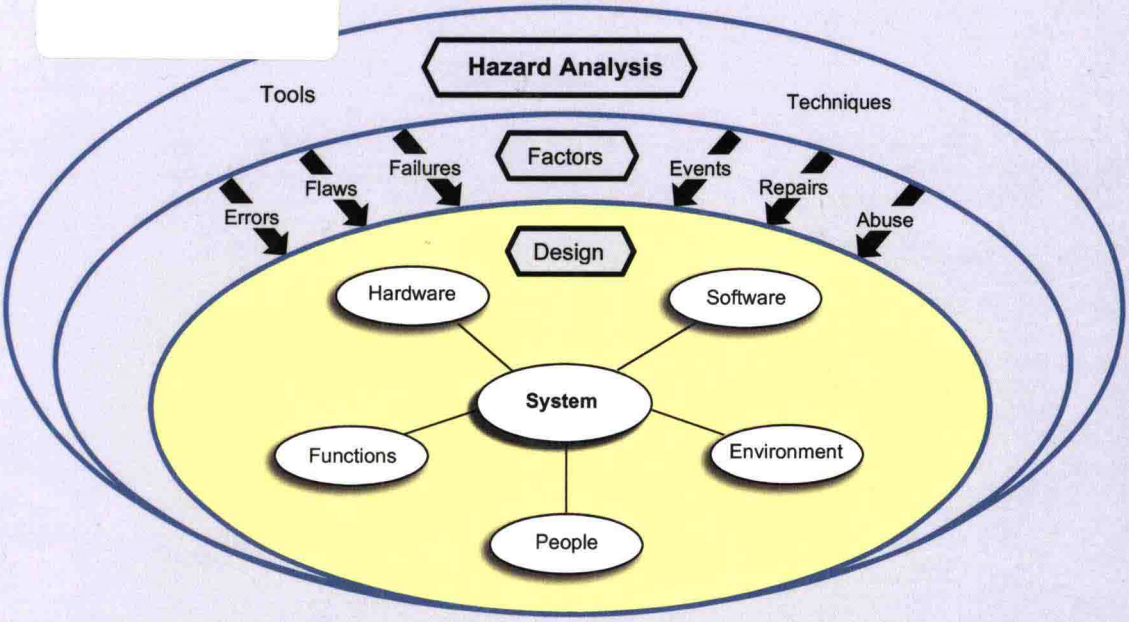
CLIFTON A. ERICSON II




# HAZARD ANALYSIS TECHNIQUES FOR SYSTEM SAFETY

SECOND EDITION

WILEY

# *Hazard Analysis Techniques for System Safety*

Second Edition

**Clifton A. Ericson, II**
Fredericksburg, Virginia



WILEY

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



***Library of Congress Cataloging-in-Publication Data***
Ericson, Clifton A., II.
Hazard analysis techniques for system safety / Clifton A. Ericson, II. – Second edition.
pages cm
Includes index.
ISBN 978-1-118-94038-9 (hardback)
1. Industrial safety–Data processing. 2. System safety. I. Title.
T55.E72 2015
363.11–dc23

2015016350

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

# *Hazard Analysis Techniques for System Safety*

# *Preface*

During my 50 year career in system safety, there have been two things about hazard analysis that have always bothered me. First, there has never been a formal description of hazard theory that defines the components of a hazard and the hazard–mishap actuation process. This is significant because risk cannot be determined unless the hazard is fully understood and described. Second, there is a lack of good reference material describing in detail how to perform the most relevant hazard analysis techniques or methodologies. This too is significant because hazard analysis is more complex than most people think, thus good descriptions and reference material are needed. I wrote this book to resolve these issues for system safety engineers and practitioners. The material in this book is applicable to both experienced professionals and those analysts just starting out in the field.

One of the main features of this book is that it describes hazard theory in detail. The hazard–risk–mishap connection is explained, with illustrations and examples provided. In addition, the three required components of a hazard are presented, along with the hazard triangle model.

Another primary feature of this book is that it describes 28 of the most commonly used hazard analysis methodologies in the system safety discipline. Each of the 28 hazard analysis methodologies covered in this book is given an entire chapter devoted to just that technique. In addition, each methodology chapter is organized in a similar pattern that is intended to provide consistency in answering the most common questions that an analyst might have. Detailed examples are provided to help analysts learn and understand these methodologies.

System safety is a proven engineering discipline that is applied during system development to identify and mitigate hazards, and in so doing eliminate or reduce the risk of potential mishaps and accidents. System Safety is ultimately about savings lives. It is my greatest hope that the readers of this book can use the material contained herein to better understand hazard identification and analysis. This in turn will help in designing and constructing systems that are safe, thereby saving many lives.

This revised version of the book has added eight new chapters, six of which are additional hazard analysis techniques. Also, this updated version has added new and revised material to reflect changes made as a result of the new MIL-STD-882, version E, which was released in 2012.

# *Acknowledgments*

In a book of this undertaking, there are naturally many people to acknowledge. This book reflects my life's journey through 50 years of engineering in the system safety discipline. My life has been touched and influenced by many people, far too many people to list and credit. For those whom I have left out I apologize. But it seems that there are a few people that always remain in the forefront of one's memory.

First and foremost, I would like to dedicate this book to my parents, Clifton Ericson I and Margaret Ericson. They instilled in me many good qualities that I might not have found without them, particularly the values of reading, education, science, religion, morality, and a work ethic.

I would like to acknowledge and dedicate this book to the Boeing System Safety organization on the Minuteman Weapon System development program. This was the crucible where the experiment of system safety really started, and this is where I started my career in system safety engineering. This group has provided my most profound work-related memories and probably had the greatest influence on my life. It was led by Niel Classon, who was an early visionary and leader in the system safety field. Other people in this organization who helped in my development included Dave Haasl, Gordon Willard, Dwight Leffingwell, Kaz Kanda, Brad Wolfe, Joe Muldoon, Harvey Moon, and Bob Schroder. Another Boeing manager who provided system safety guidance early in my career was Hal Trettin.

Later in my career, Perry D'Antonio of Sandia National Laboratories pushed me to excel in the System Safety Society and to eventually become president of this international organization. Paige Ripani of Applied Ordnance Technology, Inc. helped turn my career in a new direction, consulting for the Navy. And, last but not least, Ed Kratovil of the Naval Ordnance Safety and Security Activity (NOSSA) provided me with the opportunity to work on special Navy system and software safety projects.

In addition, I would like to acknowledge and thank the following individuals for reviewing early drafts of this manuscript: Jim Gerber, Sidney Andrews, Dave Shampine, Mary Ellen Caro, Tony Dunay, Chuck Dorney, John Leipper, Kurt Erthner, Ed Nicholson, William Hammer, and Jerry Barnette. Many of their comments and suggestions proved invaluable.

# *Contents*