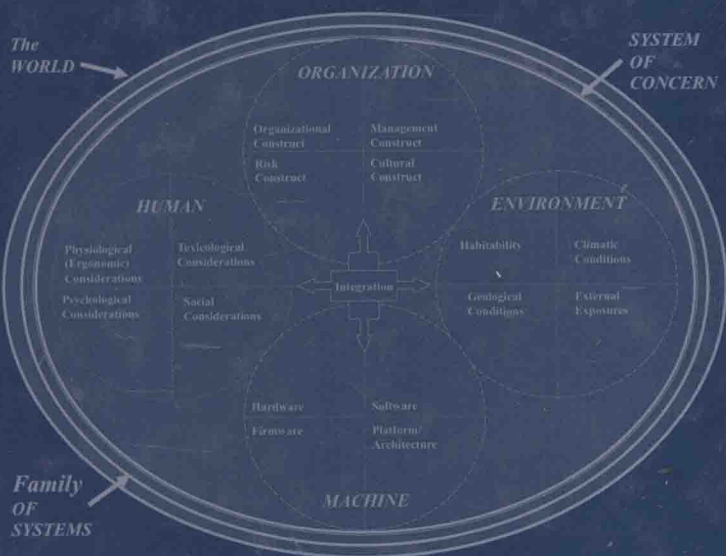


Safety Analyses of Complex Systems

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



Michael Allocco

Safety Analyses of Complex Systems

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

Michael Allocco



 **WILEY**

A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2010 by John Wiley & Sons, Inc. All rights reserved

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

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic format. For more information about Wiley products, visit our web site at www.wiley.com.

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

Part A Risk Identification

Chapter 1: Understanding Accidents and System, Synergistic, and Systemic Risks

Chapter 2: System Safety Analysis and Inclusive Approaches

Chapter 3: Evaluating Safety and Consideration of System Risk

Chapter 4: Scenario-Driven Hazard Analysis

Chapter 5: Artificial Intelligent Systems, Expert Systems, Automated Safety Approaches, and Applied Terms

Part B Risk Elimination and Control

Chapter 6: Eliminating and Controlling Risks

Chapter 7: Hazard Control: Methods, Techniques, and Applications, Terms A Through I

Chapter 8: Hazard Control: Methods, Techniques, and Applications, Terms J Through R

Chapter 9: Hazard Control: Methods, Techniques, and Applications, Terms S Through Z

Chapter 10: Safety Monitoring: Overview of Design Considerations

Part C Managing Safety-Related Risks

Chapter 11: Key Concepts and Observations Associated with a Safety Management System

Chapter 12: Safety Communication

Chapter 13: System Safety, Safety Engineering, and Safety Management Terms and Definitions

Chapter 14: Making Safety-Related Decisions

Chapter 15: Synopsis Review of Techniques Applicable to System Safety

Part D Methods and Techniques

Chapter 16: Use and Application of Generic Analysis Template

Chapter 17: Human Error: Source of Safety Problem

Chapter 18: Integration Efforts Related to Hazard Analyses

Chapter 19: Hazard Analyses Primer

Appendix A: GAT Short Form

Further Readings

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 munition 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,

¹This 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

Part A Risk Identification

1. Understanding Accidents and System, Synergistic, and Systemic Risks **3**

Hazard Analysis: Hypothesizing Accidents	3
Preventable Accidents	4
System Accidents	4
Initiators or Triggers Within Adverse Flow	4
System, Synergistic, and Systemic Risks	5
Accidents, Intentional Acts, and Prevention of Harm	6
Understanding Past Accidents and Current and Future Risks	6
Accident/Incident Investigation and Hazard Analysis	7
Management Oversight and Risk Tree	7
Project Evaluation Tree	7
Project Evaluation Tree Procedure	7
Root-Cause Analysis	8
Sequential Timed Events Plotting	9
Accident Perceptions: Adverse Process	9
Forensic Engineering: Accident Reconstruction and Liability	11
Forensic Analyses	12
Expert Witness: System Safety Engineer, Safety Professional, and Analyst	12
Credentials for Experts	13
Conducting Accident/Incident Investigations	13
Safety Monitoring	13
Safety-Related Forensic Investigations	13
Extensive Analyses and System Perspective	13
Conducting Investigations and Contingency Response	14

Crime Scene Processing, Forensic Evaluations, and Investigative Techniques 14

Sources of Information on Accident/Incident Investigation and Forensics 17

- National Academy of Forensic Engineers (NAFE®) 17
- National Safety Council (NSC) 17
- International Society of Air Safety Investigators (ISASI) 17
- Accreditation Commission for Traffic Accident Reconstruction (ACTAR) 18
- Canadian Association of Technical Accident Investigators and Reconstructionists (CATAIR) 19
- National Association of Traffic Accident Reconstructionists and Investigators (NATARI) 19
- Society of Accident Reconstructionists (SOAR) 19
- National Transportation Safety Board (NTSB) 20
- National Highway Traffic Safety Administration (NHTSA) 20
- National Center for Statistics and Analysis (NCSA) 21
- National Institute of Standards and Technology (NIST) 21
- International Association of Arson Investigators (IAAI) 21
- Chemical Safety Board (CSB) 21
- U.S. Department of Energy Accident Investigation Program 22
- U.S. Department of Labor, OSHA 23

Questions and Topics for Further Discussion 23

References 24

2. System Safety Analysis and Inclusive Approaches 25

Inclusive Approach 25

Existing Inclusive Approaches 26

Human Action or Inaction 26

Life-Cycle Perspective: Actions and Inactions 26

Integration Tool 27

System Engineering Format 27

Designing Functional Domains 27

- Subfunctions and Functional Considerations 28
- Mutually Exclusive Functions 28

Life-Cycle Phases 28

Function/Life-Cycle Arrays 29

Breadth and Depth of Analysis 29

Models Used for Safety 29

Entity Element Model 31

Vertical (Y) Axis in Array 33

Horizontal (X) Axis in Array 33

Hazard Recognition and Hazard Control Adequacy 33

Example Entities Requiring Inclusive Analyses 33

- Complex Structural Fabrication 47
- Complex Manual Tasks Required to Assemble Weapon System 49

Automated Process with Extensive Automation and Mechanical Operations	49
Laboratory Operation with Hazardous Materials and Toxic Chemicals	49
Construction Project with Specially Designed Tunnel-Boring Machine	50
Portable Medical Monitoring Device for Emergency Medical Applications	51
Questions and Topics for Further Discussion	51
References	52

3. Evaluating Safety and Consideration of System Risk **53**

Being Safe	53
Risk Perception	53
Benefits in Applying System Safety	54
Considering Risk	58
Potential Accidents	58
System Specialists	59
System Safety Engineering	60
Considering Systems	60
System Perception	61
Hazards, Risks, and Potential Accidents	61
Latent Hazards	62
Hazard Identification	62
Hazard Analysis	62
System States	63
Hazard Analysis Process	63
Total Risk Mitigation	64
Safety Verification	64
Hazard Mitigation	65
System Safety Analysis	66
Hazard Analysis Process	66
Organizing Hazard Analysis	72
Risk Assessment	72
Operational Risk Management	73
Risk-Based Decisions	73
Developing Risk Criteria	73
Refining Risk Criteria	74
Operational Risks	75
System Accident Life Cycle	75
Questions and Topics for Further Discussion	76
References	76

4. Scenario-Driven Hazard Analysis **77**

Detailed Analysis	77
Potential System Accidents (Scenarios)	77

x Contents

Detailed or Cursory Approaches	78
Real or Potential Accidents	78
Decisions and Risk	79
System Perspective	79
Behavior Affecting Analysis	79
Open-Minded Safety Integration	80
Inclusive Analysis	80
Safety Management	80
Example Application of Scenario-Driven Hazard Analysis	80
System Description	81
Example Scenario Themes	86
Modeling Scenarios	92
Comprehensive Picture of Risk	92
Models to Enhance Training and Contingency Planning	92
Digraph Depiction of Scenarios	93
Developing Scenarios and Risk Mitigation	94
Questions and Topics for Further Discussion	95
Reference	96
Additional Readings	96

5. Artificial Intelligent Systems, Expert Systems, Automated Safety Approaches, and Applied Terms **99**

Safety Analysis Approaches, Biases, and Observations	99
Decentralization of Analytical Safety Efforts	100
Applying Expert Systems in System Safety Analysis	101
Semiautomated FMEA Approach	102
Intelligent Systems and Process Safety Analyses	103
Early Use of Automated Analyses Tools with Diagraph Analysis	104
Dependable Computer Systems	104
Simulation and Model-Based Design	105
Concepts Applicable to Automation and System Safety	105
Software Safety	105
Terms and Definitions Applicable to Automation and System Safety	106
Questions and Topics for Further Discussion	126
References	126

Part B Risk Elimination and Control

6. Eliminating and Controlling Risks **131**

Imperfect World	131
Hazard Control Plan	132

Multilevel Hazard Controls	132
Accident Scenario	133
Inductive and Deductive Hazard Controls	133
Redundant Hazard Controls	133
Controlling Poor Decisions in Accident Mechanism	135
Degree of Control: Considering Excessive Complexity	136
Barrier Analysis	137
Hazard Control Effectiveness Analysis	140
Questions and Topics for Further Discussion	144
References	145

7. Hazard Control: Methods, Techniques, and Applications, Terms A Through I

147

Positive Actions	147
Synonyms for Risk Mitigation	147
Limitation on Discussion	148
Iterative Definitions	148
Hazard Control Discussions	148
Abnormal Energy Control	148
Accreditation	148
Anti-Slip/Skid Surfaces	148
Architecture Selection	149
Assessing Needs	149
Audit	149
Audit Trail	149
Authenticate	150
Backout and Recovery	150
Barrier	150
Baseline	150
Behavioral Science	150
Behavior Sampling	151
Biomedical Hazard Controls	151
Blowout/Relief Devices	151
Built-in Testing	152
Burn-in Testing	152
Cautions and Warnings	152
Capability	153
Certification	153
Certification Authority	153
Checklists	153
Coding Error Prevention	154
Color Coding	154
Communication Process	154
Communication for Safety	155
Compartmentalization	155
Configuration Engineering	155

Configuration Control	155
Configuration Item	156
Configuration Management	156
Cross-Check	156
Cyber Security Controls	156
Damage Containment and Control	156
Dead-Man Control/Switch	157
Debugging	157
Deluge Systems/Automatic Sprinklers	157
Dependability	157
Derating	157
Earthquake-Resistant Construction	158
Electromagnetic Environmental Effects Controls	158
Energy Release Controls	158
Engineering Analyses	159
Emulator	159
Environmental Engineering Controls	159
Ergonomic Controls	159
Error Prevention Controls	159
Escape and Survival Controls	160
Evacuation Controls	160
Explosion Containment Controls	160
Explosion Proof	160
Fail-Operational	161
Fail-Safe	161
Fail-Soft	161
Failure Minimization	161
Fire Load Limiting	161
Fire-Related Tests	161
Firewalls	162
Flammable/Combustible Liquid/Gas Use and Storage	162
Flood Control	162
Formal Verification	163
Formal Qualification	163
Formal Qualification Review	163
Fundamental (Core) Topics	163
Ground Fault Circuit Interruption	163
Grounding and Bonding	164
Habitable Environmental Controls	165
Hardware Controls	165
Hazardous Waste Controls	165
Hazard Tracking and Risk Resolution	166
Human Factors Engineering	167
Human Reliability Controls	167
Independent Verification and Validation	167
Inductive Analysis	167
Information Security Controls	167
Initialization, Timing, Sequencing, and Status Checks	169
Inspection	170

Instructions	170
Interlocks	171
Interrupts	171
Intrinsically Safe Designs	171
Isolation	172
Reference	172

8. Hazard Control: Methods, Techniques, and Applications, Terms J Through R

173

Illumination	173
Judgment (Rule of Judgment in Engineering)	174
Key People and Intellectual Assist Protection	174
Learning Objectives	175
Lightning Protection Systems	175
Load Securing	176
Load Shedding	176
Lockins	176
Lockouts	177
Lockout/Tagout Systems	177
Logic, Structure, Unique Codes	177
Loss Containment	177
Loss Control	178
Machine Guarding	178
Maintainability	178
Memory, Storage, and Data Transfer	178
Methodology	178
Mode Control	179
Monitoring and Detection	179
Nonprogrammable System	179
N-Version Software	179
Objective Evidence	179
Operator Notification, Human Response, and Monitoring	179
Operator Responses and Limitations	181
Optimum Safety	181
Personal Protective Equipment	181
Physical Barriers	182
Physical Security Controls	182
Practice	183
Preventing, Precluding, and Disallowing Actions	183
Process	183
Process and Flow Controls	183
Product Liability Defense	184
Process Safety Management	184
Product Service History	184
Qualification Process	185
Quality Assurance Controls	185
Quality Audit	185

Quality Evaluation	185
Quantitative Assessment	185
Reaction Time	185
Reasonableness Checks	186
Relief Systems/Pressure Control	186
Redundancy	187
Reliability	187
Requirements	187
Requirements Specification	187
Risk Management Techniques	187
Risk Assessment	188
Risk Control	188
Risk Analysis	188

References	188
------------	-----

9. Hazard Control: Methods, Techniques, and Applications, Terms S Through Z

Safe Haven	189
Safe Operating Procedures	189
Safety Communication Protocols	190
Safety Factor	190
Safety Mindset	191
Safety Programs/Safety Management	191
Scientific Method	191
Screening	191
Search, Rescue, and Recovery	191
Separation of Commands, Signals, Functions, and Operations	192
Shutdown, Recovery, and Safing	192
Signage	193
Signal Filtering	193
Signature Analysis	193
Simulation and Modeling	194
Software Reliability	194
Spill Containment	194
Standardization	195
System Approach	195
System Effectiveness	195
Systemized Safety Training	195
System Safety	196
System Safety Analysis	196
System Safety Training	197
Testing	197
Test Procedure	197
Traceability	197
Trade-off Study	198
Training Needs Analysis	198
Two-Person Control	199

Universal Applications	199
Validation	199
Valuable Data and Information: Papers, Records, and Trade Secrets Protection	199
Verification	200
Voting	200
Watchdog Timer	200
Zero Energy State	200
Questions and Topics for Further Discussion	200
References	201
Additional Readings	201

10. Safety Monitoring: Overview of Design Considerations **203**

Hierarchy of Hazard Control	203
Complexity of Problem	205
Complex Analyses	205
Extensive Software Systems	206
Legacy Systems, Reusable Software, COTS, and NDI	206
Complex Interfaces and Interactions	206
System Health Monitoring	207
Automated, Semiautomated, and Manual Safety Monitoring	207
Two-Person Monitor	207
Human in the Loop	207
Manual Monitoring	208
Contingency Response	208
Recommended Attributes of Automated or Semiautomated Safety Monitor	209
Example Detailed Requirements for Safety Monitors	210
Independent Safety-Monitoring Capability	210
Online Fault Diagnoses, Control, and Correction Capability	210
Proactive Risk Mitigation Capabilities	210
System Safety Data Analysis and Recording Capability	211
System Safety Verification and Validation	211
Contingency Response Capability	211
Independent Safety Monitoring	212
Online Fault Diagnosis, Control, and Correction	213
Proactive Risk Mitigation	214
System Safety Data Analysis and Recording	215
System Safety Validation and Verification	217
Contingency Response	219
Enhanced Risk Management	220
Host Internal Integration	220
ASM/Host External Integration	221
Facility Monitoring	222
Monitoring Documentation and Incident Analysis	223