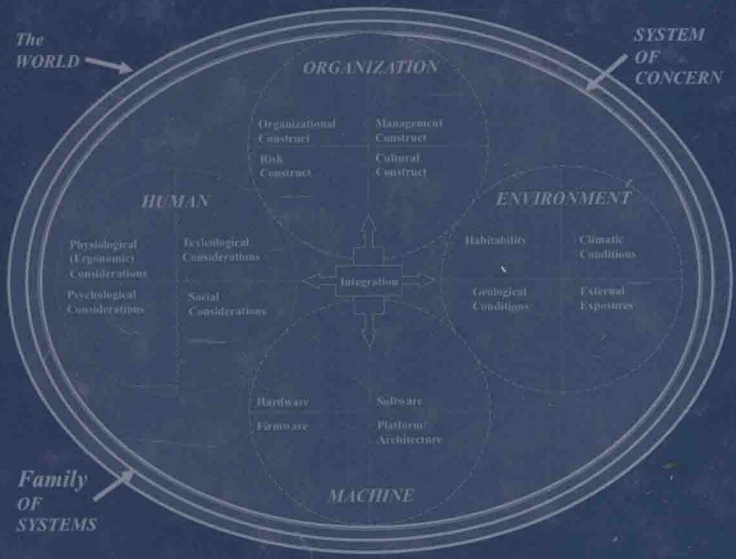
Safety Analyses of Complex Systems

Considerations of Software, Firmware, Hardware, Human, and the Environment



Michael Allocco

WILEY

Safety Analyses of Complex Systems

Considerations of Software, Firmware, Hardware, Human, and the Environment

Michael Allocco

WILEY

A JOHN WILEY & SONS, INC., PUBLICATION

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

Library of Congress Cataloging-in-Publication Data:

Allocco, Michael.
Safety analyses of complex systems : considerations of software, firmware, hardware, human, and the environment / Michael Allocco.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-58770-6 (cloth)
1. System safety. 2. Industrial safety. I. Title.
TA169.7.A45 2010
620.8′6—dc22

2009038791

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Safety Analyses of Complex Systems

Contents Overview

This book is comprised of four parts inventively: A, B, C, and D. Risk identification is addressed in Part A. Risk elimination and control is the subject of Part B. Managing safety-related risks is discussed in Part C. Part D addresses methods and techniques. The content is further decomposed into specific chapters:

Preface

Needless to say, analyzing large complex systems is not an easy task. In analyzing such complex systems semantics remain important, as well as the hazard control hierarchy. There is always the potential for analysis lock and wheel spinning; and simply looking at "things" like failures, or functions, or hardware does not assure an inclusive effort. Unfortunately, there is no easy cookbook—Remember that unbiased experience and knowledge will always make the difference.

It appears at times that highly motivated safety professionals almost communicate by safety telepathy between each other and there is usually some common general agreement on the safety axioms. It can be very disheartening to safety professionals when there are cursory analyses and deviations from safety principles and practices. Many safety people "hold paramount the safety and health of people, the protection of the environment and the protection of property"[1]; some safety people have put their livelihoods, careers, promotions, and jobs on the line because they could not deviate from the principles and practices. This book has been written for them, and dedicated to, passionate, and highly motivated safety professionals, (past and present): safety managers, safety technologists, industrial hygienists, health physicists, system safety engineers, safety engineers, safety designers, safety inspectors, safety educators and trainers, product safety professionals, compliance engineers, requirements engineers, forensics engineers and investigators, safety writers, editors, authors, fleet safety managers, process safety engineers, safety reviewers, safety statisticians, health professionals, toxicologists, human factors engineers, security professionals, firearms, weapons, and monition experts, safety board members, nuclear safety engineers and operators, hospital safety managers, operators of safety-related systems, transportation safety professionals, construction and facility safety professionals, environmental engineers, medical equipment designers, medical professionals, liability prevention, causality and property engineers, safety consultants, advisors and analysts, loss control engineers, emergency response professionals, certification engineers, and aviation safety personnel.

The world is becoming more and more complex and integrated by large systems, systems of systems, and families of systems. It becomes a challenge to understand system, systemic, and synergistic risks. Consequently there is a need for more inclusive, holistic, and integrated hazard analyses and risk assessment processes. This book discusses safety analyses of large complex systems, which are comprised of software,

[1]This is the first standard in the Code of Ethics and Professional Conduct, Board of Certified Safety Professionals, approved October 2002.

firmware, hardware, the human, and the environment. The system safety methods and techniques discussed can be applied to identify, eliminate, or control system risks.

From a system safety view, the devil is in the details and cursory high-level hazard analyses will not support the complex systems in use and in development. There are life-cycle risks to address as well as the accident life cycle to consider. There is also a need for cost-effective allocation of resources in order to conduct more inclusive, holistic, and integrated hazard analyses and risk assessments. It is hoped that the ideas, concepts, methods, techniques, processes, and approaches discussed are helpful and will enable more inclusive, holistic, and integrated hazard analyses and risk assessments.

The author wants to thank Mr. Andrew Allocco, Technical Writing Consultant, for his expertise during proofing, commenting on, and indexing of the manuscript, and Ms. Christine Punzo, Senior Production Editor and staff at Wiley for production editing.

Contents