WILEY SERIES IN QUALITY & RELIABILITY ENGINEERING

DESIGN FOR RELIABILITY

EDITED BY

DEV RAHEJA

LOUIS J. GULLO

WILEY

IEEE

IEEE PRESS

Design for Reliability

WILEY SERIES IN QUALITY & RELIABILITY ENGINEERING
*and related titles**

Electronic Component Reliability:
Fundamentals, Modelling, Evaluation and Assurance
Finn Jensen

Measurement and Calibration Requirements
For Quality Assurance to ASO 9000
Alan S. Morris

Integrated Circuit Failure Analysis:
A Guide to Preparation Techniques
Friedrich Beck

Test Engineering
Patrick D. T. O'Connor

Six Sigma: Advanced Tools for Black Belts and Master Black Belts*
Loon Ching Tang, Thong Ngee Goh, Hong See Yam, Timothy Yoap

Secure Computer and Network Systems: Modeling, Analysis and Design*
Nong Ye

Failure Analysis:
A Practical Guide for Manufacturers of Electronic Components and Systems
Marius Bâzu and Titu Bălenescu

Reliability Technology:
Principles and Practice of Failure Prevention in Electronic Systems
Norman Pascoe

Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes
Using Failure Mode and Effects Analysis
Carl Carlson

Design for Reliability
Dev Raheja and Louis J. Gullo (Editors)

Design for Reliability

Edited by

Dev Raheja

Louis J. Gullo

A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2012 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permission.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Raheja, Dev.
Design for reliability / Dev Raheja & Louis J. Gullo.
p. cm.
ISBN 978-0-470-48675-7 (hardback)
1. Reliability (Engineering) I. Gullo, Louis J. II. Title.
TA169.R348 2011
620′.00452–dc23
2011042405

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my wife, Hema, and my children, Gauri, Pramod, and Preeti
Dev Raheja

To my wife, Diane, and my children, Louis, Jr., Stephanie,
Catherine, Christina, and Nicholas
Louis J. Gullo

Contents

Contributors

Steven S. Austin
Missile Defense Agency
Department of Defense
Huntsville, Alabama

Lawrence Bernstein
Stevens Institute of Technology
Hoboken, New Jersey

Joseph A. Childs
Missiles and Fire Control
Lockheed Martin Corporation
Orlando, Florida

Jack Dixon
Dynamics Research Corporation
Orlando, Florida

Louis J. Gullo
Missile Systems
Raytheon Company
Tucson, Arizona

Samuel Keene
Keene and Associates, Inc.
Lyons, Colorado

Brian Moriarty
Engility Corporation
Lake Ridge, Virginia

Dev Raheja
Raheja Consulting, Inc.
Laurel, Maryland

Robert W. Stoddard
Six Sigma IDS, LLC
Venetia, Pennsylvania

C.M. Yuhas

Foreword

The importance of quality and reliability to a system cannot be disputed. Product failures in the field inevitably lead to losses in the form of repair cost, warranty claims, customer dissatisfaction, product recalls, loss of sales, and in extreme cases, loss of life. Thus, quality and reliability play a critical role in modern science and engineering and so enjoy various opportunities and face a number of challenges.

As quality and reliability science evolves, it reflects the trends and transformations of technological support. A device utilizing a new technology, whether it be a solar power panel, a stealth aircraft, or a state-of-the-art medical device, needs to function properly and without failure throughout its mission life. New technologies bring about new failure mechanisms (chemical, electrical, physical, mechanical, structural, etc.), new failure sites, and new failure modes. Therefore, continuous advancement of the physics of failure, combined with a multi-disciplinary approach, is essential to our ability to address those challenges in the future.

In addition to the transformations associated with changes in technology, the field of quality and reliability engineering has been going through its own evolution: developing new techniques and methodologies aimed at process improvement and reduction of the number of design- and manufacturing-related failures.

The concept of design for reliability (DFR) has been gaining popularity in recent years and its development is expected to continue for years to come. DFR methods shift the focus from reliability demonstration and the outdated "test-analyze-fix" philosophy to designing reliability into products and processes using the best available science-based methods. These concepts intertwine with probabilistic design and design for six sigma (DFSS) methods, focusing on reducing variability at the design and manufacturing levels. As such, the industry is expected to increase the use of simulation techniques, enhance the applications of reliability modeling, and integrate reliability engineering earlier and earlier in the design process. DFR also transforms the role of the reliability engineer from being focused primarily on product test and analysis to being a mentor to the design team, which is responsible for finding

and applying the best design methods to achieve reliability. A properly applied DFR process ensures that pursuit of reliability is an enterprise-wide activity.

Several other emerging and continuing trends in quality and reliability engineering are also worth mentioning here. For an increasing number of applications, risk assessment will enhance reliability analysis, addressing not only the probability of failure but also the quantitative consequences of that failure. Life-cycle engineering concepts are expected to find wider applications in reducing life-cycle risks and minimizing the combined cost of design, manufacturing, quality, warranty, and service. Advances in prognostics and health management will bring about the development of new models and algorithms that can predict the future reliability of a product by assessing the extent of degradation from its expected operating conditions. Other advancing areas include human and software reliability analysis.

Additionally, continuous globalization and outsourcing affect most industries and complicate the work of quality and reliability professionals. Having various engineering functions distributed around the globe adds a layer of complexity to design coordination and logistics. Moving design and production into regions with little knowledge depth regarding design and manufacturing processes, with a less robust quality system in place and where low cost is often the primary driver of product development, affects a company's ability to produce reliable and defect-free parts.

Despite its obvious importance, quality and reliability education is paradoxically lacking in today's engineering curriculum. Few engineering schools offer degree programs or even a sufficient variety of courses in quality or reliability methods. Therefore, a majority of quality and reliability practitioners receive their professional training from colleagues, professional seminars, and from a variety of publications and technical books. The lack of formal education opportunities in this field greatly emphasizes the importance of technical publications for professional development.

The real objective of the Wiley Series in Quality & Reliability Engineering is to provide a solid educational foundation for both practitioners and researchers in quality and reliability and to expand the reader's knowledge base to include the latest developments in this field. This series continues Wiley's tradition of excellence in technical publishing and provides a lasting and positive contribution to the teaching and practice of engineering.

ANDRE KLEYNER

Editor
Wiley Series in Quality & Reliability Engineering

Preface

Design for reliability (DFR) has become a worldwide goal, regardless of the industry and market. The best organizations around the world have become increasingly intent on harvesting the value proposition for competing globally while significantly lowering life cycle costs. The DFR principles and methods are aimed proactively to prevent faults, failures, and product malfunctions, which result in cheaper, faster, and better products. In Japan, this tool is used to gain customer loyalty and customer trust. However, we still face some challenges. Very few engineering managers and design engineers understand the value added by design for reliability; they often fail to see savings in warranty costs, increased customer satisfaction, and gain in market share.

These facts, combined with the current worldwide economic challenges, have created perfect conditions for this science of engineering. This is an art also because many decisions have to be made not only on evidence-based data, but also on engineering creativity to design out failure at lower costs. Readers will be delighted with the wealth of knowledge because all contributors to this book have at least 20 years hands-on experience with these methods.

The idea for this book was conceived during our participation in the IEEE Design for Reliability Technical Committee. We saw the need for a DFR volume not only for hardware engineers, but also for software and system engineers. The traditional books on reliability engineering are written for reliability engineers who rely more on statistical analysis than on improvements in inherent design to mitigate hardware and software failures. Our book attempts to fill a gap in the published body of knowledge by communicating the tremendous advantages of designing for reliability during very early development phase of a new product or system. This volume fulfills the needs of entry-level design engineers, experienced design engineers, engineering managers, as well as the reliability engineers/managers who are looking for hands-on knowledge on how to work collaboratively on design engineering teams.

ACKNOWLEDGMENTS

We would like to thank the IEEE Reliability Society for sowing the seed for this book, especially the encouragement from a former society president,

Dr. Samuel Keene, who also contributed chapters in the book. We would like to recognize a few of the authors for conducting peer reviews of several chapters: Joe Childs, Jack Dixon, Larry Bernstein, and Sam Keene. We also thank the guest editors—Tim Adams, at NASA Kennedy Center, and Dr. Nat Jambulingam, at NASA Goddard Space Flight Center—who helped edit several chapters. We are grateful to Diana Gialo, at Wiley, who has always been gracious in helping and guiding us.

We acknowledge the contributions of the following:

Steve Austin (Chapter 12)

Larry Bernstein (Chapter 13)

Joe Childs (Chapters 2, 6, and 15)

Jim Dixon (Chapters 9 and 16)

Lou Gullo (Chapters 4, 5, 10, 11, 14, and 18)

Sam Keene (Chapters 3 and 8)

Brian Moriarty (Chapter 17)

Dev Raheja (Chapter 1)

Bob Stoddard (Chapter 7)

C. M. Yuhas (Chapter 13)

Dev Raheja
Louis J. Gullo

Introduction: What You Will Learn

Chapter 1 Design for Reliability Paradigms (Raheja)

This chapter introduces what it means to design for reliability. It shows the technical gaps between the current state-of-art and what it takes to design reliability as a value proposition for new products. It gives real examples of how to get high return on investment to understand the art of design for reliability. The chapter introduces readers to the deeper level topics with eight practical paradigms for best practices.

Chapter 2 Reliability Design Tools (Childs)

This chapter summarizes reliability tools that exist throughout the product's life cycle from creation, requirements, development, design, production, testing, use, and end of life. The need for tools in understanding and communicating reliability performance is also explained. Many of these tools are explained in further detail in the chapters that follow.

Chapter 3 Developing Reliable Software (Keene)

This chapter describes good design practices for developing reliable software embedded in most of the high technology products. It shows how to prevent software faults and failures often inherent in the design by applying evidence-based reliability tools to software such as FMEA, capability maturity modeling, and software reliability modeling. It introduces the most popular software reliability estimation tool CASRE (*C*omputer *A*ided *S*oftware *R*eliability *E*stimation).

Chapter 4 Reliability Models (Gullo)

This chapter is on reliability modeling, one of the most important tools for design for reliability in he early stages of design, to determine strategy for

overall reliability. The chapter covers models for system reliability, component reliability, and shows the use of block diagrams in modeling. It discusses reliability growth process, similarity analysis used for physical modeling, and widely used models for simulation.

Chapter 5 Design Failure Modes, Effects, and Criticality Analysis (Gullo)

This chapter on FMECA contains the core knowledge for reliability analysis at system level, subsystem level, and component level. The chapter shows how to perform risk assessment using a risk index called risk priority number and shows how to eliminate single-point failures, making a design significantly less vulnerable. It explains the difference between FMEA and FMECA and how to us them for improving product performance and the maintenance effectiveness.

Chapter 6 Process Failure Modes, Effects, and Criticality Analysis (Childs)

The preceding chapter showed how to make design more robust. This chapter applies the FMEA tool to analyze a process for robustness, such that the manufacturing defects are eliminated before the show up in production. The end result is improved product reliability with lower manufacturing costs. It covers step-by-step procedure to perform the analysis, including the risk assessment using the risk priority number.

Chapter 7 FMECA Applied to Software Development (Stoddard)

The FMEA tool is just as applicable to software design. There is very little literature on how to apply it to software. This chapter shows the details of how to use it to improve the software reliability. It covers the lessons learned and shows different ways of integrating the FMECA into the most widely used software development model known as “V” model. The chapter describes roles and responsibilities for proper use of this tool.

Chapter 8 Six Sigma Approach to Requirements Development (Keene)

In this chapter the author explains why design of experiments (DOE) is a sweet spot for identifying the key input variables to a six sigma programs. The chapter covers the origin of this program, the meaning of six sigma

measurements, and how it is applied to improve the design. It then proceeds to cover the tools for designing the product for six sigma performance to reduce failure rates as close to zero as possible.

Chapter 9 Human Factors in Reliable Design (Dixon)

Humans are often blamed for many product failures when in fact the fault lies in the insufficient attention to human factor engineering. This chapter covers the principles of human-centered design to make man–machine interface robust and error-tolerant. It covers how to perform the human factors analysis, and how to integrate it to make the product design user-friendly.

Chapter 10 Stress Analysis During Design to Eliminate Failures (Gullo)

This chapter explains why it is critical to reduce the design stress to improve durability, as well as reliability. It introduces the concept of derating as a design tool. The author includes examples on electrical and mechanical stress analysis, including how to apply this theory to software design. The chapter also shows how to apply finite element analysis, a numerical technique, to solve specific design problems.

Chapter 11 Highly Accelerated Life Testing (Gullo)

Usually designers cannot predict what failures will occur for a new design. This chapter shows how highly accelerated life tests and highly accelerated stress tests can reveal the failure modes quickly. It covers how to design these tests and how to estimate the design margin from the test results. It shows different methods of accelerating the stresses.

Chapter 12 Design for Extreme Environments (Austin)

When a product is used in extreme cold or extreme heat, such as in Alaska or in a desert in Arizona, we must design for such environments to assure product can last long enough. This chapter shows what factors need to be considered and how to design for each condition. It shows how lessons learned from space programs and overseas experience can help make products durable, reliable, and safe.

Chapter 13 Design for Trustworthiness (Bernstein and Yuhas)

This is a very important chapter because software design methods for reliability are not standardized yet. This chapter goes beyond reliability to design software, such that it is also safe and secure from errors in engineering changes which are very frequent. This chapter covers design methods and offers suggestions for improving the architecture, modules, interfaces, and using right policies for re-using the software. The chapter offers good design practices.

Chapter 14 Prognostics and Health Management Capabilities to Improve Reliability (Gullo)

Design for reliability practices should include detecting a malfunction before a product malfunctions. This chapter covers designing prognostics and product health monitoring principles that can be designed into the product. The result is enhanced system reliability. The chapter includes condition-based maintenance and time-based maintenance, use of failure precursors to signal an imminent failure event, and automatic stress monitoring to enhance prognosis.

Chapter 15 Reliability Management (Childs)

This chapter provides both motivation and guidance in outlining the importance of good reliability management. Management participation is the key to any successful reliability in design. It shows how to manage, plan, execute, and document the needs of the program during early design. It describes the important tasks, and closing the feedback loops after reliability assessment, problem solving, and reliability growth testing.

Chapter 16 Risk Management, Exception Handling, and Change Management (Dixon)

Many risks are overlooked in a product design. This chapter defines what is risk in engineering terms, how to predict risk, assess risk, and mitigate it. It highlights the role of risk management culture in mitigating risks and the critical role of configuration management for avoiding new risks from design changes. Included in this chapter is how to minimize oversights and omissions, including requirement creeps.

Chapter 17 Integrating Design for Reliability with Design for Safety (Moriarty)

This chapter integrates reliability with safety, including how to design for safety. It covers several safety analysis techniques that equally apply to reliability. It shows the how a risk assessment code matrix is used widely in aerospace and many commercial products to make risk management decisions. It includes examples of risk reduction.

Chapter 18 Organizational Reliability Capability Assessment (Gullo)

This chapter describes the benefits of using IEEE 1624–2008 standard to describe how reliability capability of an organizational entity is determined by assessing eight key reliability practices and associated metrics. Management should know the capability of an organization to deliver a reliable product, which is defined as organizational reliability capability. It describes the process in detail with case studies.

Chapter 1

Design for Reliability Paradigms

Dev Raheja

WHY DESIGN FOR RELIABILITY?

The science of reliability has not kept pace with user expectations. Many corporations still use MTBF (mean time between failures) as a measure of reliability, which, depending on the statistical distribution of failure data, implies acceptance of roughly 50 to 70% failures during the time indicated by the MTBF. No user today can tolerate such a high number of failures. Ideally, a user does not want any failures for the entire expected life! The life expected is determined by the life inferred by users, such as 100,000 miles or 10 years for an automobile, at least 10 years for kitchen appliances, and at least 20 years for a commercial airliner. Most commercial companies, such as automotive and medical device manufacturers, have stopped using the MTBF measure and aim at 1 to 10% failures during a self-defined time. This is still not in line with users' dreams. The real question is: Why not design for zero failures if we can increase profits and gain more market share? Zero failures implies zero mission-critical failures or zero safety-critical system failures. As a minimum, systems in which failures can lead to catastrophic consequences must be designed for zero failures. There are companies that are able to do this. Toyota, Apple, Gillette, Honda, Boeing, Johnson & Johnson, Corning, and Hewlett-Packard are a few examples.

The aim of design for reliability (DFR) is to design-out failures of critical system functions in a system. The number of such failures should be

Design for Reliability, First Edition. Edited by Dev Raheja, Louis J. Gullo.
© 2012 John Wiley & Sons, Inc. Published 2012 by John Wiley & Sons, Inc.

zero for the expected life of the product. Some components may be allowed to fail, such as in redundant systems. For example, in aerospace, as long as a system can function at least for the duration of the mission and the failed components are replaced prior to the next mission to maintain redundancy, certain failures can be tolerated. This is, however, insufficient for complex systems where thousands of software interactions, hundreds of wiring connections, and hundreds of human factors affect the systems' reliability. Then there are issues of compatibility [1] among components and materials, among subsystems, and among hardware and software interactions. Therefore, for complex systems we may find it impossible to have zero failures, but we must at least prevent the potential failures we know about. Since failures can come from unknown and unexpected interactions, we should try to design-in fallback modes for unexpected events. A "what-if" analysis usually points to some events of this type. To minimize failures in complex systems, in this book we describe techniques for improving software and interface reliability.

As indicated earlier, some companies have built a strong and long-lasting reputation for reliability based on aiming at zero failures. Toyota and Sony built their world leadership mostly on high reliability; and Hyundai has been offering a 10-year warranty and increasing its market share steadily. Progress has been made since then. In 1974, when nobody in the world gave a warranty longer than one year, Cooper Industries gave a 15-year warranty to electric power utilities on high-voltage transformer components and stood out as the leader in profitability among all Fortune 500 electrical companies. Raytheon has established a culture at the highest level in the corporation of providing customers with mission assurance through a "no doubt" mindset. Says Bill Swanson, chairman and CEO of Raytheon: "[T]here must be no doubt that our products will work in the field when they are needed" (Raytheon Company, *Technology Today*, 2005, Issue 4). Similarly, with its new lifetime power train warranty, Chrysler is creating new standards for reliability.

REFLECTIONS ON THE CURRENT STATE OF THE ART

Reliability is defined as the probability of performing all the functions (including safety functions) satisfactorily for a specified time and specified use conditions. The functions and use conditions come from the specification. If a specification misses or is vague 60% or more of the time, the reliability predictions are of very little value. This is usually the case [2]. The second big issue is: How many failures should be tolerable? Some readers may not agree that we can design for zero critical failures, but the evidence supports the contrary conclusion. We may not be able to prevent failures that we did not

foresee, but we can design out all the critical failure modes that we discover during the requirements analysis and in the failure mode and effects analysis (FMEA). In over 30 years' experience, I have yet to encounter a failure mode that cannot be designed-out. The cost is usually not an issue if the FMEA is conducted and the improvements are made during the early design stage. The time specified for critical failures in the reliability definition should be the entire lifetime expected.

In this chapter we address how to write a good system specification and how to design so as not to fail. We make it clear that the design for reliability should concentrate on the critical and major failures. This prevents us from solving easy problems and ignoring the complex ones. The following incident raises issues that are central to designing for reliability.

> *The lessons learned from the Interstate 35 bridge collapse in Minnesota on August 1, 2007 into the Mississippi River on August 1, killing 13, give us some clues about what needs to be done. Similar failure mechanisms can be found in many large electrical and mechanical systems, such as aircraft and electric power plants.*
>
> *The bridge was expanded from four lanes to six, and eventually to eight. Some wonder whether that might have played a role in its collapse. Investigators said the failure resulted because of a flaw in its design. The designers had specified a metal plate that was too thin to serve as a junction of several girders.*
>
> *Like many products, it gradually got exposed to higher loads, adding strain to the weak spot. At the time of the collapse, the maintenance crews had brought tons of equipment and material onto the deck for a repair job. The bridge was of a design known as a nonredundant structure, meaning that if a single part failed, the entire structure could collapse. Experts say that the pigeon dung all over the steel could have caused faster corrosion than was predicted.*

This case history challenges the fundamentals of engineering taught in the universities.

- *Should the design margin be 100% or 800%*? "How does the designer determine the design margin?"
- *Should we design for pigeons doing their dirty job?* What about designing for all the other environmental stressors, such as chemicals sprayed during snow emergencies, tornados, and earthquakes?
- *Should we design-in redundancy on large mechanical systems to avoid disasters?* The wisdom says that redundancy delays failures but may not avoid disasters. The failure could occur in both the redundant paths, such as in an aircraft accident where the flying debris cut through all three redundant hydraulic lines.
- *Should we design for sudden shocks experienced by the bridge during repair and maintenance?*

These concerns apply to any product, such as electronics, electrical power systems, and even a complex software design. In software, the corrosion can be symbolic for applying too many patches without knowing the interactions. Call it "software corrosion."

The answers to the questions above should be a resounding "yes." An engineering team should foresee all these and many more failure scenarios before starting to design. The obvious strategy is to write a good system specification by first predicting all major potential failures and avoiding them by writing robust requirements. Oversights and omissions in specifications are the biggest weakness in the design for reliability. Typically, 200 to 300 requirements are generally missing or vague for a reasonably complex system such as an automotive transmission.

Analyses techniques covered in this book for hardware and software help us discover many missing requirements, and a good brainstorming session for overlooked requirements always results in discovering many more. What we really need is perhaps the paradigms based on lessons learned.

THE PARADIGMS FOR DESIGN FOR RELIABILITY

Reliability is a process. If the right process is followed, results are likely to be right. The opposite is also true in the absence of the right process. There is a saying: "If we don't know where we are going, that's where we will go." It is difficult enough to do the right things, but it is even more difficult to know what the right things are!

Knowledge of the right things comes from practicing the use of lessons learned. Just having all the facts at your fingertips does not work. One must utilize the accumulated knowledge for arriving at correct decisions. Theory is not enough. One must keep becoming better by practicing. Take the example of swimming. One cannot learn to swim from books alone; one must practice swimming. It is okay to fail as long as mistakes are the stepping stones to failure prevention. Thomas Edison was reminded that he failed 2000 times before the success of the light bulb. His answer, "I never failed. There were 2000 steps in this process."

One of the best techniques is to use lessons learned in the form of paradigms. They are easy to remember and they make good topics for brainstorming during design reviews.

Paradigm 1: Learn To Be Lean Instead of Mean

When engineers say that a component's life is five years, they usually imply the calculation of the mean value, which says that there is a 50% chance of failure during the five years. In other words, either the supplier or the customer has