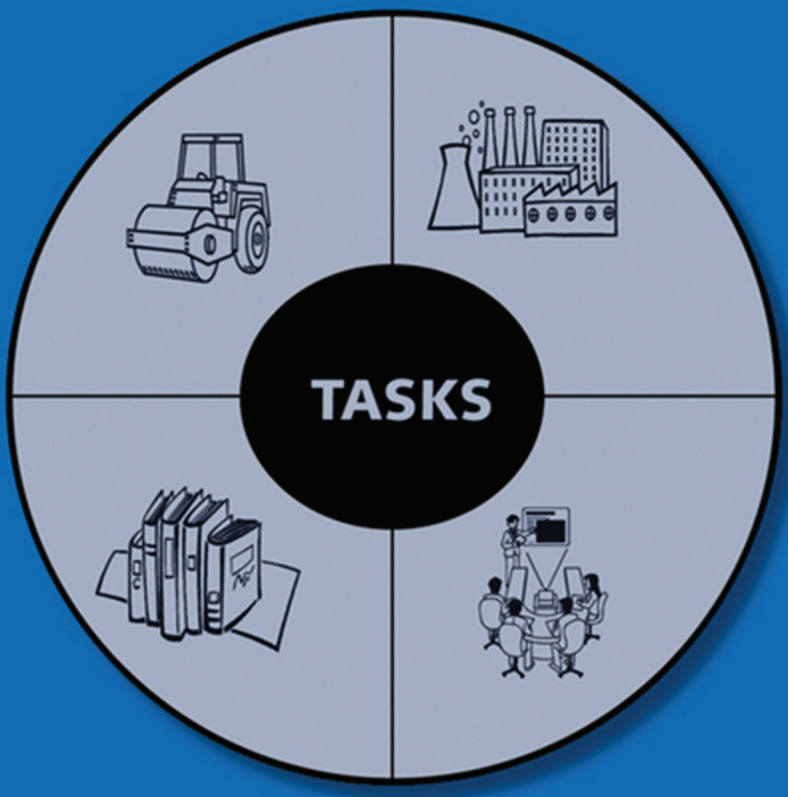
BASIC GUIDE TO

# System Safety

## Third Edition




Jeffrey W. Vincoli

WILEY

*Basic Guide to*
*System Safety*

# *Basic Guide to System Safety*

Third Edition

**Jeffrey W. Vincoli**
Manager of Environmental, Safety,
and Health Compliance Assurance and Support Services
Bechtel Global Corporation

WILEY

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



***Library of Congress Cataloging-in-Publication Data:***

Vincoli, Jeffrey W., author.
Basic guide to system safety / Jeffrey W. Vincoli. – Third edition.
p. ; cm.
Includes index.
ISBN 978-1-118-46020-7 (hardback)
I. Title.
[DNLM: 1. Occupational Health. 2. Safety. 3. Safety Management. WA 485]
T55
658.3′82–dc23 2013051270

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

*To my loving wife, Rosemary*

*Of all my accomplishments in this life, my greatest achievement was convincing you to be my wife. After more than 30 years together, I do not know how people go through life alone. I am blessed in many ways, but none more than having you as my wife. Thank you for always being there with your patience, your charm, your perspective, and your love. You are and will always be the most cherished thing about my life.*

# *Contents*

**PREFACE** **xiii**

**PART I THE SYSTEM SAFETY PROGRAM** **1**

**1 System Safety: An Overview** **3**

Background / 3
The Difference Between Industrial Safety and System Safety / 7
System Safety and the Assessment of Risk / 8

**2 System Safety Concepts** **15**

Fundamentals / 15
The System Safety Process / 16
System Safety Criteria / 18
Hazard Severity / 18
Hazard Probability / 18
The Hazard Risk Matrix / 19
System Safety Precedence / 20

Cost and Risk Acceptance / 24
Quantitative Risk Assessment / 25
Principles of Risk Management / 27
Management Commitment / 27

**3 System Safety Program Requirements 29**

The Safety Charter / 29
Selling Safety to Management / 30
The System Safety Effort / 31
Closed-Loop Hazard Tracking System / 32
Accident Risk Assessment / 33
Mishap/Accident/Incident Reporting / 33
Facility Inspection Reports / 36
System Safety Analyses / 36
Life Cycle Phases and the System Safety Process / 36
Concept Phase / 37
Design Phase / 37
Production Phase / 37
Operations Phase / 39
Disposal Phase / 39

**4 The Industrial Safety Connection 41**

The Occupational Safety and Health Act / 41
The Human Factors Element / 43
Accident Prevention Through System Design / 44
The Process of Task Analysis / 47
The Job Safety Analysis and System Safety / 48
Guidelines for Preparing a Job Safety Analysis / 50
Signatures and Approvals / 56
Changes in Hazard/Scope / 56
System Safety: an Integral Part of the Overall Organization / 57

**5 Probability Theory and Statistical Analysis 61**

Introduction / 61
Probability / 62
Statistics / 64
Summary / 67

**PART II SYSTEM SAFETY ANALYSIS: TECHNIQUES AND METHODS 69**

**6 Preliminary Hazard Analysis 71**

Introduction / 71
The PHA Development Process / 72
The PHA Report / 78
PHA Example / 78
System Description / 79
System Operation / 80
Preliminary Assessment / 81
Evaluation of System Risk / 81
Summary / 90

**7 Subsystem and System Hazard Analyses 91**

Introduction / 91
The Subsystem Hazard Analysis Report / 92
SSHA Example / 93
System Description / 93
Evaluation of Subsystem Hazard Risk / 95
Summary / 98

**8 Operating and Support Hazard Analysis 99**

Introduction / 99
Ergonomics / 99
When to Perform the O&SHA / 101
O&SHA Example / 103
Scope and Purpose of the Example O&SHA / 103
Risk Assessment / 104
Risk Assessment 1: 1B / 106
Risk Assessment 2: 1A / 107
Risk Assessment 3: 2B / 107
Summary / 109

**9 Energy Trace and Barrier Analysis 111**

Introduction / 111
The Energy–Barrier Concept / 111
Uses of the ETBA / 112

Performing the ETBA / 112
The ETBA Worksheet / 113
ETBA Example / 114
System Description / 114
The ETBA / 114
Summary / 118

**10 Failure Mode and Effect Analysis 119**

Introduction / 119
Types of FMEAs / 119
Performing an FMEA / 120
The FMEA Report / 121
FMEA Example / 124
System Component/Subassembly Description / 124
System Operation / 128
Failure Mode(s) and Effect(s) / 128
Evaluation of Potential Subsystem or Component Failures / 129
Summary / 132

**11 Fault or Functional Hazard Analysis 135**

Introduction / 135
The FHA Process / 136
FHA Example / 137
System Description / 137
The FHA Process / 139
The FHA / 141
Summary / 143

**12 Fault Tree Analysis 145**

Introduction / 145
Qualitative and Quantitative Reasoning / 146
Constructing a Fault Tree / 146
Fault Tree Symbols / 147
FTA Examples / 150
Probability Values and the Fault Tree / 153
Summary / 156

**13 Management Oversight and Risk Tree** **157**

Introduction / 157
The MORT Analytical Chart / 158
MORT Use / 159
The MORT Event Tree / 160
Symbols / 160
MORT Analysis Example / 161
MORT Color Coding / 163
Procedure for MORT Analysis / 165
Summary / 165

**14 HAZOP and What-If Analyses** **167**

Introduction / 167
Background / 168
Definitions / 168
Objectives / 169
Team Members / 169
Reference Data Requirements / 169
The Concept of "Nodes" / 170
Conducting the What-If Analysis / 171
What-If Analysis Steps / 171
The What-If Analysis Worksheet / 173
Conducting The HAZOP Study / 175
The HAZOP Worksheet / 175
The Analysis Report / 176
Summary / 177

**15 Special Use Analysis Techniques** **179**

Introduction / 179
Sneak Circuit Analysis / 180
Types and Causes of Sneaks / 180
SCA Input Requirements / 181
Advantages and Disadvantages of the SCA / 181
Software Hazard Analysis / 183
Types of SWHA Techniques / 183
Summary / 185

**Epilogue** **187**

**Appendix A Sources of Additional Information/Training** **189**

**Appendix B Acronyms and Abbreviations** **195**

**GLOSSARY OF TERMS** **199**

**BIBLIOGRAPHY** **223**

**INDEX** **225**

# *Preface*

The third edition of the *Basic Guide to System Safety* contains all of the content of the previous editions, updated (where applicable) to reflect current industry practice. The first edition of the *Basic Guide to System Safety* was the first volume issued in a series of *Basic Guide* books that focused on the topics of interest to the practicing occupational safety and/or health professional. Other books in the Series include the *Basic Guide to Environmental Compliance*, *Basic Guide to Accident Investigation and Loss Control*, and *Basic Guide to Industrial Hygiene*. Each book has been designed to provide the reader with a fundamental understanding of the subject and attempt to foster a desire for additional information and training.

In addition to updated content of the previous editions, the revised third edition of the *Basic Guide to System Safety* introduces some system safety concepts not previously discussed to further expand upon the basic knowledge that is the cornerstone of the Basic Guide Series. In this regard, the third edition contains a discussion on the concept of Design for Safe Construction where the methods and techniques associated with the system safety discipline can be effectively utilized to identify, analyze, eliminate, or control system hazards during the design phase of a construction project. As with all analytical methods and techniques presented in this text, it is suggested that the concept of design for construction safety has definite application to general industry operations.

Also, information on the use of the various methods and techniques associated with the use of system safety has been expanded in the third edition to include guidance on the evaluation and verification of compliance efforts following the implementation of system safety analysis. This additional information will attempt to close-the-loop on the effective use of system safety analysis in the industrial safety environment.

It should be noted from the onset that it is not and never has been the intention of the *Basic Guide to System Safety* to provide any level of expertise beyond that of novice. Those practitioners and users who desire complete knowledge of the subject will not be satisfied with the information contained on these pages. It is not practical or feasible to expect a "basic guidebook" to contain all possible technical information on any subject, especially one as complex as system safety. However, those that require or perhaps only desire a basic understanding of a field similar but distinctly separate from their current area of specialization will find the third edition of *Basic Guide to System Safety* a valuable reference source and introductory primer. It is also assumed that those currently involved in the practice of system safety engineering and analysis might find this material somewhat enjoyable and, at the very least, refreshing. Also, professionals not directly involved in the system safety effort but who must work in association with those that are, will also find this text useful.

Finally, although the books in the *Basic Guide Series* were always originally intended for the practicing safety professional, the *Series* has been proven to be quite useful as textbooks for introductory courses in numerous colleges and universities. In this regard, the third edition will provide some additional fodder for enhancing existing primer courses on the subject.

It has long been known by practicing safety and health professionals that organizations with excellent safety performance records have a well-rounded corporate policy or at least a firmly established administrative posture that consistently emphasizes the importance and value of working safely. The leadership of such organizations has provided their strong (and intelligent) commitment in support of the safety effort. Therefore, this text concentrates especially upon the concepts that all executives should understand concerning the role that safety programs play in the successful operation of a business. No less of a commitment is necessary to properly implement system safety into an already established occupational/industrial safety and health program.

It is also recognized that, in order to achieve operationally safe system performance, system safety programs must be conducted with defined purpose, proficiency, skill, and a sense of well-rounded responsibility to the needs of the organization that the system safety program is intended to serve. In such a supportive environment, the system safety effort can and will become a vital contributor to the overall success of the enterprise.

This text places considerable emphasis on the integration of system safety principles and practices into the total framework of the organization. Anything less would constitute unsound business management. In the 20 years since the publication of the first edition of *Basic Guide to System Safety,* this very concept has been tested and proven viable numerous times by the author and other safety and health practitioners. There are examples of the successful integration of system safety methodologies into the practice of safety and health assurance in general industry, construction, rail, maritime, and aviation. It works, as long as there is understanding and commitment.

In short, the third edition of *Basic Guide to System Safety* follows tradition of the previous two editions. Safety and health professionals, as well as managers,

engineers, technicians, designers, and college professors and their students should obtain some benefit from the information contained in this book.

## ACKNOWLEDGMENTS

In the preparation of the third edition of *Basic Guide to System Safety*, I would like to thank and acknowledge those individuals and organizations that assisted in the initial, as well as revised, versions of this text.

First, I do not want to forget the valuable advice and assistance of those colleagues and associates who helped in the development and review of the first edition. Specifically, Steven S. Phillips, Frank Beckage, Douglas J. Tomlin, George S. Brunner, and Susie Adkins.

Second, I wish to recognize and acknowledge the training firm of Technical Analysis, Inc. (TAI) in Houston, Texas for permitting me to use some of their materials in the first and subsequent editions of this text, and for developing and providing exceptional training seminars on the subject of System Safety Engineering. Their contributions to the advancement of the System Safety discipline are commendable and appreciated.

Third, I would like to thank all those who participated in bringing this third edition of *Basic Guide to System Safety* to fruition including all the reference sources used herein, and the reviewers who helped identify specific areas for improvement over the previous editions. Thanks also to Fred Manuele for his leadership as Chair of the ANSI Z590.3-2011 Committee.

Fourth, a special thanks to Bob Esposito and Michael Leventhal of John Wiley & Sons for their support in making this third edition a reality.

Finally, I want to thank my wife, Rosemary, for her patience, understanding, and encouragement during my work to complete this process, and for her dedicated support of all that I do, always.

# *Part I*

# *The System Safety Program*

In the practice of occupational safety and health in industry today, the primary concern of any responsible organization is the identification and elimination of hazards that threaten the life and/or health of employees, as well as those which could cause damage to facilities, property, equipment, products, and/or the environment. When such risk of hazard cannot be totally eliminated, as is often the case, it becomes a fundamental function of the safety professional to provide recommendations to control those hazards in an effort to reduce the associated risk to the lowest acceptable levels.

It is the intention of this *Basic Guide to System Safety* to demonstrate the effectiveness of the system safety process in identifying and eliminating hazards, recommending risk reduction techniques, and methods for controlling residual hazard risk.

Part I will introduce the reader to the system safety process, how it evolved, how it can be managed, and how it relates to the current practice of the industrial safety and health professional. In fact, upon completion of Part I, the reader shall have developed a clear understanding of this relationship and, quite possibly, have developed an interest in the further pursuit of the system safety profession. As noted in the Preface, the information provided here is introductory in scope, intended to merely acquaint the reader with the system safety approach to hazard analysis and hazard risk reduction.

As a separate discipline, system safety had its origins in the aviation and aerospace industries. Systems safety has proven its worth in the dramatic improvements in

*Basic Guide to System Safety*, Third Edition. Jeffrey W. Vincoli.

aviation safety over the past 60 years. It is not by chance that flying is demonstrably the safest mode of travel and this accomplishment has led to an undeniable understanding that all modern systems require a more logical, focused approach to identifying and controlling hazards. System safety is no longer a discipline reserved for the aerospace designer and nuclear engineer; it is the most effective method of improving the safety of any modern operation. As it has developed and matured, system safety has moved away from being the exclusive domain of design engineers and has become less mathematical or abstract and is now more practical and realistic. Modern concepts of system safety can be used by any organization or person who wants a logical, visible, and traceable method of identifying and controlling safety hazards and this is the objective of the *Basic Guide to System Safety*.

# 1

# *System Safety: An Overview*

## BACKGROUND

The idea or concept of *system safety* can be traced to the missile production industry of the late 1940s. It was further defined as a separate discipline by the late 1950s (Roland and Moriarty 1983) and early 1960s, used primarily by the missile, aviation, and aerospace communities. Prior to the 1940s, system designers and engineers relied predominantly on a trial-and-error method of achieving safe design. This approach was somewhat successful in an era when system complexity was relatively simple compared with those of subsequent development. For example, in the early days of the aviation industry, this process was often referred to as the "*fly-fix-fly*" approach to design problems (Roland and Moriarty 1983; Stephenson 1991) or, more accurately, "*safety-by-accident.*" Simply stated, an aircraft was designed based upon existing or known technology. It was then flown until problems developed or, in the worst case, it crashed (Figure 1.1). If design errors were determined as the cause (as opposed to human, or "pilot" error), then the design problems would be fixed and the aircraft would fly again. Obviously, this method of after-the-fact design safety worked well when aircraft flew low and slow and were constructed of wood, wire, and cloth. However, as systems grew more complex and aircraft capabilities such as airspeed and maneuverability increased, so did the likelihood of devastating results from a failure of the system or one of its many subtle interfaces. This is clearly demonstrated in the early days of the aerospace era (the 1950s and 1960s). As the industry began to develop jet powered aircraft and space and missile systems, it quickly became clear that engineers

*Basic Guide to System Safety*, Third Edition. Jeffrey W. Vincoli.

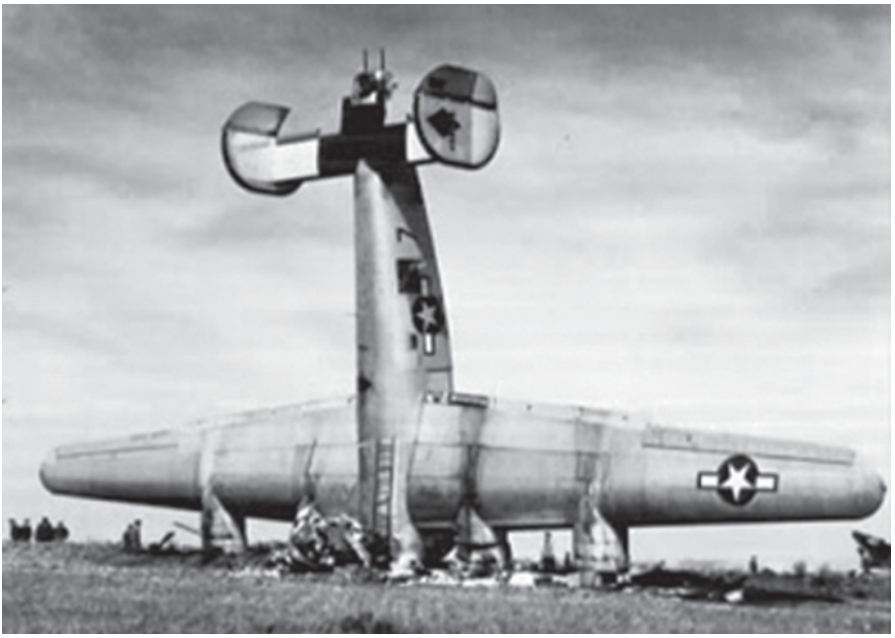


***Figure 1.1*** *The "fly-fix-fly" approach, or more accurately "safety-by-accident," focused on fixing design issues after an accident event rather than focusing on accident prevention through design.*

could no longer wait for problems to develop; they had to anticipate them and "fix" them before they occurred. To put it another way: the "fly-fix-fly" philosophy was no longer feasible. Elements such as these became the catalyst for the development of *systems engineering*, out of which eventually grew the concept of *system safety*. The need to anticipate and fix problems before they occurred led to a new approach—a consideration of the design as a "system." This means that all aspects of the design of operation (e.g., machine, operator, and environment) must be considered in identifying potential hazards and establishing appropriate controls. Another important part of this "systems" approach to safety is the realization that resources for safety are limited and there must be some logical, reasoned way to apply resources to the most serious potential problems. Systems safety provides this capability. Figure 1.2 shows a simplification of the basic elements of the systems engineering process. It is noted that safety comprises only one part of this integrated engineering design approach (Larson and Hann 1990). Taken one step further, Figure 1.3 demonstrates how the systems approach associated with the initial element of the systems safety engineering process—the design aspect—can support the identification of hazards in the earliest phases of a project life cycle. Only after the accurate identification of hazards can proper elimination or control measures be determined.

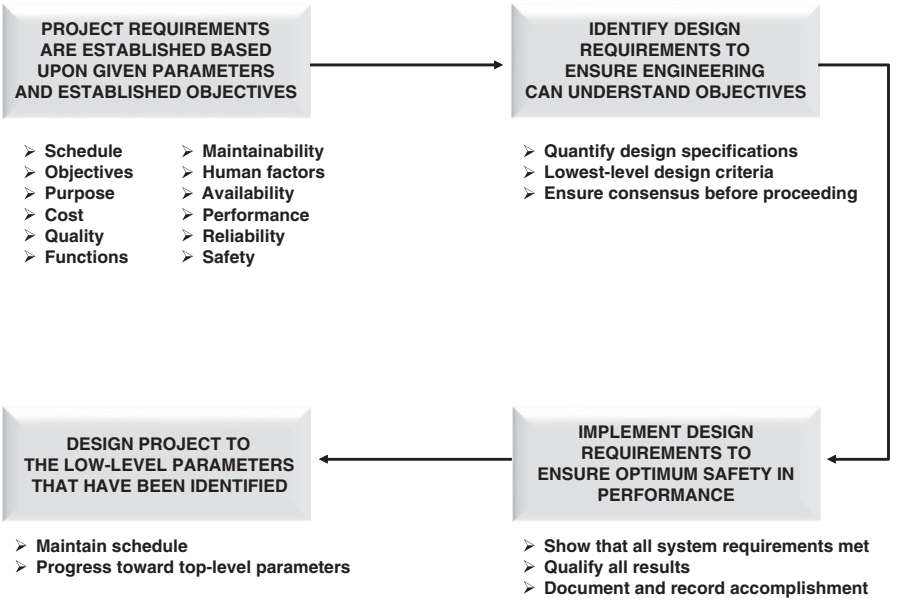



***Figure 1.2*** *The system safety engineering process (*Source: *Larson and Hann 1990).*

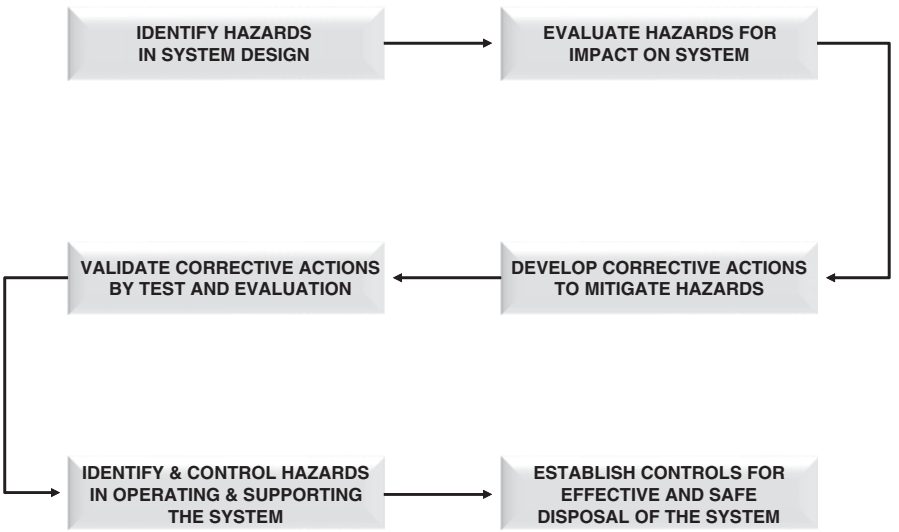



***Figure 1.3*** *The systems approach to the consideration of safety from the design phase through product disposal or project termination.*

The dawn of the manned spaceflight program in the mid-1950s also contributed to the growing necessity for safer system design. Hence, the growing missile and space systems programs became a driving force in the development of system safety engineering. Those systems under development in the 1950s and early 1960s required a new approach to controlling hazards such as those associated with weapon and space systems (e.g., explosive components and pyrotechnics, unstable propellant systems, and extremely sensitive electronics). The Minuteman Intercontinental Ballistic Missile (ICBM) was one of the first systems to have had a formal, disciplined, and defined system safety program (Roland and Moriarty 1983). In July of 1969, the US Department of Defense (DOD) formalized system safety requirements by publishing MIL-STD-882 entitled "System Safety Program Requirements." This Standard has since undergone a number of revisions.

The US National Aeronautics and Space Administration (NASA) soon recognized the need for system safety and has since made extensive system safety programs an integral part of space program activities. The early years of our nation's space launch programs are full of catastrophic and quite dramatic examples of failures. During those developing years, it was a known and quite often stated fact that *"our missiles and rockets just don't work, they blow up."* The many successes since those days can be credited in large part to the successful implementation and utilization of a comprehensive system safety program. However, it should be noted that the Challenger disaster in January 1986 and the loss of the orbiter Columbia upon reentry in February of 2003 stand as historic reminders to us all that, no matter how exact and comprehensive a design or operating safety program is considered to be, the proper *management* of that system is still one of the most important elements of success. This fundamental principle is true in any industry or discipline.

Eventually, the programs pioneered by the military and NASA were adopted by industry in such areas as nuclear power, refining, mass transportation, chemicals, healthcare, and computer programming.

Today, the system safety process is still used extensively by the various military organizations within the DOD, as well as by many other federal agencies in the United States such as NASA, the Federal Aviation Administration, and the Department of Energy. In most cases, it is a required element of primary concern in the federal agency contract acquisition process.

Although it would not be possible to fully discuss the basic elements of system safety without comment and reference to its military/federal connections, the primary focus of this text shall be placed upon the advantages of utilizing system safety concepts and techniques as they apply to the general safety arena. In fact, the industrial workplace can be viewed as a natural extension of the past growth experience of the system safety discipline. Many of the safety rules, regulations, statutes, and basic safety operating criteria practiced daily in industry today are, for the most part, the direct result of a real or perceived need for such control doctrine. The requirement for safety controls (written or physical) developed either because a failure occurred or someone with enough foresight anticipated a possible failure and implemented controls to avoid such an occurrence. Even though the former example is usually the case, the latter is also responsible for the development of countless safe operating

requirements practiced in industry today. Both, however, are also the basis upon which system safety engineers operate.

The first method, creating safety rules *after* a failure or accident, is likened to the *"fly-fix-fly"* approach discussed earlier. The second method, anticipating a potential failure and attempting to avoid it with control procedures, regulations, and so on, is exactly what the system safety practitioner does when analyzing system design or an operating condition or method. However, when possible or practical, the system safety concept goes a step further and actually attempts to engineer the risk of hazard(s) out of the process. With the introduction of the system safety discipline, the *fly-fix-fly* approach to safe and reliable systems was transformed into the *"identify, analyze, and eliminate"* (Abendroth and Grass 1987) method of system safety assurance.

We have established the basic connection between the system safety discipline and its relationship to the general industry occupational safety practice. This conceptual relationship will be examined in more detail throughout this text.

## THE DIFFERENCE BETWEEN INDUSTRIAL SAFETY AND SYSTEM SAFETY

Industrial safety, or occupational safety, has historically focused primarily on controlling injuries to employees on the job. The industrial safety engineer usually is dealing with a fixed manufacturing design and hazards that have existed for a long time, many of which are accepted as necessary for operations. Traditionally, more emphasis is often placed on training employees to work within this environment rather than on removing the hazards.

To perform their charter, industrial safety engineers collect data during the operational life of the system and eliminate or control unacceptable hazards where possible or practical. When accidents occur, they are investigated and action is taken to reduce the likelihood of a recurrence—either by changing the plant or by changing employee work rules and training. The hazards associated with high-energy or dangerous processes are usually controlled either by

- Disturbance control algorithms implemented by operators or an automated control system or
- Transferring the plant to a safe state using a separate protection system.

Safety reviews and compliance audits are conducted by industrial safety organizations within a company or, less frequently, by safety committees to ensure that unsafe conditions in the workplace are corrected and that employees are following the work rules specified in manuals, directives, and operating instructions. Lessons learned from accidents are incorporated into design standards, and much of the emphasis in the design of new plants and work rules is on implementing these standards. Often, the standards are enforced by the government through occupational safety and health legislation.