

WILEY SERIES IN QUALITY & RELIABILITY ENGINEERING

DESIGN FOR SAFETY



LOUIS J. GULLO
JACK DIXON

WILEY

A one-stop guide to design for safety principles and applications

Design for Safety (DfSa) provides design engineers and engineering managers with a range of tools and techniques for incorporating safety into the design process for complex systems. It explains how to design for maximum safe conditions and minimum risk of accidents. The book covers safety design practices, which will result in improved safety, fewer accidents, and substantial savings in life cycle costs for producers and users. Readers who apply DfSa principles can expect to have a dramatic improvement in the ability to compete in global markets. They will also find a wealth of design practices not covered in typical engineering books—allowing them to think outside the box when developing safety requirements.

Design Safety is already a high demand field due to its importance to system design and will be even more vital for engineers in multiple design disciplines as more systems become increasingly complex and liabilities increase. Therefore, risk mitigation methods to design systems with safety features are becoming more important. Designing systems for safety has been a high priority for many safety-critical systems—especially in the aerospace and military industries. However, with the expansion of technological innovations into other market places, industries that had not previously considered safety design requirements are now using the technology in applications.

Design for Safety:

- Covers trending topics and the latest technologies
- Provides ten paradigms for managing and designing systems for safety and uses them as guiding themes throughout the book
- Logically defines the parameters and concepts, sets the safety program and requirements, covers basic methodologies, investigates lessons from history, and addresses specialty topics within the topic of *Design for Safety*
- Supplements other books in the Wiley series on Quality and Reliability Engineering

Design for Safety is an ideal book for new and experienced engineers and managers who are involved with design, testing, and maintenance of safety critical applications. It is also helpful for advanced undergraduate and postgraduate students in engineering.

Design for Safety is the second in a series of "Design for" books. *Design for Reliability* was the first in the series with more planned for the future.

LOUIS J. GULLO works for Raytheon Missile Systems, Engineering Product Support Directorate (EPSD), in Tucson, AZ. He is a member of the technical staff and the technical leader for Software Reliability and Safety across Missile Systems. He has worked in the industry for 33 years. He retired as Lieutenant Colonel from the US Army Signal Corps.


JACK DIXON is President of JAMAR International, Inc., in Orlando, FL. He has worked in the defense industry for over 45 years in the areas of system safety, human factors engineering, logistics support, program management, and business development.

Cover Design: Wiley

Cover Images: (Left to right) © 3DSculptor/Gettyimages; © ms. Octopus/Shutterstock; © prosot-photography/iStock; © gali estrange/Shutterstock

www.wiley.com

WILEY

 Also available
as an e-book

ISBN 978-1-118-97429-2



9 781118 974292

GULLO
DIXON

DESIGN FOR
SAFETY

WILEY

Design for Safety

Edited by

Louis J. Gullo

Raytheon Missile Systems, Arizona, USA

Jack Dixon

JAMAR International, Inc., Florida, USA

WILEY

This edition first published 2018
© 2018 John Wiley & Sons Ltd

All rights reserved. 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 or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Louis J. Gullo and Jack Dixon to be identified as the authors of the editorial material in this work has been asserted in accordance with law.

Registered Office(s)

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office

The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

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.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication data applied for

ISBN: 9781118974292

Cover Design: Wiley

Cover Images: (Left to right) © 3DSculptor/Gettyimages; © ms. Octopus/Shutterstock;
© prosot-photography/iStock; © gali estrange/Shutterstock

Set in 10.5/13pt Palatino by SPi Global, Pondicherry, India
Printed and bound in Malaysia by Vivar Printing Sdn Bhd.

10 9 8 7 6 5 4 3 2 1

Design for Safety

Wiley Series in Quality & Reliability Engineering

Dr Andre Kleyner

Series Editor

The Wiley series in Quality & Reliability Engineering aims to provide a solid educational foundation for both practitioners and researchers in Q&R field and to expand the reader's knowledge base to include the latest developments in this field. The series will provide a lasting and positive contribution to the teaching and practice of engineering.

The series coverage will contain, but is not exclusive to,

- statistical methods;
- physics of failure;
- reliability modeling;
- functional safety;
- six-sigma methods;
- lead-free electronics;
- warranty analysis/management; and
- risk and safety analysis.

Wiley Series in Quality & Reliability Engineering

Next Generation HALT and HASS: Robust Design of Electronics and Systems
by Kirk A. Gray, John J. Paschkewitz
May 2016

Reliability and Risk Models: Setting Reliability Requirements, 2nd Edition
by Michael Todinov
September 2015

Applied Reliability Engineering and Risk Analysis: Probabilistic Models and Statistical Inference
by Ilia B. Frenkel, Alex Karagrigoriou, Anatoly Lisnianski, Andre V. Kleyner
September 2013

Design for Reliability
by Dev G. Raheja (Editor), Louis J. Gullo (Editor)
July 2012

Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Modes and Effects Analysis
by Carl Carlson
April 2012

Failure Analysis: A Practical Guide for Manufacturers of Electronic Components and Systems
by Marius Bazu, Titu Bajanescu
April 2011

Reliability Technology: Principles and Practice of Failure Prevention in Electronic Systems
by Norman Pascoe
April 2011

Improving Product Reliability: Strategies and Implementation
by Mark A. Levin, Ted T. Kalal
March 2003

Test Engineering: A Concise Guide to Cost-Effective Design, Development and Manufacture
by Patrick O'Connor
April 2001

Integrated Circuit Failure Analysis: A Guide to Preparation Techniques
by Friedrich Beck
January 1998

Measurement and Calibration Requirements for Quality Assurance to ISO 9000
by Alan S. Morris
October 1997

Electronic Component Reliability: Fundamentals. Modelling, Evaluation, and Assurance
by Finn Jensen
November 1995

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

Louis J. Gullo

To my wife, Margo.

Jack Dixon

And

to all the heroes of the world, especially all the safety heroes
that make the world a safer place.

Louis J. Gullo

Jack Dixon

Series Editor's Foreword

The Wiley Series in Quality and Reliability Engineering aims to provide a solid educational foundation for researchers and practitioners in the field of dependability, which includes quality, reliability, and safety, and expand the knowledge base by including the latest developments in these disciplines.

It is hard to overstate the effect of quality and reliability on system safety. A safety-critical system is a system whose failure or malfunction may result in death or serious injury to people. According to Federal Aviation Administration (FAA), system safety is the application of engineering and management principles, criteria, and techniques to optimize safety by the identification of safety-related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence.

Along with continuously increasing electronics content in vehicles, airplanes, trains, appliances, and other devices, electronic and mechanical systems are becoming more complex with added functions and capabilities. Needless to say, this trend is making the jobs of design engineers increasingly challenging, which is confirmed by the growing number of safety recalls. These recalls are prompting further strengthening of reliability and safety requirements and a rapid development of functional safety standards, such as IEC 61508 Electrical/Electronic/Programmable systems, ISO 26262 Road Vehicles, and others, which have increased the pressure on improving the design processes and achieving ever higher reliability as it applies to system safety.

There are no do-overs in safety. You cannot undo the damage to a human caused by an accident caused by an unsafe system; therefore it is extremely important to design a safe system the first time. This book *Design for Safety*, written by Louis J. Gullo and Jack Dixon explores the safety engineering and takes the concept of design and system safety to a new level. The book takes you step by step through the process of designing for safety. These steps include the development of system

requirements, design for safety checklist, and application of the critical design tools, such as fault tree analysis, hazard analysis, FMEA, system integration, testing, and many others.

Both authors have lifelong experience in product design, safety, and reliability, and sharing their knowledge will be a big help to the new generation of design engineers as well as to the seasoned practitioners. This book offers an excellent mix of theory, practice, useful applications, and commonsense engineering, making it a perfect addition to the Wiley Series in Quality and Reliability Engineering.

Despite its obvious importance, quality, reliability, and safety education are paradoxically lacking in today's engineering curriculum. Very few engineering schools offer degree programs, or even a sufficient variety of courses, in quality or reliability methods, and the topic of safety only receives minimal coverage in today's engineering student curriculum. Therefore, the majority of the quality, reliability, and safety practitioners receive their professional training from colleagues, professional seminars, publications, and technical books. The lack of opportunities for formal education in these fields emphasizes too well the importance of technical publications like this one for professional development.

We are confident that this book, as well as this entire book series, will continue Wiley's tradition of excellence in technical publishing and provide a lasting and positive contribution to the teaching and practice of quality, reliability, and safety engineering.

Dr. Andre Kleyner,
Editor of the Wiley Series in Quality
and Reliability Engineering

Preface

Anyone who designs a product or system involving hardware and/or software needs to ask the following questions and seek answers to:

- Will my designs be safe for the users of the product or system that I design for them?
- Will my designs be safe for people affected by the users of the product or system that I design for them?
- Are there applications that my designs may be used for that are not safe even though it is not the original intentions of my design?
- Can anyone die or be harmed by my designs?

The designers and engineers that fully answer these questions and take action to improve the safety features of a design are heroes. These engineering heroes are usually unsung heroes who don't receive nor seek any reward or recognition.

When you think of heroes, you might conjure up the image of a US Army Medal of Honor recipient, or a brave firefighter willing to sacrifice his or her life to rescue people from a towering inferno, or a policeman cited for courage in the line of duty, but you probably won't imagine an engineer willing to sacrifice his or her job or career to prevent a potential catastrophic hazard from occurring within a product or system. Every day and throughout the world, multitudes of engineers working in numerous development and production engineering career fields within a global marketplace discover and analyze safety-critical failure modes and assess risks of hazards to the user or customer, which may cause loss of life or severe personal injury. These engineers display a passion for their work with consideration for the safety aspects of their products or systems realizing the ultimate impacts to the health and well-being of their user community. The passion of

these engineers usually goes unnoticed, except by other engineers or managers who work closely with them. The passion of these engineers may be recognized in extreme or unusual circumstances with an individual or team achievement award, but they most certainly would not become hailed as heroes. Why not? Does our engineering society place value of those willing to display courage in managing challenging technical problems? Of course, there is value in this characteristic of an engineer, but only when it results in making the organization or company more money, not reducing or eliminating the potential of dangerous hazards that could harm the user community. The engineers demonstrating courage in tackling the challenging technical problems to keep people safe are just doing their jobs as system safety engineers or some other related job function, but they would not be considered as heroes.

When you think of heroes in engineering, you might say Nikola Tesla or Thomas Edison made significant contributions to the advancement of a safe world in terms of developing commercial power to light homes at night and prevent fires due to lit candles igniting window dressings or draperies. We are sure you will agree that commercial power saves lives, indirectly. As a result of commercial power, most home fires caused by candles lighting a home at night have been prevented, but fires at home will still occur regardless of the use of commercial power replacing candles. There are other mitigating factors that have a direct correlation to causes of fires at home, such as smoking cigarettes in bed or poor insulation of electrical wiring or overloaded electrical circuits.

A direct application of saving lives is a preventive action to design out an explosive hazard in an automobile due to the fuel tank during an automobile collision. As a result of an engineer's diligence, persistence, and commitment to mitigate the risk of a fuel tank explosion in a car during normal operation or during a catastrophic accident, it is clear that the engineer's actions would have saved lives, directly. This direct application of design improvements that result in no deaths or personal injuries caused by automobile fuel tank explosions should warrant the title of "Engineering Hero" to the ones worthy of such distinction.

Engineering needs more heroes [1]. Engineers with the biggest paychecks get the widest acclaim. To be a hero today, you must be considered financially successful and ahead of your peers. There must be other ways to recognize engineering heroes on a broad scale, but how? There is no Nobel Prize for engineering. There is no engineering award with similar global status and prestige. Engineers cannot routinely recognize their heroes in a similar fashion as do physicists, economists, and novelists. To be fair, in lesser known circles than Nobel, engineers are recognized by their peers through the Kyoto Prize, Charles Stark Draper Prize of the US National Academy of Engineering, and the IEEE's own Medal of Honor, to

name a few engineering honors. We agree with G. Pascal Zachary when he states that a valid criterion for an engineer to be considered an engineering hero is when one overcomes adversity. Engineering heroism appears when an engineer overcomes personal, institutional, or technological adversity to do their best job possibly while realizing what is ethically or morally right, contributing to the social and cultural well-being of all humanity.

Anyone who convinces a product manufacturer to install a safety feature on an existing product should be praised as a hero. One example of a design for safety feature that was installed on an existing product is the “safety mechanism” designed for firearms. A safety catch mechanism or safety switch used for pistol and rifle designs was intended to prevent the accidental discharge of a firearm, helping to ensure safe handling during normal use. The safety switch on firearms has two positions: one is “safe” mode and the other is “fire” mode. The two-position safety toggle switch was designed on the military grade firearm, M16 automatic rifle. In “safe” mode, the trigger cannot be engaged to discharge the projectile in the firing assembly. Other types of safety mechanisms include manual safety, grip safety, decocker mechanism, firing pin block, hammer block, transfer bar, safety notch, bolt interlock, trigger interlock, trigger disconnect, magazine disconnect, integrated trigger safety mechanism, loaded chamber indicator, and stiff double-action trigger pull. “Drop safety mechanisms” or “trigger guards” are passive safety features designed to reduce the chance of an accidental firearm discharge when the firearm is dropped or handled in a rough manner. Drop safeties generally provide an obstacle in the firing mechanism, which can only be removed when the trigger is pulled, so that the firearm cannot otherwise discharge. Trigger guards provide a material barrier to prevent inadvertent trigger pulls. Many firearms that were manufactured in the late 1990s were designed with mandatory integral locking mechanisms that had to be deactivated by a unique key before the firearm could be fired. These are intended as child-safety devices during unattended storage of firearms. These types of locking mechanisms were not intended as safety mechanisms while carrying. Other devices in this category are muzzle plugs, trigger locks, bore locks, and firearm safes.

Accidents decreased tremendously over the years as a result of safety features. Accidental discharges were commonplace in the days of the “Ole West,” circa 1850–1880. Those were the days before safety switches were designed into rifle and pistol designs. Now accidental discharges only occur when a loaded firearm is handled when the safety position is off. Since the implementation of this safety switch design, gunshots caused by accidental firing have been significantly reduced. There was a designer behind this safety switch design who thought about saving lives. In our minds, this designer was an unsung hero, one of many heroes in the development of safe firearms.

We propose these unsung heroes deserve immense credit for preventing unnecessary injury or death from accidental discharge of firearms. There are many more examples of this.

The idea for this book was conceived as a result of publishing our first book, *Design for Reliability*. We saw the need for additional books discussing various topics associated with the design process. As a result, we are planning to create a series of *Design for X* books with this one, *Design for Safety*, being the second in the series. Our book fills the gap between the published body of knowledge and current industry practices by communicating the advantages of designing for safety during the earliest phase of product or system development. This volume fulfils the needs of entry-level design engineers, experienced design engineers, engineering managers, and system safety engineers/managers who are looking for hands-on knowledge of how to work collaboratively on design engineering teams.

Reference

- [1] Zachary, G. P. (2014), Engineering Needs More Heroes, *IEEE Spectrum*, 51, 42–46.

Louis J. Gullo
Jack Dixon

Acknowledgments

We would like to thank Dev Raheja for his contributions to this book and for his co-editing of *Design for Reliability*, the first book in our planned *Design for X* series. Without the inspiration from Dev Raheja, only a few of these words would have been written. We have been humbled by his knowledge and grateful for his contributions to this book in offering us a cohesive framework using the ten paradigms in which to tie the pages together. We also are indebted to Nancy Leveson and her publishers. Her contributions to the field of system software safety are immense and greatly appreciated. There are many others who have made this work possible, adding to the body of knowledge from which we have drawn on. Among them, we especially want to thank Mike Allocco, Brian Moriarty, Robert Stoddard, Joseph Childs, and Denis W. Stearns.

Louis J. Gullo
Jack Dixon

Introduction: What You Will Learn

Chapter 1 Design for Safety Paradigms (Raheja, Gullo, and Dixon)

This chapter introduces the concept of design for safety. It describes the technical gaps between the current state of the art and what it takes to design safety into new products. This chapter introduces ten paradigms for safe design that help you do the right things at the right times. These paradigms will be used throughout the book as guiding themes.

Chapter 2 The History of System Safety (Dixon)

This chapter provides a brief history of system safety from the original “fly-fix-fly” approach to safety, to the 1940s’ hints at a better way of doing aircraft safety, to the 1950s’ introduction of the term “system safety,” and to the Minuteman program that brought the systematic approach to safety to the mainstream. Next, the development of and history of MIL-STD-882 is discussed. The growth of system safety and various hazard analyses techniques over the years are covered in detail. The expansion of system safety into the nonmilitary, commercial arena is discussed along with numerous industry standards. Tools of the trade, management of system safety, and integration of system safety into the business process are summarized.

Chapter 3 System Safety Program Planning and Management (Gullo and Dixon)

This chapter discusses the management of system safety in detail. It describes how system safety fits into the development cycle, how it is integrated into the systems engineering process, and what the key interfaces are between system safety and other disciplines. The System Safety Program Plan is described in detail as well as how it is related to other management plans. Another important document, the Safety Assessment Report, is also outlined in detail.

Chapter 4 Managing Risks and Product Liabilities (Gullo and Dixon)

In this chapter, the importance of product liability is emphasized beginning with some financial statistics and numerous examples of major losses due to bad design. The importance of risk and risk management is described. This chapter includes a brief summary of product liability law and what it means to the safety engineer and the organization developing the product or system.

Chapter 5 Developing System Safety Requirements (Gullo)

This chapter's main emphasis is on developing safety requirements including why we need them and why they are so important. We discuss what requirements are and how they enter into various types of specifications. This chapter covers in detail how to develop good safety requirements and provides examples of both good and bad requirements.

Chapter 6 System Safety Design Checklists (Dixon)

This chapter introduces various types of checklists and why they are an important tool for the safety engineer. It covers procedural, observational, and design checklists and provides examples of each type. The uses of checklists are also discussed, and several detailed checklists are provided in the appendices of the book.

Chapter 7 System Safety Hazard Analysis (Dixon)

This chapter introduces some terminologies and discusses risk in detail as an introduction to hazard analyses. After that, it covers several of the most widely used hazard analysis techniques including preliminary hazard list, preliminary hazard analysis, subsystem hazard analysis, system hazard analysis, operating and support hazard analysis, and health hazard analysis. The chapter ends with a discussion of hazard tracking and its importance.

Chapter 8 Failure Modes, Effects, and Criticality Analysis for System Safety (Gullo)

This chapter describes how the Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects, and Criticality Analysis (FMECA) are useful for system safety analysis. It discusses various types of FMEAs including Design FMECA, Software Design FMECA, and Process Failure Modes, Effects, and Criticality Analysis (PFMECA) and how they may be applied in a number of flexible ways at different points in the system, hardware, and software development life cycle.

Chapter 9 Fault Tree Analysis for System Safety (Dixon)

Fault Tree Analysis (FTA) is covered in this chapter. It is a very popular type of analysis used in system safety. It is a representation in tree form of the combination of causes (failures, faults, errors, etc.) contributing to a particular undesirable event. It uses symbolic logic to create a graphical representation of the combination of failures, faults, and errors that can lead to the undesirable event being analyzed. The purpose of FTA is to identify the combinations of failures and errors