DECISION-MAKING IN HIGH RISK ORGANIZATIONS UNDER STRESS CONDITIONS

ANTHONY J. SPURGIN AND DAVID W. STUPPLES

CRC Press
Taylor & Francis Group

DECISION-MAKING IN HIGH RISK ORGANIZATIONS UNDER STRESS CONDITIONS

ANTHONY J. SPURGIN AND DAVID W. STUPPLES

CRC Press
Taylor & Francis Group

DECISION-MAKING IN
HIGH RISK ORGANIZATIONS
UNDER STRESS CONDITIONS

DECISION-MAKING IN HIGH RISK ORGANIZATIONS UNDER STRESS CONDITIONS

ANTHONY J. SPURGIN AND DAVID W. STUPPLES

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

Printed on acid-free paper
Version Date: 20160317

International Standard Book Number-13: 978-1-4987-2122-6 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Spurgin, Anthony J., author. | Stupples, David W., author.
Title: Decision-making in high risk organizations under stress conditions /
Anthony J. Spurgin and David W. Stupples.
Description: 1 Edition. | Boca Raton : Taylor & Francis Group, 2016. |
Includes bibliographical references and index.
Identifiers: LCCN 2016000967 | ISBN 9781498721226 (alk. paper)
Subjects: LCSH: Decision making. | Job stress. | Management.
Classification: LCC HD30.23 .S7217 2016 | DDC 658.4/03--dc23
LC record available at http://lccn.loc.gov/2016000967

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

No Man Is an Island

No man is an island entire of itself; every man
is a piece of the continent, a part of the main;
if a clod be washed away by the sea, Europe
is the less, as well as if a promontory were, as
well as any manner of thy friends or of thine
own were; any man's death diminishes me,
because I am involved in mankind.
And therefore never send to know for whom
the bell tolls; it tolls for thee.

MEDITATION XVII
Devotions upon Emergent Occasions
John Donne 1573-1631

Contents

Preface
Acknowledgments
Authors

Chapter 1 Introduction

1.1 Purpose of the Book
1.2 Potential Use of the Book
1.3 Philosophy of the Authors

Chapter 2 Background

2.1 Introduction
2.2 Applications of Technology
2.2.1 Submarines
2.2.2 Aircraft Development
2.2.3 Computers
2.2.4 Instruments
2.3 Comments

Chapter 3 Cybernetic Organizational Model

3.1 Overview
3.2 Controller Design and Operation
3.3 Controller Response
3.4 VSM System
3.5 Use of Feedback in VSM
3.6 Complexity of Operations
3.7 Enhanced VSM Representation
3.8 VSM Application to Aircraft Traffic Control Study
3.9 ATC in Saudi Air Space
3.10 Analysis of the ATM Operation
3.11 Human Reliability Assessment
3.12 Linking VSM and CAHR
3.13 Comments
3.14 Summary

Chapter 4 Ashby's Law of Requisite Variety and Its Application

4.1 Introduction
4.2 General Approach to Control of Systems
4.3 Impact of Ashby's Law
4.4 Examples: Application of Ashby's Law

4.4.1 Fermi's Chicago Pile (CP1) Nuclear Experiment and Xenon
4.4.2 Effect of Management Decisions on the Fukushima Accident Progression
4.4.3 Failure of San Onofre NPP Steam Generators
4.5 Methods to Enhance the Probability of Good Decision-Making
4.6 Conclusions

Chapter 5 Probability Risk Assessment

5.1 Introduction to PRA
5.2 PRA Structure
5.3 Applications of PRA
5.4 Summary

Chapter 6 Rasmussen's Human Behavior Groups

6.1 Introduction to Skill-, Rule-, and Knowledge-Based Behavior
6.2 Application of Skill, Rule, Knowledge Behavior Rules
6.3 Comments

Chapter 7 Case Studies of Accidents for Different Industries

7.1 Scope: Analysis of Accidents
7.2 Accidents: Analysis Approach
7.3 List of Accidents
7.4 Nuclear Industry Accidents
7.4.1 Three Mile Island Unit #2
7.4.1.1 Accident Analysis
7.4.1.2 Organizational Analysis
7.4.1.3 Review of a VSM Model following TMI Organizational Analysis
7.4.2 Chernobyl
7.4.2.1 Description of Plant
7.4.2.2 Accident Description
7.4.2.3 Accident and Organizational Analysis
7.4.2.4 Comments on Chernobyl Organization
7.4.3 Fukushima Daiichi Accident
7.4.3.1 TEPCO and Fukushima Plant Organizations
7.4.3.2 Comments on the Preaccident Status
7.4.3.3 Accident Description
7.4.3.4 TEPCO Daiichi Organization—Prior to Accident
7.4.3.5 Reorganized Daiichi during Response to Emergency
7.5 Chemical Industries
7.5.1 Union Carbide Sevin (Pesticide) Plant, Bhopal, India, 1984
7.5.1.1 Introduction
7.5.1.2 Accident Analysis
7.5.1.3 Organizational Analysis
7.6 Oil and Gas Industries

7.6.1 *Deepwater* Horizon/Macondo Blowout Gulf of Mexico Oil Accident
7.6.1.1 Introduction
7.6.1.2 Accident Description
7.6.1.3 Accident Analysis
7.6.1.4 Organizational Analysis
7.6.1.5 Conclusions
7.6.1.6 Organization (VSM) Comments
7.6.1.7 Postscript on the Macondo Well Accident
7.7 Railways
7.7.1 Introduction
7.7.1.1 Kings Cross Underground Fire, November 18, 1987
7.7.1.2 Organization Analysis
7.7.1.3 Comments on Railway Accidents
7.8 NASA and Air Transport
7.8.1 NASA *Challenger* Accident, January 28, 1986
7.8.1.1 Background
7.8.1.2 Description of the Shuttle
7.8.1.3 Analysis
7.8.1.4 Description of Accident
7.8.1.5 Accident Analysis
7.8.1.6 Comments
7.8.2 Tenerife, Canary Islands Runway Accident, March 1977
7.8.2.1 Background
7.8.2.2 Accident Location
7.8.2.3 Accident: Sequence of Events
7.8.2.4 Analysis
7.8.2.5 Comments
7.9 Ancillary Safety-Related Incidents
7.9.1 NPP Containment Sump Blockage
7.9.2 Hungarian VVER Fuel Cleaning Accident
7.9.3 San Onofre NPP: Replacement Steam Generators
7.9.4 Northeast Utilities: Impact of Management Change

Chapter 8 Lessons Learned from a Series of Accidents

8.1 Introduction
8.2 Listing of the Lessons Learned for Each Accident
8.2.1 Three Mile Island Unit #2 Accident
8.2.2 Chernobyl Accident
8.2.3 Fukushima Accident
8.2.4 Bhopal Accident
8.2.5 BP Oil Refinery Accident
8.2.6 *Deepwater* Horizon/Macondo Oil Release Accident
8.2.7 Railways Accidents, Including Subsurface Railways
8.2.8 NASA *Challenger* Accident

8.2.9 Tenerife Accident
8.2.10 NPP Containment Sump Blockage
8.2.11 Fuel Cleaning Accident
8.2.12 Replacement of Steam Generators
8.2.13 Impact of Management, NU Operations
8.3 Summary

Chapter 9 Role of Regulation in Industrial Operations

9.1 Introduction
9.2 Regulation Process
9.3 Lessons from Review of NRC Reports
9.3.1 Comment on Report
9.4 Comments

Chapter 10 Integration of Tools Related to Decision-Making

10.1 Introduction
10.2 Integration and Roles of Each Element
10.2.1 Beer's Cybernetic Model
10.2.2 Ashby's Law of Requisite Variety
10.2.3 Probabilistic Risk Assessment Studies
10.2.4 Rasmussen's Human Behavior Types
10.2.5 Case Studies of Accident for Different Industries
10.2.6 Training Methods and Role of Advisors
10.2.6.1 Use of Advisors
10.2.7 Simulation of Processes and Its Value
10.2.8 Summary
10.2.8.1 Organizational Dynamic Model
10.2.8.2 Ashby's Law
10.2.8.3 Probabilistic Risk Assessment
10.2.8.4 Rasmussen's Human Behavioral Models
10.2.8.5 Accident Case Studies
10.2.8.6 Training Methods
10.2.8.7 Simulation Processes

Chapter 11 Use of Simulation for Different Operations

11.1 Introduction
11.2 Simulators
11.3 Simulations
11.4 Future Uses: Decision-Making
11.5 Summary

Chapter 12 Training Approaches for Management

12.1 Introduction
12.2 Education

12.3 Technical Tools for Managers
12.4 Conclusions

Chapter 13 Investment in Safety

13.1 Introduction
13.2 Managing for Shareholder Value
13.3 Brief Overview of the Principles of MSV
13.4 Using the *J*-Value to Estimate the Level of Investment Needed for Safety
13.4.1 Formulation of the *J*-Value
13.4.2 Limiting Risk Multiplier
13.4.3 Application of the *J*-Value
13.4.3.1 *J*-Value Analysis
13.5 Conclusion

Chapter 14 Conclusions and Comments

14.1 Introduction
14.2 Analytical Elements
14.3 Conclusion

Appendix: Admiral Rickover's Management Principles

References

Index

Preface

We have been interested in the occurrence of accidents and the relationships of organizational operations to the accidents. Potentially a lot more can be done to reduce the number and severity of accidents. In this, we have been confirmed in the study of ranges of accidents that have occurred in different industries and countries. Our studies in this field are reflected in this book.

The world is strongly affected by accidents—from local incidents to more global accidents that lead to the deaths of thousands of people and economic stresses in impacted countries The accidents range from a single death because of a traffic accident to a whole country affected by the arrival of a tsunami that destroys houses, kills hundreds of people, and floods the countryside with salt water that restricts the capability of the land to produce food for the population, possibly leading to hunger and malnourishment for years.

History tells us that every country is affected by accidents, and it appears that we cannot escape from being burdened by these events occurring and affecting us, individually, with pain and financial hardship.

We have been involved in the study of organizations and the impact of accidents on organizations. The idea of an accident being a random event over which we have no control and are in no way capable of preventing is an undesirable one. Closer examination of accidents reveals that if different decisions were made, better studies carried out, and the attitude of key persons were open to think more clearly about the likely consequence of actions, then the probability of an accident occurring could be heavily reduced.

The managers of more complex systems are required to be better prepared than for simple systems. From our background in the study of systems and related accidents, we have become more aware that the frequency of accidents in all kinds of situations can be reduced. It may not be totally possible to eliminate all accidents, because one lacks the ability to control everyone and everything. However, one can develop methods and techniques to enable persons directing and carrying out actions to minimize the potential for inadvertent decisions and actions being taken that lead to accidents.

This philosophy flies in the face of the “normal” approach to accidents (Perrow, 1999). Perrow’s model seems very much influenced by the Three Mile Island accident sequence. His point was that as people make mistakes, big accidents have small beginnings and failures are those of organizations. The main idea is that failures are built into society’s complex and tightly coupled systems, and as such accidents are unavoidable and cannot be designed around. We believe that organizations can be helped to reduce the probability of accidents and we lay out the processes here to accomplish this.

Our reanalysis constructs a different view of an accident (see Chapter 7). Our studies of a variety of accidents indicate that there are key events in most accident sequences where if the key decisions are approached differently, it would be very likely that the accident would not occur. In the field of accident analyses, there are parallel situations in which one decision path leads to failure and another path leads to success. This shows that it is not inevitable that a single failure will lead to an accident. The awareness of the decision-maker of an undesirable situation can be increased by being subject to better background training. This training should make a difference and lead to a reduced probability of a situation escalating to a damaging accident. It is better to avoid an accident than try to recover from the effects of an accident progression. The progression of an accident can tend to obscure the root causes of the accident and make it much more difficult for the organization to recover.

Some accidents occur because people, carrying out simple tasks, fail to realize that the repeated operations cannot be continued forever without a change occurring (linear extrapolations have limits). A case that comes to mind is the South Wales Aberfan coal tip accident in which 116 children and 28 adults died at a school on October 21, 1966. Here the local coal mines continuously tipped waste from the coal diggings onto a pile that grew ever closer to the school. No one gave thought to the fact the pile of waste could slide. However, the coincidence of the buildup and rain ended with a slide/avalanche that covered the school and led to the deaths! Thought about the configuration should have caused someone to be concerned about what might happen and its consequence. The failure of someone considering the characteristics of the pile was one of the accidents, along with others, that drove us to try to improve the decision-making process. The inquiry (October 1966 onward) found that the coal board was at fault: “The coal board was at fault due to ignorance, ineptitude, and a failure of communication.” This finding indicates to us that it is possible to move away from the coal board-type of organization to one that is more responsive to potential accidents!

Another example of simple failures to think about situations and consequences is the emergency evacuation of very ill patients from hospitals in the Boston area following the *Sandy* storm surge of October 2012. The evacuation was needed due to the poor location of standby emergency power in the basements of the hospitals without adequate protection from floodwaters. Clearly, the standby power source should have been protected from the floodwater by either placing the power source higher in the building or having adequate flood damage control. The press expresses great concern that nuclear power plants in Japan are not protected from tsunamis, but we forget to take simple actions in our cities to save people here!

Clearly, we need to think about the subject of weather protection as whole, including flooding. Tsunamis are known throughout the world and people need some protection from these events. Fairly regularly, large numbers of people lose their lives from tsunamis. A typical example is the Aceh tsunami of December 26, 2004, in which some 170,000 Indonesian people were killed or were missing (see Aceh Tsunami, 2004). This does not cover people who died in India and elsewhere, because of the Indian earthquake-induced tsunamis.

We are encouraged that the authorities in England decided to protect London and surrounding areas from the combination of North Sea storm surges coupled with high tide with the Thames Barrier (see Thames Barrier, 1982). It was estimated that the design basis of the barrier should exceed the highest floodwater height that could occur once in a thousand years. It is interesting that the English authorities decided to act to build such a barrier. The feature of the barrier was that it could allow ships to pass normally and could be raised in response to predicted weather conditions, like those imagined occurring once in a thousand years. Raising the barrier has occurred several times since it was built to combat significant but smaller water levels.

The probability of the Fukushima tsunami was about the same number, and Tokyo Electric Power Company, Incorporated (TEPCO) and the Japanese government decided not to act! The failure to act led to 20,000 deaths and 140,000 houses damaged/destroyed. Seems that it was not only a failure by TEPCO, but also of the Japanese and local governments to act. The Fukushima nuclear plant's losses affected TEPCO's viability with the loss of power generation and the future costs to protect the public from possible releases from the damaged fuel, including plant clean-up. This accident gives all management concerns about the cost of decisions that can lead to destruction of the company. It should be pointed out that further to the north, at a place called Onagawa, both the surrounding people and the nuclear plant were protected by the actions of the power company vice president, Yanosuke Hirai.

These examples have brought us to a point where we want to help reduce the probability of these kinds of events. We believe that this can be achieved by approaching how management decision-making can be improved. Clearly, there seem to be some shortcomings in what is being done now. There does appear to be a defeatist attitude in thinking that accidents cannot be prevented, whereas one can appreciate that people with well-prepared and -trained minds can take actions to help mitigate the effects of an accident or even prevent its occurrence.

We see that to accomplish this objective, several techniques need to be brought together. Candidates for top management positions need to be educated in appropriate technologies. Their training needs to be one of continuing exposure to testing their decision-making skills. The training process that is proposed is based upon Adm. Rickover's principles, as are applied by the military, and applied to train naval submariners, marines, and others. In addition, two more tools are proposed to be included. Control systems should be changed to match variations in accidents by using an understanding of Ashby's law of requisite variety (more on this later). The other is training on the impact of human behavior on human limitations in responding to developing accidents. From his research a Danish researcher (Rasmussen) developed categories of behavior called skill-, rule-, and knowledge-based behavior. People respond differently to circumstances depending on their degree of preparedness to a situation, so if they are well practiced in the requirements of a given circumstance, they are said to be operating in a skilled-based mode and correspondingly their errors are likely to be small. The response of people to accidents therefore depends on their preparation to combat a given accident. This topic is discussed in later chapters of the book.

Early in our studies it was decided that a cybernetic model of organizations was needed so that one could develop a good understanding of how organizations react to accidents. The normal organizational chart does not supply this dynamic interrelationship. The normal organization chart is a linear arrangement of who answers to whom and who the chief executive officer (CEO) is or who is a controlroom operator, but this is not dynamic. What is needed is a different model of an organization, so Beer's model (Beer, 1975) was selected, since it gave these insights.

Analysis of various accidents can provide two contributions to the enhancement of decision-making in high-risk organizations. By studying the analysis of accidents, it can be shown that the accidents that have occurred in different industries have many of the same sources and are not so different from one industry to another. The other contribution is to make the point to management that it is not above making a poor choice of action that can lead to accidents and end in the demise of the organization. Management needs to be concerned with not only making a profit, but also reducing the probability of thoughtless actions leading to an accident that badly affects the public and the workers. As can be seen in Chapter 7, accidents can lead to destroying the countryside, death of large numbers of individuals, the loss of jobs, and the loss of viability of the organization.

With the application of appropriate techniques and with training, management can be encouraged to pay more attention to the details and enhance both the safety and economics of organizations. Admiral Hyman G. Rickover showed that with the right approach, this could happen in the operation of the US nuclear Navy in terms of safety and effectiveness.

Acknowledgments

Tony thanks his wife, Margaret Jill Spurgin, for her support during the time that he was working on this book. Without her support, it is unlikely that it would have seen the light of day.

David thanks his wife, Magda, his son, Oliver, his daughter, Claudia, and all his friends and colleagues who, over the years, have put up with him burying himself in the world of research.

Both authors thank Dr. Natalia Danilova for her insights into the application of Ashby's law of requisite variety to fields beyond the narrow interpretation, to the world of decision-making in high-risk organizations. Her thesis is "Integration of Search Theories and Evidential Analysis to Web-Wide Discovery of Information for Decision Support," and her PhD was granted by City University, London.

Thanks also to Dr. Saleh H. Al-Ghamdi, for allowing the authors to use some material from his PhD thesis on safety, controller reliability, and organizational structures in airspace control in Saudi Arabia commercial airspace. His PhD was granted by City University, London. His thesis is "Human Performance in Air Traffic Control Systems and Its Impact on Safety."

Many thanks to Cindy Carelli, acquisitions editor, for her help and advice.

Many thanks to Heidi Spurgin for the design of the cover.

The contributions that Admiral Hyman G. Rickover (1900-1986) made to the field of safety by his work on submarines based on nuclear reactor power are remembered. A key element in the safety of the nuclear submarines is the skill of the crews, based on his training and selection methods.

Thanks to Lt. Col. Dom D. Ford, for insights into US Marine Corps training methods.

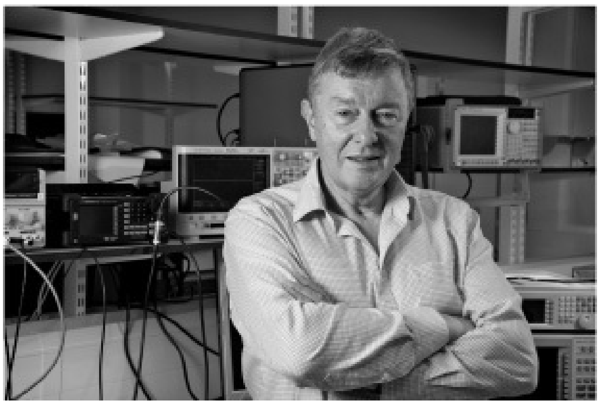
Authors

Anthony J. Spurgin, PhD, is an engineer whose interest is in the improvement of safety and economics of various industries by the enhancement of managerial decisionmaking. He is also involved in human reliability analytical techniques for estimating probabilities of human action under accident conditions. He was educated in England and earned a BSc in aeronautical engineering. Much later he earned a PhD in engineering and mathematics from City University, London. After attending the university, Dr. Spurgin was a graduate apprentice at an aircraft factory and afterward, as an engineer, performed aeroelastic calculations for a number of aircraft, including a supersonic plane.

Subsequently, he moved to the nuclear energy field and was engaged in design station control systems for gas-cooled reactors (Magnox and AGRs) and developed digital simulations of stations to help in the design process. For a period, he was with the UK Electric Generating Board (CEGB) and was involved in the study of the dynamics of gas-fired and coal plants and their control systems.

Dr. Spurgin moved to the United States to work further in this area and was the principal designer of the control and protections systems for 3 Loop PWRs and later for high-temperature gas-cooled reactors. He was involved in the design of various test rigs covering steam generator behavior and loss of flow (LOCA) experiments.

Later, he became involved in human reliability assessment. He has been involved in developing the methods and techniques to enhance the safety of nuclear power plants (NPPs). He has been supporting efforts in this direction in various countries and aided the efforts of IAEA in enhancing NPP safety. He has published the book *Human Reliability Assessment: Theory and Practice* (2009, Boca Raton, FL: CRC Press).



David W. Stupples, PhD, focuses on research and development of radar systems and electronic warfare. For a number of years, he undertook research in this area at the Royal Signals and Radar Establishment (RSRE) at Malvern in the United Kingdom, followed by surveillance and intelligence systems research for the UK government. He then spent three years developing surveillance systems and satellites for Hughes Aircraft Corporation in the United States. In his early career, Dr. Stupples was employed in radar and electronic warfare by the Royal Air Force. Later, he was a senior partner with PA Consulting Group, where he was responsible for the company's consultancy work in surveillance technology and in risk analysis of safety-critical infrastructure.

1 Introduction

1.1 PURPOSE OF THE BOOK

The purpose of the book is to discuss the topic of decision-making as it applies to high-risk industries and how one can apply the lessons from accident analysis. This work is an attempt to improve the whole attitude of the business community as to what it really takes to select and train decision-makers in the control of these types of industries. It should be noted that the approach taken here can have applications to other fields of management endeavor. Even the word *accident* has the context of something unavoidable and uncontrollable and that despite actions taken by people, the inevitable will occur and we have no way to prevent it. This, of course, is not correct. Random events may occur; our position is that one should be in a position to minimize the effect of the incident. Here the words of the Boy Scouts are appropriate: “Be prepared.” If an organization is prepared, then the consequences of an event can be reduced.

The authors have been employed in various industries and involved in studies of how decisions made during designing, locating, building, and operating nuclear power plant (NPP) units can affect subsequent operations. All of the decisions related to these actions can have an impact on the safety and economics of high-risk industries. High-risk industries are those industries where accidents can have a significant financial impact on the organization and affect the safety and health of the nearby population.

The authors have extensive experience in the fields of safety, design, and economics of plant operations of high-risk industries. The purpose of the book is to draw upon that experience, as well as insights derived from the study of a series of accidents in different industries, from nuclear to railways. A key element in our studies of accidents was the evaluation of the responses of organizations, both at the manager and operator levels—before, during, and after an accident. It was these observations that helped us develop our approach to the integration of various techniques, such as Rasmussen’s skill, rule, and knowledge-based behavior (Rasmussen, 1997) and Ashby’s law of requisite variety (Ashby, 1956) along with Beer’s work (Beer, 1981) on cybernetic modeling of organizations.

From our studies, it became obvious that the top managers have been very much caught up in the economics of day-to-day running of the organizations and often have been trained to deal with these kinds of problems, such as MAs in the art of management. This approach was very much the standard for managing ordinary operations—involving capital cost and expenditures, profit and loss, and direction of staff to help ensure their productivity. However, it seemed that the bigger potential losses resulting from random accidents are not seriously embedded in the training of management personnel. It could be that many managers did not really understand the