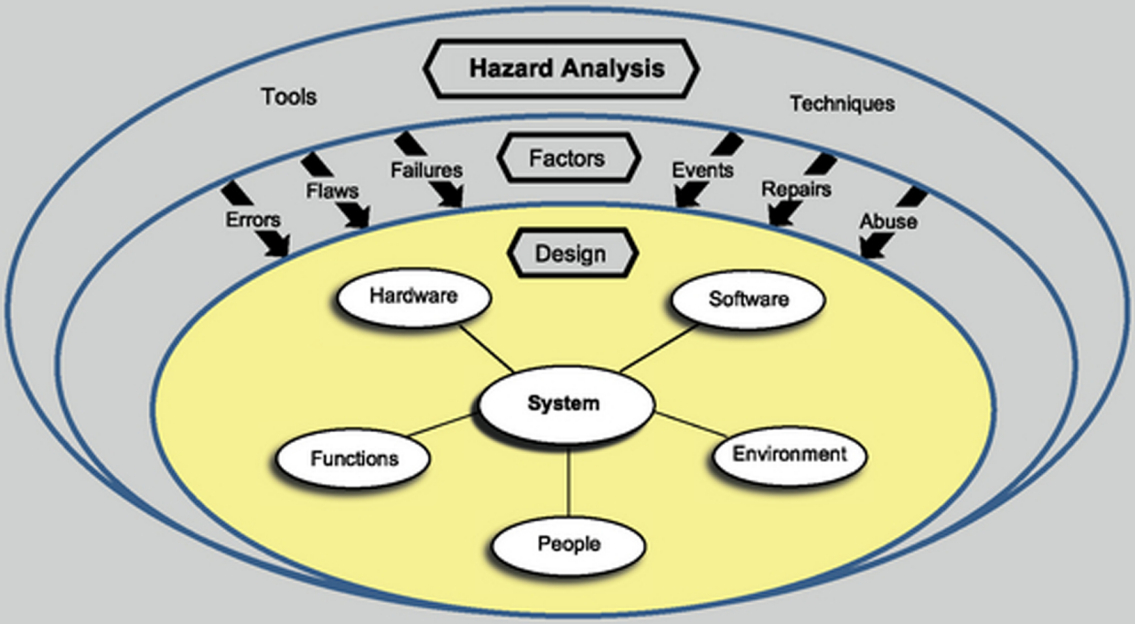
CLIFTON A. ERICSON II



HAZARD ANALYSIS TECHNIQUES FOR SYSTEM SAFETY

SECOND EDITION

WILEY

Hazard Analysis Techniques for System Safety

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

Contents

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.

Chapter 1

System Safety and Hazard Analysis

1.1 INTRODUCTION

We live in a world comprised of systems. When viewed from an engineering perspective, most aspects of life involve systems. For example, houses are a type of system, automobiles are a type of system, and electrical power grids are another type of system. Commercial aircraft are systems that operate within a larger transportation system that in turn operate in a larger worldwide airspace system. Systems have become a necessity for modern living.

As a result of living in a system-centric world, we also live in a world comprised of hazards and risk. With systems and technology also comes exposure to hazards and potential mishaps. A hazard is a potential condition existing within a system, which when actuated becomes an actual mishap event resulting in damage, loss, injury, and/or deaths. Risk is the probability that a hazard occurs accompanied by the severity of the resulting outcome.

Hazard risk is a metric that predicts the likelihood and severity of a possible mishap. We live with risk, and make risk decisions, on a daily basis. For example, there is the hazard that a traffic light will fail, resulting in the mishap of another auto colliding with your auto. Automobiles, traffic, and traffic lights form a unique system that we use daily and accept the hazard risk potential because the risk is small. There is the danger that the gas furnace in our house will fail and explode, thereby resulting in the mishap of a burned house, or worse. This is another unique system, with known adverse side effects that we choose to live with because the mishap risk is small and the benefits are great. We live in a world comprised of many different systems with many different risks.

Our lives are intertwined within a web of different systems, each of which can affect our safety. Each of these systems has a unique design and a unique set of components. In addition, each of these systems contains inherent hazards that present unique mishap risks. We are

Hazard Analysis Techniques for System Safety, Second Edition. Clifton A Ericson, II.

always making a tradeoff between accepting the benefits of a system and the mishap risk they present. As we develop and build systems, we should be concerned about eliminating and reducing mishap risk. Some risks are so small that they can easily be accepted, while other risks are so large that they must be dealt with immediately. Risks are akin to the invisible radio signals that fill the air around us, in that some are loud and clear, some very faint, and some are distorted and unclear. Life, as well as safety, is a matter of knowing, understanding, and choosing the risk to accept.

System safety is the formal engineering discipline and process for identifying and controlling hazards, and the risk associated with these hazards. As systems become more complex and more hazardous, more effort is required to understand and manage system mishap risk. Hazard (and mishap) risk can be intentionally reduced and controlled to a small and acceptable level through the system safety process.

The key to system safety and effective risk management is the identification and mitigation of hazards. To successfully control hazards, it is necessary to understand hazards and know how to identify them. The purpose of this book is to better understand hazards and the tools and techniques for identifying them, in order that they can be effectively controlled during the development of a system. The system safety process is sometimes referred to as *design for safety* (DFS).

1.2 THE NEED FOR HAZARD ANALYSIS

Forensic engineering is the detailed investigation of a mishap after it has occurred, performed to determine the specific causes for the mishap in order that corrective action can be applied to prevent reoccurrences. System safety, on the other hand, is a form of preemptive forensic engineering, whereby potential mishaps are identified, evaluated, and controlled before they occur. Potential mishaps and their causal factors are anticipated and identified during the design stage, and then design safety features are incorporated into the design to control the occurrence of the potential mishaps – safety is intentionally designed in and mishaps are effectively designed out. This proactive approach to safety involves hazard analysis, risk assessment, risk mitigation through design, and testing to verify the design results. Potential mishaps are recognized and identified by the hazards that ultimately cause them. System safety is a proactive approach to affecting the future (i.e., preventing mishaps before they occur) by identifying hazards and then eliminating or controlling the risk they present.

Systems are intended to improve our way of life, yet they also contain the inherent capability to spawn many different hazards that present us with mishap risk. It is not that systems are intrinsically bad; it is that systems can go awry, and when they go awry they typically result in mishaps. System safety is about determining how systems can go bad and implementing design safety mitigations to eliminate, correct, or work around safety imperfections in the system.

Murphy's law states that "if anything can go wrong, it will." This truism illustrates that the unexpected and undesired must be anticipated and controlled in order to prevent mishaps, and this can be achieved only through the system safety process. Hazards and risk often cannot be eliminated; however, hazards and risk can be anticipated and mitigated via safety design features, thereby preventing or reducing the likelihood of mishaps. If system safety is not applied, accidents and loss of life will not be prevented. System users are typically not aware of the actual risk they are exposed to, and without system safety this risk may be much higher than the users realize.

Hazard analysis is the basic key component of the system safety process. Therefore, it is necessary to fully understand the hazard theory and the hazard analysis process in order to develop safe systems.

1.3 SYSTEM SAFETY BACKGROUND

The primary guidance document for system safety is MIL-STD-882, System Safety Standard Practice. Version E was released on May 11, 2012. This standard has been in existence since 1969; its predecessor MIL-S-38130 was released in 1963.

MIL-STD-882 and its predecessor MIL-S-38130 are the genesis of system safety. The US military, along with US aerospace companies, saw the need for a holistic and proactive "systems" approach for the design, development, test, and manufacture of "safe" systems. Working together, these two groups developed the system safety methodology and discipline. MIL-S-38130 was originally released on September 30, 1963 and replaced by MIL-STD-882 on July 15, 1969. System safety was actually documented as a process prior to any formal documentation of the systems engineering discipline. System safety as a formal discipline was originally developed and promulgated by the military-industrial complex to prevent aircraft and missile mishaps that were costing lives, dollars, and equipment loss. As the effectiveness of the discipline was observed by other industries, it was adopted and applied to these industries and technology fields, such as commercial aircraft, nuclear power, chemical processing, rail transportation, the FAA, and NASA, to name a few.

The ideal objective of system safety is to develop a system free of hazards. However, absolute safety is not possible because complete freedom from all hazardous conditions is not always possible, particularly when dealing with complex inherently hazardous systems, such as weapon systems, nuclear power plants, commercial aircraft, etc.

Since it is generally not possible to eliminate all hazards, the realistic objective becomes that of developing a system with acceptable mishap risk. This is accomplished by identifying potential hazards, assessing their risks, and implementing corrective actions to eliminate or mitigate the identified hazards. This involves a systematic approach to the management of mishap risk. Safety is a basic part of the risk management process.

Hazards will always exist, but their risk can and must be made acceptable. Therefore, safety is a relative term that implies a level of risk that is measurable and acceptable. System safety is not an absolute quantity, but rather an optimized level of mishap risk management that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated and the level of risk accepted or rejected by an appropriate decision authority. Mishap risk management is the basic process of system safety engineering and management functions. System safety is a process of disciplines and controls employed from the initial system design concepts, through detailed design and testing to system disposal at the completion of its useful life (i.e. "cradle to grave" or "womb to tomb").

The fundamental objective of system safety is to identify, eliminate or control, and document system hazards. System safety encompasses all the ideals of mishap risk management and design for safety; it is a discipline for hazard identification and control to an acceptable level of risk. Safety is a system attribute that must be intentionally designed into a product.

From a historical perspective, it has been learned that a proactive preventive approach to safety during system design and development is much more cost-effective than trying to add safety to a system after the occurrence of an accident or mishap. System safety is an initial investment that saves future losses that could result from potential mishaps.

1.4 SYSTEM SAFETY OVERVIEW

System safety is effectively a design-for-safety process, discipline, and culture. DFS means that the design process utilizes the system safety process to intentionally design-in safety. This process anticipates potential safety problems (i.e., hazards) and eliminates them or reduces the risk they present. Safety risk is calculated from the identified hazards, and risk is eliminated or reduced by eliminating or mitigating the appropriate hazard causal factors. System safety, by necessity, considers function, criticality, risk, performance, and cost parameters of the system. Risk mitigation is achieved through a combination of design mechanisms, design features, warning devices, safety procedures, and safety training to counter the effect of hazard causal factors.

System safety involves a systems approach, which accounts for the distinctive name. System safety is the art and science of looking at all aspects and characteristics of a system as an integrated whole, rather than looking at individual components in isolation from the system. System safety is a holistic approach that considers the subject as an integrated sum-of-the-parts combination, rather than a piecemeal approach of looking at separate individual and solitary pieces of the system.

Often, system safety is not fully appreciated for the contribution it can make to creating safe systems that present a minimal chance of deaths and serious injuries. System safety applies a planned and disciplined methodology for purposely designing safety into a system. A system can be made safe only when the system safety methodology is consistently and properly applied. Safety is more than eliminating hardware failure modes; it involves designing the safe system interaction of hardware, software, humans, procedures, and the environment, under all normal and adverse failure conditions. Safety must consider the entirety of the problem, not just a portion of the problem, that is, a systems perspective is required for full safety coverage. System safety anticipates potential problems and either eliminates them or reduces their risk potential, through the use of design safety mechanisms applied according to a safety order of precedence.

System safety is the process of managing the system, personnel, environmental, and health mishap risks encountered in the design development, test, production, use, and disposal of systems, subsystems, equipment, materials, and facilities.

A system safety program (SSP) is a formal approach to eliminate hazards through engineering, design, education, management policy, and supervisory control of conditions and practices. It ensures the accomplishment of the appropriate system safety management and engineering tasks. The formal system safety process has been primarily established by the US Department of Defense (DoD) and its military branches and promulgated by MIL-STD-882. However, the same process is also followed in private industry for the development of commercial products, such as commercial aircraft, rail transportation, nuclear power, and automobiles, to mention a few.

The goal of system safety is the protection of life, systems, equipment, and the environment. The basic objective is the elimination of hazards that can result in death, injury, system loss, and damage to the environment. When hazard elimination is not possible, the next objective is to reduce the risk of a mishap through design control measures. Reducing mishap risk is achieved by reducing the probability of the mishap and/or the severity of the mishap.

This objective can be attained at minimum cost when the SSP is implemented early in the conceptual phase and is continued throughout the system development and acquisition cycle. The overall complexity of today's systems, particularly weapon systems, is such that system