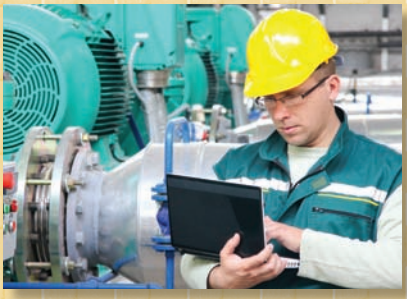
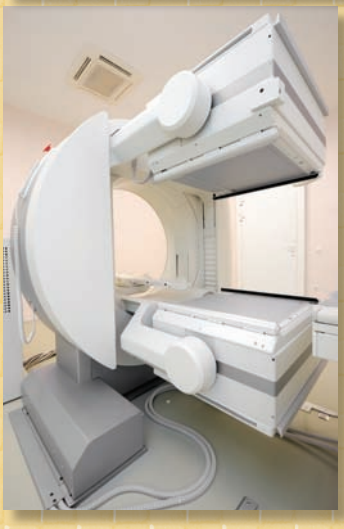
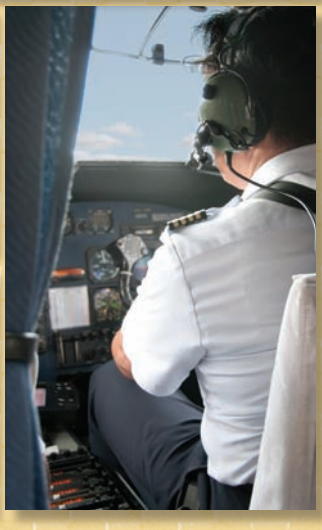
Safety and Human Error in Engineering Systems





B. S. Dhillon

CRC Press
Taylor & Francis Group

Safety and Human Error in Engineering Systems

This page intentionally left blank

Safety and Human Error in Engineering Systems

B. S. Dhillon

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20120625

International Standard Book Number-13: 978-1-4665-0695-4 (eBook - PDF)

This book is affectionately dedicated to all my friends including Matt Farrow, Joe Hazelton, and Archy during my teenage years in England for their kindness and guidance.

This page intentionally left blank

Contents

Preface

Nowadays, engineering systems are an important element of the world economy because each year billions of dollars are spent to develop, manufacture, and operate various types of engineering systems around the globe. Their safety and failure due to human error have become an important concern because of increasing accidental deaths and cost. For example, in regard to automobile accidents on highways alone, in the United States around 42,000 deaths occur annually and, in 1994, the cost of motor vehicle crashes was estimated to be about $150 billion to the United States economy.

Furthermore, around 70–90% of transportation-related crashes were directly or indirectly due to human error. Needless to say, safety and human error in engineering systems have become more important than ever before. Over the years, a large number of journal and conference proceedings articles on various aspects of safety and human error in engineering systems have appeared, but to the best of this author's knowledge there is no specific book on the topic. This causes a great deal of difficulty for information seekers because they have to consult many different and diverse sources.

Thus, the main objective of this book is to combine safety and human error in regard to engineering systems into a single volume and to eliminate the need to consult many different and diverse sources in obtaining desired information. The book contains a chapter on mathematical concepts considered necessary to understand material presented in subsequent chapters.

The topics covered in the book are treated in such a manner that the reader will require no previous knowledge to understand the contents. At appropriate places, the book contains examples along with their solutions, and at the end of each chapter there are numerous problems to test the reader's comprehension. The sources of most of the materials presented are given in the reference section at the end of each chapter. An extensive list of publications dating from 1926 to 2009, directly or indirectly on safety and human error in engineering systems, is provided at the end of this book to give readers a view of the intensity of developments in the area.

This book is composed of 11 chapters. Chapter 1 presents various introductory aspects of safety and human error including safety and human error-related facts and figures, terms and definitions, and sources for obtaining useful information on safety and human error in engineering systems. Chapter 2 reviews mathematical concepts considered useful to understanding subsequent chapters. Some of the topics covered in the chapter are Boolean algebra laws, probability properties, probability distributions, and useful definitions.

Chapter 3 presents various introductory safety and human factors and error concepts. Chapter 4 presents a total of 10 methods considered useful

for performing safety and human error analysis in engineering systems. These methods are interface safety analysis, technic of operations review, root cause analysis, hazards and operability analysis, preliminary hazard analysis, failure modes and effect analysis (FMEA), probability tree method, error-cause removal program, Markov method, and fault tree analysis. Chapter 5 is devoted to transportation systems safety. Some of the topics covered in this chapter are railroad tank car safety, light-rail transit-system safety issues, truck and bus safety-related issues, causes of airplane crashes, and ship port-related hazards.

Chapters 6 and 7 present various important aspects of medical systems safety and mining equipment safety, respectively. Chapter 8 is devoted to robot and software safety. It covers topics such as safety considerations in robot life cycle, human factors issues in robotic safety, general guidelines to reduce robot safety problems, software hazard causing ways, basic software system safety-related tasks, and software hazard analysis methods. Chapter 9 covers various important aspects of human error in transportation systems including railway personnel tasks prone to serious human error, typical human error occurrence areas in railway operation, common driver errors and ranking of driver errors, contributory factors to flight crew decision errors, and shipping systems human error-related facts and figures.

Chapter 10 is devoted to human error in healthcare systems and in mining equipment. Some of the topics covered in the chapter are healthcare systems human error-related facts and figures, medical device operator errors and medical devices with a high incidence of human errors, general guidelines for reducing medical device/equipment user interface-related errors, causes and classifications of human errors resulting in fatal mine accidents, common mining equipment-related maintenance errors and their contributory factors, and methods to perform mining equipment human error analysis. Finally, Chapter 11 presents various important aspects of human error in power plant maintenance and aviation maintenance.

The book will be useful to many individuals including system engineers, design engineers, human factors engineers, safety engineers, engineering managers and administrators, researchers and instructors involved with engineering systems, and graduate and senior undergraduate students in system engineering, human factors engineering, safety, and psychology.

The author is deeply indebted to many individuals, including family members, friends, colleagues, and students for their invisible input. The unseen contributions of my children also are appreciated. Last, but not least, I thank my wife, Rosy, my other half and friend, for typing this entire book and for her timely help in proofreading.

B. S. Dhillon

About the Author

B. S. Dhillon, PhD, is a professor of Engineering Management in the Department of Mechanical Engineering at the University of Ottawa, Ontario, Canada. He has served as a chairman/director of the Mechanical Engineering Department/Engineering Management Program for over 10 years at the same institution. Dr. Dhillon is the founder of the probability distribution called *Dhillon Distribution* used by statistical researchers in their publications around the world. He has published over 362 (i.e., 215 journal and 147 conference proceedings) articles on reliability engineering, maintainability, safety, engineering management, etc. He is or has been on the editorial boards of 11 international scientific journals. In addition, Dr. Dhillon has written 39 books on various aspects of reliability, safety, healthcare, engineering management, design, and quality that were published by John Wiley & Sons (1981), Van Nostrand (1982), Butterworth (1983), Marcel Dekker (1984), Pergamon (1986), among others. His books are being used in over 100 countries and many of them are translated into languages such as German, Russian, Chinese, and Persian (Iranian).

He has served as general chairman of two international conferences on reliability and quality control that were held in Los Angeles and Paris in 1987. Dr. Dhillon also has served as a consultant to various organizations and has many years of experience in the industrial sector. At the University of Ottawa, he has been teaching reliability, quality, engineering management, design, and related areas for over 31 years and he has lectured in over 50 countries as well, including keynote addresses at various international scientific conferences held in North America, Europe, Asia, and Africa. In March 2004, Dr. Dhillon was a distinguished speaker at the Conference/Workshop on Surgical Errors (sponsored by the White House Health and Safety Committee and the Pentagon) held on Capitol Hill (One Constitution Avenue, Washington, D.C.).

Dr. Dhillon attended the University of Wales where he received a BS in electrical and electronic engineering and an MS in mechanical engineering. He received a PhD in industrial engineering from the University of Windsor, Ontario.

This page intentionally left blank

1

Introduction

1.1 Background

Each year billions of dollars are spent to develop, manufacture, operate, and maintain various types of engineering systems throughout the world. Their safety and failure due to human error have become a pressing issue because of a large number of accidental deaths and a high cost. For example, in the United States automobile accidents on highways alone cause around 42,000 deaths annually and, in 1994, the total cost of motor vehicle crashes was about $150 billion to the United States economy [1–4]. Furthermore, around 70–90% of transportation-related crashes are due to human error to a certain degree [1].

The history of safety, directly or indirectly, in regard to engineering products may be traced back to 1868 when a patent was awarded for the first barrier safeguard and to 1877 when the Massachusetts legislature passed a law requiring appropriate safeguards on hazardous machinery [5,6]. In regard to human error in engineering systems, the history goes back to the late 1950s when H. L. Williams clearly pointed out that the reliability of the involved human element must be included in the prediction of engineering systems reliability; otherwise the predicted system reliability would not depict the actual picture [7].

Over the years, a large number of publications directly or indirectly related to safety and human error in engineering systems have appeared. A list of over 500 such publications is provided in the Further Reading.

1.2 Facts and Figures

Some of the facts and figures directly or indirectly concerned with safety and human error in engineering systems are as follows:

- In 1995, work-related accidents cost the United States economy about $75 billion [8].

- Each year the United States industrial sector spends over $300 billion on plant operation and maintenance and around 80% of this figure is spent to rectify the chronic failure of machine, systems, and humans [9].
- A study of safety-related issues concerning onboard fatalities of jet fleets worldwide for the period 1982 to 1991, indicated that inspection and maintenance were clearly the second most important safety issue, with a total of 1481 onboard fatalities [10,11].
- As per Ref. [12], the annual cost of world road crashes is over $500 billion.
- Maintenance error contributes about 15% of air carrier accidents and costs the United States industrial sector over $1 billion per year [13].
- The work-related accidental deaths by cause in a typical year in the United States are poison (gas, vapor): 1.4%, water transport-related: 1.65%, poison (liquid, solid): 2.7%, air transport-related: 3%, fire-related: 3.1%, drowning: 3.2%, electric current: 3.7%, falls: 12.5%, motor vehicle-related: 37.2%, and others: 31.6% [5,14].
- In 2004, around 53% of the railway switching yard accidents (excluding highway rail crossing train accidents) in the United States were the result of human factors-related causes [15].
- In 1969, the U.S. Department of Health, Education, and Welfare special committee reported that over a period of 10 years in the United States, there were around 10,000 medical device-related injuries and 731 resulted in fatalities [16,17].
- In 2000, there were 5200 fatalities due to the occurrence of work-related accidents in the United States [6,18].
- During the period 1970–1998, about 62% of the 13 railway accidents that caused fatalities or injuries in Norway were due to human error [19].
- In 1986, the Space Shuttle Challenger exploded and all its crew members were killed [6,20].
- In 1985, a Japan Airlines Boeing 747 jet accident due to incorrect repair caused 520 fatalities [21].
- During the period 1983–1996, there were 371 major airline crashes, 29,798 general aviation crashes, and 1,735 commuter/air taxi crashes [3,23]. A study of these crashes reported that pilot error was a probable cause in 38% of major airline crashes, 85% of general aviation crashes, and 74% of commuter/air taxi crashes [3,23].
- During the period 1978–1987, there were 10 robot-related fatal accidents in Japan [24].
- A study of 6091 accident claims, over $100,000, associated with all classes of commercial ships over a period of 15 years, performed by

the U.K. P&I Club reported that 62% of the claims were attributable to human error [25–27].

- In 1986, a nuclear reactor in Chernobyl, Ukraine, exploded and directly or indirectly caused around 10,000 fatalities [6,20].
- A study reported that over 20% of all types of system failures in fossil power generation plants occur due to human errors and maintenance errors account for around 60% of the annual power loss due to human error-related problems [28].
- Human error is cited more frequently than mechanical-related problems in about 5000 truck-related fatalities that occur annually in the United States [3,29].
- Two patients died and a third patient was injured severely because of a software error in a computer-controlled therapeutic radiation machine called Therac 25 [30–32].
- In 1979, 272 people died in a DC-10 aircraft accident in Chicago because of incorrect procedures followed by maintenance workers [33].
- According to a Boeing study, in over 73% of aircraft accidents around the world, the failure of the cockpit crew has been a contributing factor [34,35].
- In 1990, a study of 126 human error-related significant events in the area of nuclear power generation revealed that around 42% of the problems were linked to modification and maintenance activities [36].
- A study of 199 human errors that occurred in Japanese nuclear power generation plants during the period 1965–1995 reported that about 50% of them were concerned with the maintenance activities [37].
- A study reported that in about 12% of major aircraft accidents, inspection and maintenance are the important factors [38,39].

1.3 Terms and Definitions

This section presents some useful terms and definitions directly or indirectly related to safety and human error in engineering systems [3,4–6,40–46].

- **Safety:** This is conservation of human life and the prevention of damage to items as per mission-specified requirements.
- **Human error:** This is the failure to perform a stated task (or the performance of a forbidden action) that could result in disruption of scheduled operations or damage to property and equipment.

- **Hazard:** This is the source of energy and the behavioral and physiological factors which, when uncontrolled, lead to harmful occurrences.
- **Human performance:** This is a measure of actions and failures under specified conditions.
- **Unsafe act:** This is an act that is not safe for an employee/individual.
- **Human factors:** This is a body of scientific facts concerning the characteristics of humans. The term includes all types of biomedical and psychosocial considerations. It also includes, but is no way restricted to, personnel selection, training principles and applications in the area of human engineering, aids for task performance, life support, and evaluation of human performance.
- **Safeguard:** This is a barrier guard, device, or procedure developed to protect humans.
- **Human performance reliability:** This is the probability that a human will satisfy all specified human functions subject to stated conditions.
- **Unsafe condition:** This is any condition, under the right set of conditions, that will lead to an accident.
- **Unsafe behavior:** This is the manner in which a person carries out actions that are considered unsafe to himself/herself or other people.
- **Accident:** This is an event that involves damage to a certain system that suddenly disrupts the current or potential system output.
- **Safety process:** This is a series of procedures followed to enable all safety requirements of an item/system to be identified and satisfied.
- **Human error consequence:** This is an undesired consequence of human failure.
- **Risk:** This is the probable occurrence rate of a hazardous condition and the degree of harm severity.
- **Continuous task:** This is a job/task that involves some kind of tracking activity (e.g., monitoring a changing condition).
- **Downtime:** This is the time during which the item/system is not in a condition to carry out its stated mission.
- **Reliability:** This is the probability that an item/system will carry out its stated function satisfactorily for the desired period when used according to the specified conditions.
- **Safety plan:** This is the implementation details of how the safety requirements of the project will be achieved.
- **Redundancy:** This is the existence of more than one means to perform a specified function.

- **Safety assessment:** This is quantitative/qualitative determination of safety.
- **Mission time:** This is that element of uptime needed to perform a stated mission profile.
- **Maintainability:** This is the probability that a failed item/system will be restored to satisfactorily operational condition.
- **Failure:** This is the inability of an item/system to carry out its specified function.

1.4 Useful Sources for Obtaining Information on Safety and Human Error in Engineering Systems

This section lists books, journals, conference proceedings, technical reports, data sources, and organizations considered useful to obtain information directly or indirectly concerned with safety and human error in engineering systems.

1.4.1 Books

- Stephans, R. A., Talso, W. W., Eds., *System Safety Analysis Handbook*, System Safety Society, Irvine, CA, 1993.
- Spellman, F. R., Whiting, N. E., *Safety Engineering: Principles and Practice*, Government Institutes, Rockville, MD, 1999.
- Dhillon, B. S., *Engineering Safety: Fundamentals, Techniques, and Applications*, World Scientific Publishing, River Edge, NJ, 2003.
- Leveson, N. G., *Safeware: System Safety and Computers*, Addison-Wesley, Reading, MA, 1995.
- Hammer, W., Price, D., *Occupational Safety Management and Engineering*, Prentice Hall, Upper Saddle River, NJ, 2001.
- Handley, W., *Industrial Safety Handbook*, McGraw Hill Book Company, London, 1969.
- Heinrich, H. W., *Industrial Accident Prevention*, 3rd ed., McGraw Hill Book Company, New York, 1950.
- Kandel, A., Avni, E., Eds., *Engineering Risk and Hazard Assessment*, CRC Press, Boca Raton, FL, 1988.
- Strauch, B., *Investigating Human Error: Incidents, Accidents, and Complex Systems*, Ashgate Publishing, Aldershot, U.K., 2002.
- Hall, S., *Railway Accidents*, Ian Allan Publishing, Shepperton, U.K., 1997.

- Dhillon, B. S., *Human Reliability, Error, and Human Factors in Engineering Maintenance*, CRC Press, Boca Raton, FL, 2009.
- Karwowski, W., Marras, W. S., *The Occupational Ergonomics Handbook*, CRC Press, Boca Raton, FL, 1999.
- Dhillon, B. S., *Human Reliability: With Human Factors*, Pergamon Press, New York, 1986.
- Sanders, M. S., McCormick, E. J., *Human Factors in Engineering and Design*, McGraw Hill Book Company, New York, 1993.
- Dhillon, B. S., *Human Reliability and Error in Transportation Systems*, Springer Inc., London, 2007.

1.4.2 Journals

- *Journal of Safety Research*
- *Safety Science*
- *Nuclear Safety*
- *Professional Safety*
- *International Journal of Reliability, Quality, and Safety Engineering*
- *Safety and Health*
- *Hazard Prevention*
- *Accident Analysis and Prevention*
- *Product Safety News*
- *Reliability Engineering and System Safety*
- *Safety Management Journal*
- *Human Factors in Aerospace and Safety*
- *Transportation Research Record*
- *Ergonomics*
- *Applied Ergonomics*
- *Human Factors*
- *International Journal of Industrial Ergonomics*
- *Human Factors and Ergonomics in Manufacturing*
- *Modern Railways*
- *International Journal of Man-Machine Studies*
- *Journal of Occupational Accidents*
- *Journal of Quality in Maintenance Engineering*
- *Risk Analysis*
- *Asia Pacific Air Safety*
- *National Safety News*