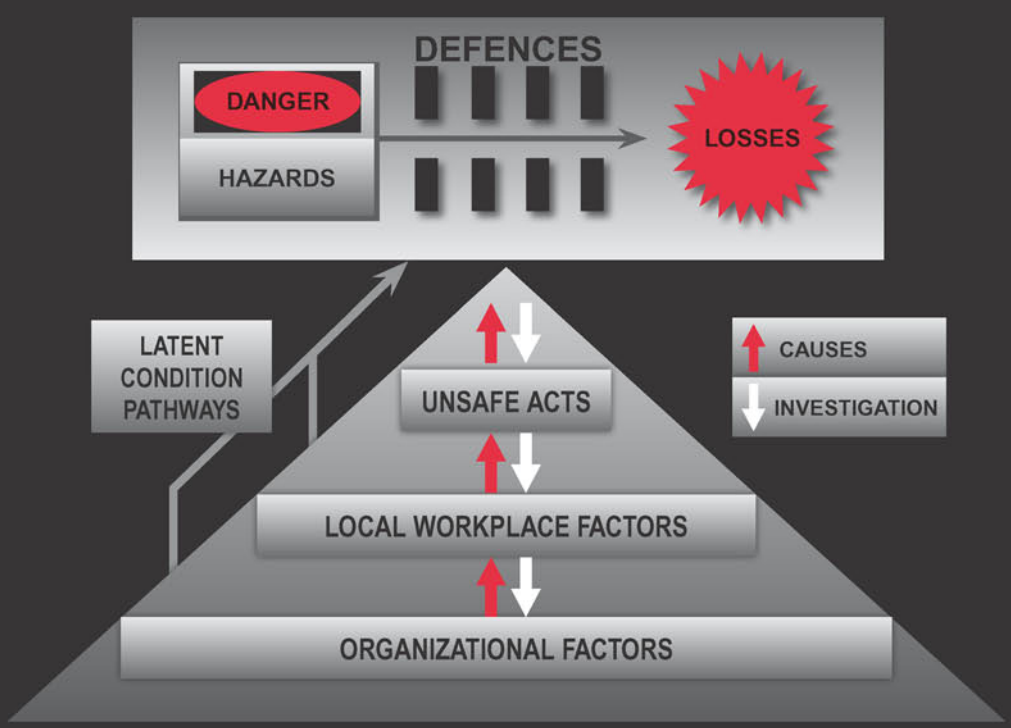
An **Ashgate** Book

ROUTLEDGE

Managing the Risks of Organizational Accidents

JAMES REASON



MANAGING THE RISKS OF ORGANIZATIONAL ACCIDENTS

This book is dedicated to two pilots and two surgeons who have greatly enhanced the safety of their respective domains:

Captain Gordon Vette

Captain Daniel Maurino

Dr Lucian Leape

Mr Marc de Leval

MANAGING THE RISKS OF ORGANIZATIONAL ACCIDENTS

JAMES REASON

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 1997 by Ashgate Publishing

Published 2016 by Taylor & Francis
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
711 Third Avenue, New York, NY 10017, USA

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
Reason, James
Managing the risks of organizational accidents
1.Industrial accidents 2. Hazardous substances – Safety measures 3. Industrial safety – Management
I. Title
363.1´1´06

Library of Congress Cataloging-in-Publication Data
Reason, J. T.
Managing the risks of organizational accidents / James Reason.
p. cm.
ISBN 13: 978 1 84014 105 4 (Pbk) ISBN 13: 978 1 84014 104 7 (Hbk)
1. Industrial accidents. 2. Risk assessment. I. Title.
T54.R4 1997
658.3´82—dc21 97–24648
CIP

ISBN 13: 978 1 84014 104 7 (Hbk)
ISBN 13: 978 1 84014 105 4 (Pbk)

Published by
Ashgate Publishing Limited
Gower House
Croft Road
Aldershot
Hants GU11 3HR
England

Ashgate Publishing Company
131 Main Street
Burlington, VT 05401-5600 USA

Ashgate website:http://www.ashgate.com

Reprinted 1998, 1999, 2000 (twice), 2001, 2002, 2003, 2004, 2005, 2006, 2008

British Library Cataloguing in Publication Data
Reason, James
Managing the risks of organizational accidents
1.Industrial accidents 2. Hazardous substances – Safety measures 3. Industrial safety – Management
I. Title
363.1′1′06

Library of Congress Cataloging-in-Publication Data
Reason, J. T.
Managing the risks of organizational accidents / James Reason.
p. cm.
ISBN 1 84014 105 0 (pbk) 1 84014 104 2 (hbk)
1. Industrial accidents. 2. Risk assessment. I. Title.
T54.R4 1997
658.3′82—dc21 97–24648
CIP

ISBN 13: 978 1 84014 104 7 (Hbk)
ISBN 13: 978 1 84014 105 4 (Pbk)

Typeset by Manton Typesetters, 5–7 Eastfield Road, Louth, Lincolnshire, UK.
Printed in Great Britain by MPG Books Ltd, Bodmin, Cornwall

Contents

List of Figures

This page intentionally left blank

List of Tables

This page intentionally left blank

List of Abbreviations

ACAA	Australian Civil Aviation Authority
ALARP	as low as reasonably practicable
AMMS	Aurora Mishap Management System
AOC	Air Operators Certificate
ASRS	Aviation Safety Report System (NASA)
BASI	Bureau of Air Safety Investigation (Australia)
BASIS	British Airways Safety Information System
BB & Co.	Barings Brothers & Co.
BFS	Barings Futures (Singapore) Pte Limited
BSL	Barings Securities Limited
CEO	chief executive officer
CIMAH	Control of Industrial Major Hazards
COSHH	Control of Substances Hazardous to Health
CRIEPI	Central Research Institute for the Electrical Power Industry
CRM	crew (cockpit) resource management
EC	European Commission
EM	error management
EPC	error-producing condition
FAA	Federal Aviation Administration (US)
FDR	flight data recorder
FEA	failure mode and effects analysis
FMS	flight management system
FSA	formal safety assessment
GFT	general failure type
HAZAN	hazards operability study
HAZOP	hazard and operability study
HEA	human error analysis
HEART	Human Error Assessment and Reduction Technique
HEMP	Hazardous Effects Management Process
HRA	human reliability analysis
HRO	high-reliability organization
HSC	Health and Safety Commission
HSE	Health and Safety Executive
IAEA	International Safety Advisory Group

IDA	Influence Diagram Approach
IFSD	inflight engine shutdown
INPO	Institute of Nuclear Power Operations (US)
JAL	Japan Airlines
KB	knowledge-based
LII	lost-time injury
MEDA	Maintenance Error Decision Aid
MESH	Managing Engineering Safety Health
MSA	Marine Safety Agency
NASA	National Aeronautics and Space Administration
NCO	non-commissioned officer
NRC	Nuclear Regulatory Commission
NTSB	National Transport Safety Board
NUREG	Report series issued by Nuclear Regulatory Commission
NWA	Northwest Airlines
O & M	organizational and managerial
PIF	performance-influencing factor
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PWR	pressurised water reactor
RAMS	reliability and maintainability study
RB	rule-based
RPF	railway problem factor
RBMK	A Soviet-built nuclear power plant
SB	skill-based
SESMA	Special Event Search and Master Analysis
SIMEX	Singapore Monetary Exchange
SOP	standard operating procedure
SPC	Statistical Process Control
SR & QA	Safety Reliability and Quality Assurance Program
TBR	to-be-remembered
TMI	Three Mile Island
TQM	Total Quality Management
VPC	violation-producing factor

Preface

This book is not meant for an academic readership, although I hope that academics and students might read it. It is aimed at 'real people' and especially those whose daily business is to think about, and manage or regulate, the risks of hazardous technologies. My imagined reader is someone with a technical background rather than one in human factors. To this end, I have tried—not always successfully—to keep the writing as jargon-free as possible.

The book is not targeted at any one domain. Rather, it tries to identify general principles and tools that are applicable to all organizations facing dangers of one sort or another. This includes banks and insurance companies just as much as nuclear power plants, oil exploration and production, chemical process plants and air, sea and rail transport. The more one moves towards the upper reaches of such systems, the more similar their organizational processes—and weaknesses—become.

In a book of this type the 'big bang' examples inevitably tend to predominate, but, although I have used case study examples to illustrate points, this is not intended to be yet another catalogue of accident case studies. My emphasis is upon principles and practicalities—the two must work hand-in-hand. But the real test is whether or not these ideas can eventually be translated into some improvement in the resistance of complex, well defended systems to rare, but usually catastrophic, 'organizational accidents'.

James Reason

This page intentionally left blank

1 Hazards, Defences and Losses

Individual and Organizational Accidents

There are two kinds of accidents: those that happen to individuals and those that happen to organizations. Individual accidents are by far the larger in number, but they are not the main concern of this book. Our focus will be upon *organizational accidents.* These are the comparatively rare, but often catastrophic, events that occur within complex modern technologies such as nuclear power plants, commercial aviation, the petrochemical industry, chemical process plants, marine and rail transport, banks and stadiums.

Organizational accidents have multiple causes involving many people operating at different levels of their respective companies. By contrast, individual accidents are ones in which a specific person or group is often both the agent and the victim of the accident.[1] The consequences to the people concerned may be great, but their spread is limited. Organizational accidents, on the other hand, can have devastating effects on uninvolved populations, assets and the environment. Whereas the nature (though not necessarily the frequency) of individual accidents has remained relatively unchanged over the years, organizational accidents are a product of recent times or, more specifically, a product of technological innovations which have radically altered the relationship between systems and their human elements.

Finding the Right Level of Explanation

Organizational accidents are difficult events to understand and control. They occur very rarely and are hard to predict or foresee. To the people on the spot, they happen 'out of the blue'. Difficult though they may be to model, we have to struggle to find some way of understanding the development of organizational accidents if we are

to achieve any further gains in limiting their occurrence. Quite apart from the human costs in deaths and injuries, there are very few commercial organizations that can survive the fallout from a major accident of this kind.

It has been said that nothing in logic is accidental. But does the reverse hold true? Is there nothing logical about accidents? Are there no underlying principles of accident causation? This book is written in the belief that such principles do exist. Organizational accidents may be truly accidental in the way in which the various contributing factors combine to cause the bad outcome, but there is nothing accidental about the existence of these precursors, nor in the conditions that created them. The difficulty, however, lies in finding the appropriate level of description.

If we consider only their surface details—the kind of information that is reported in press accounts—organizational accidents are dauntingly diverse. They involve a variety of systems in widely differing locations. Each accident has its own very individual pattern of cause and effect. Apart from the fact that they are all bad news, this level of description seems to defy generalization and implies that we clearly need to investigate more deeply into some common underlying structure and process to find the right level of explanation.

At the other extreme, it can be claimed that all organizational accidents involve the unplanned release of destructive agencies such as mass, energy, chemicals and the like. This is indeed a generalization, but it does not take us very far. However, like gunners, we have bracketed the target. The appropriate level of understanding has to lie somewhere between the highly idiosyncratic superficial details and the vagueness of this overly broad definition.

The aim is to find ideas that could be applied equally well to a wide range of low-risk, high-hazard domains. The basic thesis of this book is that the framework illustrated in Figure 1.1 will serve this purpose well. Figure 1.1 shows the relationship between the three elements that make up the title of this chapter: hazards, defences and losses. All organizational accidents entail the breaching of the barriers and safeguards that separate damaging and injurious hazards from vulnerable people or assets—collectively termed 'losses'. This is in sharp contrast to individual accidents where such defences are often either inadequate or lacking.

Figure 1.1 directs our attention to the central question in all accident investigation: By what means are the defences breached? Three sets of factors are likely to be implicated—human, technical and organizational—and all three will be governed by two processes common to all technological organizations: production and protection.

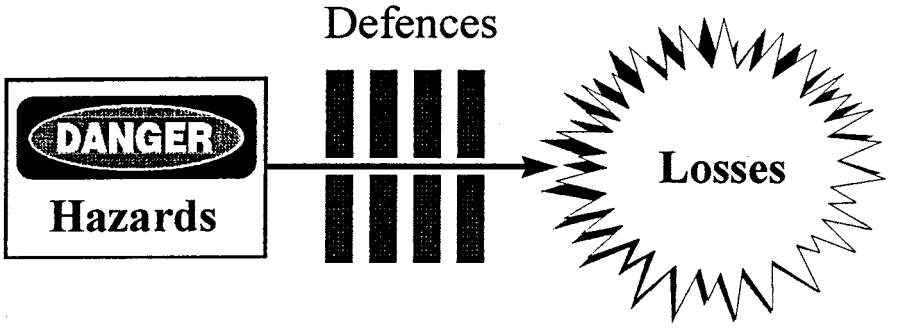


Figure 1.1 The relationship between hazards, defences and losses

Production and Protection: Two Universals

All technological organizations produce something—manufactured goods, the transportation of people, financial or other services, the extraction of raw materials and the like. But, to the extent that productive operations expose people and assets to danger, all organizations (and the larger systems within which they are embedded) require various forms of protection to intervene between the local hazards and their possible victims and lost assets.

While the productive aspects of an organization are fairly well understood and their associated processes relatively transparent, the protective functions are both more varied and more subtle. Figure 1.2 introduces some of the issues involved in the complex relationship between production and protection. In an ideal world, the level of protection should match the hazards of the productive operations—the parity zone.[2] The more extensive the productive operations, the greater is the hazard exposure and so also is the need for corresponding protection. But different types of production—and hence different organizations—vary in the severity of their operational hazards. Thus, low-hazard ventures will require less protection per productive unit than will high-hazard ventures. In other words, the former can operate in the region below the parity zone, whereas the latter must operate above it.

This broad operating zone (the lightly shaded area in Figure 1.2) is bounded by two dangerous extremes. In the top left-hand corner lies the region in which the protection far exceeds the dangers posed by the productive hazards. Since protection consumes productive resources—such as people, money and materials—such grossly overprotected organizations would probably soon go out of business.

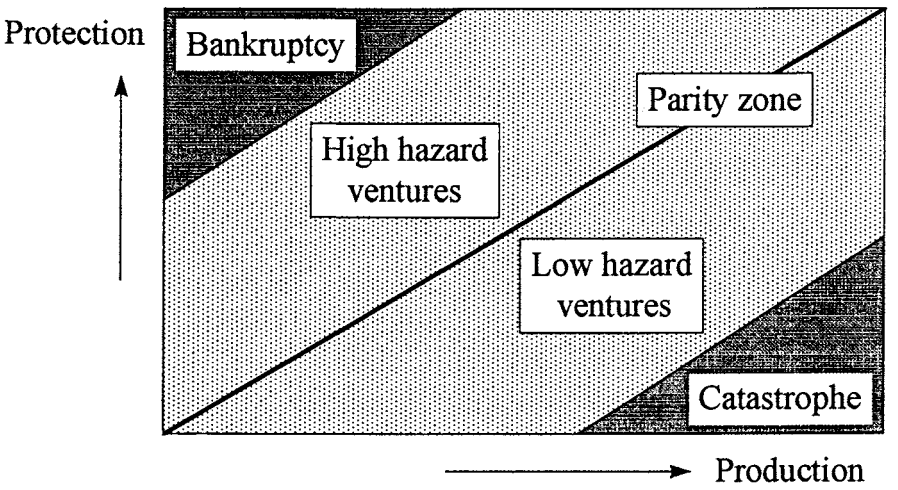


Figure 1.2 Outline of the relationship between production and protection

At the other extreme, in the bottom right-hand corner, the available protection falls far short of that needed for productive safety, and organizations operating in this zone face a very high risk of suffering a catastrophic accident (which probably also means going out of business). These obviously dangerous zones are generally avoided, if only because they are unacceptable to both the regulators and the shareholders. Our main concern is with how organizations navigate the space bounded by these two extremes.

Despite frequent protestations to the contrary, the partnership between production and protection is rarely equal, and one of these processes will predominate, depending on the local circumstances. Since production creates the resources that make protection possible, its needs will generally have priority throughout most of an organization's lifetime. This is partly because those who manage the organization possess productive rather than protective skills, and partly because the information relating to production is direct, continuous and readily understood. By contrast, successful protection is indicated by the absence of negative outcomes. The associated information is indirect and discontinuous. The measures involved are hard to interpret and often misleading. It is only after a bad accident or a frightening near-miss that protection comes—for a short period—uppermost in the minds of those who manage an organization.

All rational managers accept the need for some degree of protection. Many are committed to the view that production and protection

necessarily go hand-in-hand in the long term. It is in the short term that conflicts occur. Almost every day, line managers and supervisors have to choose whether or not to cut safety corners in order to meet deadlines or other operational demands. For the most part, such short-cuts bring no bad effects and so can become an habitual part of routine work practices. Unfortunately, this gradual reduction in the system's safety margins renders it increasingly vulnerable to particular combinations of accident-causing factors.

Figure 1.3—the main purpose of which is to introduce the two important features of organizational life described below—plots the unhappy progress of one hypothetical organization through the production–protection space. The history starts towards the bottom left-hand corner of the space where the organization begins production with a reasonable safety margin. (The organization's progress between events is indicated by the black dots.) As time passes, the safety margin is gradually diminished until a low-cost accident occurs. The event leads to an improvement in protection, but this is then traded off for productive advantage until another, more serious, accident occurs. Again, the level of protection is increased, but this is gradually eroded by an event-free period. The life history ends with a catastrophe.

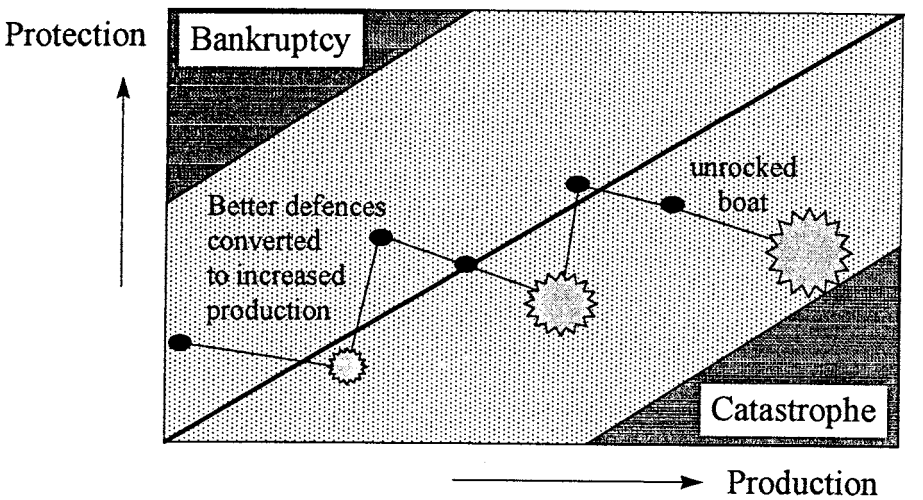


Figure 1.3 The lifespan of a hypothetical organization through the production–protection space

Trading off Added Protection for Improved Production

Improvements in protection are often put in place during the period immediately following a bad event. Although the aim is to avoid a repetition of an accident, it is soon appreciated that the improved defences confer productive advantages. Mine owners in the early nineteenth century, for example, quickly realized that the invention of the Davy lamp permitted coal to be extracted from areas previously considered too dangerous because of the presence of combustible gases. Ship owners soon discovered that marine radar allowed their merchant vessels to travel at greater speed through crowded or confined seaways. In short, protective gains are frequently converted into productive advantages, leaving the organization with the same inadequate protection that prevailed before the event or with something even worse. The incidence of mine explosions increased dramatically in the years following the introduction of the Davy lamp, and the history of marine accidents is littered with radar-assisted collisions—to name but two of the many examples of accidents brought about by sacrificing protective benefits for productive gains. This process has been termed 'risk compensation' or 'risk homeostasis'.[3]

The Dangers of the 'Unrocked Boat'[4]

There is plentiful evidence to show that a lengthy period without a serious accident can lead to the steady erosion of protection as productive demands gain the upper hand in this already unequal relationship. It is easy to forget to fear things that rarely happen, particularly in the face of productive imperatives such as growth, profit and market share. As a result, investment in more effective protection falls off and the care and maintenance necessary to preserve the integrity of existing defences declines. Furthermore, productive growth is regarded as commercially essential in most organizations. Simply increasing production without the corresponding provision of new or extended defences will also erode the available safety margins. The consequence of both processes—neglecting existing defences and failing to provide new ones—is a much increased risk of a catastrophic, and sometimes terminal, accident.

We will return to the interplay between production and protection later, but for now we need to focus on protection—the layers of defences, barriers and safeguards that are erected to withstand both natural and manmade hazards. The one sure fact about an accident is that the defences must have been breached or bypassed. Identifying how these breakdowns can occur is the first step in understanding the processes common to all organizational accidents.

Just as production can involve many different activities, so protection can be achieved in a variety of ways. In the remainder of this book, we will reserve the term 'protection' for the general goal of ensuring the safety of people and assets, and we will use the term 'defences' to refer to the various means by which this goal can be achieved. At this point it would be convenient to focus on the various ways by which defences may be described or classified.

The Nature and Variety of Defences

Defences can be categorized both according to the various functions they serve and by the ways in which these functions are achieved. Although defensive functions are universals, their modes of application will vary between organizations, depending on their operating hazards.

All defences are designed to serve one or more of the following functions:

- to create *understanding* and *awareness* of the local hazards
- to give clear *guidance* on how to operate safely
- to provide *alarms and warnings* when danger is imminent
- to *restore* the system to a safe state in an off-normal situation
- to *interpose* safety barriers between the hazards and the potential losses
- to *contain* and *eliminate* the hazards should they escape this barrier
- to provide the means of *escape* and *rescue* should hazard containment fail.

Implicit in the ordering of this list is the idea of 'defences-in-depth'—successive layers of protection, one behind the other, each guarding against the possible breakdown of the one in front. When understanding, awareness and procedural guidance fail to keep potential victims away from hazards, alarms and warnings alert them to the imminent danger and direct the system controllers (or engineered safety features) to restore the system to a safe state. Should this not be achieved, physical barriers stand between potential losses and the hazards. Other defences act to contain and eliminate the hazards. Should all of these prior defences fail, then escape and rescue measures are brought into play.

It is this multiplicity of overlapping and mutually supporting defences that makes complex technological systems, such as nuclear power plants and modern commercial aircraft, largely proof against single failures, either human or technical. The presence of sophisti-

cated defences-in-depth, more than any other factor, has changed the character of industrial accidents. In earlier technologies, there were—and to the extent that they continue to operate, still are—relatively large numbers of individual accidents. In modern technologies, such as nuclear power generation and air transportation, there are very few individual accidents. Their greatest danger comes from rare, but often disastrous, organizational accidents involving causal contributions from many different people distributed widely both throughout the system and over time.

The defensive functions outlined above are usually achieved through a mixture of 'hard' and 'soft' applications. 'Hard' defences include such technical devices as automated engineered safety features, physical barriers, alarms and annunciators, interlocks, keys, personal protective equipment, non-destructive testing, designed-in structural weaknesses (for example, fuse pins on aircraft engine pylons) and improved system design. 'Soft' defences, as the term implies, rely heavily upon a combination of paper and people: legislation, regulatory surveillance, rules and procedures, training, drills and briefings, administrative controls (for example, permit-to-work systems and shift handovers), licensing, certification, supervisory oversight and—most critically—front-line operators, particularly in highly automated control systems.

In earlier technologies, human activities were primarily productive: people made or did things that led directly to commercial profit. However, the widespread availability of cheap computing power has brought about a dramatic change in the nature of human involvement in modern technologies. These changes are seen most starkly in nuclear power plants and 'glass cockpit' commercial aircraft. Instead of being physically and directly involved in the business of production (and hence in immediate contact with the local hazards), power plant operators and pilots act as the planners, managers, maintainers and the supervisory controllers of largely automated systems.[5] A crucial part of this latter role involves the defensive function of restoring the system to a safe state in the event of an emergency.

Defences-in-depth are a mixed blessing. One of their more unfortunate consequences is that they make systems more complex, and hence more opaque, to the people who manage and operate them. Human controllers have, in many such systems, become increasingly remote, both physically and intellectually, from the productive systems which they nominally control. This allows the insidious build-up of latent conditions, to be discussed later.