light weight sprocket with ferrous sintered alloy	5	3	2	30
		Jerking noises	Uneven torque transfer	5	Tooth crack Tooth breakage	4	Inspection	4	80	Proper assembly Proper material selection	Light weight sprocket with ferrous sintered alloy	5	3	2	30
		Uneven torque	Differential receives varying torque	4	Improper installation leading to improper engagement, i.e. slipping between sprocket tooth and chain shoe	4	Inspection	4	64	Proper assembly Proper installation	Proper chain sprocket assembly	4	3	2	24
Differential	Transfers torque from sprocket to each axle	Uneven torque transfer	Axles will receive uneven torques, one more and other less	4	Wear misassembly loosening of carrier bolts	4	Inspection assembly procedures	4	64	Proper assembly redesign of fasteners	Proper assembly redesign of fasteners, used longer bolts with long nuts	4	3	2	24
		No drive transfer to the axes	Vehicle does not move	6	Gearbox bearing seize	3	Prerace inspection	3	54	Check bearings for vibrations	Vibration test on bearings check oil level periodically	6	2	2	24

(*Continued*)

Item	Function	Potential failure mode	Potential effects of failure	SEV	Potential cause of failure	OCC	Current design	DET	RPN	Recommended actions	Actions taken	SEV	OCC	DET	RPN
		Insufficient drive transfer	Axles do not get sufficient drive	5	Gear teeth stripped	4	Prerace inspection	4	80	Check gear teeth for wear	Wear test on gear redesign of gears	5	2	2	30
		Lack of dive transfer	No sufficient drive from gear box	5	Improper lubrication low oil level	4	Prerace inspection	4	80	Proper lubrication check oil level periodically	Oil level indicator placed on front board, proper lubrication and oil level checked periodically	5	3	2	30

7.9

Line reference	Function	Potential failure mode	Potential effect of failure	SEV	Potential causes	OCC	Current design controls	DET	RPN
1	Power switch providing on/off function to a power tool	Switch unable to turn on unit	No power	7	Worn parts	2	Select part rated for expected use; power cycling life test	3	42
2		Switch intermittent behavior	Notable to power off tool	9	Corroded contacts	4	Select part rated for expected environment, power cycling life test	3	108
3		Switch unable to turn unit off	Notable to power off tool	9	Switch hard to reach when operating	2	Switch has high contract color; power cycling life test	3	54

- Provide an alternate means to power on the unit to lower the detection score of line 1.
- Provide an alternate means to power down the unit to lower the occurrence score of line 2.
- Provide an alternate location of the switch to lower the occurrence score of line 3.

Provide a safety switch that bypasses the power switch to reduce the severity score of line 2 and 3.

7.11 Pick out the best answer in each of these multiple choice questions:

(a) When prioritizing actions to be taken in an FMEA, which of the following priority rankings should be considered first?
- Overall RPN (risk priority number)
- **Highest severity ranking**
- Highest occurrence ranking
- Highest severity times occurrence ranking

(b) An FMEA is being constructed for the manufacture of a syringe cartridge. The team has developed risk ranking scale criteria for calculating the risk priority number (rpn). The team has assigned 5 values for ranking likelihood of occurrence (O), 10 values for ranking the risk associated with severity (S), and 5 values for ranking the risk associated with detection (D). Using this method will most likely:
- Ensure that all values for O, S, and D are equally represented in rpn
- Give severity a disproportionate representation in rpn
- **Give occurrence and severity an equal representation in rpn**
- Ensure rpn reflects the priority for addressing failure modes

(c) Which of following is NOT a part of risk priority number for FMEA ?
- Severity
- **Catastrophic**
- Occurrence
- Detection

(d) All of the following are examples of design FMEA detection controls, EXCEPT for:
- Whole system testing
- Finite element analysis (FEA)
- Lab testing
- **Adding extra thickness to a part's notched area**

(e) The intent of a recommended action in an FMEA is to reduce rankings in which of the following orders of priority?
- **Severity, Occurrence, Detection**
- Occurrence, Severity, Detection
- Severity, Detection, Occurrence
- Occurrence, Detection, Severity

(f) A potential infant mortality failure has been identified as the failure mode with the highest RPN in a design FMEA. What should you do next?
- Take no action until the failure modes actually occur
- Update the reliability growth plan to indicate that reliability targets will not be achieved
- **Start a team to identify the possible factors that can cause poor product quality during manufacturing in order to identify corrective action for this failure mode.**
- Institute a burn-in test for each product to find infant mortality failure modes before delivery to the customer.

(g) A potential failure mode for an electronics device is the complete inability of the power switch to activate (or power on) the device. In an FMEA this failure mode would be considered in which
category?
- **No function**
- Partial degraded function

- Intermittent function
- Unintended function

(h) Which of the following is a good design control to reduce severity or occurrence that is identified in a design FMEA?
- Change the system requirements to reduce system function
- Add additional inspection(s) in production
- Enhance design validation testing
- **Modify the design to reduce stress on a component**

Chapter 8 Loads, Capacity, and Reliability

8.1 (a) 1.39×10^{-3}, (b) 721 V, (c) 2161 V.

8.3 $r = 1 + \frac{1}{a\gamma}\left(e^{-2a\gamma} - e^{-a\gamma}\right)$

8.5 $\widetilde{R} = 0.2090$.

8.7 >10 strands.

8.9 15.7 Nm.

8.11 $c_0/l_0 = 4.64$.

8.13 9%.

8.15 (a) 0.269, (b) 0.00669.

8.17 (a) Nine cables, (b) nine cables.

8.19 85.6 lbs.

8.21 0.0436.

8.23 10^{-15}

8.25 0.670.

8.27 (a) 0.18, (b) 0.06, (c) 2.40 years.

8.29 (a) 87 cycles, (b) 1.25×10^6 cycles.

Chapter 9 Maintained Systems

9.1 (a) 0.885, (b) every 6300 hours, (c) every 4275 hours.

9.3 No, maximum value is 0.934.

9.5 (a) 0.7225, (b) 0.8825, (c) 0.7188.

9.7 (a) 4.04θ, (b) 455%.

9.9 1.044θ.

9.11 (a) 18.4 hours, (b) 12.9 hours, 29.5 hours.

9.13 (a) 0.9315, (b) 20.4 hours.

9.15 0.980.

9.17 65.5 days.

9.19 2.2×10^{-4}/day.

9.21 (a) 0.897, (b) $\lambda = 0.013$/hour, $\mu = 0.111$/hour, (c) 2% difference.

9.23 (a) 0.968, (b) 0.946, (c) every 18.6 days.

9.25 (a) 0.9594, (b) every 87.5 days.

9.27 Every 1980 hours.

Chapter 10 Failure Interactions

10.1 (a) 0.058 MTTF, (b) 0.129 MTTF, (c) 0.182 MTTF.
10.3 (a) $1 - \lambda\,(2\lambda^* - \lambda)t^2$, (b) 1.56.
10.5 (a) $2/\lambda$, (b) $\lambda^2 t/(1+\lambda t)$.
10.7 Standby: $2/\lambda^2$, active parallel: $5/4\lambda^2$.
10.9 (a) Shared-load system, (b) 1.063.
10.11 (a) Proof, (b) $\approx 1 - 3/8\,(\lambda t)^4$, (b) active: 0.99990, standby: 0.99996.
10.13 (a) $2(1+\lambda t)e^{-\lambda t} - (1+\lambda t)^2 e^{-2\lambda t}$, (b) $1 - 1/4\lambda^4 t^4$, active parallel: $1 - \lambda^4 t^4$.
10.15 1.2×10^{-3}.
10.17 (a) 0.9998, (b) 0.9996.
10.19 0.09902.
10.21 With $\varepsilon \equiv \lambda/\nu$, (a) $\dfrac{1+\varepsilon+\varepsilon^2+\varepsilon^3}{1+\varepsilon+\varepsilon^2+\varepsilon^3+\varepsilon^4}$, (b) $\approx 1 - \varepsilon^4$, (c) identical, $\approx 1 - 1.6 \times 10^{-7}$.
10.23 (a) 0.9961, (b) yes.

Chapter 11 System Safety Analysis

11.1 Passive-inlet line rupture, either valve closed when stop fails, active-all other failures.
11.3 (a) 0.01, (b) 0.0185.
11.5 $A \cap B$, $A \cap C$, $B \cap C$.
11.7 (a) Graph, (b) 9.15×10^{-4}.
11.9 0.12800, 0.12385, 0.12387.
11.11 (a) M_1: 0.382, M_2: 0.637, (b) A: 0.382, B: 0.382, C: 0.637.
11.13 (a) 5.9×10^{-3}, (b) 0.0508, 0.1016, 0.847 (c) 0.847, 0.0678, 0.0339, 0.0339, 0.0169.

11.15

(λ_P)		(α)		(ε)		(t)	
Item Failure Rate	×	Failure Mode Ratio	×	Probability of Worst Case Failure Effects	×	Time	= CRITICALITY

Therefore,

$$\text{Criticality} = \left(10 \times 10^{-6}\right)(0.50)(1.0)(72) = 3.6 \times 10^{-4}$$

11.17

Item Function	Potential Failure modes	Potential Effect(s) of failure	Severity	Potential Cause(s) Mechanisms of failure	Occur	Current Controls	Detect	RPN	Criticality
Wake-up	Alarm	Late to work	6	Wrong time set	4	More than one alarm	5	120	24
Getting dressed	No clean clothes/ wrinkled	Delayed	7	Forgot to check clothes	4	Check the night before	1	28	28
Getting ready	Kids	Late to work	6	They **are** kids	10	Time-outs	5	300	60
Breakfast	Nothing available	Hungry/ delayed/ angry	8	No time to make it/no groceries	3	Cafeteria fast food	1	24	24
Drive	Weather	Late to work	6	God	5	N/A	10	300	30
Drive	Traffic/ lights	Late to work	5	DMV	4	N/A	10	200	20
Drive	Accident	Late to work	10	Sleepy, cell phone, inattentive	3	Coffee	4	120	30
Drive	No gas	Late to work	8	Forgot to check or to expense	4	Check the night before	1	32	32
Drive	No ID badge	Late to work	6	Misplaced	4	One location	1	24	24
Drive	Flat tire	Late to work	8	Wear	2	Check pressure/ Daily	1	16	16
Drive	No keys	Late to work	8	Misplaced	1	One location	1	8	8

IF you have kids, they will (usually) be the highest criticality for being late to work!

Index

Introduction to Reliability Engineering, Third Edition. James E. Breneman, Chittaranjan Sahay, and Elmer E. Lewis.

Companion website: www.wiley.com/go/breneman/relabilityengineering3e

l

m