SINTEF A17034 - Unrestricted

REPORT

Organisational Accidents and Resilient Organisations: Six Perspectives. Revision 2

Ragnar Rosness, Tor Olav Grøtan, Geir Guttormsen, Ivonne A Herrera, Trygve Steiro, Fred Størseth, Ranveig K Tinmannsvik, Irene Wærø

SINTEF Technology and Society
Safety Research

December 2010

SINTEF

SINTEF

SINTEF Technology and Society
Safety Research

P.O.Box: 4760 Sluppen
Address: NO-7465 Trondheim, NORWAY
Location: S P Andersens veg 5 NO-7031 Trondheim
Telephone: +47 73 59 03 00
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

Organisational Accidents and Resilient Organisations: Six Perspectives
Revision 2

AUTHOR(S)

Ragnar Rosness, Tor Olav Grøtan, Geir Guttormsen, Ivonne A. Herrera, Trygve Steiro, Fred Størseth, Ranveig K. Tinmannsvik, Irene Wærø

CLIENT(S)

The Petroleum Safety Authority Norway

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
SINTEF A17034	Unrestricted	Avrop nr: 6303-01-2009 – 706350 (AID)	
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Unrestricted	978-82-14-05056-1	60S027	141 pages
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
Kvalitetssikret- report Org Accidents ver 2.docx		Ragnar Rosness	Camilla K. Tveiten
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2010-12-15	Lars Bodsberg, Research Director	

ABSTRACT

Several major accidents are related to the interplay of organisational properties and technology. The aim of this report is to present a set of perspectives that can help us understand the organisational mechanisms related to major accidents. Six perspectives are discussed:

1. The energy and barrier perspective;
2. The theory of Normal Accidents;
3. The theory of High Reliability Organisations;
4. The information processing perspective;
5. A decision-making perspective;
6. The Resilience Engineering perspective.

The target groups of the report are researchers, students and advanced practitioners.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Organisation	Organisasjon
SELECTED BY AUTHOR	Accident	Ulykke
	Resilience	Robusthet
	Vulnerability	Sårbarhet

TABLE OF CONTENTS

Preface to Revision 1 ..... **9**

Preface to Revision 2 ..... **11**

1 Prelude: The Snorre A blow-out and the need for multiple perspectives on organisational accidents and resilient organisations **13**
1.1 The blow-out 13
1.2 The recovery 15
1.3 Learning from the Snorre A blow-out 15

2 Introduction **19**
2.1 Background 19
2.2 Definitions and delimitations 20
2.3 Structure of the report 21

3 Two cases for discussion: **23**
3.1 The train collision at Åsta 23
3.2 The Snorre A blow-out 25
3.2.1 The broader political, organisational and economical context of the Snorre A blow-out 25
3.2.2 The history of well P-31A 26
3.2.3 The planning of the slot recovery operation 27
3.2.4 The execution of the slot recovery operation and the loss of control 29
3.2.5 A second look at the recovery 30
3.2.6 The aftermath 31
3.2.7 Concluding remark on the Snorre A Blow-out 32

4 Uncontrolled transfer of energy as the target of hazard control: The energy and barrier perspective **35**
4.1 Energy transfer as the focus of accident research and prevention 35
4.2 What is a barrier? Barrier functions, barrier elements and barrier systems 36
4.3 Defence in depth and organisational accidents 37
4.4 Analytical risk control 39
4.5 The energy and barrier perspective and the Åsta accident 39
4.6 The energy and barrier perspective and the Snorre A blow-out 40
4.7 Strengths and limitations of the energy perspective 41
4.8 The Energy and Barrier perspective summarised 43
4.9 Key questions for the applicability of the energy-barrier perspective 44
4.10 References 44
4.11 New references 45

5 The challenge of interactive and tightly coupled technologies: Perrow's theory of Normal Accidents **47**
5.1 Component failure accidents versus system accidents 47
5.2 Complexity and coupling 48
5.3 Organising for coupling and complexity 48
5.4 Implications for risk reduction 49
5.5 A Normal Accident perspective on the Åsta accident 50

5.6 A Normal Accident perspective on the Snorre A blow-out 51
5.7 Strengths and limitations of Normal Accident theory 52
5.8 Further development of Normal Accident theory 53
5.9 The Normal Accident perspective – a summary 53
5.10 Key questions for the applicability of the Normal Accident perspective 54
5.11 References 54
5.12 New references 55

6 Organisational redundancy and spontaneous reconfiguration: The theory of High Reliability Organisations 57
6.1 "Working in practice but not in theory" 57
6.2 Organisational redundancy as a means to build fault tolerant organisations 57
6.3 Spontaneous reconfiguration of the organisation 59
6.4 Culture as a means to build organisations that are both centralised and decentralised 60
6.5 The notion of "mindfulness" 60
6.6 Implications for risk reduction 61
6.7 HRO theory and the Åsta accident 61
6.8 HRO theory and the Snorre A blow-out 62
6.9 Normal Accident theory versus High Reliability Organisations 63
6.10 Strengths and limitations of HRO theory 64
6.11 The HRO perspective – a summary 65
6.12 Key questions for the applicability of the HRO perspective 65
6.13 References 66
6.14 New references 66

7 Accidents as a breakdown in the flow of information: Turner's theory of Man-made Disasters 69
7.1 Notion of root causes and immediate causation 69
7.2 The main stages in the Man-made Disaster model 70
7.3 Cultures with requisite imagination 71
7.4 Emergency plans as fantasy documents 72
7.5 Risk control strategies 73
7.6 How can major accident risks be monitored? 73
7.7 Information processing related to the Åsta accident 74
7.8 The information perspective and the Snorre A blow-out 75
7.9 Strengths and limitations of the information perspective 75
7.10 The Information perspective – a summary 76
7.11 Key questions for the applicability of the Information perspective 76
7.12 References 77
7.13 New references 77

8 Risk handling in the face of conflicting objectives: Risk taking, adaptation and drift .. 79
8.1 Taking a risk or running a risk? 79
8.2 Migration of activities towards the boundary of acceptable performance 80
8.3 Distributed decision making 81
8.4 Levels of decision-making 83
8.5 The diversity of decision contexts and decision processes: A contingency model 84
8.6 Adherence to rules, culture and resources 87
8.7 The Challenger disaster and normalisation of deviance 88
8.8 Practical drift 89
8.9 Implications for risk control and risk reduction 90
8.10 Conflicting objectives and the Åsta accident 91
8.11 Conflicting objectives and the Snorre A blow-out 92

8.12 The Conflicting Objectives perspective – a summary 93
8.13 Key questions for the applicability of the Conflicting Objectives perspective 94
8.14 References 94
8.15 New references 95

9 The Resilience Engineering perspective 97
9.1 Resilience and Resilience Engineering 97
9.2 Comparing RE aspects with aspects borrowed from other perspectives 98
9.2.1 Intractability and interactive complexity 98
9.2.2 Functional resonance and combined complex interactions 98
9.2.3 ETTO – Efficiency-Thoroughness Trade-Off and handling conflicting goals 99
9.2.4 Barriers within RE and the other perspectives 99
9.3 Systemic proaction: an overarching paradigm of control 100
9.3.1 Underspecification and the variability that cannot be removed 100
9.3.2 Unexampled events and loss of control 100
9.3.3 Systemic proaction 101
9.4 Some key concepts of Resilience Engineering 102
9.4.1 Emergent phenomena (“prepare to be surprised”) 103
9.4.2 Proactive Safety Management Systems targeting the coping ability of the system 103
9.4.3 Addressing systemic dynamics and dynamism 104
9.4.4 Improvisation 105
9.4.5 Support and redundancy 105
9.5 Functional Resonance Analysis Method 105
9.6 The Snorre A blow-out from a resilience engineering perspective 107
9.7 The Resilience Engineering (RE) perspective – a summary with special emphasis on the relation to other perspectives 107
9.8 Key questions for the applicability of the Resilience Engineering perspective 109
9.9 References 109

10 Summary and comparison of the perspectives 113
10.1 Notions of immediate causes of accidents 113
10.2 Notions of “root causes” of accidents 113
10.3 Critical assumptions 117
10.4 The relationship between major and minor accidents: The popular version of the iceberg theory 118

11 From theory to practice: Implications for risk control and accident prevention 121
11.1 Monitoring the risk of organisational accidents 121
11.2 Risk reduction strategies 126
11.3 Learning from disasters and precursors 128
11.4 Resilience and change 130
11.5 Epilogue 132

12 References 133

TABLE OF FIGURES

Figure 1. Simplified outline of the gas blow-out at Snorre A. The arrows indicate the uncontrolled gas flow. 14
Figure 2. The situation immediately prior to the collision at Åsta. The northbound train had left from track 1 at Rudstad, forcing open the switch at the northern exit of the station. Not all signals are shown.....24
Figure 3. The energy and barrier model of accidents (adapted from Haddon, 1980). 35
Figure 4. Defence in depth. (Adapted from Reason, J.: Managing the Risks of Organizational Accidents. Aldershot: Ashgate, 1997, p. 12).....38
Figure 5. The two dimensions of organisational redundancy. 59
Figure 6. Main stages in the Man Made Disaster model of Turner (1978; Turner and Pidgeon (1997). 70
Figure 7. A typology of how organisations treat information. Adapted from Westrum (1993). 72
Figure 8. Under the pressure of conflicting objectives activities tend to migrate toward the boundary of acceptable performance (Adapted from Rasmussen, 1996).....81
Figure 9. Adaptation in a complex organisation, where several actors are migrating more or less independently within the space of acceptable performance. (Adapted from Rasmussen, 1994b).....82
Figure 10. The socio- technical system involved in risk management (Adapted from Rasmussen, 1997).....84
Figure 11. Two dimensions for characterising setting for safety related decision making, adapted from Rosness (2001). (IMO - The International Maritime Organisation; NPD - The Norwegian petroleum Directorate; CEO - Chief Executive Officer.).....85
Figure 12. Classes of decision processes. Adapted from Rosness (2001). 86
Figure 13. The four systems states involved in Practical Drift. Adapted from Snook (2000:186). 90
Figure 14. Resilience Engineering and its links to other perspectives.....103
Figure 15. The Iceberg theory. Adapted from Heinrich (1931), cited in Hale (2000). 118

Preface to Revision 1

This report gives an overview of theoretical perspectives on organisational accidents and resilient organisations. We hope that the overview will prove useful to researchers, students and advanced practitioners in search of a richer understanding of the mechanisms that make some organisations accident-prone, whereas other organisations experience remarkably few accidents.

In order to keep the task manageable with the available resources, we had to concentrate on theories related to major accidents. We hope it will be possible to extend the scope in a later version to cover more topics related to external threats and intentional damage. Even within this narrower scope, the overview is far from exhaustive.

This work was sponsored by The Research Council of Norway through the project *Risk and Uncertainty: management, understanding and adaptation*. More information on this project and other online publications can be found on our website www.risikoforsk.no. We want to thank Jan Hovden, Hilde K. Sæle, Terje Aven, Helene Blakstad and Camilla Knudsen Tveiten for constructive comments.

Trondheim, 2004-01-14

Ragnar Rosness

Preface to Revision 2

The second revision of this report was sponsored by the Petroleum Safety Authority, Norway (PSA). The main modifications are:

- A new first chapter has been added. Here where we argue for the need for several perspectives, taking the uncontrolled gas blow-out at the Snorre A platform on 28 November 2004 as a starting point.
- The Snorre A blow-out is also introduced as a main case in addition the Åsta train collision. The blow-out and its context are described in Chapter 3. We have also added new sections throughout the report where the Snorre A blow-out is discussed with reference to each perspective.
- The presentation of Turner's theory of Man-made Disaster in Chapter 7 has been expanded with an outline of the stages in his model.
- New sections on Vaughan's account of the Challenger disaster and Snook's theory of practical drift have been included in Chapter 8.
- A new chapter presenting Resilience Engineering as a sixth perspective has been added. This chapter mentions several recent contributions to the field.
- The summary tables in Chapters 10 and 11 have been expanded to include Resilience engineering as a sixth perspective.
- The discussion on the Iceberg Theory in Section 11.4 has been revised and the implications have been elaborated.
- An updated list of references has been added to each chapter. The second parts of these lists include recent references that were not included in the original report.
- The new references have also been included in the list of references at the end of the report.

It has been both inspiring and frustrating to revise this report. It has been inspiring because the research field covered by the report has seen an exciting development during recent years. The frustration arises from our recognition that we are not able to adequately reflect these developments within the boundaries given by the available resources and the format of the report. We also recognise that we are not yet able to give a pregnant, coherent and easily understandable account of Resilience Engineering.

Trondheim, 2010-11-09

Ragnar Rosness

1 Prelude: The Snorre A blow-out and the need for multiple perspectives on organisational accidents and resilient organisations

1.1 The blow-out

At 21:20 on 28 November 2004, personnel were sent to check the area outside Module F11 on the offshore production platform Snorre A because several gas alarms had gone off in this area.[1] They discovered that the sea was "boiling" with gas. Huge amounts of flammable hydrocarbon gas were emerging from somewhere below the sea surface.

A grossly simplified[2] outline of the situation is shown in Figure 1. Snorre A is a tension leg platform, i.e. a large floating structure of concrete and steel which is moored to the seabed with steel tethers in each corner attached concrete blocks on the seabed. Living quarters, production and drilling facilities are integrated on the same platform. Snorre A is situated in the Norwegian North Sea, at 300-350 meters water depth. There were 261 persons on the platform when the gas leakage was discovered.

The wells are drilled through slots in a template on the seabed below the platform. This template contains slots for up to 40 wells. Each well is connected to the platform with a vertical tube (riser). Below the seabed, each well is enclosed by a casing, i.e. a wide metal tube. At the bottom of the well, a perforated tail pipe allows hydrocarbon to enter the well from the reservoir. Alternatively, a well may be used to pump gas or liquid into the reservoir in order to increase the pressure and allow more hydrocarbons to be extracted from adjacent wells. Only one of the wells, P-31A, is shown in the figure.

The gas emerged from well P-31A. This well had been shut in after the casing had been damaged in December 2003. However, it had been decided to drill a sidetrack from the abandoned well, in order to recover and reuse this slot in the drilling template at the bed. During the execution of this slot recovery operation, the drilling crew lost control of the well. Gas under high pressure leaked out of the well approximately 1500 meters under the seafloor through a damaged part of the casing.

[1] This account is based on the investigation report issued by the Petroleum Safety Authority (Petroleumstilsynet, 2005), a report prepared for Statoil by Schiefloe et al. (2005) and an analysis by Ger Wackers (2006).

[2] A more detailed illustration can be found in Petroleumstilsynet (2005). The following are some of the simplifications: There is not one, but many wells with corresponding risers attached to the Snorre A platform. Only a part of well P-31A is vertical; the major part is oblique. The upper part of the well is enclosed by several layers of casing with different diameters. There are several control valves in the tail pipe, which allow different parts of the reservoir to be accessed for production of oil and gas or injection of gas or liquids into the reservoir. We have also omitted a section of 5 ½" production tubing and a 4"straddle, which had been dropped in the well. The figure is, of course, grossly out of proportion.

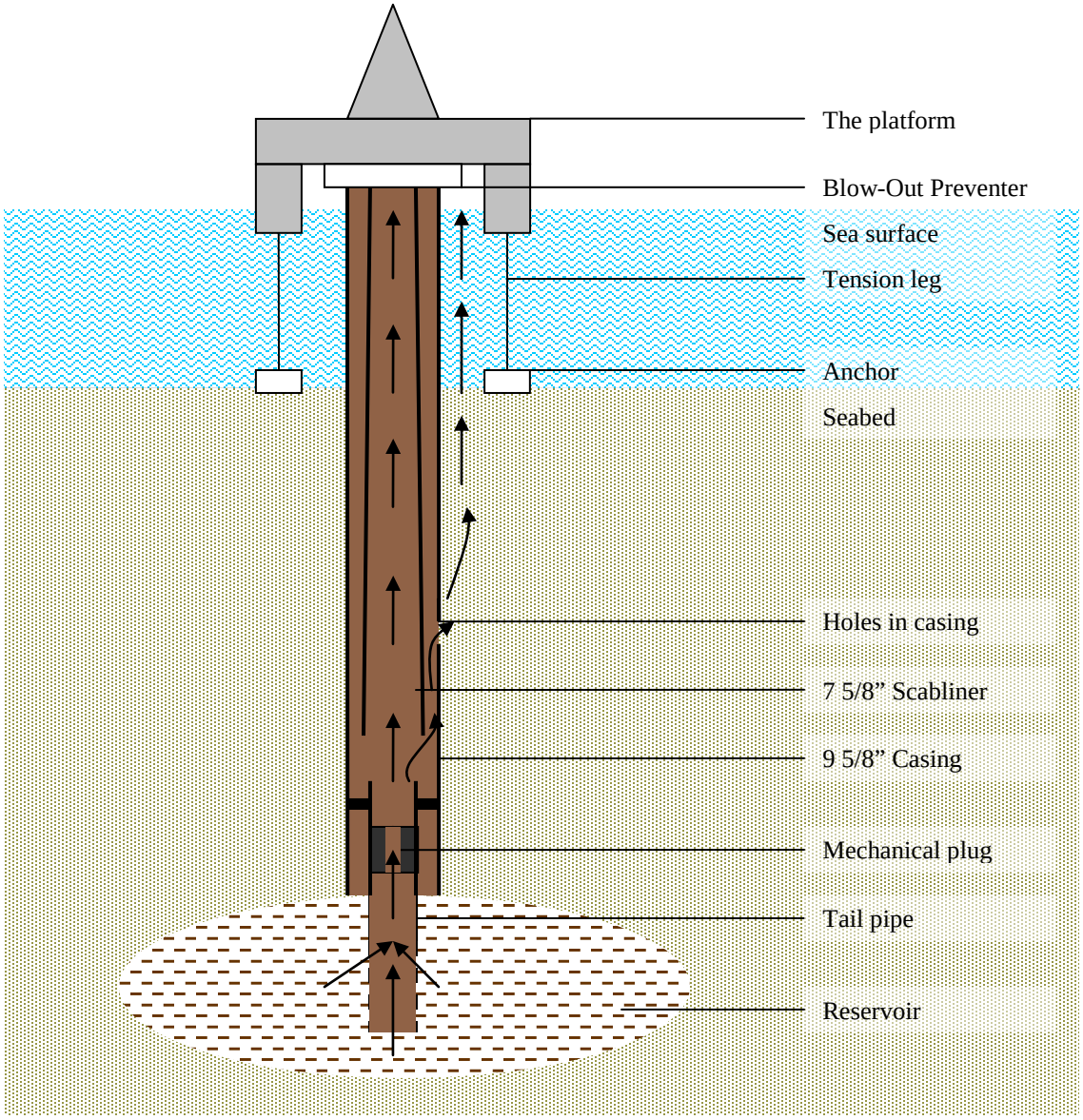

Figure 1. Simplified outline of the gas blow-out at Snorre A. The arrows indicate the uncontrolled gas flow.

The gas found its way through the seabed and emerged through craters below the platform. The two largest craters were later found to be 2.5 and 3 meters in diameter respectively. It was this blow-out that caused the sea to be "boiling" with gas. A parallel gas leak occurred through the Blow-out preventer (BOP). The BOP is a stack of devices designed to close the well if necessary during drilling and well servicing. It is located at the lowest deck on the platform. This leak was stopped by increasing the pressure in the hydraulic line to one of the valves in the BOP (the annulus safety valve).

The situation was critical. The gas might, if ignited, cause multiple fatalities, and loss of the platform. There was also a risk that the gas emerging from the sea-bottom might cause the steel tethers at one corner of the platform to become unfastened. This might cause the whole platform

to capsize. In the worst case, the capsized platform might damage the well template at the sea bottom and cause several parallel blowouts from the reservoir. Huge amounts of oil might then flow freely into the sea for several months. This scenario might result in extensive environmental damage, and might cause irreparable damage to the reputation of Statoil.

1.2 The recovery

In order to control the well, large amounts of heavy drilling mud with high viscosity needed to be injected into the well under high pressure.[3] The mud had to be heavy to act as a counterweight against the pressure in the reservoir. It needed to be so viscous (thick and sticky) that it would get stuck when it reached the perforations in the casing and start to solidify. This required large amounts of mud and sufficient pumping capacity to counteract the flow from the reservoir. The supplies of ordinary drilling mud turned out to be insufficient, and the ignition risk prevented vessels from approaching the platform with additional supplies. The main power supply on the platform had to be closed down to eliminate potential sources of ignition of the gas emerging from the seabed. This caused the capacity of the mud pumps to be insufficient. There were several other problems as well. There was not sufficient liquid nitrogen available to extinguish the flare, which formed another potential source of ignition. The cement pumps did not rely on main power, but they took in air from the underside of the platform, and might thus suck in gas. The equipment room lost ventilation and overpressure protection when the ventilation system stopped. Again, the ventilation system took in air from the underside of the platform. It was not possible inspect the well template and get an overview of what had happened by means of an ROV (small, unmanned submarine), because the accompanying vessel could not be allowed to get sufficiently close to platform due to the ignition risk.

In spite of the odds, the platform manager decided to try to control the well. Non-essential personnel were evacuated by helicopter. The crew prepared 160 m^3 of emergency drilling mud by mixing available water, barite and bentonite. They experimented with different compositions until they found one which was suitably heavy and viscous. The intakes for the cement pumps were modified to take air from the upper side of the platform, so that the pumps could be used later on if they were needed. The platform manager decided to restart the main power supply, based on the fact that no gas had been detected on the platform during the last hour. An experienced electrician found a way to do this which minimised ignition risk. The crew then started the mud pumps in a final attempt to control the well. At 10:22 in the morning, when only 8-10 m^3 of emergency mud remained, a pressure of 0 bars was recorded. The attempt was successful.

1.3 Learning from the Snorre A blow-out

There is much more to be told about the Snorre A blow-out. We will present additional context and details in Chapter 2. At this point, we will use the Snorre A blow-out to illustrate how different perspectives on organisational accidents and resilient organisations can help us to achieve a richer understanding of a complex unwanted event.

The brief summary of the Snorre A blow-out leaves us with two puzzles:

1. How could a blow-out, with a potential to develop into a human, environmental and economic disaster, occur during an operation which had been planned in detail over the course of several months, within a regulatory regime considered by many to be among the

[3] An alternative strategy was to inject concrete into the well. This strategy was abandoned, because an unsuccessful attempt to kill the well with concrete might make further attempts difficult or impossible due to concrete in well-bore (Wackers, 2006:68).

strictest in the petroleum industry worldwide? This puzzle concerns the occurrence of *organisational accidents*, i.e. accidents that can only be understood properly if we examine the functioning of the organisation.

2. How did the platform crew manage to avoid disaster and regain control of the well despite all the odds that were against them? They lacked essential resources such as power and drilling mud, they had to act within a very short time frame compared to the planning process, and a single source of ignition such as a spark might ignite the gas cloud. This issue is an important aspect of *organisational resilience*, i.e. the capacity of organisations to accommodate failures and disturbances without producing serious accidents.[4]

Finding good answers to first puzzle might help us prevent similar or even more serious events in the future. Finding good answers to the second puzzle might help us build and maintain a capacity to handle similar crises in the future. But where can we look for good answers?

The purpose of this report is to propose directions in which we may look for answers to issues related to organisational accidents and resilient organisations. We have outlined six different perspectives from which we may seek understanding of organisational accidents and resilient organisations. Looking at a mountain from different angles gives us a different view, or perspective, of the mountain. The more perspectives we are familiar with, the better we know the mountain, and the better is the chance that we will find a good path to the top. We may also think of the perspectives as different glasses or different filters which allows us to "see" different aspects of a phenomenon. Trying out different glasses or filters allows us to gain a richer understanding. A richer understanding allows us to think of new ways to build resilient organisations and prevent organisational accidents.

Let us consider how we might look at the issues related to the Snorre A blow-out and which questions we would ask, taking one perspective at a time:

1. *The energy and barrier perspective* tells us to consider the dangerous energies in a system and the means by which such energies can be reliably separated from vulnerable targets (Gibson, 1961; Haddon, 1970; 1980). Several dangerous energies were involved in the Snorre A blow-out. The reservoir pressure, the potential for a major release of thermal energy if the gas cloud were to be ignited, the thermal energy of potential ignition sources including the flare, and the power supply, and mechanical energies related to the possibility that the gas emerging from the sea bottom might cause one of the tension legs to become unfastened and the platform to capsize. The occurrence of the blow-out was clearly related to the removal or loss of barriers between the reservoir pressure and vulnerable targets such as the platform and the crew. One example of a barrier that failed was the 9 5/8" casing, which failed to contain the reservoir pressure. The blow-out would not have occurred if all barriers had been effective. Energies were also involved in the recovery action, for instance related to the weight of the mud needed to counteract the reservoir pressure, the effects needed to pump the mud into the well. A key to the successful recovery was the ability of the platform crew to muster the energies necessary to control the wells without igniting the gas.

2. *The Normal Accident perspective* tells us to consider the degree to which the technology is characterised by tight coupling and/or complex interactions (Perrow, 1984). A system is tightly coupled if disturbances propagate rapidly throughout the system and there is little natural slack or redundancy that allows people to improvise ways to contain the disturbances. Complex interactions cause systems to behave in unexpected ways and take people by surprise. It can be argued that both these properties were crucial aspects of the Snorre A blow-

[4] The meaning of "resilience" will be further elaborated in the chapter on resilience engineering.

out. An intervention 1500 meters into the well rapidly created a critical situation on the platform. Such things only happen in tightly coupled systems. Nobody had expected this scenario, in spite of all the efforts that go into risk analysis and emergency planning for an offshore platform. Such surprises are characteristic of a system with complex interactions. In order to understand how the Snorre A blow-out could occur and the challenges facing the platform crew, it is not enough to consider the energies involved. We also have to take into account the tight coupling and the complexity of the production system.

3. *The High Reliability Organisations (HRO) perspective* was developed to account for the extraordinary capacity of some organisations to handle complex and potentially dangerous technologies under condition of high production pressure without generating major accidents (Rochlin et al., 1987, LaPorte and Consolini, 1991). This perspective tells us to consider the presence or absence of *organisational redundancy*, i.e. patterns of cooperation that allow the organisation as a whole to perform more reliably than each individual in isolation. Was there a failure of organisational redundancy during the planning of the slot recovery operation? Did organisational redundancy contribute to the successful recovery? This perspective also suggests that HROs profit from a capacity to reconfigure, i.e. to change structure and interaction style in response to peak demands or crises. Did this happen to the platform organisation of Snorre A during the crisis?

4. *The information processing perspective,* (Turner, 1978; Turner and Pidgeon, 1997) tells us to examine the flow and interpretation of information that is linked to physical events. Was all the information available that was necessary either to plan for a safe slot recovery operation or to do decide that this operation could not be performed without unacceptable risk? Were the crucial pieces of information combined and interpreted in an appropriate manner? How did the platform crew manage to assemble and interpret the requisite information during the recovery phase?

5. *The decision-making perspective* is concerned with the choices we make when faced with conflicting objectives, for instance when safety has a price in terms of money, time, effort or other factors. The decision to perform the slot recovery operation despite the problems associated with well P-31A is an example of this. Another example is the decision of the platform manager to attempt to control the well rather than evacuating all personnel on the platform. A more detailed analysis of the context of the Snorre A blow-out will reveal additional decisions where safety was pitted against competing objectives. Such decisions give rise to several questions: Were the decisions prudent, given the knowledge available to the decision-makers and the pressures they were exposed to when they made their decisions? Why did they decide as they did? Do we need to change some aspects of the decision process or decision context in order to ensure prudent decision-making in similar situations in the future?

6. The *resilience engineering* perspective (e.g. Hollnagel, 2004; Hollnagel et al., 2006) tells us, among other things, to monitor and improve the capacity of the sociotechnical system to cope with unexpected events. The crew on Snorre A displayed an extraordinary capacity to improvise in a critical situation. We should try to understand how they managed to perform these improvisations, and what the preconditions that enabled this performance were. Such understanding can help us develop and monitor the capacity for improvisation in other organisations. Another message from the resilience engineering literature is that we should pay attention to normal operations, and not only to undesired events. This suggests that we should examine the daily operations prior to the blow-out. Were there signs in the way normal operations were carried out that pointed to a lack of resilience? Were there signs that the organisations failed to improve or maintain its resilience? For instance, were maintenance and

modification tasks needed to maintain a resilient system postponed due to production pressures?

The main message of this discussion is that each perspective helps us draw new lessons from the Snorre A blow-out. Each perspective helps us ask new questions and find new ways to account for the loss of control and the successful recovery. Thus each perspective directs us to new ways in which we can use the Snorre A experience to prevent loss of control and/or facilitate recovery from critical situations in the future. Taken together, the perspectives help us make sense of the Snorre A blow-out in a more productive manner. Leaving out one or more perspectives could lead us to miss valuable lessons from this incident.

This is not only a matter of generating a long action list of improvements based on a single incident. The perspectives help us see what is in front of our eyes. They help us recognise inconspicuous signs that our organisations are less resilient than we want to think. The perspectives can also help to broaden the scope of our discussions about safety. They provide concepts that may facilitate the process of putting into words alternative problem analyses. New perspectives may also help us identify alternatives to remedies that have tried and tested with limited success, and that are reused only because we do not find alternatives.

This capacity to look at organisational accidents and resilience from several perspectives is a prerequisite for any safety policy seriously aiming at Zero accidents and continuous improvement. People and technology will never become perfect. Prohibiting erroneous actions will therefore bring us nowhere. Neither is it sufficient to repeat old lessons or to reapply the means that proved effective yesterday. The only way to continuously approach the target of Zero accidents is to learn and implement *new* lessons from the successes and failure of ourselves and others. Learning new lessons requires the capacity to see things in new ways, too look at things from new angles. The perspectives outlined in this report are intended to help the reader develop the capacity to look at organisational accidents and resilience from new angles, and thus to derive new practical insight form the successes and failures experienced by the organisation.

2 Introduction

2.1 Background

On December 25 1998 two workers were killed and eight others were injured in an explosion at an Esso gas plant at Longford in Australia (Hopkins, 2000b). Due to tight interconnections with two other gas plants, the gas supply to Melbourne was cut for two weeks. At the 30th of September, *The Age* brought the following witness from the operators that Esso blamed for the accident[5]:

> Things happened on that day that no one had seen at Longford before. A steel cylinder sprang a leak that let liquid hydrocarbon spill onto the ground. … Ice formed on pipework that normally was too hot to touch. Pumps that never stopped, ceased flowing and refused to start. Storage tank liquid that was normally stable plummeted …

The gas plant at Longford had enjoyed excellent LTI-rates for years prior to the explosion. However, the public investigation of the Longford explosion revealed several serious safety management deficiencies which contributed to the accident (Hopkins, 2000b). Many of the shortcomings could plausibly be viewed as results of extensive cost-cutting. This cost-cutting effort was actually part of a world-wide phenomenon, and thus paralleled the NORSOK initiative to reduce costs in the Norwegian petroleum industry (Hovden and Steiro, 2000).

The Longford accident was spectacular in its impact on regional gas supply, but it was not unique (Hopkins, 2000b). In fact, it makes sense to speak of a family of organisational accidents. These are often major accidents. They often come as "fundamental surprises" to many of the people that manage and operate the dangerous systems (Woods, 1990). However, several precursors are usually discovered if a public investigation is launched (Turner and Pidgeon, 1997). Some of the companies involved display excellent LTI-records. This suggests that the concepts and approaches that have been developed to handle minor accidents are not sufficient to understand and control the risk of organisational accidents.

We have recently witnessed major changes in technologies of hazardous systems, in the organisations that operate the systems, and in the political and economic environments of these organisations. The present dynamic society brings with it some dramatic changes of industrial risk management (Rasmussen and Svedung, 2000:10):

- A very fast pace of change of technology
- The scale of industrial installations is steadily increasing
- High degree of integration and coupling of systems
- A very aggressive and competitive environment.

Faced with these trends, many researchers and practitioners feel the need for new concepts that can help us understand how organisations become susceptible to organisational accidents. Many of us search for strategies and methods to build organisational resilience, i.e. to build organisations that are not prone to experience major accidents. It is important to understand why accidents occur in order to learn and benefit from them. But it is also important to study how the

[5] Cited from Hopkins (2000b:1).

organisations handle their daily operations, correct deviations and learn from normal and abnormal situations.

As also presented in the prelude in chapter 1 the aim of this report is to present a set of perspectives that may help us understand the organisational mechanisms that may be involved in major accidents. We emphasise perspectives that have emerged from work on major accident risks in industry and transportation. Many challenges and issues at the organisational level are of a generic nature, i.e. they are common across many sectors. For instance, few if any organisations avoid the challenge of handling conflicting objectives. At the same time, the specific risk control strategies and measures need to be adapted to the threats and the constraints facing a specific organisation. For instance, civil aviation can "absorb" a few major accidents each year on world basis, whereas the nuclear power industry worldwide may need more than a decade to recover from a single event. This implies that civil aviation may afford to learn by hindsight to a greater extent than the nuclear power industry (Rasmussen, 1997).

2.2 Definitions and delimitations

At this point the reader may expect to find clear-cut definitions of "resilient organisations" and "organisational accidents". This leads to a bootstrap problem, since the perspectives we are going to present, focus on different aspects when they categorise accidents and account for organisational resilience.

As a starting point, we may define an accident as a sudden, unintended event or series of events where significant harm is inflicted on humans, the environment or material assets. This definition excludes intentional harm, such as terror, hacking or sabotage. The definition also excludes harm that occurs gradually, such as the long-term effects of continual emissions of toxic substances. The notion of "vulnerability" usually includes a system's susceptibility to intentional harm. Additional perspectives, or extension of the perspectives presented here, may be needed to adequately cover the issues related to an organisation's susceptibility to intentional harm.[6]

We may then consider Reason's (1997:1) conception of *organisational accidents*:

> [Organizational accidents] 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. 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. … [Organizational] accidents are a product of … technological innovations which have radically altered the relationship between systems and their human elements.

Reason's definition is rather eclectic, and thus captures aspects that are important to several of the perspectives to be discussed.

Foster (1993: 36) defined *resilience* as an ability to accommodate change without catastrophic failure, or a capacity to absorb shocks gracefully. The word *resilience* conveys an ability to recover or spring back into shape or position after being pressed or stressed (elasticity), but also an ability to recover strength, spirits and good humour. In this report, the focus is on accidents.

[6] Readers interested in practical approaches to vulnerability and vulnerability analysis will find interesting material at the website http://www.ipk.ntnu.no/rams/ (partly in Norwegian).

We can thus define a resilient organisation as *an organisation that has a capacity to accommodate failures and disturbances without producing serious accidents*.

Our main concern is how organisational accidents are related to the properties of the organisation during normal operations. We pay less attention to such issues as planning and training for emergencies.

The third limitation concerns the emphasis on the organisation's interactions with its environment. External threats have not been given much attention, although some general impacts of a competitive and dynamic environment are considered.

Since our topic is resilient *organisations*, we pay limited attention to issues related to the individual level, the regulatory level and the political level (see Figure 10, page 84). However, we acknowledge that organisations are parts of larger systems. For instance, vertical interactions between levels of decision making are discussed in Section 8.4. Moreover, problems and tensions at the organisational level are reflected at the level of individuals. Individuals may be caught in a double-bind situation where they face irreconcilable demands, or they face incomprehensible situations due to inadequate information handling at the organisational level.

Although this is a report on organisational accidents and resilient organisations, we have included a chapter on the energy and barrier perspective. The energy and barrier perspective pervades practical safety work, and therefore becomes a topic in some organisational theories of accidents. Moreover, the feasibility of controlling the risk by means of barriers may have an impact on an organisation's choice of risk control strategies (Rasmussen, 1994a).

We have not tried to be exhaustive, but rather to select a few complementary perspectives that are central in practical safety management or that have had a major impact on research and discussions in safety science.

2.3 Structure of the report

The main theoretical contributions to the understanding of organisational resilience are partly overlapping, partly complementary, and partly contradictory. We have not found any obvious way to systematise or synthesise this diversity. Trying to force everything into a single model would do injustice to the diversity and probably make for a complicated model that would be hard to communicate. Imposing a rigorous classification scheme on the theories is also problematic, since many theories are too complex and comprehensive to fit into a neat category.

Given this dilemma, we decided to group the material into six perspectives on organisational resilience. The perspectives represent different sets of assumptions and metaphors to make sense of organisations. The six perspectives are:

1. The *energy and barrier perspective*, according to which accidents can be understood and prevented by focussing on dangerous energies and means by which such energies can reliably be separated from vulnerable targets (Gibson, 1961; Haddon, 1970;1980). This perspective has been included because of its impact on practical safety management.

2. Perrow's theory of *Normal Accidents*, which explains some major accidents in terms of a mismatch between the properties of the technology to be controlled and the structure of the organisation responsible for controlling the technology (1984). This theory has provoked a lot of fruitful controversy, mainly because it concludes that some technologies should be

abandoned in their current form because they cannot be adequately controlled by any conceivable organisation.

3. The theory of *High Reliability Organisations* (HRO) was developed partly as a reply to the challenge posed by Normal Accident theory (Rochlin et al., 1987, LaPorte and Consolini, 1991). HRO theory is grounded in intensive studies of organisations that have demonstrated an outstanding capacity to handle fairly complex technologies without generating major accidents. Important concepts from this research tradition are *organisational redundancy* and a capacity of organisations to reconfigure in adaptation to peak demands and crisis.

4. *The information processing perspective*, taking Turner's theory of *Man-made disasters* as a starting point. (Turner, 1978; Turner and Pidgeon, 1997). In this perspective, an accident is viewed as a breakdown in the flow and interpretation of information that is linked to physical events.

5. A *decision-making perspective,* with a focus on the handling of conflicting objectives. Here we introduce Rasmussen's (1997) model of activities migrating toward the boundary of acceptable performance, as well as the notion of distributed decision-making.

6. The *Resilience Engineering* perspective, which combines and elaborates concepts and ideas from the previous perspectives in an effort to build a more coherent understanding of resilience in socio-technical systems and to provide tools to help organisations monitor and build resilience.

The clustering of subjects we have done can of course be discussed, as can the way we have delimited the perspectives. We have tried to give a reasonably "rounded" presentation of each perspective. This implies that there are some overlaps, for instance between the information processing perspective and the HRO perspective.

Each perspective has been devoted a separate chapter. We have emphasised the following aspects of the theories in the presentations and the summary chapters (Chapters 10 and 11):

- Notion of immediate causation
- Notion of root causes
- Risk control strategies
- How can major accident risks be monitored?
- Critical assumptions
- How can organisational change influence risk levels?
- How can we learn from disasters and incidents?
- What is the relationship between minor and major accidents?

In organisational theory Morgan (1984) and Bolman and Deal (1986) have stressed the importance of combining perspectives in order to understand the organisations. A similar attitude is implicit in the way authors such as Reason (1997) and Hopkins (2000b) combine different perspectives in their discussions on organisational accidents. We think it is important to have a sense of all the perspectives to make better analyses and make decisions. We will not claim that one perspective is better than another is, but rather focus on what could be learned from the different perspectives.

Before we turn to the outline of each perspective, we shall outline two events that will later be used to illustrate how each perspective can help us examine real events.

3 Two cases for discussion:

To get a better grasp on the perspectives presented in this report, we will discuss how each of them can be applied to actual events. We have selected two events:

1. A train collision that occurred at Åsta in Norway on 4 January 2000.
2. The gas blow-out at Snorre A, which we introduced in Chapter 1.

We will summarise the event sequence and background of these accidents in the following sections. Some readers may feel a bit overwhelmed by the complexity of the Snorre A blow-out. It is not necessary to understand the cases in detail to profit from reading this report. However, it may be useful to expose oneself to some of the complexity of the cases, to get a grip on the challenges facing people operating complex systems.

3.1 The train collision at Åsta[7]

On 4 January 2000, a northbound train from Hamar was scheduled to stop at Rudstad station on the Røros line and wait for a southbound train from Trondheim to pass. However, the northbound train left Rudstad before the southbound train had passed. The two trains collided seven kilometres further north at Åsta station. The engine car of the northbound train was completely wrecked, while the steering car received minor damage and remained upright on the rails. The southbound locomotive train was severely damaged. The locomotive toppled over onto its side and the front carriage buckled and derailed. A major fire broke out immediately in the area around locomotive and the rest of the engine car. Few minutes later fire broke out in the front carriage and the fire eventually spread to the remaining two carriages. Out of a total of 86 people, 19 people were killed. The situation immediately prior to the collision is shown in Figure 2 on the next page.

The commission of inquiry identified two possible direct causes of the accident. They could not exclude the possibility that the exit signal for the northbound train at Rudstad station was green instead of red due to a short-term operational malfunction of the signalling and safety systems.[8] Neither could they exclude the possibility that the northbound train had driven out of Rudstad against a red exit signal.

[7] The summary of the accident is based on the report from the Commission of inquiry appointed by the Norwegian Government (NOU 2000:30).

[8] Several weak points were identified related to the safety and signalling system. It was known that the system could show an erroneous green signal for a moment due to the slowness of the relay system.

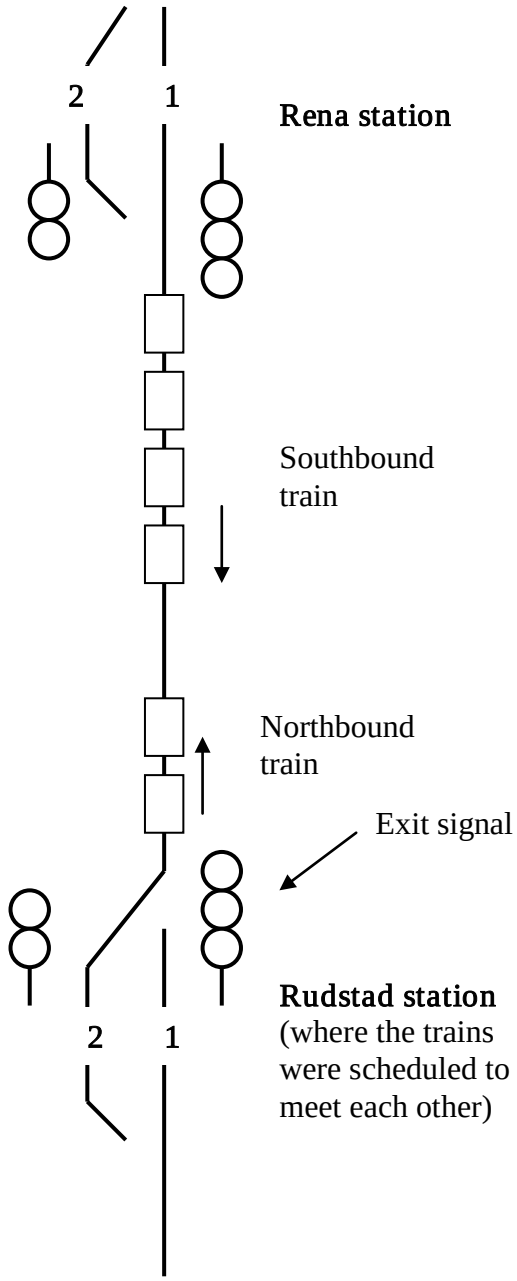

Figure 2. The situation immediately prior to the collision at Åsta. The northbound train had left from track 1 at Rudstad, forcing open the switch at the northern exit of the station. Not all signals are shown.

The Røros line did not have an operative Automatic Train Control[9] system (ATC) at the time of the Åsta accident. Automatic Train Control might have prevented the collision by automatically braking the northbound train if the exit signal was red when it started from Rudstad station. An audible alarm to warn of a train on collision course had not been installed at Hamar rail traffic control centre, from where the trains were directed. The rail traffic controller discovered a red

[9] The function of an Automatic Train Control system is to warn the driver and, if necessary, brake the train automatically if the driver exceeds speed limits or fails to brake the train adequately when approaching a red signal.

warning text on one of his displays about four minutes after the northbound train had left Rudstad and only *one* minute before the collision occurred. The Røros line is not electrified, so he could not prevent the collision by switching off the power supply to the trains. Train radios had not been installed on the Røros line. Both trains had mobile phones and both trains had reported in their phone numbers to the traffic controller at Hamar. The reporting of mobile telephone numbers was done to secure the traffic flow and service to the passengers. No safety grounds had been given for keeping a list of mobile telephone numbers, in spite of the requirements in the regulations about a rapid two-way contact between train and the control centre in case of an emergency. But the traffic controller on the previous shift did not add the numbers to the list. When the traffic controller on duty realised that a collision was imminent, he was not able to find the telephone numbers and contact the trains in time to prevent the collision. More detail about the Åsta accident can be found in the public investigation report (NOU 2000:30) and in Rosness (2009b).

3.2 The Snorre A blow-out

We gave a short summary of the blow-out at the Snorre A platform in Chapter 1. This thin description of the Snorre A blow-out gave an idea of its severity and of the challenges that the platform crew overcame in bringing well P-31A under control. However, to get a proper understanding of this event we need to add more detail and more context, and to go further back in time. This account is based on the investigation report issued by the Petroleum Safety Authority (Petroleumstilsynet, 2005), a report prepared for Statoil by Schiefloe et al. (2005) and an analysis by Ger Wackers (2006).

Readers that are unfamiliar with the accident may want to review the outline in Chapter 1 before they proceed to the more detailed account below.

3.2.1 The broader political, organisational and economical context of the Snorre A blow-out

How far back in time do we need to go to understand how the Snorre A blow-out could happen? Let us start with a political compromise which was established in the early 1970s. It was then decided that three Norwegian oil companies should be given opportunities to take part in the exploration of the Norwegian shelf: The fully state-owned Statoil, the half state-owned Norsk Hydro, and the privately owned Saga Petroleum.

Saga became operator[10] of the Snorre field, which was among the largest oil fields on the Norwegian shelf (Wackers, 2006). The Norwegian state, Statoil and Norsk Hydro were major partner licensees in this field. Saga collaborated with Esso to build the Snorre A platform. Oil production from Snorre A started in august 1992.

Towards the end of the 90s, Saga experienced financial problems after the acquisition of another Oil Company, Santa Fe, in a period with low and declining oil prices. After a sharp decline in the stock value, Saga's management sought ways to ensure the maximisation of shareholder value (Nore, 2003). One of the options considered was sale of the company. A move from Elf to take over Saga was countered by a successful joint bid from Statoil and Norsk Hydro. Saga's assets were then split between Statoil and Norsk Hydro. As part of this deal, it was decided that Norsk Hydro should take operator responsibility for Snorre A for 3.5 years and thereafter hand it over to Statoil.

[10] The license for exploration and development of an oil field on the Norwegian shelf is usually granted to a group of companies, who take a share in the capital investments and earn the right for a corresponding share of the revenues. The Norwegian authorities also select the operator, i.e. the company that will be responsible for operating the field and its installations.

It appears that this deal was made by top management, based on business considerations only, with no consideration of the possible impact on the safety of the operations (Wackers, 2006). However, the impacts on the operational organisation were strong. A change of operator implies that the whole organisation has to adapt to new procedures and new management systems. Personnel in an operating organisation depend on extensive networks with resource persons (e.g. technical experts) in other parts of the organisation. These networks were uprooted – not once, but twice within a four year period. After the second change of operator, when Statoil took over Snorre A from 1st of January 2003, a dominant reaction was a desire to "be left alone". This reaction was to a considerable degree respected by Statoil (Schiefloe et al., 2005). During planning and execution of the slot recovery operation on well P-31 A, the Snorre A operating organisation was not fully integrated in the culture and the competence networks of Statoil.

Another effect of the frequent shifts of operator responsibility was a change in the time perspective of the operator (Schiefloe et al., 2005). Norsk Hydro knew that they would be operators for only 3.5 years. When operator responsibility was transferred from Norsk Hydro to Statoil, the two companies had an agreement that revenues for non-operator partners in the license would be calculated on the basis of the operational cost level that Norsk Hydro had achieved prior to the transfer (Wackers, 2006). Although this agreement turned out to be unworkable in practice and was renegotiated, it illustrates the point that Snorre A was turned into a money machine. Emphasis on long term planning and robustification of the installation and organisation was reduced, and preventive maintenance was deferred into the future (Schiefloe et al., 2005).

The operator shift from Norsk Hydro to Statoil was part of a major reorganisation of the operations on the Tampen area. Statoil became the operator of all installations in the area. As part of a strategy to integrate the Tampen area and gain efficiency, Statoil decided to bring all well and drilling operations in the Tampen area under one contractor (Wackers, 2006). As a consequence, Snorre A changed drilling contractor from Prosafe to Odfjell Drilling. After a period of uncertainty, eighty percent of Prosafe's personnel on Snorre A kept their jobs, but changed employer. The others decided to find a new job elsewhere. As with the change of operator, a change of employer imposes extra workload on the employees. Moreover, the position of the rig manager was removed. This led to increased workload on the tool pusher and the driller (Schiefloe et al., 2005).

3.2.2 The history of well P-31A

Well P-31 was drilled as an observation well in 1994, in order to collect geological data to optimise the path for the horizontal section of the well. A part of the casing got stuck while it was being inserted in the borehole at a depth of 1817 meters and had to be cut. The lower part of the original well was then shut off permanently with a concrete plug. A sidetrack, P-31A, was drilled in 1995.

New problems occurred during the drilling of the sidetrack. During a cementing operation, the drill string got stuck in concrete and had to be drilled out again (milling). The actions that were taken to recover this problem led to extensive wear in the 9 5/8" casing at a point 1561 meters into the well. A new tube, a 7 5/8" scab liner, with somewhat smaller diameter than the damaged part of the casing and a length of 2578 meters, was installed to cover the holes and partly eroded sections in the casing and reinforce the integrity of the well. After a pressure test, the well was downgraded to 255 bar from the original pressure specification of 345 bar. The well was mainly used to inject gas into the reservoir.

Well P-31A was used for production of oil for about one year and then converted to a gas injection well. A gas injection well is used to increase the reservoir pressure by injecting gas in order to extract more oil from adjacent wells.

In June 2001, Norsk Hydro discovered extensive corrosion in the production tubing in the lower part of the well. The production tubing is small diameter pipe running inside the casing in a production well.[11] A new 4" scab liner (also called a "straddle") was then inserted to reinforce the lowermost section of the production tubing.

In Januar 2003, Statoil performed a pressure test after observing leakage between two of the tubes. During this test, the pressure went to 194 bar and then fell to 94 bar. This indicated that a burst in the 9 5/8" casing had occurred during the test. Statoil then decided to temporarily suspend the well without further analysis of the leakage point and the seriousness of the leak. A mechanical plug was inserted to isolate the damaged part of the well from the reservoir pressure, and the well was filled with brine (i.e. heavy salt water solution).

According to the investigation report of the Petroleum Safety Authority (Petroleumstilsynet, 2005:11), Statoil considered well P-31A complex due to

- Factors which give the well reduced integrity (corrosion, leaks).
- Unconventional well completion with a great many small completion elements.
- Additional completion elements installed in the well in connection with repairs (scabliner and straddle).
- Downhole well control valves.

We should not jump to the conclusion that the mental picture of the well among those who planned and executed the slot recovery operation was identical to the picture we have constructed on hindsight, with knowledge about the outcome of the operation. The information about the well was stored in different databases, and a lot exist only on paper. Statoil's accident report suggests that "some data and documentation has probably disappeared in the transfers between Saga Petroleum, Hydro and Statoil" (Wackers, 2006:52).

3.2.3 The planning of the slot recovery operation

As mentioned above, the purpose of the slot recovery operation was to make the slot occupied by well P-31A available for drilling a new well. The status of P-31A had to be changed from temporarily suspended to permanently abandoned. An important task in this operation was to replace or supplement the mechanical plug that was inserted in 2003 with a more permanent barrier against the reservoir pressure.

The plan for the operation was developed in the course of several months in 2004. Several planning meetings were held where specialist contractors were involved (but not the drilling contractor). Early in the planning process, historical well data were collected. The many challenges related to the status of well P-31A were documented in a presentation given early in the planning process.

The initial plan for the slot recovery operation took into account the integrity problems related to the well. The reservoir section below the mechanical plug was not to be opened and cemented. Instead, the production tubing was to be cut above the mechanical plug, and an additional cement

[11] The main function of the production tubing is to protect the casing from corrosion by the produced fluids. The tubing string can be pulled out of the well for repair if necessary, whereas the casing is cemented in the well.

plug was to be set above the planned cut. This would provide a robust barrier against the reservoir pressure. The initial plan also took into account a requirement in the Activity Regulations that during drilling and well activities there, there shall at all times be at least two independent and tested well barriers in place.[12]

The original plan was, however, changed in October 2004. The reservoir engineering group in the Snorre operating organisation suggested that the reservoir section of tail pipe *under* the mechanical plug should be filled with concrete. The purpose was to prevent unwanted cross flows in the reservoir between P-31A and the new sidetrack (P-31B) which was to be drilled in the recovered slot. The drilling and well engineering group in the Snorre operating organisation initially opposed this solution because it would complicate the planning and execution of slot recovery, but they accepted the change in a later meeting.

The revised plan included the following suboperations (among others):

1. The tail pipe was to be perforated above the mechanical plug while the well was still filled with brine (salt water solution).
2. The brine was to be replaced by oil-based mud.
3. The 5 1/2" production tubing was to be cut and pulled out of the well.
4. The 7 5/8" scab liner was to be pulled out through the BOP in a single piece.
5. The well's reservoir section was to be cemented (filled with concrete).
6. …

The planning team discussed potential problems with the perforations in the 9 5/8" casing, but did not identify this as a risk or a violation of barrier requirements. The revised plan was developed in detail and submitted for verification, recommendation and approval. A risk review meeting for the entire program was, however, postponed from 12 November to 19 November because of a collision of meeting times. However, the drilling rig happened to be ready for the slot recovery operation two days ahead of time. To avoid rig downtime, the slot recovery was started on 19 November and the risk review meeting was cancelled.

In their investigation report, the Petroleum Safety Authority identified the folowing problems with this plan:

1. Once the tail pipe was perforated (step 1), the well would be opened for communication with the reservoir pressure of up to 325 bar, whereas the secondary barrier (i.e. the casing with the 7 5/8" scab liner in place) was only rated for 94 bar.
2. When the scab liner was cut (step 2), the holes in the 9 5/8" casing would be exposed to the reservoir pressure. This would further degrade the secondary barrier.
3. When the 7 5/8" scab liner was pulled through the Blow-out preventer (step 4), two of the three safety valves in the Blow-out preventer would be blocked in an open position

These observations were made with the benefit of hindsight. There is no evidence in the available documentation that the personnel involved in the planning process were aware of problems 1 and 2 (Wackers, 2006). We do not know whether any of the safety problems would have been detected and resolved if the final risk review meeting had been held.

[12] The Activity Regulations, Section 76. The requirement does not apply during the initial phase of drilling, before the surface casing is in place.

3.2.4 The execution of the slot recovery operation and the loss of control

The slot recovery operation started on 21 November 2004. On 21 November the drilling crew perforated the 2 7/8" tail pipe. The well was now in communication with the reservoir pressure. The heavy salt water solution (brine) in the well took over the function as primary barrier. In the evening, the brine was replaced by oil-based drilling mud, which was to serve as primary barrier during the subsequent operations.

The 5 ½" production tubing was cut and pulled out of the well on 23-24 of November. However, this operation had to be interrupted because the production tubing had only been partially cut, and the lower part of the 4" straddle also followed in the pulling operation. The straddle could not be pulled through the Blow-out preventer. It was then decided to leave the 5 ½" tubing and the straddle in the well. This was done on 27 November.

On 27 November, the crew punctured the 7 5/8" scab liner and observed the well to check if gas under pressure had accumulated outside the scab liner. No gas was observed.

The crew then started to pull the 7 5/8" scab liner. The annular space between the scabliner and the 9 5/8" casing was filled with a salt water solution (brine) which was heavier than the drilling mud. According to the detailed program for the operation, this should lead to a "U-tube effect", i.e. a pressure increase in the mud system, at the onset of the pulling operation. No such effect was observed.

A suction effect, called "swabbing", occurred as the scab liner was pulled. The scab liner worked like a piston moving slowly out of the well, sucking gas from the reservoir into the well bore from below. The symptom of this effect was an apparent 2 m^3 increase in the volume of the reservoir fluid. The drilling crew recognised the phenomenon, which is not regarded as abnormal during the first phase of a pulling operation. They responded by pulling the scab liner very slowly out of the well and observing the well carefully. Attempts to solve the problem by circulating mud between the scab-liner and the casing did not succeed.

From this point, the symptoms of problems multiplied. On 15:30 on 28 November, gas rose up through the BOP. After a brief pressure increase, the well started to loose pressure. This implies that mud was leaking out of the well. The drilling crew attempted to replace the mud.

At about 18:00 the pressure started to increase sharply. Gas was entering the well from the reservoir and expanding on its way towards the surface. The gas bubbles contained in the mud reduced its specific density, and thus its capacity to offset the pressure from the reservoir.

As a response to the problems with well P-31A, the platform manager summoned an emergency meeting at 19:05. This meeting decided to mobilise the emergency responsible management.

At 19:14 gas was detected in the cooling water for the Vigdis compressors, which is part of the production system of the platform. This was initially misdiagnosed as an internal leak. The crew stopped this part of the production system, but blocked the local gas detector to prevent the main power on the platform from being shut down.

At approximately 19:30 the platform manager decided to shut down all production at Snorre A due to the unclarified situation in well P-31A, but to let the main power supply continue to operate. Notifications were made to standby vessels, helicopters, Statoil's emergency centre outside Stavanger, the public Rescue Coordination Centre and the Petroleum Safety Authority. A general alarm was sounded on the platform, mustering personnel to the lifeboats. The first phase

of evacuation was carried out between 20:58 and 22:05. Non-essential personnel were evacuated, reducing the crew on the platform from 216 to 75 persons.

At the same time, the drilling crew tried to control the well by pumping mud into it.

From 21:20, several gas alarms went off outside one of the modules. This is when the personnel discovered that the sea was "boiling with gas". The emergency management team then activated an emergency shutdown. This closed down main power in order to remove possible sources of ignition.

3.2.5 A second look at the recovery

The recovery phase was outlined in Section 1.2 above. We will not detail the many actions and events of this phase.[13] However, many questions can be raised concerning the successful recovery. How did the crew manage to handle such a complex situation under very stressful conditions, and within such a short timeframe? Why did the platform manager not decide to abandon the platform when he understood how serious the situation was? Why did the essential crew accept the decision to stay on the platform in a very dangerous and stressful situation? We will add some information that may throw light on these issues.

When the platform manager activated the crisis management organisation, decision power shifted from the Snorre A onshore operations unit to the platform manager. Statoil had a pre-established policy for the management of unanticipated crisis situations on the platform (Wackers, 2006). This was called *pro-active management*. The main principles were to plan for the worst case scenario, to mobilise external resources, to think ahead and prioritise regaining control, while at the same time keeping retreat options open. This was done in a quite fast and cyclic process which included the following steps (Wackers, 2006):

1. assessing the situation and deciding on countermeasures in focus meetings between the platform manager, the heads of various technical disciplines and safety manager;
2. informing personnel on board over the personal address system or by sending people to the life boats;
3. reporting to the second tier emergency centre on land;
4. collecting observations on the developing situation and effects of countermeasures.

Wackers (2006) reports that the platform manager made extensive use of rich pictures based on previous events to make sense of the situation and communicate his understanding of the situation to the other crew members. His worst case scenario included aspects of the Bravo oil blow-out in 1977, and the multiple oil wells that were destroyed due to blow-out in Kuwait during the first Gulf War. The prospect of huge amounts of oil flowing freely into the sea for several months in Kuwait made him consider alternatives to an immediate full evacuation of the platform.

At the same time, he wanted to make the members of the platform management stay *voluntarily* on the platform during the critical phase of the incident, based on a sound evaluation of the risks involved. In order to achieve this, he needed to *defuse* another scenario, the Piper Alpha disaster in 1988, where 165 persons were killed in a hydrocarbon fire or while jumping from the platform or drowning in the water before being rescued. According to Wackers (2006:66), he compared the likely effects of an ignition of the gas cloud with the experiences many people have with trying to ignite an under-pressurised gas stove: "there will be a dull plop, but not the blasting, violent

[13] Readers who are interested in the details of the recovery phase may study the PSA investigation report (Petroleumstilsynet, 2005).

release of energy that you see in an explosion. … Being dispersed by the wind, this gas will burn away quickly without an explosion. Hence, you will not die in an explosion."

The platform manager also needed to counter the potential fear that the crew would be killed by the heat if the gas were ignited and started burning like torches from the surface of the sea under the platform. The mobilization of helicopters and fire fighting ships helped to create a reasonable expectation that the remaining crew would be able to evacuate successfully in case of such a fire (Wackers, 2006).

3.2.6 The aftermath

Nobody was physically injured in the Snorre A blow-out. The Snorre A platform survived the blow-out. Statoil resumed production from a limited number of wells in February 2005. Statoil has later started an upgrade of Snorre A to prepare the platform for continued production in spite of falling reservoir pressure.

The blow-out was investigated by the police, the Petroleum Safety Authority (PSA) and by Statoil. The PSA characterized the incident as one of the most serious to occur on the Norwegian shelf. The PSA (2005:3-4) concluded that

> Serious failures and deficiencies have been uncovered in all phases of Statoil's planning and implementation on well P-31A. These relate to:
>
> • Failure to comply with governing documentation
> • Deficient understanding and implementation of risk assessments
> • Deficient involvement of management
> • Breach of well barrier requirements.
>
> The non-conformities relate to failure on the part of both individuals and groups in Statoil and with the drilling contractor. The non-conformities occurred at several levels in the organization on land and on the facility.
> The investigation shows that the list of non-conformities and items that could be improved is extensive. Therefore, there is nothing to indicate that the incident was caused by chance circumstances.
> The non-conformities found in the investigation would all have been intercepted and corrected if the barriers had functioned. Individual barriers fail from time to time, but failure of so many barriers in different phases of an operation is extremely rare. The PSA is critical of the fact that such an extensive failure of the established systems was not uncovered. We question why this was not discovered and corrected at an earlier point in time.

Statoil published conclusions from their own investigation on their home pages in November 2005:

> The principal conclusions in the causal analysis relate to the following areas:
>
> - the Snorre organisation was gradually and cautiously phased into the Statoil system after the group took over as operator for the field from Norsk Hydro on 1 January 2003, but this integration should have been faster and stronger
> - the Snorre organisation's mode of working has not been systematic, planned and long-term
> - changes made to the organisation were not sufficiently understood and created lack of clarity about responsibilities – at the same time as the level of activity on the field was high
> - professional objections and critical questions have not been sufficiently welcomed, which in turn weakened safety barriers

- expertise on and understanding of risky operations was not good enough in the Snorre organisation.[14]

At the same web-page, Statoil lists some of the measures taken by the company in response to the blow-out:

These measures include:

- wells on Snorre have been planned and drilled in line with Statoil's best practice since the incident
- the Snorre organisation has been strengthened both on land and offshore
- Snorre personnel have received better training in Statoil's governing documents
- a special project has been established to improve and simplify in-house procedures in Statoil
- the quality of planning and risk assessment on Snorre A has been improved
- the Snorre management is more strongly involved in all operations.

We may note that neither the PSA nor Statoil paid attention to the successful recovery in their main conclusions listed above.

No individuals were prosecuted after the event, but the state attorney of Rogaland served Statoil (as a company) with Penalty notice (fine) of NOK 80 million. Statoil accepted the fine, and there will be no further scrutiny of the event in a court of law.

The incident attracted attention in the media during the critical phase and again when Statoil was fined. Apart from this, media interest in the event has not been overwhelming. The worst-case scenario, with multiple uncontrolled blow-outs, has hardly reached public attention. As these lines are being written (autumn 2009), we witness a fierce political controversy concerning whether the fertile fishing grounds around Lofoten and Vesterålen should be opened for petroleum exploration. However, we are not aware that the participants in this discussion have asked what would happen if the worst case scenario from Snorre A were to materialise in this area.

3.2.7 Concluding remark on the Snorre A Blow-out

We anticipate that many readers will feel overwhelmed by technical detail when they reach this concluding section. However, readers who are familiar with drilling and well operations, may want more detail, whereas readers who are familiar with the Snorre A blow-out, may miss particular facts or feel that certain points of view are not properly represented. We contend that it was necessary to include a certain amount of detail to give the readers a notion of the complexity of the operations. At the outset, the slot recovery operations was *not* considered particularly critical or complex by the people who planned and executed it, although it was recognised that P31-A was a rather complex well. The point we want to make is that operations of high complexity and criticality is the order of the day at many workplaces. Theories about organisational accidents and resilient organisations need to explain both why people are capable of handling these complex systems without accidents most of the time, and why they occasionally fail.

We also want to remind the reader that there is no such thing as an absolutely neutral or objective account of an accident. The writer is forced to make decisions on what include and what to leave out, when to start and stop the account, where and how far to trace causal chains. More specifically, this account of the Snorre A blow-out is influenced by our desire to demonstrate that several perspectives are needed to understand organisational accidents and organisational resilience.

[14] http://www.statoilhydro.com/en/NewsAndMedia/News/2005/Pages/SnorreABlowoutCausesAnalysed.aspx

In the following chapters, we will present different perspectives on major accidents and discuss the Åsta accident and the Snorre A well P-31 blow out on the basis of these perspectives.

4 Uncontrolled transfer of energy as the target of hazard control: The energy and barrier perspective

In cartoons, dangers are typically visualised in terms of energy – for instance a cliff and an abyss, a bomb or a bundle of dynamite with an ignited fuse. The idea that accidents can be conceptualised in terms of dangerous energies and inadequate barriers pervades theory and methods in the safety disciplines as well as practical safety work.

4.1 Energy transfer as the focus of accident research and prevention

Both practitioners and researchers are challenged by the diversity of accidents. The event sequences that lead to unintentional harm appears to be very different, the consequences range from trivial to catastrophic, and accidents occur in very different social and technological settings. Gibson (1961) introduced the energy model as a means to find some order in this perplexing diversity. He suggested that the most effective way of classifying sources of injury for research purposes is according to the forms of physical energy involved. The energy model was thus used by the medical discipline to systematise the analysis of accident causes in a way similar to that of analysing causes of diseases.

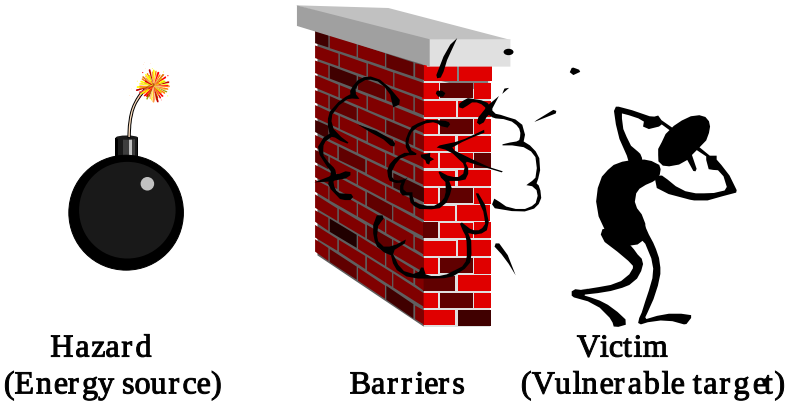

Figure 3. The energy and barrier model of accidents (adapted from Haddon, 1980)

William Haddon (1970, 1980) popularised the energy and barrier perspective and its implications for accident prevention. The basic idea is that accidents occur when objects are effected by harmful energy in the absence of effective barriers between energy source and the object (Figure 3). Haddon systematised known principles of accident prevention into 10 different strategies for loss reduction.[15] These are related to different points of intervention according to Figure 1:

[15] Haddon also noted that each strategy could be turned into its opposite, i.e. a strategy to increase damage. In principle, the list may thus be used to identify strategies, which an actor may choose to intentionally inflict damage (e.g. sabotage). He even outlined how the principles could be applied to birth control.

1. Prevent build-up of energy (thermal, kinetic, or electrical); e.g. avoid car driving.
2. Reduce the amount of energy; e.g. reduce the speed of vehicles.
3. Prevent uncontrolled release of energy; e.g. sanding and salting of roads.
4. Modify rate or distribution of the released energy; cars with shock absorbing zones, safety belts.
5. Separate in space or time, the victims from the energy being released; i.e. the use of sidewalks and the phasing of pedestrians and vehicular traffic.
6. Separate the victims from the energy by physical barriers; i.e. cars with safety cage.
7. Modify the qualities of the energy (the contact surface, subsurface, or basic structures), i.e. softening of hard objects in the car cabin.
8. Make the vulnerable target more resistant to damage from the energy flow; i.e. safety helmets.
9. Limit the development of damage; i.e. first aid.
10. Rehabilitate the victim(s).

Strategies 1, 2, 3, 4 and 7 are related to reduce *the hazard,* strategies 5 and 6 to *barriers*, while strategies 8, 9 and 10 are related to *protection and rehabilitation the victim(s)*. Higher-level loss control strategies may be formulated with reference to the ten basic strategies, e.g. "when feasible, prioritise risk-reducing measures directed at the hazard itself". Haddon argued that the larger the amount of energy involved, the earlier in the countermeasure sequence the strategy must lie.

4.2 What is a barrier? Barrier functions, barrier elements and barrier systems

The term 'barrier' has been given various definitions in the literature. In the basic energy and barrier model (Figure 3), a barrier is understood a means to separate a vulnerable target from a dangerous energy source. In concordance with this, Johnson (1980: 508) defined barriers as "The physical and procedural measures to direct energy in wanted channels and control unwanted releases." Kjellén et al. (1987) referred to the whole set of strategies proposed by Haddon as 'barriers'. These conceptions of 'barrier' thus include administrative measures such as procedures and work permit systems. However, some authors (e.g., Kjellén, 2000: 82) prefer to limit the term 'barrier' to *physical countermeasures* that intervene in the accident process to eliminate or reduce the harmful outcome.

The popular representation of the energy model (e.g. Figure 3) leads us to think of barriers as very concrete physical structures or devices. However, a *functional view* may be more productive when it comes to systematic loss control. A functional view implies that we think in terms of goals and means. We may think of a function as a *task* which is defined by one or more objectives to be achieved under specified conditions, for instance "prevent ignition of hydrocarbons after an uncontrolled hydrocarbon release in the process module"[16]. By taking a functional view, we thus focus on the *tasks that are necessary to adequately control a specific hazard.* These tasks may be performed by passive physical structures (e.g. fire proof walls), by active technical systems (e.g. the gas detection and emergency shutdown system on a production platform), or by humans, usually in interaction with technology and supported by procedures (e.g. the control of hot work so as to keep it separate from inflammable objects and substances). Thinking in terms of functions invites us to consider alternative means to implement a loss reduction strategy. For instance, if a gas detection system has to be inoperative during maintenance, an operator with a portable gas meter and radio communication with the control room operator may perform its task. Moreover,

[16] In this context, we should *not* think of a task as detailed, stepwise prescription of *how* a given objective is to be achieved. This would make us think in terms of part-whole-relations rather than goals-means-relations, and thus switch from a functional perspective to a system perspective (Rasmussen, 1986; 1997).

we need to consider that barriers can deteriorate and need to be monitored and maintained. This functional view fits well to the way Haddon formulated his loss reduction strategies, since each strategy is formulated as a task (e.g. 'Separate, in space or time, the victims from the energy being released'). The term 'safety function' is sometimes used in a sense similar to 'barrier function'.

Having defined a barrier function, we may identify the *barrier elements*, i.e. the hardware, humans, and software components (including procedures and routines) that are needed to implement the barrier function under given conditions. The totality of barrier elements that are necessary and sufficient to implement a given barrier function may be labelled a *barrier system*. The barrier system may thus be seen as the substratum or embodiment of the barrier function.[17]

Barrier systems are *open systems*. They do not function in isolation from their environment. Most technical devices can be disabled and need maintenance. Even passive barriers can fail due to human interventions. For instance, the performance of a fireproof wall may be dramatically reduced if it is penetrated by a cable bundle with flammable isolation. The distinction between physical and non-physical measures is thus not absolute. This is not just academic hair-splitting, because it points to a need for monitoring and maintaining barriers.

4.3 Defence in depth and organisational accidents

Haddon's model is relevant for the minor accidental event, as well as for major accidents. The prevention of accidents through *barrier functions* is an engineering approach and is a main principle behind safety in design (Kjellén, 2000:20). High hazard systems may employ several levels of defences in order to bring the total calculated risk to an acceptable level. For instance, a hydrocarbon processing plant (refinery or offshore installation) may include the following barrier functions related to hydrocarbon fires and explosions (Kjellén, 2000:85):

- Process control (automatic or manual);
- High quality containment;
- Gas detection and emergency shutdown;
- Isolation of ignition sources and ventilation;
- Fire detection and emergency shutdown;
- Area separation, fire/blast walls and passive fire protection;
- Active fire protection (e.g. deluge system);
- Provisions for escape and evacuation.

This hazard control strategy is commonly referred to as "defence in depth"[18]. A major accident in such a system is usually not caused by a single, isolated failure. This point is illustrated by Reason's (1997:12) "Swiss cheese model". An adaptation of this model is shown in Figure 4.

[17] See E. Hollnagel: "Accidents and Barriers". Undated course note, Linköping: University of Linköping. Available at http://www.iav.ikp.liu.se/hfa/Coursemasters/Course%20materials/accidbarri.pdf

[18] The expression 'defence in depth' is of military origin. Lack of defences in depth can be demonstrated by the history of the Roman army. The Roman army was at most 300 000 soldiers deployed in the empire ranging from North Africa in south to northern Britain. The army was based on quick transport to areas where they were needed, but there was no real defence in depth. When the pressure towards the empire from the great people moving in Europe started, there were not enough soldiers to provide a defence in depth in several areas at the same time.

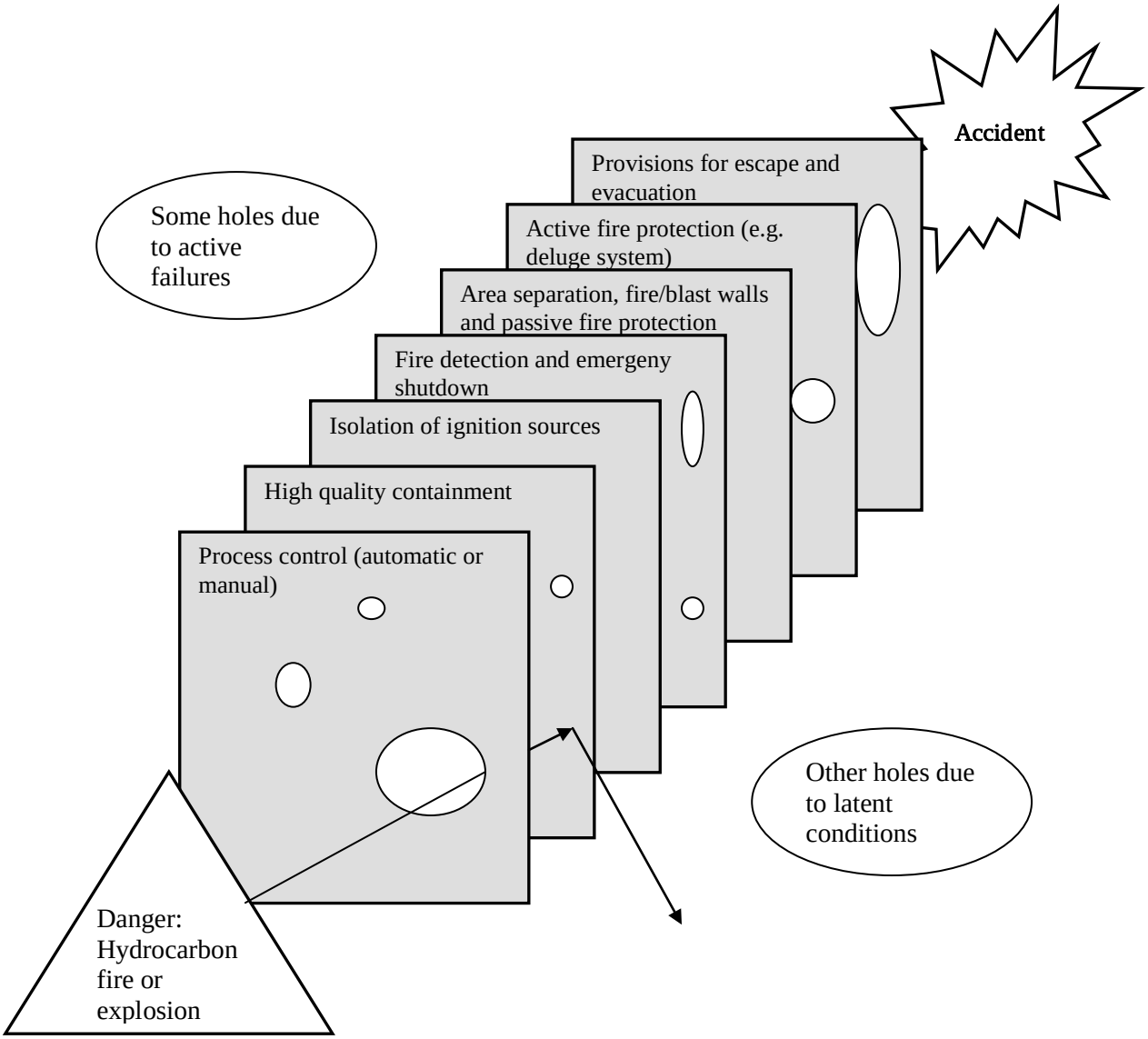

Figure 4. Defence in depth. (Adapted from Reason, J.: Managing the Risks of Organizational Accidents. Aldershot: Ashgate, 1997, p. 12).

The figure shows an accident emerging due to holes in barriers and safeguards. In an ideal world all defensive layers should be intact allowing no penetration to happen. However, in the real world defences may deteriorate over time, such as the corroded sprinklers on the *Piper Alpha.* Modification or redesign may weaken or eliminate defences. Defences can be removed during calibration, maintenance and testing, or as a result of errors and violations. The control room operators of the Chernobyl nuclear reactor successive removed layers of defence in order to complete their task of testing a new voltage generator.

Reason distinguishes between *active failures* and *latent conditions*. Active failures are those that trigger unwanted events. They include violations and errors by pilots, doctors, and control room operators. These are the people in the operation or what Reason calls the "sharp end" of the system. Latent conditions do not immediately trigger an accident. However, they lie dormant in system and may contribute to a future accident. Examples are poor design, maintenance failures,

poor and impossible procedures etc. These failures arise from top-level and strategic decisions and have indirect influence. Latent conditions can increase the likelihood of active failures.

In order to assess the effectiveness of defence in depth, it is not enough to assess the effectiveness of each barrier per se. We also need to consider *dependencies* among barriers. Dependencies will occur if two or more barriers can be weakened by the same event or condition. A failure in the electricity supply (blackout) may, for instance, leave several active technical barriers inoperative. This dependency may be increased if one or more backup energy supplies are likely to fail due to inadequate maintenance. Organisational conditions may thus create dependencies among barriers.

4.4 Analytical risk control

The energy perspective permeates major hazards control in the process industry and the nuclear power industry. For instance, the Quantitative Risk Analyses (QRAs) for Norwegian production platforms contain detailed models of the possible event sequences following hydrocarbon leaks in the process area. These models emphasise the contribution of barriers and the number of persons that may be exposed to a fire or explosion. On the other hand, the conditions that lead to hydrocarbon leaks are not explicitly modelled.[19]

This is an example of *analytical risk control* (Rasmussen, 1997). Major explosions on production platforms or in nuclear power plants are rare and unacceptable events. Rather than learn from trial and error, we need to determine whether the risk level is acceptable before the system is built. The energy and barrier perspective allows us to do this, since we can design a system with several barriers and estimate the risk level based on assumptions concerning the effectiveness of these barriers.

In performing a QRA, one makes implicit and explicit assumptions related to the effectiveness of barriers. Assumptions concerning the effectiveness of barriers are thus implicit premises for a risk acceptance decision based on a QRA. The system can drift to a risk level not deemed acceptable if the effectiveness of barriers deteriorates significantly. The organisation should therefore establish programs to monitor and maintain barrier functions throughout system life. The methodology for continuous monitoring of the operational risk level is currently less developed than the methodology for design analysis (Øien, 2001).

An example of further use of the energy and barrier thinking is from the Swedish national road administration. The Swedish approach opens up for risk based setting of speed limits. Where there are a possible conflict between vehicle and pedestrian and no barrier is present, the speed limit should be maximum 30 km per hour. The fatality rate increases dramatically after the 30-km per hour limit is crossed in case of conflict. We know that unwanted energy can not always be avoided, so amount of energy should be reduced.

4.5 The energy and barrier perspective and the Åsta accident

We presented a brief description of the accident in Chapter 3. The commission of inquiry relied heavily on the barrier perspective in their analysis and evaluations. This is illustrated by the following excerpts from the investigation report (NOU 2000:30, p. 202):

> We know that technical systems can malfunction. We also know that people make mistakes. Consequently, there must be a safety system to ensure that individual faults do not result in

[19] In a production platform QRA, the frequency of hydrocarbon leaks is calculated by counting components that may leak and multiply by standardised leak frequencies.

> accidents. ... Nonetheless, in the Røros incident, a signal failure or a mistaken observation by an engine driver led to a serious accident. ATC had not been installed on the Røros line … [Changes] were made without performing risk analyses for the individual change or for the Røros line. If the Norwegian National Railway Administration had done so, it would and should have been possible to see that an individual fault could lead to an accident. …
>
> With no barriers to prevent an emergency from arising, there should at least have been measures designed to avert it...

The investigation commission identified several defences which might have prevented the collision if they had been in place, for instance (NOU 2000: 30, pp. 171-175):

1. The presence of a train dispatcher at Rudstad would have reduced the risk that an error in the signaling system would develop to a critical situation. The driver of the northbound train would then have to obey signals given by the train dispatcher.

2. A different departure procedure, which required the conductor to independently check the exit signal, might have allowed a red signal to be observed, or prevented a transient green flash from being mistaken for a steady green signal.

3. An Automatic Train Control system (ATC) would probably have stopped the northbound train in front of the exit signal, or at least a short distance behind the signal. The function of the ATC is to brake the train automatically in case the driver fails to observe a stop signal or a speed limitation.

4. An acoustic collision alarm in the train control centre at Hamar would have given the traffic controllers three to four minutes more time to notify the train drivers, provided that they reacted promptly to the alarm.

5. Rules as to how often the traffic controllers were to monitor their screens, combined with more staff at the control centre, could have reduced the time taken before an abnormal situation is noticed.

6. A train radio system would have allowed the traffic controller to reliably reach all trains on a railway section using a single number.

The accident commission concluded that the Røros line lacked adequate barriers against single failure accidents.

Here the problem of lacking barriers is demonstrated. Technical failures, deviations from procedure or erroneous actions happen. Therefore a barrier is needed. In the Norwegian rail, the Railway Inspectorate demands "the single fault principle". The principle states that no single technical failure, erroneous action or mistake should lead to fatalities or serious injuries.

4.6 The energy and barrier perspective and the Snorre A blow-out

In Chapter 1, we identified several dangerous energies involved in the Snorre A blow-out: The reservoir pressure, the potential for a major release of thermal energy if the gas cloud were to be ignited, the thermal energy of potential ignition sources including the flare, and the power supply, and mechanical energies related to the possibility that the gas emerging from the sea bottom might cause one of the tension legs to become unfastened and the platform to collapse.

The occurrence of the blow-out was clearly related to the removal or loss of barriers between the reservoir pressure and vulnerable targets such as the platform and the crew. The lost barriers included, amongst others, the scab liner, which was cut and pulled, and the 9 5/8" casing, which had been damaged during a cementing operation. The blow-out would not have occurred if all barriers had been effective.

We should also note the complexity and the dynamic nature of the barrier envelope that was to keep the reservoir pressure under control during this operation. There are many barriers involved, some of them change status as the operations proceeds, and others may change status as a consequence of unexpected events. For instance, drilling mud will loose density if it contains gas bubbles. The regulations require planners to foresee how each step in an operation may change the status of the barrier functions. This is not a simple task.

The successful recovery involved the reinstatement of the mud balance as an effective barrier against the reservoir pressure. The mud had to be sufficiently heavy to counterbalance the reservoir pressure. It also had to be sufficiently viscous to seal the hole in the casing. The energy and barrier perspective points to the dilemmas that faced the platform crew. For instance, they needed the main power supply to run the mud pumps with sufficient effect, but the main power supply had been shut down to prevent ignition of the gas that emerged from the sea. The energy perspective was also prominent in the deliberations of the platform manager when he decided not perform a full evacuation of the platform.

The energy and barrier perspective also pervades the investigation report issued by the Petroleum Safety Authority. Many of the deviations identified concern failure to assure that two independent barriers against reservoir pressure were available during all phases of the operation.

4.7 Strengths and limitations of the energy perspective

Why has the energy perspective acquired a dominant position in major hazard control? There are several reasons:

- The energy perspective has proved very useful in hazard identification and as a basis for identifying hazard control strategies.
- The energy perspective is the basis for analytical risk control.
- It is possible to devise generic accident models by focusing on the uncontrolled release and transfer of energy.

Barrier functions allow individuals, groups and organisations *learning opportunities* which would not be available in an undefended system. An unintended shutdown in a process plant may be expensive, inconvenient and even hazardous, but it may force operators to practise skills that are not practised during normal operations. A shutdown may also provide information on the functioning of devices that are never used in normal operations, for instance emergency shutdown valves. This benefit of a well-defended system is often ignored, because it goes beyond the energy and barrier perspective.

The energy perspective may be most relevant for systems where the technical core and the hazard sources are well defined, physically confined and stable, for instance nuclear power plants or offshore oil production platforms (Rasmussen, 1994a). The scenarios following the release of a major hazard in such systems are usually confined to one or a few paths (e.g. fire/explosion or

structural collapse on an oil platform). In this case, quantitative risk analyses may emphasise the reliability of barrier functions.

In contrast, air transport is a distributed large-scale system. The functional technical core is divided among aircraft and infrastructures. Safe operations depend on the co-ordination of decentralised activities. Moreover, it is simply not feasible to design an aircraft strong enough to withstand a head-on mid-air collision. For these reasons, risk reduction efforts should emphasise preventing the release of hazardous energy, for instance by ensuring that critical systems are operative when they are needed.

Road transport could, however, benefit from more use of the energy/ barrier model. Haddon developed the energy barrier model for the road safety. And we have seen that the Swedish road authorities use it extensively (Johanson, 2009), for instance by introducing mid-barriers on rural roads.

Some authors include the notion of energy transfer in their definition of the term 'accident'.[20] From a physical point of view, any event has to involve a transfer of energy in order to be noticed. The occurrence of an energy transfer does not distinguish accidents from other events. Moreover, there are categories of accidents where the energy aspect is trivial. In an operating theatre, a pinprick with an infected syringe contains no more energy than a pinprick with a sterile syringe, although the former may cause a fatal infection (Hale, 2000). We may think of *information* – in the form of, e.g., DNA molecules, data viruses or computer bugs – as an alternative "medium" for the development of accidents. The barrier metaphor may prove useful even in the prevention of "information-driven" accidents, but this will require a different conception of barrier – one which is not linked to the energy model.

A limitation of the barrier model as it is used in QRAs of Norwegian production platforms is that factors influencing the initial event in analysis – e.g. hydrocarbon leaks – are not included in the model. This has an impact on what risk reducing measures are chosen if the QRA shows that the risk level is too high. The QRA does not give credit to measures devised to reduce the leak rate from a given component type. In this way, the energy and barrier perspective may lead to selection of sub-optimal measures for risk reduction in cases where new or improved barriers are not the most efficient measures.

Reason (1997: 41) gave a picturesque example of soldiers that were *"killed by their armour".* Heavily armoured French knights were thrown from their disabled horses by a storm of yard-long-steel-tipped arrows from English archers at Agincourt in 1415. The armour was so heavy, that they were unable to move or get on their feet in the mud. They were slaughtered by English foot soldiers equipped with mallets, spikes and daggers. In a similar manner, defences introduced to reduce the risk level may exacerbate an event under unfavourable conditions.

One common variety of this problem is the inflation of work procedures which can be observed in many organisations. Writing a new procedure is often perceived as a quick and inexpensive way to implement or reinforce a barrier function. One problem with this risk reduction strategy is that the total amount of procedures can become intractable. Operators may no longer find the time to identify all procedures applying to a given job, and the organisation may no longer find the resources to ensure that the total body of procedures is consistent, realistic and updated.

[20] For instance Johnson (1980: 507): Accident: An unwanted transfer of energy, because of lack of barriers and/or controls, producing injury to persons, property, or process, preceded by sequences of planning and operational errors, which failed to adjust to changes in physical or human factors and produced unsafe conditions and/or unsafe acts, arising out of the risk in an activity, and interrupting or degrading the activity.

Moreover, a very tight system of procedures may lead to more frequent conflicts between compliance with rules and efficient performance of the job. Such conflicts are often resolved through “silent deviations”. Routine violations of procedures become tacitly accepted practice. Discrepancies between rules and actual performance multiply, and activities may gradually drift out of control.

Active technical barriers may add to the complexity of the system, and thus increase the scope for maintenance-induced errors as well as operator errors. For instance, an automatic control system may be introduced to reduce a system’s vulnerability to operator errors. However, if the automatic control system fails, the operator may face an extremely difficult situation which he was not prepared for, since he no longer obtains the hands-on experience with the process (Bainbridge, 1987). Moreover, the automatic control system may add to the total complexity of the system, and thus make it more difficult to operate. Such paradoxes inspired Charles Perrow to formulate a theory of Normal Accidents, which we will discuss in the following chapter.

4.8 The Energy and Barrier perspective summarised

The starting point of the Energy and Barrier perspective is a focus on energy transfer and the core principle of separating harmful physical energy and potential victims by the use of separating barriers that can absorb or divert the energy. This principle comprises three main classes of protective measures, reducing the hazard (the amount of energy), building the physical barriers, and protecting and rehabilitating the potential victims.

Barriers are defined as physical and procedural measures to direct energy in wanted channels, and avoiding, or at least controlling, unwanted energy releases. The notion of the barrier has a concrete, physical meaning from the outset, but it is easily extendable into a functional view of tasks, comprising a number of diverse barrier elements of a technical/physical as well as procedural nature. A collection of barrier elements thus constitute a barrier system that implements a barrier function. This generalization of the barrier function enables an interchangeability and flexibility that is very useful, e.g. in relation to maintenance or non-routine situations in which (e.g.) a physical barrier element can be temporarily substituted by a procedural barrier element.

The energy-barrier principle is easily transferable to other situations and problems, to the extent that it can be seen as a metaphor for protection strategies in a variety of contexts. E.g., the “energy” can be a computer virus, and the “barrier” can be procedural not only in a human performance sense, but also in the organisational and cultural sense.

Hence, the energy-barrier perspective is very versatile for safety design and engineering. Based on the premise that linear, potentially dangerous sequences of events can be predicted analytically, it is possible to establish defense-in-depth both in terms of different barriers at different locations in the sequence, as well as redundant barriers. Consequently, all three types of measures from the core principle can be framed within a unified model comprising barriers. This prepares the ground for analytical risk control, in which principles of reliability engineering (combinatorial, effects of aging/deterioration) offer added value to the analysis of presumed sequences of events.

The energy-barrier perspective thus derives from the energy-transfer principle, which is mainly oriented at physical-technical issues. As this principle is increasingly used as a metaphor to mobilize human as well as organisational contributions to the prevention of uncontrolled releases of “energies” of many kinds, the issues of (emergent) holes or weaknesses of barriers, and the distinction between active failures and latent conditions which may derive from a broader context of technical, human and organisational factors, becomes increasingly important.

4.9 Key questions for the applicability of the energy-barrier perspective

- ⇨ Can the protection problem at hand be informed by the principle of energy-transfer?
- ⇨ Is it possible to apply the three classes of protective measures?
- ⇨ It is possible to analytically identify potentially dangerous sequences of events? (successive failures)
- ⇨ It is possible to apply technical or procedural barriers onto these sequences?
- ⇨ May barriers introduce new possibilities of risks and hazards or hazardous behaviour?

4.10 References

Bainbridge, L. (1987). Ironies of automation. In J. Rasmussen, K. Duncan and J. LePlat (eds.). *New Technology and Human Error.* Chichester: Wiley (271-283).

Gibson, J. J. (1961). The contribution of experimental psychology to the formulation of the problem of safety – a brief for basic research. In *Behavioral Approaches to Accident Research,* New York: Association for the Aid of Crippled Children, pp. 77-89. Reprinted in W. Haddon.

Haddon, W. (1970). On the escape of tigers: An ecological note. *Technological review, 72* (7), Massachusetts Institute of Technology, May 1970.

Haddon, W. (1980). The Basic Strategies for Reducing Damage from Hazards of All Kinds. *Hazard prevention,* Sept./ Oct. 1980.

Hale, A. (2000). Conditions of occurrence of major and minor accidents. 2me séance du séminaire "Le risque de défaillance et son contrõle par les individus et les organisations", 6-7 novembre, Gif sur Yvette.

Johnson, W. G. (1980). *MORT Safety Assurance Systems.* New York: Marcel Dekker.

Kjellén, U. 2000: *Prevention of Accidents Through Experience Feedback.* Taylor & Francis, London and New York.

Kjellén, U., Tinmannsvik, R.K., Ulleberg, T., Olsen, P.E., Saxvik, B. (1987). *SMORT: Sikkerhetsanalyse av industriell organisasjon. Offshore-versjon.* [MORT. Safety analysis of industrial organisations. Offshore version.] Oslo: Yrkeslitteratur.

Rasmussen, J. (1994a). High Reliability Organizations, Normal Accidents, and other dimensions of a risk management problem. Paper. *NATO Advanced Research Workshop on Nuclear Arms Safety.* Oxford, UK, August 1994.

Rasmussen, J. (1997). Risk management in a Dynamic Society: A Modelling Problem, *Safety Science, 27* (2-3), pp. 183-213.

Reason, J. 1997: *Managing the Risks of Organizational Accidents*. Ashgate.

Øien, K. (2001). *Risk control of offshore installations. A framework for the establishment of risk indicators.* Ph.D. Thesis. Department of Production and Quality Engineering. Trondheim: NTNU.

4.11 New references

Hollnagel, E. (2004). *Barriers and Accident Prevention*. Aldershot, UK: Ashgate.

Hollnagel, E. (2008). Risk + barriers = safety? *Safety Science, 46,* 221-229.

Rosness, R. (2004). *Ti tommeltotter og null ulykker?: Om feiltoleranse og barrierer*. Trondheim: SINTEF.

Sklet, S. (2006). *Safety Barriers on Oil and Gas Platforms. Means to Prevent Hydrocarbon Releases.* Trondheim: Doctoral Theses, NTNU.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494-506.

5 The challenge of interactive and tightly coupled technologies: Perrow's theory of Normal Accidents

Major accidents, such as the Three Mile Island accident, often come as fundamental surprise to the people that manage and operate the system (Turner, 1978; Woods, 1990). However, Charles Perrow (1984) insisted that some systems have structural properties that make such accidents virtually inevitable. He therefore labelled these fundamentally surprising events *"Normal Accidents".* We will summarise his argument in this chapter.

5.1 Component failure accidents versus system accidents

Perrow (1984; see also Perrow, 1986:140ff) suggested that some major accidents are fundamentally different from minor events. Minor events are typically *component failure accidents*. They are caused by a failure of one or two components in a system, and they do not involve any unexpected interactions. The potential for component failure accidents can to a considerable extent be identified through standard risk analysis methods. For instance, in a Failure Mode and Effect Analysis (FMECA), the analyst considers one system component at a time, and identifies the possible failure modes. This analysis should capture a fair share of component failure accidents triggered by hardware failure, provided the analyst is able to cover each component, failure mode and relevant system state.

In contrast to component failure accidents, *system accidents* involve *the unanticipated interaction of several latent and active failures in a complex system*. Such accidents are difficult or impossible to anticipate. This is partly because of the combinatorial problem – the number of theoretically possible *combinations* of three or four component failures is far larger than the number of possible component failures. Moreover, some systems have properties that make it difficult or impossible to predict how failures may interact. We will return to these properties in the next section.

In the introduction to this report, we introduced Reasons's (1997) concept "organisational accident". What is the relationship between Reason's concept "organisational accident" and Perrow's concept "normal accident"? "Organisational accidents" are distinguished by the number of persons involved and the degree to which they belong to different parts of the organisation. "Normal accidents" are distinguished by the number of component failures involved and the quality of surprise – i.e. whether the event sequence was anticipated, or at least foreseeable. It seems plausible that these dimensions are correlated. An event sequence involving multiple failures seems more likely to involve several organisational units than a single failure accident. However, we should not jump to the conclusion that *all* "organisational accidents" are "normal accidents" and vice versa. The event sequence of some "organisational accidents" can, to a significant extent, be anticipated. For instance, the Åsta accident involved several agents belonging to several organisational units, and thus qualifies as an organisational accident. However, the event sequence did not constitute a fundamental surprise. It resembled the Tretten accident which occurred in 1975, and several persons had warned that this kind of accident might occur.

5.2 Complexity and coupling

Perrow proposed that some socio-technical systems have structural properties that are conducive to system accidents.

Some systems, such as major nuclear power plants, are characterised by *high interactive complexity*. These systems are difficult to control, not only because they consist of many components, but also because the interactions among components are *non-linear.* Linear interactions lead to predictable and comprehensible event sequences. In contrast, non-linear interactions lead to unexpected event sequences. Non-linear interactions are often related to feedback loops. A change in one component may thus escalate due to a positive feedback loop, it may be suppressed by a negative feedback loop, or it may even turn into its opposite by some combination of feedback loops. Such feedback loops may be introduced to increase efficiency (e.g. heat exchangers in a process plant). Even some safety systems may add to the interactive complexity of a system, for instance if overheating of a given component initiates automatic cooling. Interactive complexity makes abnormal states difficult to diagnose, because the conditions that cause them may be hidden by feedback controls designed to keep the system stable under normal operations. Moreover, the effects of possible control actions are difficult to predict, since positive or negative feedback loops may propagate or attenuate or even reverse the effect in an unforeseeable manner. *Unknown side effects* are another source of interactive complexity.

Another system characteristic that makes control difficult is *tight coupling*. Tightly coupled systems are characterised by the absence of "natural" buffers. A change in one component will lead to a rapid and strong change in related components. This implies that disturbances propagate rapidly throughout the system, and there is little opportunity for containing disturbances through improvisation. Tight couplings are sometimes accepted as the price for increased efficiency. For instance, Just-in-time production allows companies to cut inventory costs but makes them more vulnerable if a link in the production chain breaks down. In other cases, tight couplings may be the consequence of restrictions on space and weight. For instance, the technical systems have to be packed more tightly on an offshore platform than on a refinery, and this may make it more challenging to keep fires and explosions from propagating or escalating.

5.3 Organising for coupling and complexity

What we have presented thus far is a two-dimensional typology of socio-technical systems. Perrow used this typology to build an argument that some systems are intractable because they pose an organisational dilemma. The argument can be summarised as follows (see also Table 1):

1. *A system with high interactive complexity can only be effectively controlled by a decentralised organisation*. Highly interactive technologies generate many non-routine tasks. Such tasks are difficult to program or standardise. Therefore, the organisation has to give lower level personnel considerable discretion and encourage direct interaction among lower level personnel.

2. *A system with tight couplings can only be effectively controlled by a highly centralised organisation*. A quick and co-ordinated response is required if a disturbance propagates rapidly throughout the system. This requires centralisation. The means to centralise may, e.g., include programming and drilling of emergency responses. Moreover, a conflict between two activities can quickly develop into a disaster, so activities have to be strictly coordinated to avoid conflicts.

3. If follows from this that *an organisational dilemma arises if a system is characterised by high interactive complexity* ***and*** *tight couplings*. Systems with high interactive complexity can only be effectively controlled by a decentralised organisation, whereas tightly coupled systems can only be effectively controlled by a centralised organisation. Since an organisation cannot be both centralised and decentralised at the same time, systems with high interactive complexity and tight couplings cannot be effectively controlled, no matter how you organise. Your system will be prone to "Normal accidents".

Table 1. Organising for coupling and complexity.

Interactions Coupling	Linear	Complex
Tight	*Centralise to handle tight coupling!*	*Centralise to handle tight couplings AND decentralise to handle unexpected interactions!*
Loose	*Centralise or decentralise! (Both will work.)*	*Decentralise to handle unexpected interactions!*

Perrow applied his theory on the Three Mile Island accident. He concluded that the technology of the Three Mile Island power plant was so interactive and tightly coupled that it created the organisational dilemma described above.

5.4 Implications for risk reduction

According to Perrow, system accidents thus arise from a mismatch between the properties of a system (coupling and complexity) and the organisation controlling the system (centralisation versus decentralisation). The theory points to several risk control strategies:

1. With a complex system, you should try to reduce the degree of interactive complexity.

2. With a tightly coupled system, you should seek ways to loosen the couplings.

3. If you have to live with a high degree of interactive complexity, you should build a decentralised organisation.

4. If you have to live with tight couplings, you should centralise your organisation.

5. If your system has catastrophic potential, and you are not able to apply any of the above strategies, then you should discard your system.

Based on the last strategy, Perrow (1984) argued that some technologies, such as large, complex nuclear power stations and strategic nuclear weapon systems, should be discarded. The safety systems that are supposed to safeguard nuclear reactors create a degree of interactive complexity that may confuse operators and make system disturbances intractable.

5.5 A Normal Accident perspective on the Åsta accident

A few questions derived from Normal Accident theory may help us explore the Åsta accident in its structural context:

1. *Was the system characterised by a high degree of interactive complexity?* Traffic control on a railway system may be complex in the sense that there are many components such as trains, signals and switches. Moreover, the system is highly dynamic – its state changes from minute to minute. However, the interaction among components is largely linear. It is easy to predict what track a train will follow if you know the position of the switches. However, components within the technical systems that control the states of switches and signals may occasionally interact in a more complex manner. Because the electromagnetic relays do not always react instantaneously, a green light may occasionally occur for a second or two when the signal should have been red.

2. *Was the system characterised by tight couplings?* The basic idea of railways involves very tight physical couplings. Trains are confined to rails, and two trains on a collision course have no way to divert from their trajectories at the last moment. Moreover, it may be argued that the absence of effective communication equipment made the system more tightly coupled than it needed to be, since this reduced the scope for improvisation in an emergency.

3. *Was the organisation too centralised to cope with its interactive complexity?* We have argued that railway traffic control is mainly characterised by linear interactions. Linear interactions can, according to Perrow, be effectively controlled by centralised as well as decentralised organisations. The problem with electromagnetic relays is confined to a subsystem, and hardly calls for a decentralised organisation.

4. *Was the organisation too decentralised to cope with its tight couplings?* According to Normal Accident theory, a tightly coupled system such as a railway system can only be effectively controlled by a centralised organisation. However, it is not straightforward to judge exactly the degree of organisational centralisation in railway operations. Centralised Train Control (CTC) by definition implies a high degree of centralisation of traffic control decisions and of the operation of signals and switches. Very detailed rules and procedures also promote centralisation. Moreover, the train movements to a large extent pre-planned. However, once the northbound train had left Rustad station, it operated as an autonomous unit due to the lack of effective communication equipment. Moreover, one may ask whether fragmentation of responsibility among decision levels may have contributed to the slow pace in introducing Automatic Train Control (ATC) on Norwegian Railways.

It is difficult to build a strong argument that the tragic event at Åsta was a clear-cut system accident in Perrow's sense of the word. One might argue that Åsta was a component failure accident, since a single active error was sufficient to trigger a catastrophe. It was known that trains occasionally pass a signal at danger. It was also known that this could lead to a catastrophe on a single-track railway without Automatic Train Control and without effective means for the Traffic Control Centre to detect and recover the error. The problem was not that the defences made the system opaque, but rather that the system lacked adequate defences. On the other hand, one might argue that the absence of effective means for communication between the traffic control centre and the train crew created a mismatch between the tightly coupled technology and an organisation where train crews temporarily operated as autonomous units.

A theory or perspective directs attention to some aspects of an accident, at the expense of others. The Normal Accident perspective does not focus on the absence of barriers designed into the system, such as Automatic Train Control in the case of the Åsta accident. Neither does it focus on the decision processes that led to a railway system that was highly vulnerable with regard to human error, although Perrow is highly aware that some systems remain error-inducing due to the distribution of power and interests among major stakeholders (Perrow, 1986:152f).

5.6 A Normal Accident perspective on the Snorre A blow-out

Is an offshore production platform characterised by tight coupling and high interactive complexity? Most of us would accept that an operative production platform is a tightly coupled system. A lot of equipment handling large amounts of energy is packed into a rather small volume. Barriers thus have to be designed into the system to prevent disturbances from spreading and escalating into major accidents. A centralised organisation is needed to coordinate work in order to prevent jobs from interacting in dangerous ways. The work permit system is an important aspect of this centralised organisation. Moreover, during an emergency, centralised control is necessary to ensure coordinated action to control the situation and, if necessary, evacuate the crew.

Opinions may be more divided when it comes to interactive complexity. Some may argue that the physical processes are well understood, and that the process unit of an offshore installation is much simpler than a petrochemical plant. A well is basically a hole in the earth, enclosed by a casing. Even if there is a considerable amount of piping, valves and control systems on a platform, one might argue that they interact in foreseeable (linear) ways. One may thus be tempted to conclude that the degree of interactive complexity is moderate. As a consequence, an offshore production platform belongs in the upper left cell in Table 1, and the recommendation to centralise to handle tight coupling remains valid. This is in accordance with the perception of the personnel planning the slot recovery operation at Snorre A. They considered the well somewhat complex, but they did not consider the slot recovery operation particularly complex or dangerous (Wackers, 2006).

The Snorre A blow-out demonstrated that a well attached to an offshore platform may display complex interactions. Immediately after the loss of control of Well P-31A, the crew had no means to observe directly what was happening. They had to make inferences based on vague symptoms such as the absence of an expected pressure increase in the mud system at the outset of the pulling of the scab liner and an apparent increase in volume of the reservoir fluid. A volume increase could occur even during a normal pulling operation, and thus did not constitute a compelling sign that something was wrong. Even the first gas alarms did not give strong clues as to what was happening. Only when somebody observed huge amounts of gas emerging through the sea did the crew have sufficient clues to diagnose the situation. Another example of the combination of tight coupling and complex interactions is the potential that gas emerging through the seabed might cause the tension legs in one corner of the platform to become detached from the anchor. This would cause the platform to capsize, possibly leading to damage to the wellheads and several parallel blow-outs.

The impact of tight coupling and complex interactions was also apparent during the recovery phase. The means that the crew needed to control the well were unavailable because of the possible side effects of providing them. Additional supplies of mud could not be delivered, because a vessel approaching the platform could ignite the gas leaking out of the sea. The main power supply, which was needed to force drilling mud into the well, had been shut down due to ignition risk. It is symptomatic of complex interactions that nobody had anticipated that this

situation could occur, despite the effort that goes into analysis of risk and emergency preparedness for an offshore installation.

To summarise, the Snorre A blow-out demonstrated that a system with an apparently moderate degree of interactive complexity may turn dramatically more complex as a result of unexpected events. This suggests that tight coupling and interactive complexity may be more dynamic system properties than implied by Perrow.

5.7 Strengths and limitations of Normal Accident theory

An important contribution of Normal Accident theory was to raise a discussion concerning the limits of safety in complex systems. Normal Accident theory thus inspired a research tradition on High Reliability Organisations, which will be discussed in the following chapter. The controversy following Perrow's book also inspired significant empirical research, for instance Scott D. Sagan's case study of the U.S. strategic nuclear weapons systems during the Cuba crisis (Sagan, 1993).

Perrow also drew attention to the possibility that some technologies may force us to adopt organisational structures and practices that are incompatible with central values in western democracies. In order to attain the degree of centralisation that is required to handle some tightly coupled systems, we may be forced to create work environments characterised by harsh discipline and very little autonomy.

Several objections have been raised against Normal Accident Theory:

- The notions of "interactive complexity" and "tight coupling" are so vague that it is difficult or impossible to subject the theory to empirical tests.
- It is difficult to derive a simple and effective prescription for assessing or monitoring major accident risk from Normal Accident theory, because it is difficult to measure or monitor such attributes as "interactive complexity" or "decentralisation".
- Analysis of recent major accidents suggests that most accidents result from other problems than a mismatch between complexity/coupling and degree of centralisation (Hopkins, 1999).
- Some critics find the suggestion that some technologies should be discarded too pessimistic, too fatalistic, or politically unacceptable.
- The assertion that an organisation cannot be centralised and decentralised at the same time sounds like a tautology. However, this assertion has been challenged by researchers that study so-called High Reliability Organisations (Weick, 1987). We will consider this challenge in the following section.

Some of Perrow's critics seem to assume that Normal Accident theory is only relevant to systems characterised by extreme interactive complexity and tight coupling. However, the theory has important implications for other organisations as well. For instance, Perrow claims that centralised control is necessary to handle a tightly coupled system. This implies that the operation of a major railway system, i.e. a tightly coupled technology, calls for centralised control. In practice, this may imply that the operational rules should be detailed, and not only specify functional requirements on task performance. This implication is neither obvious nor trivial, but it received some support in an interview study among operating personnel on Norwegian railways (Guttormsen et al., 2003).

Perrow's book was written at a time when technical systems were less integrated and competition was less fierce than it is today. We will probably be in a better position to appreciate the significance of his perspective after a few more years of exposure to current technologies and economic climate.

5.8 Further development of Normal Accident theory

Perrow seems to treat coupling and complexity as rather stable properties of sociotechnical systems. However, Weick (1990) argued that these attributes change during periods of crisis or high demand. For instance, the collision between two jumbo-jets at Tenerife airport in 1977 happened on a day when the airport was extremely crowded, it had to handle very large aircraft on a narrow runway, and visibility was poor. At least from the air traffic controllers' point of view, the system must have been more complex and more tightly coupled than on an ordinary day. Moreover, several errors occurred in communication between the tower and the two aircraft involved. Weick argued that these errors caused the system to become even more interactive and tightly coupled. In this way, Weick indicated that Normal Accident theory might be extended from a static, structural theory to a dynamic theory of how several failures can combine into an accident by making a system increasingly difficult to control.

Clarke and Perrow (1996) claimed that plans used to justify increasingly complex systems can impede organisational learning. We will return to this claim in Section 7.4, in the context of failures in information processing.

Many of Perrow's ideas have been adopted by researchers in the Resilience Engineering tradition. However, these researchers tend to be more optimistic about the possibility of controlling tightly coupled systems with complex interactions by means of new analysis methods and new organisational coping strategies. We shall present the Resilience Engineering perspective in Chapter 9.

5.9 The Normal Accident perspective – a summary

The energy-barrier perspective is in principle well suited to capture even multiple failures, however, with the linearity premise of predictability and comprehensibility of the effects of singular failures. The task of identifying the potential organisational contributions to failure is more difficult that it may seem at a first glance, especially when the mix of technological, human and organisational contributions is complex.

Perrow (1984) argued that complex systems are prone to experience a type of complexity that goes beyond what linear models can accommodate. Multiple technological, human and organisational failures, whether being active failures or latent conditions, may interact with each other and produce non-linear effects that no one can anticipate in advance. Moreover, in systems with high *interactive* complexity, unintended side-effects can emerge on the basis of irregular events that cannot even be denoted failures. Feedback loops and even (automatic) safety systems contribute to such interactive complexity. If the system also is tightly coupled, that is, characterised by the absence of "natural" buffers, then disturbances, failures or side-effects may propagate rapidly, contributing even more to complexity and causing an escalation effect. Systems with high interactive complexity *and* tight coupling may thus be "loaded" with a vast array of incomprehensible, multiple, propagating failures or side effects.

Perrow claimed that high interactivity and tight coupling demand two different organisational characteristics, namely decentralized and centralized control, and that organisations cannot

provide both types of control at the same time. Hence, a combination of high interactivity *and* tight coupling must be avoided if the damage potential is large, because the result is that a future accident is "normal" in the sense of being unavoidable in the long run.

Hence, the normal accident perspective deflects the question "what may fail" with the proposition that the multiple, interactive failures that we cannot anticipate in advance will be uncontrollable. With the combination of high interactive complexity and tight coupling, the claim is that something will go (terribly) wrong, even in the absence of single failure accidents.

5.10 Key questions for the applicability of the Normal Accident perspective

- ⇨ Can the protection problem at hand be informed by the possibility of multiple, interacting failures with potential non-linear effects?
- ⇨ Is the system characterised by high interactive complexity that may produce unintended side-effects,
- ⇨ Is the system tightly coupled, and thus susceptible to rapid propagation and escalation of disturbances?
- ⇨ Is the organisation that controls the system through which unintended side-effects may propagate, bound to be centralized or decentralized as a whole?

5.11 References

Clarke, L. and Perrow, C. (1996). Prosaic Organizational Failure. *American Behavioral Scientist, 39* (8) 1040-1056.

Guttormsen, G., Randmæl, S. and Rosness, R. (2003). *Utforming av regelverk for togframføring.* Report STF38 A03408. Trondheim: SINTEF Industrial Management. (Design and formulation of operational rules for railways. In Norwegian.)

Hopkins, A. (1999). The limits of Normal Accident theory. *Safety Science, 32* (2-3), 93-102.

Perrow, C. (1984). *Normal Accidents.* New York: Basic Books.

Perrow, C. (1986). *Complex Organizations. A Critical Essay.* New York: Random House.

Reason, J. 1997: *Managing the Risks of Organizational Accidents*. Ashgate.

Sagan, S. D. (1993). *The limits to safety. Organizations, accidents, and nuclear weapons.* Princeton, New, Jersey: Princeton University Press.

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review, 29,* (2) 112-127.

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management, 16* (3), 571-593.

Woods, D. D. (1990). Risk and human performance: Measuring the potential for disaster. *Reliability Engineering and System Safety, 29,* 387- 405.

5.12 New references

Cohen, M., March, J. and Olsen, J. (1988). A garbage can model of organisational choice. In March, J. (Ed.). *Decisions and Organisations*. Oxford: Blackwell, 294-334.

LaPorte, T.R. and Rochlin, G. (1994). A Rejoinder to Perrow. *Journal of Contingencies and Crisis Management, 2,* (4), 221-227.

Perrow, C. (1994). The limits of safety: the enhancement of a theory of accidents. *Journal of Contingencies and Crisis Management, 4,* (2), 212-220.

Perrow, C. (2007). *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters.* New Jersey: Princeton University Press.

6 Organisational redundancy and spontaneous reconfiguration: The theory of High Reliability Organisations

6.1 "Working in practice but not in theory"

The previous chapter concluded in a pessimistic vein. Perrow claimed that highly interactive and tightly coupled technologies pose an intractable control problem. It is impossible to design an organisation, which is sufficiently decentralised to handle the interactive complexity, and at the same time sufficiently centralised to handle the tight coupling. This conclusion was challenged by a group of researchers who studied so-called High Reliability Organisations (HROs). Certain systems, such as aircraft carriers, nuclear submarines, air traffic control systems and nuclear power plants are only of benefit to society if they manage to deliver nearly failure-free performance (LaPorte and Consolini, 1991). At the same time, these organisations handle complex, demanding technologies and have to meet periods of very high peak demand.

The basic claim of this research tradition is conveyed in the title of a paper by LaPorte and Consolini (1991): *"Working in practice but not in theory".* They claimed that some systems, which, according to Normal Accident theory, should be haunted by major accidents and not even able to produce anything useful, in fact do amazingly well. For instance, the conditions to be handled by the crew of an aircraft carrier was summarised as follows by a senior officer (Rochlin et al., 1987):

> So you want to understand an aircraft carrier? Well, just imagine that it's a busy day, and you shrink San Francisco Airport to only one short runway and one ramp and gate. Make planes take off and land at the same time, at half the present time interval, rock the runway from side to side, and require that everyone who leaves in the morning returns that same day. Make sure the equipment is so close to the edge of the envelope that it's fragile. Then turn off the radar to avoid detection, impose strict controls on radios, fuel the aircraft in place with their engines running, put an enemy in the air, and scatter live bombs and rockets around. Now wet the whole thing down with salt water and oil, and man it with 20-year-olds, half of whom have never seen an airplane close-up. Oh, and by the way, try not to kill anyone.

Given the inherent hazards, the complexity and tight couplings of this system, the safety records are remarkable according to HRO theorists. "For a deployment period of six months there will typically be over 10000 arrested landings with no accidents. Over 600 daily aircraft movements across potions of the deck are likely with a "Crunch rate"- i.e. the number of times two aircraft touch each other- of about 1 in 7000 moves". (LaPorte and Consolini, 1991: p. 21). The research challenge was not to explain why accidents occurred, but rather to explain *why so few serious accidents occurred*.

It is outside the scope of this report to evaluate the claims concerning the safety records of the HROs. We will concentrate on how HRO researchers explain excellent safety performance and on the relevance of this research for less exotic activities.

6.2 Organisational redundancy as a means to build fault tolerant organisations

Engineers are sometimes confronted with the task of building a reliable system from less reliable components. They achieve this by building in redundancy, i.e. but including extra (i.e. redundant) components that can take over in case a critical fails. Thus the braking system of a car comprises two separate hydraulic circuits, although a single circuit could do the job perfectly well. LaPorte

and Consolini (1991) found that the HROs used the principle of redundancy to derive highly reliable performance from less than perfect human beings. The organisation had its share of errors and deviations, but unlike less reliable organisations, it was able to correct the errors immediately. The crew members had overlapping tasks and competence. They had eye-to-eye contact and could easily communicate with each other. They were thus able to spot each other's slips and mistakes, and the culture supported intervention to recover the errors. For these reasons, nearly all critical errors were recovered.

Rosness et al. (2000) termed this error recovery capability "organisational redundancy".[21] They proposed that organisational redundancy depends on (1) structural/instrumental preconditions and (2) cultural preconditions (Figure 5). The *structural/instrumental dimension* of organisational redundancy concerns the personnel's possibility of direct observation of each other's work, overlapping competence, and overlapping tasks or responsibilities. Roberts (1989) and Bierly and Spender (1995) noted that HROs devote much attention to the development and maintenance of individual and collective competence. Some organisations build structural robustness by distributing veto powers, particularly in situations where inaction is a safer state than action (Schulman, 1993). Another important aspect of this dimension is the diversity and quality of communication channels. Weick (1987) argued that rich communication, for instance face-to-face discussion, is in general more powerful in promoting reliability in a complex system than sparse communication such as formal written messages.[22]

The *cultural dimension* of organisational redundancy concerns the capability and willingness to exchange information, provide feedback, reconsider decisions made by oneself and colleagues, and intervene to recover erroneous actions. LaPorte and Consolini (1991: 29) observed apparently contradictory production-enhancing and error-reducing activities in HROs. People reported errors without encouraging a lax attitude toward the commission of errors. They took initiatives to identify and improve flaws in Standard Operating Procedures. Error avoidance was achieved without stifling initiative or operator rigidity. People monitored each other's performance without counterproductive loss of operator confidence, autonomy and trust. In critical situations the crew gave each others orders and instructions independent of the military rank.

[21] Rosness et al. proposed the following definition of organisational redundancy: "By 'organisational redundancy' we refer to *co-operation patterns that allow the organisation as a whole to perform more reliably than each individual operator."*

[22] There are, however, some situations where restrictions and standardisation may be necessary to prevent critical misinterpretation, e.g. in communication between pilots and Air Traffic Control operators.

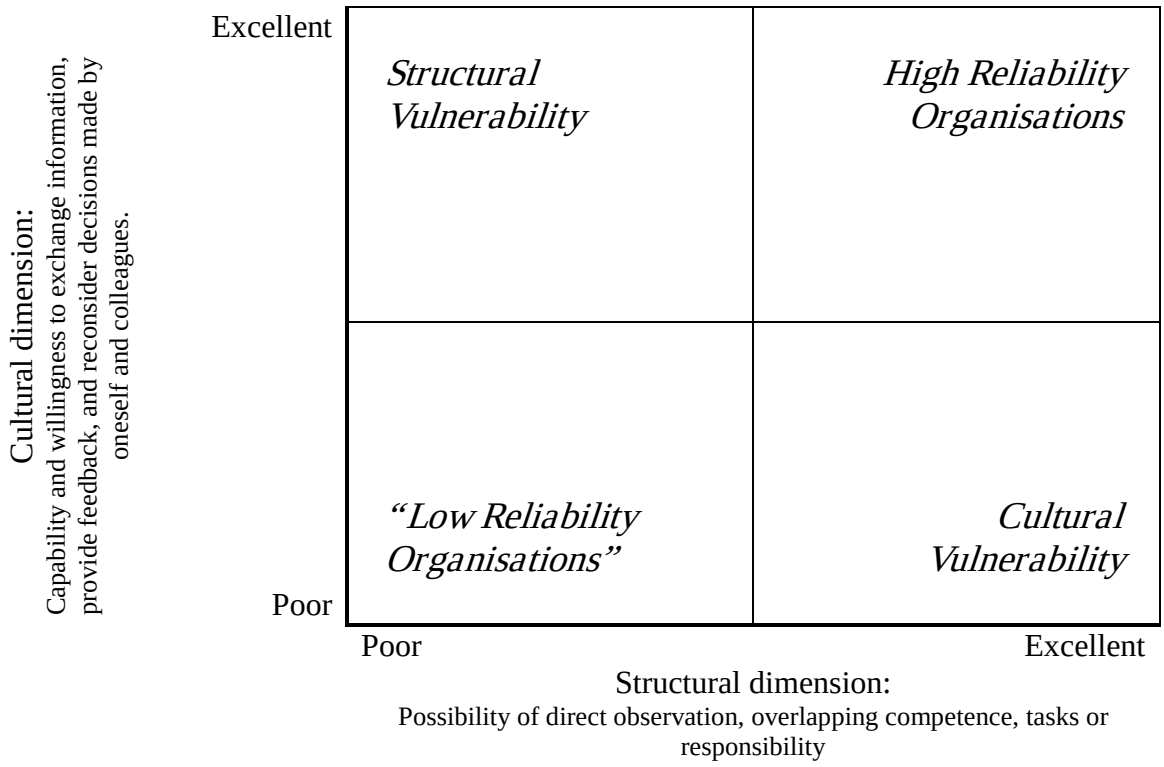

Figure 5. The two dimensions of organisational redundancy.

6.3 Spontaneous reconfiguration of the organisation

LaPorte and Consolini (1991) demonstrated another important aspect of HROs, which Perrow had not paid attention to. HROs are able to reconfigure spontaneously in during demanding operating situations and crisis. The aircraft carrier had a traditionally military system with commando lines clearly defined. But in situations with peak demand, the HRO changed into a more flexible and resilient pattern. Informal authority was granted on the basis of competence rather than rank. Interaction style became informal. In an air traffic control centre, controllers may even change the distribution of tasks and their physical location in the control room. For instance, extra personnel may join operators with particularly demanding tasks in order to provide "an extra pair of eyes".

Situational factors are well known in organisational theory. Burns and Stalker (1961) demonstrated that a hierarchy could be efficient during stable and predictable conditions, but inefficient under dynamic and changing condition. Bolman and Deal (1986) provide an example of a commando group during World War 2. Needless to say, these operations carried out behind enemy line were risky. On the other hand, these groups tried to avoid direct confrontation and therefore minimise the interactions with the enemy. The most successful commando unit during the allied operations, was very participate and involving all the members when planning the mission. The best suggestion was sought after. However, during the operations the commanding officer was the one handling all the decisions and had the right and duty to improvise when needed. One of the main points of Bolman and Deal (1986) is that organisations must be understood and managed by the combination of different perspectives and frameworks.

6.4 Culture as a means to build organisations that are both centralised and decentralised

A central claim in Perrow's theory of normal accidents is that an organisation cannot be centralised and decentralised at the same time. This is the reason why interactive and tightly coupled organisations create an irresolvable dilemma, see Section 5.3, p. 48. Weick (1987) challenged this claim. He argued that culture can impose a high degree of order and predictability in an organisation, and thus substitute formal means of centralisation such as a tight control structure or detailed operating procedures. Weick suggested that story-telling is one of the most important means for culture co-ordination, since natural language is a far richer means of communication than formal procedures, accident report forms, or statistics.

6.5 The notion of "mindfulness"

Weick and Sutcliffe (2001) introduced the notion of "mindfulness" to capture prominent characteristics of HROs. They state that HROs accept the fact of failures, that there is no perfection of zero errors. If errors are inevitable, the organisation needs to develop skills to detect errors and to contain these errors at early stages. Weick and Sutcliffe also emphasise the willingness of people to revise their own expectations. The idea of mindfulness is the equivalent of continuous surveillance of the existing situation based on expectations, updating these expectations based on new experiences and willingness and capability to invent new expectations. Mindfulness concerns detection and containment of unexpected events that could appear everywhere in the organisation.

Weick and Sutcliffe identified five elements that characterised mindfulness. These elements are organised under two tittles: *Anticipation and awareness of the unexpected* and *Contain the unexpected*, see Table 2.

Table 2. Elements of "Mindfulness". Summarised from Weick and Sutcliffe (2001)

Anticipation and awareness of the unexpected	**Description**
Preoccupation with failure	People in HROs know that all potential failures modes have not been experienced or exhaustively deduced. Because the cost of the failure is so high, people in HROs look for symptoms and encourage reporting of errors.
Reluctance to simplify interpretations	Simplify less and see more. Simplifications could produce blind spots, HROs use people that represent different functional background to expand the organisation's sensing mechanisms.
Sensitivity to operations	Normal operations can reveal deficiencies – free lessons could be learned. This allows early problem detection before problems become too substantial.
Contain the unexpected	**Description**
Commitment to resilience	HROs are not error free, but errors do not disable the system. People in HROs with varied experience come together as the situation demands, it increases the knowledge and actions can be brought to solve the problem
Defence to expertise	Decisions are made in the front line. Decisions migrate to the persons with experience and expertise to solve the problem.

Weick and Sutcliffe present "mindfulness" as a more or less universal cluster of features characterising HROs. They give little attention to the possibility that the means to achieve high

reliability may depend on factors such as the properties of their technology, as suggested by Normal Accident Theory.

6.6 Implications for risk reduction

Weick and Sutcliffe (2001) proposed a broad set of practices to develop mindfulness. The following are examples of practices that aim to *enhance awareness and anticipation to detect the unforeseen:*

- Leaders help employees to cope with conflicts, preserving a balance of values.
- Restate goals in the form of things that should not happen. This will provide more focus on the unexpected, disconfirming expectations and on issues of reliability.
- Remember that mindfulness takes effort. It is difficult to pay more attention to failures than to success. Look at failures, assume nothing, look closely at the work involved in the problem, brainstorm a resilient response, and pinpoint the expert in handling the problem rather the person accountable for the problem.
- Create awareness of vulnerability. What is risky around here? People need to worry about vulnerability as this increases opportunities for learning, commitment to reliability and accepting the fact at even though the system is understood, it can fail.
- Present mistakes as opportunities for enlarged learning and deeper understanding.
- Create an "error friendly" learning culture, by promoting behaviours such as seeking feedback, sharing information, asking for help and talking about errors.
- Encourage alternative frames of reference, strengthen fantasy.
- Communicate, promote scepticism, seek out bad news, test your expectations.
- Welcome uncertainty, treat all unexpected events as information and share them.

A second set of practices concerns *containment once the problem is evident:*

- Ambivalence builds resilience. Begin to contain the event by doing what experience tells you but watch for what you have not seen before and deal with it immediately.
- Use rich communication media, e.g. face to face communication rather than e-mails. Make sure that everyone's voice is heard.
- Think out publicly when you question your categories, spot limitations and see new features of the context.
- Enlarge competencies and responses repertoires, then people will be able to see more hazards.
- Create flexible decision structures, let the problem migrate to the people who have the most expertise to deal with the problem.
- Accelerate feedback so the initial effect of the attempted improvisations can be detected quickly and the action altered or abandoned if the effects are making things worse
- Balance centralisation with decentralization, maintain local and centralized capacity for detection of problems this will enhance awareness in the organisation.

A more comprehensive description of these practices is found in Weick and Sutcliffe (2001:159ff).

6.7 HRO theory and the Åsta accident

But how can the Åsta accident be seen in an HRO theory? One of the issues that were discussed following the Åsta accident was whether the departure procedure for trains should formalise double-checking of the exit signal at stations. Until 1997, the departure procedure stated that the train driver and the main conductor has to check independently that the train has received a green exit signal before it starts after a stop on a station. This was an attempt to build organisational

redundancy. From 1997, the procedure was changed, so that this responsibility was only assigned to the train driver. This change was implemented by the Norwegian National Railway Administration and by the Norwegian State Railways even though the Norwegian Railway Inspection Authority refused to accept the change. In spring 2001, the Norwegian National Railway Administration decided to revert to a departure procedure that involves double-checking of the exit signal.

As an aside, we may note that before Centralised Train Control system was installed on the Røros line, traffic control was based on an old-fashioned, manual system. The railway section between two stations was reserved for a specific train by an exchange of telegraph signals between the two stations. When the train had passed the section, a new exchange of telegraph signal served to release the section, so that it could be reserved for another train. A detailed human reliability analysis of this apparently antiquated system has shown that extensive organisational redundancy was built into the procedures.[23] For instance, the train drivers would know in advance on what station they had to wait for a meeting train. They would thus refuse to start the train if the station personnel erroneously gave them permission to leave a station before the meeting train had arrived. This illustrates that organisational redundancy is not restricted to high-tech systems. Moreover, it shows that organisational redundancy can in some cases be highly formalised. The success of this system is attested by the fact that catastrophic train collisions were very rare events, even when fallible humans had to carry out tasks that are now performed by failsafe interlock systems.

6.8 HRO theory and the Snorre A blow-out

The crew of the Snorre A platform managed to control well P-31A despite overwhelming difficulties. Can HRO theory help us explain their success?

The accounts that we have reviewed do not discuss *organisational redundancy* during the recovery phase explicitly. However, it appears that the situation was analysed and critical decisions made in a setting where the available expertise on the platform and in the emergency group onshore would have a fair opportunity to challenge inadequate reasoning. It also appears that the logic of pro-active management would encourage the emergency management group to challenge too optimistic evaluations of the situation and unrealistic assessments of the effects of the proposed countermeasures.

A *reconfiguration of the organisation* took place once the emergency management was mobilised. This reconfiguration involved a decentralisation in the sense that the onshore organisation submitted their authority to make decisions and commit resources to the platform manager. This moved decision authority to the sharp end, i.e. close to the sources of hazard. Another aspect of decentralisation was that the platform crew improvised an action plan in a situation that was not covered by emergency plans or procedures. At the same time, the platform crew maintained the degree of centralisation necessary to respond to the crisis in a coordinated manner.

Did an absence of organisational redundancy contribute to the deficiencies in the planning of the slot recovery operation? The reports that we have reviewed do not provide any firm evidence on this issue. A risk review meeting at the conclusion of the planning process was cancelled because the drilling rig was available for the slot recovery operation earlier than expected. Such a meeting might in principle have provided organisational redundancy, as the participants might have

[23] This claim is based on an Action Error Mode Analysis performed by SINTEF and the Norwegian National Railway Administration.

detected some of the problems that led to the blow-out. However, this possibility remains hypothetical.

6.9 Normal Accident theory versus High Reliability Organisations

HRO theory emerged partly as a response to Perrow's pessimistic view on the feasibility of reliably operating highly interactive and tightly coupled technologies. Sagan (1993) summarised the contrasting position as shown in Table 3.

Table 3. Competing perspectives on safety with hazardous technologies. Adapted from Sagan (1993:46).

High Reliability Theory	Normal Accidents theory
Accidents can be prevented through good organisational design and management.	Accidents are inevitable in complex and tightly coupled systems.
Safety is the priority organizational objective.	Safety is one of a number of competing objectives.
Redundancy enhances safety: Duplication and overlap can make "reliable systems out of unreliable parts."	Redundancy often causes accidents: it increases interactive complexity and encourages risk-taking.
Decentralised decision-making is needed to permit prompt and flexible field-level responses to surprises.	Organizational contradiction: Decentralization is needed for complexity, but centralization is needed for tightly coupled systems.
A "culture of reliability" will enhance safety by encouraging uniform and appropriate responses by field-level operators.	A military model of intense discipline, socialisation, and isolation is incompatible with democratic values.
Continuous operations, training, and simulations can create and maintain high reliability organizations.	Organizations cannot train for unimagined, highly dangerous, or politically unpalatable operations.
Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.	Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts.

In an attempt to validate the conflicting claims of Normal Accident theory and HRO theory, Sagan (1993) examined the operations of the U.S. nuclear forces during the Cuba crisis. This case was selected because the public safety records of the U.S. nuclear forces were excellent, the Defence Department claimed that risk accidentally releasing a nuclear attack was virtually zero. The idea was to submit Normal Accident theory to the "tough test". Through his investigations, Sagan discovered several serious incidents. These incidents revealed the types of problems that Perrow claimed would haunt highly interactive and complex systems (see the right column in Table 3). He found that extreme discipline could "encourage excessive loyalty and secrecy, disdain for outside expertise, and in some cases cover-ups of safety problems, in order to protect the reputation of the institution" (p. 254). Although the official commitment to avoiding mistakes, miscalculations or misunderstanding was very clear, lower level decisions repeatedly reflected other priorities, such as the maximisation of military preparedness. Sagan was particularly concerned that organisational learning can be constrained by the strong disincentives against exposing serious failures.

Rasmussen (1994a) argued that Normal Accident theory and HRO theory may be more compatible than Sagan's analysis suggests. Perrow did not claim that redundancy should be avoided, and HRO researchers did not claim that HROs never fail. Rasmussen noted that redundancy is difficult to manage, and that recent large-scale accidents were caused by systematically letting the system drift outside the design envelope. The willingness to pay for

redundancy directed at very rare events might decline dramatically in periods of high competitive pressure. However, redundancy is essential for the operation of high hazard systems. It is not feasible to eliminate human errors. Over time, operators will explore the boundaries of safe operations, either deliberately or inadvertently.[24] Moreover, an organisation *needs* a certain frequency of reports on failures and incidents in order to validate the design assumptions and risk predictions and to support risk management. It is thus difficult to see how a high hazard system can be managed without redundancy.

There is another contrast between Normal Accident Theory and HRO theory, which has received little attention. Proponents of HRO theory tend to assume that a single set of mechanisms can account for organisational reliability, across differences in technology, processes and organisational environments. In contrast, Normal Accident Theory postulates that the means to achieve reliable performance depend on the properties of the socio-technical systems: Systems with complex interactions call for decentralised control, whereas tightly coupled systems call for centralised control. We are not aware of empirical work directed at this issue.

6.10 Strengths and limitations of HRO theory

An important contribution of HRO theory is to direct attention to organisations with remarkable safety records and provide new insights into the functioning of these organisations. The dominating research approach is case studies of a single organisation or a few organisations. This approach does not allow researchers to isolate causal factors in the manner of a laboratory experiment.[25] However, we believe that a case study approach is the only feasible way to study complex patterns of organisational functioning in depth.

Most of the "classical" studies in the HRO tradition was directed at military organisations (aircraft carriers, nuclear submarines) or organisations that are strongly influenced by military culture (nuclear power plants[26], air traffic control). The discipline associated with some of these organisations would be unacceptable in Scandinavian work environments. It is necessary to ask whether the performance of HRO requires a culture characterised by military discipline. An alternative hypothesis is that organisations can build redundancy and received highly reliable performance in different ways. Preliminary results reported by Rosness et al. (2000) suggest that some offshore production platforms may have built a considerable degree of organisational redundancy. It is also an interesting issue whether the rapid turnover of personnel on aircraft carriers is an advantage or a disadvantage with regard to establishing a culture of high reliability.

HRO refers to organisational practices and not just mindsets of individuals (Hopkins, 2008:144f.). It is not possible to build an HRO culture through attitude change campaigns or behavioural training alone. People in HROs report errors and take initiatives to improve flawed procedures because they expect these actions to lead to improvements. HRO theory thus does not provide an inexpensive alternative to continuous improvements of technology and working practice.

Rosness et al. (2000) suggested that concepts from HRO theory may help us understand how downsizing processes and low staffing levels may influence the safety performance of an

[24] In Section 7.2 we will discuss how systems tend to drift toward the boundary of acceptable performance when faced with conflicting objectives.
[25] Showing that an organisation with safety performance has characteristic X (e.g. extensive organisational redundancy) does not constitute a proof that characteristic X is the *cause* of the excellent safety performance. However, even case studies may be used for hypothesis testing (Yin, 1994). Sagan's (1993) is an example of a hypothesis testing case study.
[26] U.S: nuclear power plants were to large extent staffed by personnel with a navy background (former nuclear submarine crews).

organisation. Too low staff levels may remove the instrumental conditions for building organisational redundancy. Outsourcing might threaten the cultural preconditions for organisational redundancy, since personnel from different organisations might lack the mutual trust and openness necessary to consult, check and correct each other.

6.11 The HRO perspective – a summary

While the previous perspectives aim to explain why accidents occur, the HRO perspective is founded on a research tradition that seeks to explain why so *few* serious accidents actually occur, especially in certain complex systems that operate under demanding circumstances where other perspectives, say, NAT, directs the expectations in a more pessimistic vein.

One way of explaining such success is to use the more technical discipline of reliability engineering as a metaphor for organisational resistance to and recovery from error. As reliability engineering is about building a reliable system from unreliable components, the key word is redundancy. Organisational redundancy means that organisations have sufficient (redundant) resources in order to correct and compensate for improper conduct of "imperfect", failure-prone human beings. Such a redundancy requires both a *structural* dimension in terms of the personnel's possibility of direct observations of their colleagues, and a *cultural* dimension in terms of the conditions for dialogic intervention and improvement of behaviors as well as procedures.

Opposing Perrow's rather rigid argument of organisations being either centralized or decentralized, the HRO perspective maintains that organisations may be many things at the same time, and that spontaneous reconfigurations in response to to critical situations may be observed empirically. E.g., Weick (1987) argued that culture can impose a high degree of order and predictability, and thus substitute formal (technically articulated) means of centralization. Cultural co-ordination can stem, e.g., from storytelling (narratives).

Recent contributions (e.g., Weick and Sutcliffe, 2007) suggests *mindfulness* as a notion to capture the prominent characteristics of HROs, based on the premise that errors are inevitable. Hence, the HRO needs to develop skills to detect and contain errors at an early stage. A main issue thus becomes the ability to revise expectations, and to maintain a continuous focus on anticipation and awareness of the unexpected, as well as the capability of containing the unexpected once the problem is evidenced.

6.12 Key questions for the applicability of the HRO perspective

- ⇨ Is it interesting to investigate and strengthen the organisation's (assumed[27]) ability to cope with circumstances that "normally" may lead to accidents?
- ⇨ Is the organisation able to defend the use of redundant resources over a sustained period of time?
- ⇨ Is the organisation able and willing to invest in structural and cultural flexibility, capabilities and skills (that is, beyond the technical approach of routines/procedures)?
- ⇨ Is the organisation able and willing to invest in anticipation and containment skills, including extensive training?

[27] Such an assumption must be based on a realistic intention, that is, acknowledging that HRO capabilities do not come for free

6.13 References

Bolman, L.G. and Deal, T.E. (1986). *Modern approaches to understanding and managing organizations.* San Francisco: Jossey-Bass.

Burns, T. R. and G. M. Stalker (1961). *The Management of Innovations*. London: Tavistock.

LaPorte, T. R. and Consolini, P.M. (1991). Working in practice but not in theory: Theoretical challenges of "High-Reliability Organisations". *Journal of Public Administration Research and Theory, 1,* 19-47.

Rasmussen, J. (1994a). High Reliability Organizations, Normal Accidents, and other dimensions of a risk management problem. Paper. *NATO Advanced Research Workshop on Nuclear Arms Safety.* Oxford, UK, August 1994.

Rochlin, G. I., LaPorte, T. and Roberts, K. H. (1987). The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review 40*(4), 76-90. Also available on the Internet site:
http://www.nwc.navy.mil/press/review/1998/summer/art7su98.htm

Rosness, R., Håkonsen, G., Steiro, T. and Tinmannsvik, R.K. (2000). The vulnerable robustness of High Reliability Organisations: A case study report from an offshore oil production platform. Paper presented at the 18th ESReDA seminar *Risk Management and Human Reliability in Social Context.* Karlstad, Sweden, June 15-16, 2000.

Sagan, S. D. (1993). *The limits to safety. Organizations, accidents, and nuclear weapons.* Princeton, New, Jersey: Princeton University Press.

Schulman, P. R. (1993). The negotiated order of organizational reliability. *Administration & Society, 25* (3), 353-372.

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review, 29,* (2) 112-127.

Weick, K.E. and Sutcliffe, K.M. (2001). *Managing the Unexpected.* San Francisco: Jossey-Bass.

6.14 New references

Hopkins, A. (2008). *Failure to Learn. The BP Texas City Refinery disaster.* Sydney: CCH.

Hopkins, A., ed. (2009). *Learning from High Reliability Organisations*. Sydney: CCH.

Marais, K., Dulac, N. and Leveson, N. (..). Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems. Paper presented at the *Engineering Systems Division Symposium,* MIT, Cambridge, MA, March 29-31.

Roberts, K.H. (1993). *New Challenges in Understanding Organizations.* New York: Macmillan Publishing Company.

Roe, E. and Schulman, P.R. (2008). *High Reliability Management. Operating on the Edge.* Stanford, California: Stanford Business Books.

Weick, K.E. (2001). *Making sense of the organization*. Oxford: Blackwell.

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the unexpected: Resilient Performance in an Age of Uncertainty.* San Francisco: Jossey-Bass.

Weick, K.E. (2009). *Making sense of the organization, volume 2: The impermanent organization*. Oxford: Blackwell.

7 Accidents as a breakdown in the flow of information: Turner's theory of Man-made Disasters

Most major disasters are perceived as "fundamental surprises" by the media as well as by the organisations involved. However, several precursors or warnings are nearly always identified on hindsight by the media or accident investigators. This paradox is at the heart of Barry Turner's theory of man-made disasters (Turner, 1978; Turner and Pidgeon, 1997; Pidgeon and O'Leary, 2000).

The essence of Turner's information processing framework is that a disaster is almost always associated with recognition of a disruption or collapse of the existing cultural beliefs and norms about hazards. In seeking for a theory of disaster, Turner find himself concerned, not merely with systems of physical events. He is concerned with a larger system which includes not only physical events, but also the perception of these events by individuals.

7.1 Notion of root causes and immediate causation

In developing his theory, Turner used reports from 84 accidents, which he systematically studied. The theory thus reflects recurring findings in the material he studied. He studied three serious accidents in depth in order to elaborate the theory (Turner and Pidgeon, 1979:42). These accidents were a landslide in Aberfan in 1966, a collision where a large road transporter was hit by a train at a railway crossing at Hixon 1968, and a fire in a holiday leisure complex at Isle of Man in 1973. A common feature of these three accidents was that a large and complex safety problem was dealt with by a number of groups operating in separate organisations, and in separate divisions within organisations. They could thus be considered organisational accidents.

The Man-made Disaster model proposes that accidents or disasters develop through a long chain of events, leading back to root causes such as lack of information flow and misperception among individuals and groups. Chains of discrepant events develop and accumulate unnoticed. This, Turner agues, is a result of a culture where information and interpretations of hazard signals fail. Erroneous assumption about the hazards can lead to the acceptance of informal norms that do not comply with existing regulations, and thus to violations of these regulations. Disaster development should be viewed as a process, often over years, developing from an interaction between the human and organisational arrangements of the socio- technical systems.

Based on these considerations, Turner proposes a narrow definition of accidents (Turner and Pidgeon, 1997:70). He considers this more limited kind of disaster as "an event, concentrated in time and space, which threatens a society or a relatively self-sufficient subdivision of society with major unwanted consequences as a result of the collapse of precautions which had hitherto been culturally accepted as adequate".

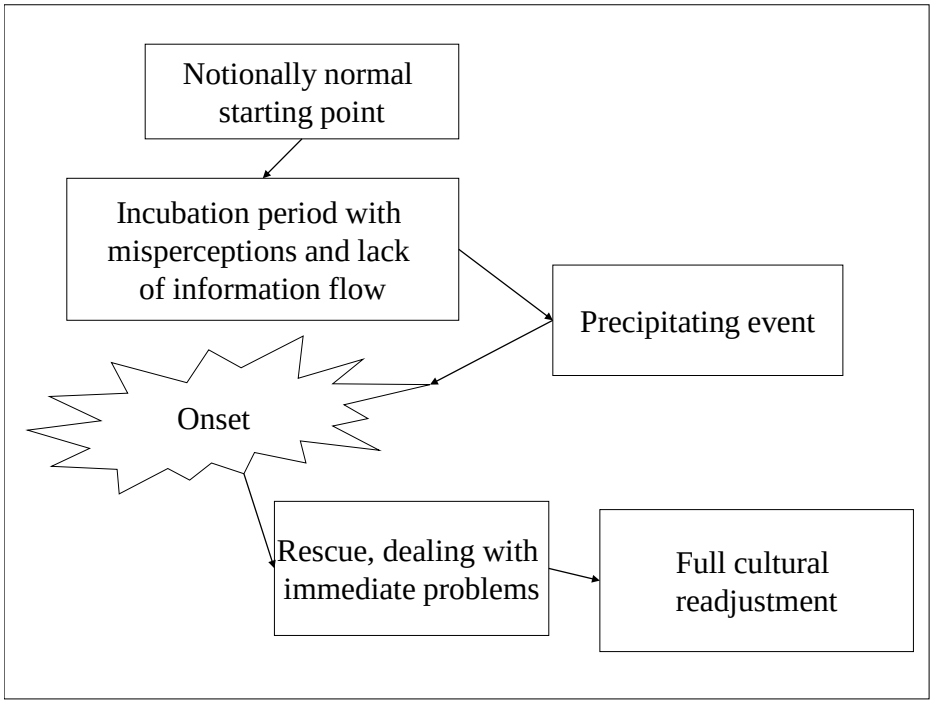

Figure 6. Main stages in the Man Made Disaster model of Turner (1978; Turner and Pidgeon (1997).

7.2 The main stages in the Man-made Disaster model

Turner is not so concerned about immediate causation, but he emphasises the breakdown in the flow and interpretation of information, which is linked to the energy or physical events. The critical assumptions in his theory concern the process leading up to disasters. However, the Man-made Disaster model also includes stages after the actual disaster, including rescue and a final stage of full cultural readjustment to the surprise associated with the event. The whole model comprises six stages (Figure 6):

The starting point of the model is a situation where matters are reasonably 'normal' (Turner and Pidgeon, 1997:71). This implies that the set of culturally held beliefs about the world and its hazards are sufficiently accurate to enable individuals and groups to survive successfully. Individuals and groups adhere to a set of normative prescriptions, ranging from informal norms to laws and regulations, which are culturally accepted as being advisable and necessary precautions to keep risks at an acceptable level.

The second stage, the incubation period, is characterised by the accumulation of an unnoticed set of events that are at odds with the accepted beliefs about the hazards and the norms for their avoidance (p. 72). The incubation period starts with rigidities of belief and misperception of danger signals; events happen unnoticed or are misunderstood. Events may also go unnoticed or be misunderstood because of a reluctance to fear the worst outcome (p. 87). An important factor in this stage is the structure of communication networks (p. 89-92), in particular the boundaries where knowledge is not shared or where it is distorted or simplified. If someone takes action to the signals, it often results in what Turner label "the decoy phenomenon". This is action taken to deal with a perceived problem which, on hindsight, is found to distract the attention from the problems that actually cause trouble. In many cases the company disregards complaints from

outsiders and fails to disseminate and analyse pertinent information. At the same time, the situation is not getting better when individuals often become insecure because of "out of date"-regulations and procedures. This makes the situation even more ambiguous, and may cause violations of formal rules and regulations to be accepted as normal.

The incubation period is brought to conclusion by a precipitating event which in a compelling manner reveals the inadequacy of the beliefs about risks that developed during the incubation period. A dramatic event, such as an explosion or a burning building, creates a large-scale disruption of cultural expectations. The precipitating event is by definition unpredictable for those sharing the culturally accepted beliefs about the system.

The precipitating event is followed by the onset, i.e. the stage when the direct and unanticipated consequences of the failure occur. The onset, which Turner offers very little attention, is followed by the rescue and salvage stage. This is also the first stage of cultural readjustment to the precipitating event (Turner and Pidgeon, 1997:77). Involved persons and onlookers make rapid and ad hoc redefinitions of the situation. However, the circumstances during the rescue and salvage stage do not allow for prolonged analyses or comprehensive revision of beliefs.

A full cultural readjustment takes place in the last phase of Turner's model. An inquiry or assessment is carried out, and precautionary norms are adjusted to fit the newly gained understanding of the world (p. 72). The inquiry may reveal errors and breaches of good practice that did not contribute to the particular accident, but which might contribute to future accidents. The outcome of the final stage is thus the establishment of a new level of precautions and expectations.

7.3 Cultures with requisite imagination

Ron Westrum's (1993) notion of cultures with requisite imagination nicely complements Turner's theory of Man-Made disasters. The expression "requisite imagination" is a paraphrase of Ashby's notion of "requisite variety". In its most compressed form, the law of requisite variety states that "only variety can destroy variety" (Ashby, 1981: 106). For an organisation to gain control over system it must be able to take as many distinct actions as the observed system can exhibit.

Westrum notes that organisations are very different in their ability to react to problems. He proposes the following key criterion of successful information flow in organisations (1993: 402):

> The organization is able to make use of information, observations or ideas wherever they exist within the system, without regard for the location or status of the person or group having such information, observations or ideas.

The variety in how organisations treat information is summarised in the typology shown in Figure 7. According to this typology, pathological organisations actively suppress warning, innovations and bridging, whereas these are actively promoted in generative organisations. Westrum cites several examples of projects where undesirable outcomes can be related to suppression of information.[28]

[28] An extended version of Westrum's typology is included in the TRIPOD safety management scheme, which was devised by researchers at The University of Leiden and the University of Manchester, and in the closely related "Heart and Minds" safety management scheme implemented by Shell International. The extended version includes five categories of organisations: pathological, reactive, calculative, proactive and generative.

Figure 7. A typology of how organisations treat information. Adapted from Westrum (1993).

Pathological	Bureaucratic	Generative
Don't want to know	May not find out	Actively seek information
Messengers are shot	Listened to if they arrive	Messengers are trained
Responsibility is shirked	Responsibility is compartmentalized	Responsibility is shared
Bridging is discouraged	Bridging is allowed but neglected	Bridging is rewarded
Failure is punished or covered up	Organization is just and merciful	Inquiry and redirection
New ideas are actively crushed	New ideas present problems	New ideas are welcome

7.4 Emergency plans as fantasy documents

Can an emergency plan contribute to misperception of danger signals? Clarke and Perrow (1996) claimed that organisational planning can produce "fantasy documents" which an organisation can come to believe in, to the extent that they ignore the bulk of experience showing that these fantasy documents may be inaccurate. They backed their claim by a study of an evacuation plan devised by the Long Island Lighting Company (LILCO). The plan should ensure rapid evacuation of a major area of Long Island in case of a catastrophe at the Shoreham Nuclear Power Station. Parts of the plan were put to test through a series of real-time exercises. The most extensive test was judged a success by LILCO itself as well as by the Federal Emergency Agency, whereas a three-judge panel threw the quality of the emergency organisation's preparations into doubt. Clarke and Perrow shared the latter view, and listed several rather serious problems that occurred during the exercise. They argued that the failure was not due to problems specific to LILCO, such as incompetent management, lack of preparation and expertise or lack of commitment. Rather, they launched a more general claim that *plans used to justify increasingly complex systems are often wildly unrealistic and they can impede organisational learning*. There is often no relevant historical record that may function as a reality check. Many accidents may not be covered by the plan. The plans are designed to be maximally persuasive to regulators, lawmakers and opponents of the system, and therefore tend to make benign assumptions about the environment. A bureaucratic emergency organisation with long lines of communication and excessive spans of control[29] may look impressive on the paper, but is not likely to produce an effective response in an emergency.

Clarke and Perrow claimed that such "fantasy documents" normalise the danger associated with complex, highly interactive systems by allowing organisations to claim that the problems are under control. This claim provides a possible link between the Normal Accident perspective and the information processing perspective on organisational accidents.

[29] "Span of control" refers to the number of subordinates that a superior is responsible for, as well as the variety of functions those subordinates must fulfil (Clarke and Perrow, 1996). Large spans of control (e.g. 10 – 20 subordinates) can be acceptable in routine jobs that are easily monitored, of similar function, and not interdependent.

7.5 Risk control strategies

Turner also proposed some strategies to control risk and prevent disasters. First, Turner stresses the significance of information flow when discussing risk control. It is important to be aware of some usual phenomena in organisations:

1) *Completely unknown prior information:* Where the information which foretells disaster is completely unknown, it is clear that there is little that can be done, except searching for better procedures for information flow in the relevant arena. This is not a common situation; there is usually someone who knows something relevant.
2) *Prior information noted but not fully appreciated:* Where information is potentially available, but not fully appreciated. The situation indicates that the information may not have been understood completely because individuals have a false sense of security when faced with danger signals. Often this emerges from distractions or pressure of work, which can give the subject an impression of the information as irrelevant.
3) *Prior information not correctly assembled:* When information about danger signals is carried in minds of individual humans, others can't reach it. A key to prevent disaster is therefore to place information in places where everybody can reach it.
4) *Information available to be known, but which could not be appreciated because of conflict with prevailed understanding:* In cases of disaster, Turner saw that relevant information was available, but when it was in conflict with prior information, rules or values, it was neglected and not taken into discussion.

To control risk, these "irrational" events have to be continuously evaluated by the organisation. A key factor is to make intensive efforts to collect and analyse information about hazards and find out what we do not know. Experiences from Man-made Disasters have shown that someone, somewhere do actually know something. The outcome of risk control therefore depends on the *quality* of monitoring risk.

Westrum (1993) discusses what can be done to develop organisations with requisite imagination. The organisation should provide incentives for thought. The only valid incentive for thinking is to use people's ideas – and to make sure they know that their ideas are used. The organisation also needs to cultivate and reward efforts to bridge the boundaries between organisational layers, departments, subcultures and different sites. "Pop-out programmes" encourage the person with ideas and concerns to share them effectively. Pop-out programmes may, for instance, encompass the institution of new channels for information flow, empowering people to act when they see something that needs correcting, establishing open fora where workers can meet top-managers face to face and air complaints. It should be realised that pop-out programmes will only work if the organisation has the resources to act on the ideas and concerns that emerge from the process.

Many of the practices described in Section 6.6 are also relevant in an information processing perspective.

7.6 How can major accident risks be monitored?

The recurrent pattern of administrative and human failure, coupled with misinterpretation of warnings of disasters might, in theory at least, be identified through a holistic approach to safety auditing (Turner and Pidgeon, 1997: 185). Detailed findings from the auditing process should be put together, in order to assess how the organisation handles information related to its vulnerabilities. We would need to identify indicators of the developing incubation period. Pidgeon

argues that existing technical hazard audits, such as Hazard and Operability Studies (HAZOPS), might be extended to incorporate relevant aspects of human and organisational failures.

It is difficult to unambiguously define good and poor performance, which may be highly dependent on the context within which an activity actually occurs. Pidgeon notes that a number of the discussions of safety auditing share common ground with Total Quality Management (TQM). He therefore considers TQM a promising tool to control and audit risk.

Pidgeon also emphasises the role of safety culture as a key to handle and continuously monitoring risk (Turner and Pidgeon, 1997: 187-189). He argues that a good safety culture might both reflect and be promoted by at least four facets:
- Senior management are committed to safety
- Shared care and concern for hazards and their impact upon people
- Realistic and flexible norms and rules about hazards
- Continual reflection upon practice through monitoring, analysis and feedback systems

At the same time in Pidgeon emphasise the role of organisational learning to help initiating better risk perception among individuals, and by this overcome poor beliefs, norms and information flow in organisations (Turner and Pidgeon, 1997, 191-195). He emphasises the need for so-called double-loop learning (Argyris and Schön, 1978). It is not enough to change behaviour in response to feedback. We also need to improve out procedures for gathering and assessing signals about hazards, and to challenge our theories in use for interpreting the world.

7.7 Information processing related to the Åsta accident

One of the factors that made the Åsta accident possible was the absence of an Automatic Train Control system (ATC) on the Røros line. An ATC system would probably have stopped the northbound train within the station area of Rudstad, and the signalling system would have ordered the southbound train to stop before it entered the station area.

The initial plan for installation of Centralised Traffic Control on the Røros line included installation of ATC. However, the funding for ATC on the Røros line in 1993 was reallocated to other purposes. Repeated reallocations were made the following years, with the result that ATC installation did not start before 1999.

The absence of ATC on the Røros line violated the stated policy of the Norwegian State Railways, which was that all lines with remote control of signals should be equipped with ATC by 1995. The traffic safety manager warned about remote controlled sections without ATC at two top management meetings in the Norwegian State Railways (NSB) where the managing director was present in 1995. In 1996 the traffic safety manager issued a memo where he repeated his concerns. In 1997 he repeated his concerns in a new memo.

The Commission of inquiry asked the managing director of NSB at that time about his knowledge about the safety manager's concerns (NOU 2000:30, p. 153, our translation):

> The managing director of NSB at that time, Ueland, could not remember that he had received [the memo from the traffic safety manager. He explained to the commission that he was confident that the consequences of [not giving priority to ATC installation] had been assessed, and said that there had been no disagreement in the organisation about the reordering of priorities. He claimed that nobody in the organisations had said that the priorities could not be changed, and that one could not postpone installation of ATC any longer. He further claimed that it was a clear judgement in the organisation that they had a safe and good system. On a question from the Commission about whether he

> considered the safety on the Røros line on the 4th of January 2000 adequate, Ueland explained that the issue of safety was simple to him; it was either safe to drive trains, and then the trains would roll, or otherwise the trains stood still. He claimed that he, like many others, had been living in the belief that it was safe to drive on the Røros line.

This excerpt illustrates the paradox which inspires the information processing perspective. The knowledge about the problem exists somewhere in the organisation or its close environment, but this knowledge is not shared by the dominant decision makers, and therefore not acted on.

How did this situation come into being? The safety director at the time accepted the first reallocation of funding, since it implied a delay for one year only. However, his follower was placed at a position lower down the organisational hierarchy, and thus had more difficult access to the attention of the top management. At the same time, the confidence was developing in top management that the organisation tackled its safety challenges well enough to concentrate on other issues, such as punctuality and the development of new services. This conviction was founded on hard data – a favourable long time trend in fatal railway accidents, culminating in two very good years (1996 and 1997). There existed no strong external "watchdog" who could effectively challenge this conviction[30]. This pattern fits well into Turner's notion of an incubation period where the organisation systematically disregards warning signals. It also suggests that power relations play an important role in organisational information processing.

7.8 The information perspective and the Snorre A blow-out

The investigation report issued by the Petroleum Safety Authority identified several deficiencies in the planning of the slot recovery operation for Snorre A. Apparently, the planners failed to anticipate correctly how the barrier status of well P-31A would change as each step of the revised plan was carried out. As a consequence, the plan for the slot recovery operation failed to comply with the regulatory requirement that at least two independent and tested well barriers shall be in place at all times.

We should not underestimate the complexity of this planning task. P-31A was a complex well with a complex history. Planning was made difficult by the fact that the information about the history of well P-31A was stored in different data bases, and some of it existed only on paper. We noted that some of the documentation may have disappeared as responsibility for the operations of Snorre A was transferred from Saga to Norsk Hydro, and then to Statoil. Another problem was that the Snorre A operating organisation had been uprooted twice due to change of operator from Saga to Hydro and then to Statoil. They therefore lacked strong networks with expertise in other parts of Statoil.

7.9 Strengths and limitations of the information perspective

An important contribution of the information perspective is Turner's finding that during the incubation period, there is nearly always someone who is aware of the imminent danger. This finding has strong implications for safety management: The accumulation of more data *per se* does not prevent accidents. It is necessary to focus on the processes through which information is disseminated, combined and interpreted. We need to understand the mechanisms through which some warnings gain the attention of decision-makers and eventually lead to preventive action, whereas other warnings are ignored or rejected. The research challenges raised by this finding are far from resolved. It may prove necessary to go beyond a narrow information perspective and, for

[30] NSB was thus not subject to external regulation of safety before the Norwegian Railway Inspectorate was established in 1996. The Inspectorate had very limited resources in its first years (NOU 2000:30).

instance, explore whether a political or power perspective is also needed to get a grip on these phenomena.

A fundamental challenge for researchers applying the information perspective is to *show that their claims are meaningful and valid to actors who do not have the benefit of hindsight*. This can be illustrated by an example. Turner reported that organisations often fail to take action on danger signals because "decoy phenomena" distract the attention from the "real" danger signal. Was it really possible to distinguish between "decoys" and warnings that would materialise *before* the accident happened? Or do we need the information provided by the accident to be able to label some warnings as "decoys" and others as "real"? If this distinction can only be made based on hindsight, then this finding is of little help to persons charged with preventing accidents. When reporting findings based on hindsight, researchers should therefore strive to take the perspective of actors who do not have the benefit of hindsight, and ask themselves whether the finding still makes sense.

7.10 The Information perspective – a summary

The Information perspective is concerned with two related issues;

1) that an accident often can be understood comprehensively[31] in *retrospect* to the extent that it can be claimed that precursory events and available information were ignored or misinterpreted at the prior to the occurrence of the accident
2) that the notion of the accident itself actually should be extended to incorporate the disruption or collapse of the cultural beliefs and norms about hazards, existing before the accident.

It follows by implication that existing beliefs and norms are at least accessory to the failure of recognizing the upcoming accident, as they provide the grounds for the "incubation period" in which chains of discrepant events develop and accumulate unnoticed. During this period, the actions actually taken often distract attention from the problems that actually (will) cause trouble. In the aftermath of the accident, a *full cultural adjustment* to the fundamental surprise of the event is often needed.

Hence, the Information perspective is less concerned with immediate (physical) causation than with the breakdown in the flow and interpretation of information that is linked to the energy flow or other physical events. Indirect causation of this kind implies that organisational capabilities of *requisite imagination* may make a crucial difference in avoiding accidents. Westrum (1993) distinguished between *cultures* that range between being *pathological* in the sense of suppressing warning, innovation, bridging and other mechanisms that facilitate alternative interpretation, and being *generative* in the sense of actively promoting such mechanisms and efforts.

Existing, inert cultural beliefs, norms and patterns of interpretations are maybe even more dangerous when used as foundations for proactive planning. Clarke and Perrow (1996) claim that ("fantasy") plans used to justify increasingly complex systems are often wildly unrealistic and can impede organisational learning.

7.11 Key questions for the applicability of the Information perspective

- ⇨ Is there sufficient reason to believe that the context and inner dynamics of the organisation is so stable that it can rely on existing cultural beliefs, norms and patterns of interpretation in order to avoid the fundamental surprise?

[31] That is, supported by substantial argument and thus well beyond "everyday" wisdom of hindsight

- ⇨ Is the organisation able to implement a full cultural adjustment after being fundamentally surprised?
- ⇨ Is the culture of imagination pathological, bureaucratic or generative? How does this fit with the anticipated context?
- ⇨ Does the organisation rely on "fantasy plans"?

7.12 References

Argyris, C. and D. A. Schön (1978). *Organizational Learning*. Reading, Massachusetts: Addison-Wesley.

Ashby, W.R. (1981). Self-regulation and requisite variety. In F.E. Emery (ed.). *Systems Thinking. Volume One.* Harmondsworth: Penguin Education, 100-120. Earlier published as Chapter 11 in W.R. Ashby (1956). *Introduction to Cybernetics,* Wiley.

Clarke, L. and Perrow, C. (1996). Prosaic Organizational Failure. *American Behavioral Scientist, 39* (8) 1040-1056.

Pidgeon, N. and O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science, 34,* 15- 30.

Turner, B. A. (1978). *Man-made disasters.* London: Wykeham Science Press.

Turner, B. A., Pidgeon, N. F. (1997). *Man-made disasters*. 2nd Edition. London: Butterworth-Heinemann.

Westrum, R. (1993). Cultures with Requisite Imagination. In J.A. Wise, V. D. Hopkin and P. Stager (eds). *Verification and Validation of Complex Systems: Human Factors Issues.* Berlin: Springer, 401-416.

7.13 New references

We have not included a list of new references for the information processing perspective, because this perspective has in many ways converged with the High Reliability Organisations perspective and the Resilience Engineering perspective. Readers looking for recent contributions to the information processing perspective are therefore referred to Sections 6.13 and 9.9.

8 Risk handling in the face of conflicting objectives: Risk taking, adaptation and drift

We live in an open market economy. This economical regime is "designed" to exterminate organisations that use more resources than absolutely necessary to deliver a given product. Organisational survival is thus a matter of balancing on the edge. Risk control and safe performance often requires considerable resources such as money, time, and competent personnel. Humans or groups may make risky choices when facing a dilemma. Moreover, performance at the level of individuals, groups and larger organisational units may drift over time under the pressure of conflicting objectives. It is thus impossible to give a balanced view on organisational resilience without considering how organisations handle conflicting objectives.

8.1 Taking a risk or running a risk?

What exactly happens when people face the choice between a risky course of action and a less risky course of action, and act in a manner that eventually triggers an accident or fails to recover a dangerous situation? Very often, they do not *face* the choice at all. In a study of 57 accidents at sea, Wagenaar and Groeneweg (1987) investigated whether the negative outcomes were the result of deliberate risk-taking, i.e. whether the captain deliberately selected a dangerous course of action, knowing that there existed feasible and less risky alternatives. They found that this was the case in only one of the 57 accidents.[32] In 21% of the cases the information of the immanent danger was not even available, and in another 27% the situation was not recognised as problematic. In a further 36 % the consequences were either not foreseen, or the likelihood of disaster was underestimated. Wagenaar and Groeneweg thus claimed that a large majority of the captains had been completely taken by surprise. They had been *running a risk* rather than *taking a risk*.

This result should not be uncritically generalised to all settings were risk-related decisions (or "non-decisions") are made. Personnel at the "sharp end", those who work close to the sources of danger (e.g. process operators, train drivers, pilots, captains), face very strong incentives to avoid accidents. They and their fellow workers may risk their lives if an accident should occur. They are also particularly susceptible to blame, since the causal chain between actions at the sharp end and the unwanted consequences is usually short and conspicuous.

Things may be different at the "blunt end" – for instance at the administrative quarters of shipping companies. Before the capsize of the Harold of Free Enterprise, the company management turned down several applications for an alarm on the bridge to prevent the ship from leaving harbour with the bough doors open, despite the fact that this had happened to a sister ship. Several other requests to correct urgent safety problems had been handled in similar manner.[33] In this case, company management was informed about the risks resulting from their decisions, and alternative courses of action had been proposed. It is thus a reasonable claim that these managers were deliberately *taking a risk*. High level managers may be more prone to taking risks for two reasons (Rasmussen, 1994a). Due to their professional background (e.g. business schools) and their distance from daily operations, some of them may fail to fully comprehend the implications of the

[32] In that case the captain claimed that the risk of a collision was smaller than the risk of grounding, a judgement which the Dutch Shipping Council decided had been wrong.

[33] Department of Transport/1987): mv Herald Of Free Enterprise. Formal Investigation. Report of Court No. 8074. London: Her Majesty's Stationery Office.

warnings they receive from the sharp end. Secondly, the incentive systems of many managers may direct their attention to short term profits at the expense of the prevention of adverse events that they perceive as unlikely to happen during the few years before they move to another position.

8.2 Migration of activities towards the boundary of acceptable performance

Rasmussen (1997) suggested that we may think of the handling of conflicting objectives in terms of activities migrating toward the boundary of acceptable performance (Figure 8). The basic idea is that human activities are characterised by continuous adaptive search in the face of partially conflicting pressures and needs. Individuals and groups strive to keep the workload at a comfortable level, to find some intellectual joy in the activity, and to avoid failure. They face requirements and pressures with regard to e.g. productivity and quality. In practice, the work place allows them considerable freedom to try out different ways to handle these partially conflicting needs and constraints. This is depicted as the space between (1) the boundary of financially acceptable behaviour, (2) the boundary to unacceptable workload, and (3) the boundary of functionally acceptable behaviour with regard to risk. In seeking for a viable adaptation, humans will explore this “work space”. Rasmussen compared this to the brownian movements of molecules in a gas. Both the “effort gradient” and the “cost gradient” are likely to drive the activities towards the boundary of safe (i.e. functionally acceptable) performance. An error or accident may occur if the crossing of this boundary is irreversible.

This model directs our attention to what happens at the boundary of safe performance. Management may seek to define a narrower boundary through safety campaigns, and thus increase the safety margins in the activities. We may also ask what happens when an activity approaches or crosses the boundary? Will the actors receive an insistent warning from the system and have the opportunity to reverse their actions? Since many dangerous situations do *not* lead to disaster, is there a risk that they will adapt to warnings over time? May they even modify their mental models of the system in such a way that they ignore the dangers involved in crossing the boundary of safe performance?

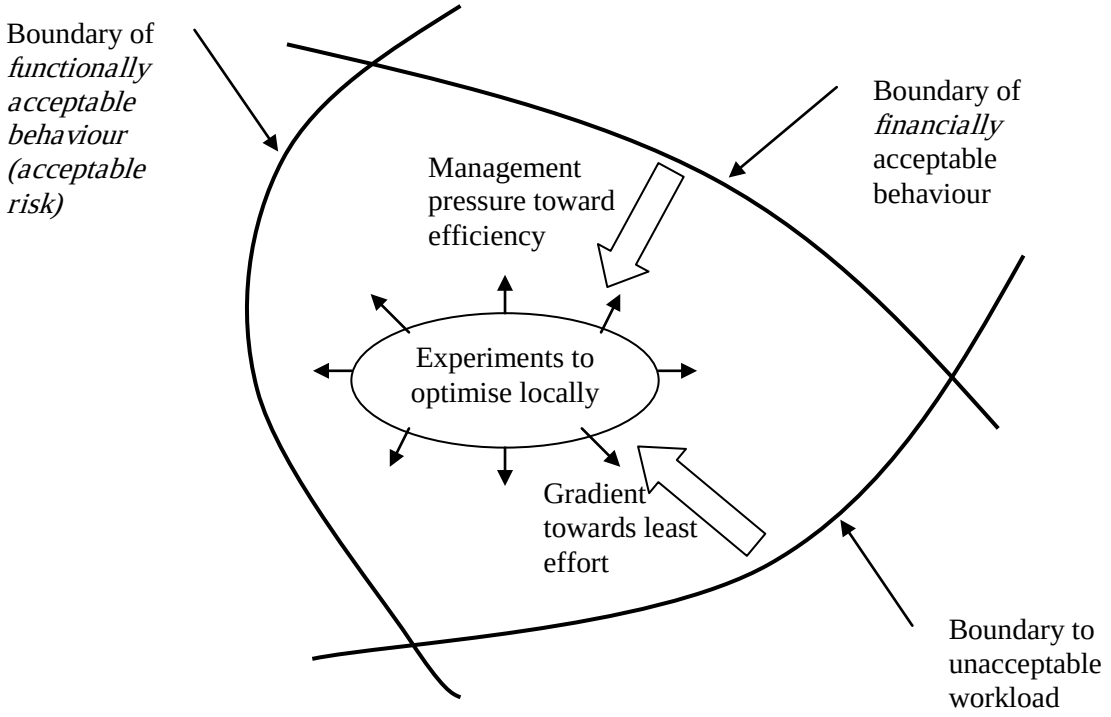

Figure 8. Under the pressure of conflicting objectives activities tend to migrate toward the boundary of acceptable performance (Adapted from Rasmussen, 1996).

8.3 Distributed decision making

In a complex system, many activities take place in parallel. At a given moment, each actor may have incomplete or inaccurate knowledge about the state of the system and the ongoing activities. Moreover, the parallel activities may interact in non-obvious manners if the system is characterised by high interactive complexity (see Section 5.3). A system is characterised by *distributed decision making* to the extent that it lacks a centralised decision-maker and each decision-maker has a model and information of a limited part of the problem (Brehmer, 1991)[34].

The migration model as presented in Figure 8 above captures a single activity performed in isolation. Figure 9 illustrates the adaptation process in a complex system with distributed decision making (Rasmussen, 1994b). Actions within one activity may change the boundary of acceptable performance for another activity. For instance, on an offshore production platform, one work team may open a valve on the flare system to drain off liquids before they replace a valve. Another work team at a different place may at the same time need to release hydrocarbons into the flare

[34] Distributed decision making differs from group decision making, where the problem is to achieve consensus when everyone is capable of understanding the whole problem.

system in order to start a their job. However, due to the first activity, the second work team cannot safely perform a normal pressure release. The figure therefore contains two different boundaries for acceptable (i.e. safe) performance. The inner boundary delimits the *unconditionally* acceptable state of affairs, i.e. acceptable without regard to the behaviour of the other actors. The outer boundary delimits the *conditionally* acceptable state of affairs. A single actor can enter the area between the two boundaries without unacceptable risk of triggering an accident. However, the risk may become unacceptable if two or more actors enter the area between the two boundaries. Rasmussen (1994b: 28) termed such coincidences 'singularities'. They are characterised by dramatic shifts in system performance and are often perceived as "basic surprises".

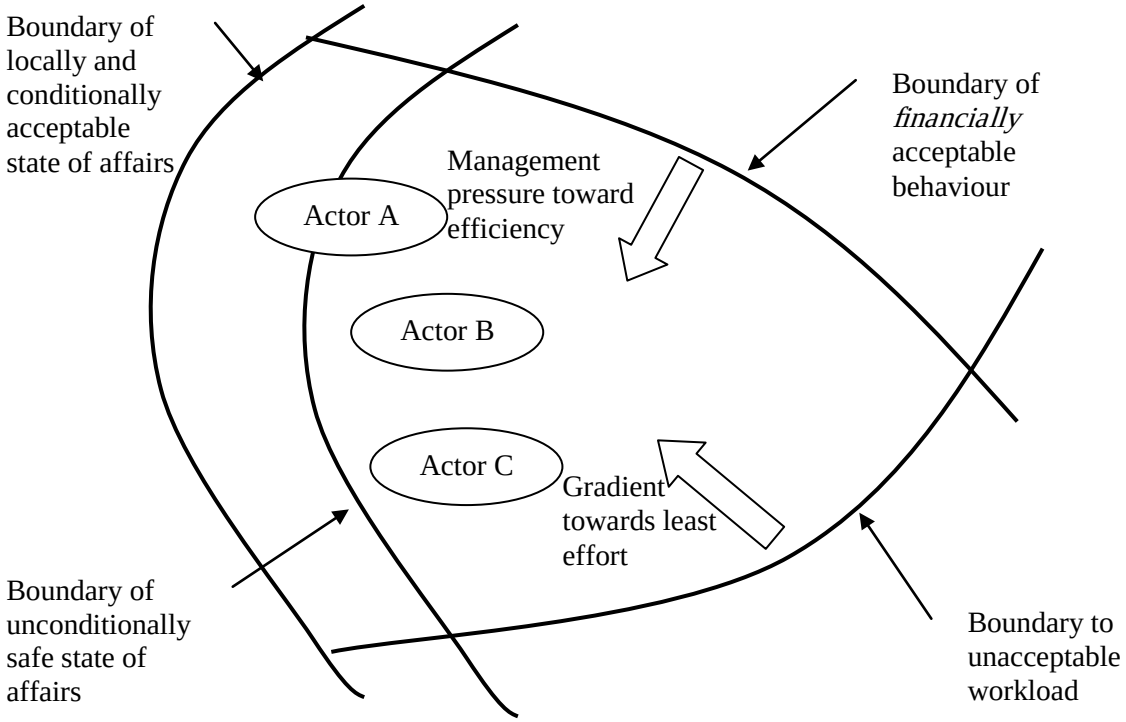

Figure 9. Adaptation in a complex organisation, where several actors are migrating more or less independently within the space of acceptable performance. (Adapted from Rasmussen, 1994b).

Again, the crucial issue is how the actors behave with regard to the two boundaries. In this case, we may expect actors to strive for *local optimisation*, based on their incomplete knowledge about the system. They will take into account the dangers and potential scenarios they know about, but not those that are not "visible" from their local point of view. The implication is that actors will run risks and singularities will occur, unless the inner boundary is made active and able to bound the natural migration towards the outer boundary. Rasmussen (1994b) suggests that it is feasible to provide the necessary decision support to help operators stay within the unconditionally safe boundary in a well-structured process plant. Providing visible margins to safety boundaries may even increase operations efficiency, since the operators will not need to maintain an excessive margin to an invisible boundary.

Distributed decision making is an answer to the complexity of the problems and fast pace of changes in the decision contexts facing the decision-makers. Moreover, the degree of centralised

control may be reduced as a consequence of efforts to reduce management and administration costs. This sometimes happens through explicit organisational change. At other times, the reduction of centralised control may be unplanned and inconspicuous. Managers may be given new responsibilities and time-consuming tasks, and adapt by reducing the attention they give to supervisory tasks (e.g., checking that work permit forms have been adequately completed).

Many organisations have developed administrative systems in order to manage the risks associated with parallel activities and distributed decision making. For instance, work permit systems are used in the process industry to make sure that critical tasks are properly co-ordinated, and that necessary precautions are taken. These administrative systems may be even more safety-critical than many technological barriers, because some tasks involve the temporary removal of several technical barriers. A failure related to the work permit system might thus hit the system in a very vulnerable state.

8.4 Levels of decision-making

Yet another dimension of decision- making remains to be explicated. The control of risk, as well as the production of accidents, takes place at many levels, ranging from political systems to individual operators and even technical systems (e.g., automatic process control and safety systems). This is illustrated in Figure 10. Each level can influence each other in an integrated and tightly coupled system. Higher levels can influence lower levels through, e.g., explicit instructions, by the provision and limitation of resources, by establishing incentive systems, or by determining *how* decisions are to be made at lower levels. On the other hand, lower levels may use discretion when they interpret and implement directives from higher levels, they may control the information flow to higher levels, or they may bypass a level and direct a lobbying effort at the level above.

The figure also illustrates the traditional formal means used by each level to control the level(s) below. Rasmussen (1997) argued that the classical prescriptive command-and-control approach, where rules and conduct are derived top-down, works far too slowly to tackle the dynamics of modern economies.

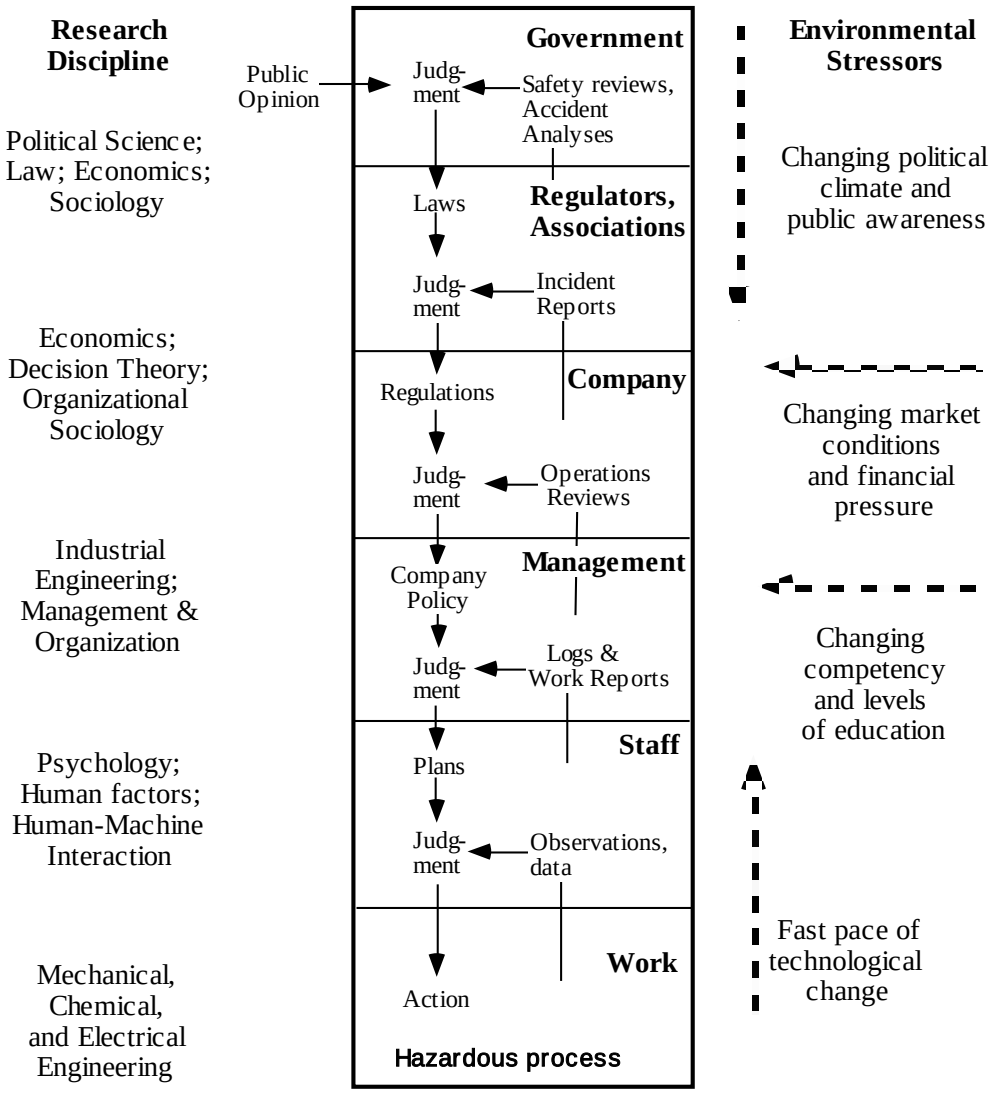

Figure 10. The socio- technical system involved in risk management (Adapted from Rasmussen, 1997).

8.5 The diversity of decision contexts and decision processes: A contingency model

We have hinted at the diversity of decision settings in earlier sections in this chapter. We will now present a typology, which may make this diversity more comprehensible.[35] We have noted that some decisions are made at the "sharp end", i.e. close to the hazard sources. Others are made at the blunt end, removed from the hazard sources. Decisions makers and decision settings also differ in their level of authority. A manager can issue orders and directives to his or her subordinates, and an inspectorate can issue directives to and impose sanctions on companies. We can thus characterise decision settings according to two dimensions, (1) proximity to the hazard source, and (2) level of authority. This is illustrated in Figure 11. Pilots, offshore platform superintendents or aircraft line maintenance personnel usually find themselves at the sharp end, i.e. close to the hazard source. Designers, planners, analysts and regulatory institutions typically operate at the blunt end. Some actors may be "operationally" close to the hazard source, even though they are physically remote, for instance air traffic control operators or centralised train

[35] The typology was introduced by Rosness (2001) and has been elaborated in an unpublished draft paper by Rosness and Hovden and in a paper by Kørte et al. (2002).

control operators. We will consider these actors as belonging to the sharp end, even though they are less vulnerable in case of an accident. Actors at the sharp end are often mostly event-driven and thus operate within a shorter time horizon most of the time. We also expect actors at the sharp end to have more updated and detailed hands-on knowledge of the system they operate than actors at the blunt end.

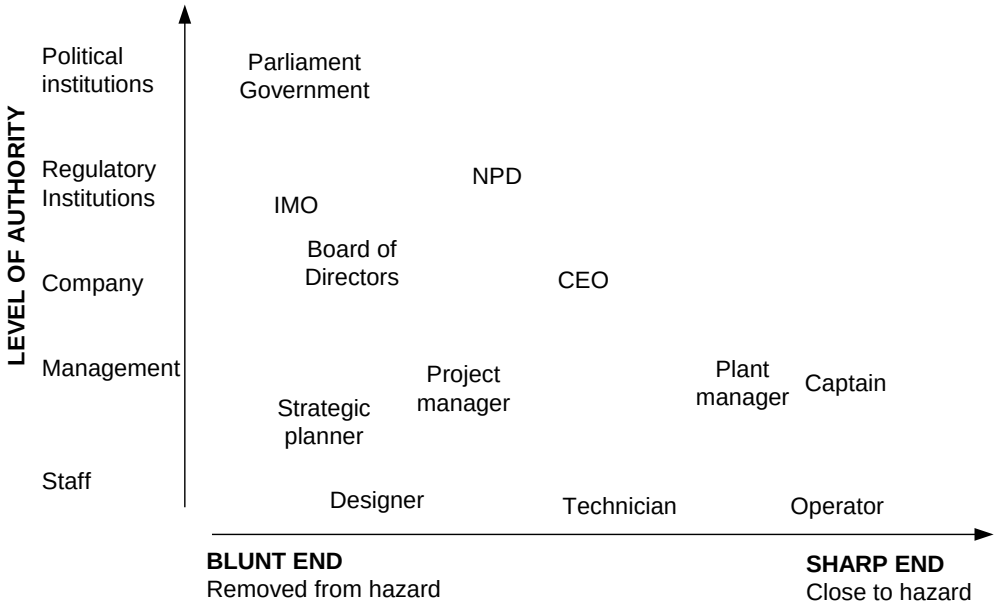

Figure 11. Two dimensions for characterising setting for safety related decision making, adapted from Rosness (2001). (IMO - The International Maritime Organisation; NPD - The Norwegian petroleum Directorate; CEO - Chief Executive Officer.)

The conditions under which actors make decisions strongly influence the decision processes and outcomes. We thus expect decision criteria, procedures, and outcomes to be related to (1) how close an actor or decision forum is to the hazard and (2) the level of authority of the actor or forum. These relationships are complex, since decision-makers also adapt to circumstances not covered by these two dimensions. However, we believe that even a grossly simplified model of these relationships may be helpful in sensitising us to the way decision-makers adapt to their setting. We therefore identify five distinct decision settings and propose an associated typology of decision modes, see Figure 12 and Table 4.

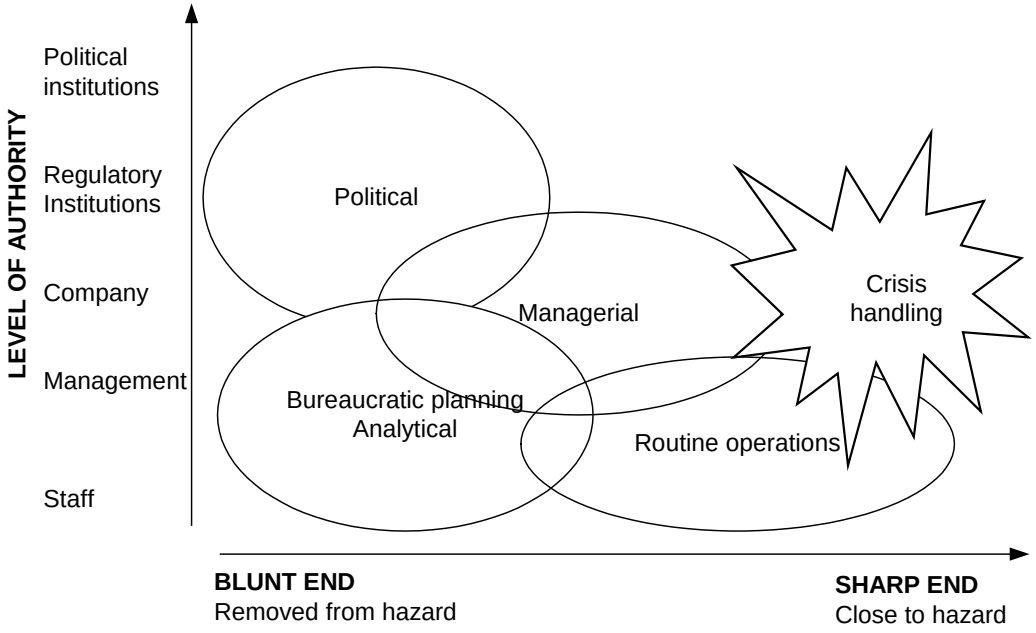

Figure 12. Classes of decision processes. Adapted from Rosness (2001).

In order to illustrate the logic of the model, we will consider *routine operations* in some detail. Actors at a low level of authority and close to the hazard, such as drivers, process operators, and ship crews, often experience uneven workloads because their tasks are event driven. Their decision making is often constrained by limited situation awareness (Woods et al., 1994). They may not receive the requisite information to build a complete and updated model of the situation, they may not have enough free information processing capacity to maintain an updated system model, or they may lack mental models that adequately represent the properties of the larger system. Actors in complex systems are likely to resolve goal conflicts within a condition of local rationality. He/she is not in a position to assess the overall impact of their choices, or to assess how their choices interact with those of the other actors (Brehmer, 1991; Rasmussen, 1997).

We propose that sharp end actors at low levels of authority tend to focus on smooth and efficient operations. At the same time they try to keep the workload at a comfortable or at least tolerable level. Human behaviour in routine tasks is to a great extent automated and feed-forward driven, with occasional, progress checks, references to rules or reactions to signals from the environment (Rasmussen, 1986; Reason, 1990). This mode of behavioural control allows very efficient and smooth performance. However, due to the limited attention and feedback control, highly automated behaviour is prone to slips ("actions not as planned"). The reaction to danger signals may be automated to a point where the signal escapes conscious processing. Operators' mental models of the system may decay over time because some aspects of the models are not maintained through their daily working experience. Safety margins may erode over time if the system fails to provide clear warnings if the operator performance approaches or crosses the boundary to unacceptable risk or if the operator adapt to these warnings.

The example also illustrates the gross simplifications inherent in this model. The work of sharp-end operators at low authority levels may include significant amounts of non-routine work, for instance concerned with the handling of irregularities in the production system. The share of non-routine tasks may be increasing in many production systems, as routine tasks become automated. One might think of a continuum of decision modes, ranging from "pure" routine operations" via

skill-based, rule-based and knowledge-based problem handling to the handling of crisis situations with imminent danger of a catastrophic outcome.

Table 4. Dominant constraints, decision criteria and typical problems in different decision modes.

Decision mode	Dominant constraints	Dominant decision criteria	Typical problems
Political	Conflicts of interest	Robust consensus	Inconsistency Non-optimal decisions Erosion of safety margins
Managerial	Information processing capacity	Find an option that is good enough (satisficing)	Inadequate problem definitions Stick to SOP Erosion of safety margins
Analytical & Bureaucratic	Hands-on knowledge	Comply with rules & standards Optimise selected attributes	Unrealistic assumptions Deficient models Erosions of safety margins
Routine operations	Workload Situation awareness	Smooth, efficient operation Optimise workload	Slips Miss warnings Local rationality Erosion of safety margins
Crisis handling	Stress Time to obtain information and act	Avert catastrophic outcomes Avoid extreme stress levels	Defective coping if danger materialise

As summarised in Table 4, we may expect actors in other types of decision settings to face other constraints, and to adapt by focussing on different decision criteria. On this basis, we may make informed speculations on the types of problems that may be related with the outcomes of decisions. More comprehensive presentations of the model are given in Rosness (2001) and in Kørte et al. (2002).

8.6 Adherence to rules, culture and resources

We have all heard that rules are there to be broken. It has also become a commonplace in discussion on organisations to point to the gap between espoused theory and theory in use (Argyris and Schön, 1978), between what people say they do and what they actually do. Is it then a law of nature that any rule or procedure will be bent or broken as soon as it meets the harsh reality of conflicting objectives and rapidly changing environments?

This issue brings us back to research on High Reliability Organisations. Bourrier (1998) studied the daily adjustment and modifications made to maintenance procedures and work orders in two French and two U.S. nuclear power plants. The need for adjustment may arise from unplanned situations and changes, wear and tear problems, or the availability of tools.

In one French power plant, she found that workers did make minor adjustments, which they did not report to management. The adjustments were not totally out of control, since the maintenance staff shared among themselves a set of tacit rules that were different from the formal rules. These rules were conveyed to new workers through a socialisation process. However, upper management was left with very limited knowledge about the exact way in which the problems

were handled. In the two U.S. power plants, however, Bourrier found that workers were strictly following the rules, asking their foremen for help and guidance or new work orders each time they ran into an unplanned difficulty.

It is tempting to explain this contrast by referring to the national cultural clichés, e.g. rigorous American contractual orientation versus a pragmatic French habit of getting along and muddling through. However, Bourrier found that an alternative explanation could be based on organisational differences. She examined the opportunities for bridging the gap between procedures and practice. At the French plant, no resources were provided for adaptation of formal procedures to unforeseen situations. The personnel authorised to revise procedures were not available to the maintenance staff. Compliance with procedures was thus not an option if the job was to be done. The maintenance personnel compensated by developing and propagating their own norms, for instance tolerances that were somewhat larger then those accepted in the formal procedures. Such unofficial norms were saved in personal notebooks and conveyed to trainees, but they were not known to plant management or to the engineers who wrote and revised maintenance procedures.

One of the US plants (Diablo Canyon) bridged the gap between procedures and practice by making the engineers responsible for procedure updates available to maintenance personnel. The workers responded by taking all problems to the engineers. It was part of the worker culture at this plant to take very few initiatives, since managers and engineers were paid to do the thinking. At the other US plant (North Anna) maintenance foremen had the formal authority to initiate procedure adjustments and updates. They also had the time needed to handle these problems.

The issue of compliance thus has two sides. It is not only a matter of controlling operator actions. This was to some extent achieved in all three power plants. The crucial difference is that the US power plants functioned as self-correcting organisations. They were able to develop explicit (as opposed to tacit) mechanisms to reconcile formal norms with the realities of daily work. However, this learning does come at a cost. At Diablo Canyon, the operating costs were very high due to the staffing level. The US plants also had better availability factors than then the French plant.

8.7 The Challenger disaster and normalisation of deviance

The Challenger space shuttle was launched at Kennedy Space Center at 11:38 A.M. on January 28, 1986. A fireball erupted about one minute after launch, and the space shuttle system disintegrated 73 seconds after launch. All seven crew members perished.

The technical investigation concluded that leak had occurred at a joint at one of the solid rocket boosters. This joint was sealed by two O-rings, but the O-rings had failed to seal completely. The hot gases emanating from the leak led to an event sequence which culminated with a fireball fuelled by the external fuel tank of the space shuttle system, and subsequently the total disintegration of the space shuttle system.

The initial public investigations emphasised the decision processes during the last hours prior to launch in their account of the accident. The engineers that had worked with the technical problems related to the sealing function of the O-rings had been concerned about the possibility that the O-rings might not seal properly due to the unusually low temperature prior to launch time. They proposed a delay of the launch, but this proposal was rejected during a telephone conference a few hours prior to launch.

In an ethnographic-historic study of the Challenger disaster, Vaughan (1996) proposed an alternative account. She argued that a *culture of deviance* had developed as a consequence of the environmental conditions that faced NASA and its contractors during the space shuttle

programme. Repeated signals of potential danger occurred in the form of O-rings that had been burnt or chafed during flights. These signals were processed in accordance with the formal rules, each time leading to acceptance of the risk and a new shuttle launch. However, the repeated definition of anomalies as acceptable risk led engineers and managers to build and institutionalise a cultural construction of the risk. It was considered safe to fly in spite of increasingly serious signs that the O-rings might fail to contain the burning gases inside the solid rocket boosters. According to Vaughan, the repeated handling of anomalies under production pressure thus lead to a change in culture, including a change in basic assumption concerning what is normal and acceptable. Vaughan termed this process "normalisation of deviance".

8.8 Practical drift

Snook (2000) devised a complex model of "practical drift" based on the concept of "practical action". Practical action refers to locally efficient action acquired through practice and maintained through unremarkable repetition. Practical action is thus shaped by the situational factors rather than by the prescriptions given in procedures and instructions. Practical drift involves two dimensions of change. One dimension concerns the pattern of tight and loose couplings, i.e. strong or weak interdependence between subunits. The other dimension concerns rule- versus task-based logics of action – going by the book versus adapting behaviour to the local practical circumstances. Snook proposed that sociotechnical systems tend to cycle through four states

1. The "designed" organization, which follows global rules[36] in a tightly coupled world. This is because sociotechnical systems are designed to be capable of handling critical situations when couplings are tight.
2. The "engineered" organization, which initially operates as designed. The global rules are followed initially, but most of the time coupling may be looser than the design basis. This state is unstable because the global rules are likely to be perceived as unnecessarily rigorous.
3. The "applied" organization, where local, task-based logics take over in a loosely coupled environment.
4. "Failure", which may emerge if a tightly coupled situation occurs when local, task-based action prevails. Although the sociotechnical system may have been designed to handle the tightly coupled situation, it is no longer operated according to the initial global rules, and has thus become vulnerable.

The relationships between the four states are illustrated in Figure Figure 13. The shaded cells (states 2 and 4) are unstable, whereas states 1 and 3 are relatively stable. According to the theory of practical drift, complex sociotechnical systems tend to cycle through the four states show in the table. Because systems are loosely coupled most of the time, the actors can gradually adapt their behaviour to the local circumstances without receiving strong signals from the system that they are running a risk. This is what makes state 2 unstable. Snook thus explicitly links aspects of Normal Accident theory with the notion drift towards the boundary of acceptable risk.

[36] A global rule is a rule that has been devised with the total system in mind. This is in contrast to local rules, which emerge from a more restricted view of the system. Local rules may thus not take into account possible interaction effects that are invisible to the actors who develop local rules by adapting their practice to the local circumstances.

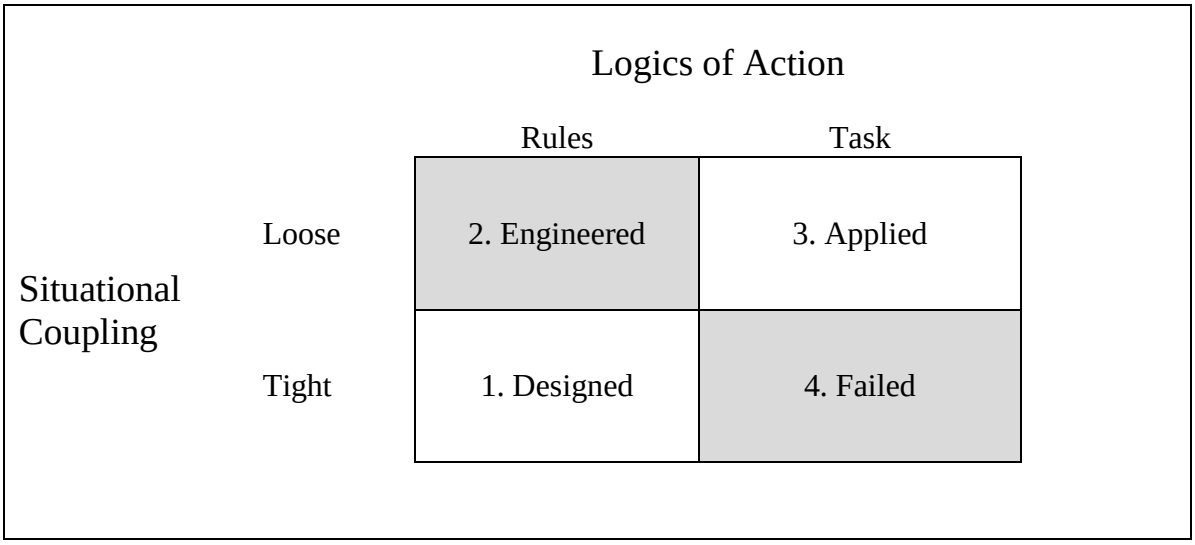

Figure 13. The four systems states involved in Practical Drift. Adapted from Snook (2000:186).

8.9 Implications for risk control and risk reduction

The organisations studied by LaPorte and Consolini (1991) had abundant resources to fulfil their strategic missions and to prevent catastrophic failure. They were not under the pressure of a competitive market. Some of the nuclear power plants (e.g. Diablo Canyon) had a very large and complex organisation (Schulman, 1993), and could allocate a lot of time and engineering capacity to the planning of maintenance shutdowns (Bourrier, 1998). However, such abundance is the exception rather than the rule. Building an enormous organisation is simply not an option in most industries. Conflicting objectives are here to stay, and the safety discipline has to find ways to cope with scarcity and dilemmas.

A common strategy for handling conflicting objectives is to create independent institutions or organisational units ("watchdogs") to regulate or monitor safety performance (e.g. Lindblom, 1959). For instance, Lord Cullen, in his investigation of the Piper Alpha disaster, pointed out the importance of the regulatory body being perceived as independent of commercial interests.

Some strategies for proactive risk reduction efforts can be derived from Rasmussen's "migration" model (e.g., Rasmussen and Svedung, 2000; see Section 8.2 above):

- The boundaries of safe performance should be made visible and touchable. The actors should have a way to know when they approach or exceed the boundaries. Design envelopes should be communicated effectively to operators. A friendly system will also allow them to recover in case he or she momentarily exceeds the boundary. This strategy is complicated by the fact that humans tend to adapt to warnings. We also need to bear in mind that human information processing capacity is limited. In many systems, the filtration of unnecessary alarms may be an effective measure to make the boundaries visible.
- Pressures that drive decision-makers toward the boundaries of safe performance can to some extent be counteracted. Managers may, for instance, by follow up safety performance on a par with economic performance.

- It is a good idea to communicate explicitly about trade-offs. Operators are put in a difficult double-bind situation if managers state that safety has priority, but tacitly communicates the opposite message through planning, follow-up, resource-allocation or their own example (Woods et al., 1994).

External pressures on organisations do not only cause dilemmas. Many dilemmas arise from high level decisions, for instance when insufficient time is allocated to the completion of a project. It is important that high level decision makers who are in a position to put lower level actors under pressure also are held accountable for the accident risks associated with their decisions.

The migration model suggests that regulations and procedures have two important functions with regard to safety. The first function is to help actors stay within the boundary of safe performance. The second function is to prevent conflicts between activities when decision-making is distributed. The first function does not always call for a detailed specification of the one and only acceptable way to perform a given task. The point is rather to help the actor identify the boundaries of safe performance. The second function calls for procedures, which highlight the interfaces with other activities, where there is a potential for conflict. In the latter case, a rather rigorous standardisation may be necessary to make the performance of other actors predictable.

8.10 Conflicting objectives and the Åsta accident

Based on the public investigation report, we may identify examples of conflicting objectives related to safety at several levels:

- The investment in Automatic Train Control had been postponed for years on the Røros line, in spite of several warnings. In the early nineties, funding was made available, but the organisation did not allocate sufficient planning resources and top management attention to ATC installation. In the later nineties, the project was given low priority in the budgets. ATC seems to have competed with preparations for the 1994 winter games, as well as the Gardermoen railway and the introduction of high-speed trains.

- In 1997, the Norwegian Railway Administration introduced a new departure procedure. The former departure procedure required the train guard and the driver to check exit signals independently. The new departure procedure was adapted to main lines equipped with ATC. Since a failure of the driver to obey a red exit signal would be recovered by the ATC, the conductor was not required to observe the exit signal. He could thus concentrate on the safety on passengers leaving and boarding the train. The problem was, of course, that no double-checking would take place on railway sections without ATC. It is not clear whether this was merely a conflict between two competing safety considerations, i.e. safety of embarking and disembarking passengers versus collision risk. The Åsta commission mentions that according to the new departure procedures, the Norwegian Railway Administration might permit passenger trains to operate without a conductor, thus reducing personnel costs.

We discussed the context of the decisions to postpone ATC installation in Section 7.7. We are now in a position to add another factor. Safety management in Norwegian railway operations has traditionally taken a reactive approach, with a focus on detailed operational rules (NOU 2000:142). Managerial action to improve safety was typically taken in response to incidents and accidents, whereas it was uncommon to systematically assess whether a proposed change might jeopardise safety, or whether a given activity or system was safe. This approach may have led to a *lack of clear and compelling criteria to identify the boundaries for acceptable risk* in decision situations that are not covered by the operational rules. This problem is also illustrated by the way

the managing director at the time commented on the safety of the Røros line. Note that there is no reference to criteria as to what is safe enough (NOU 2000:30, p. 153, our translation):

> He further claimed that it was a clear judgement in the organisation that they had a safe and good system. On a question from the Commission about whether he considered the safety on the Røros line on the 4th of January 2000 adequate, Ueland explained that the issue of safety was simple to him; it was either safe to drive trains, and then the trains would roll, or otherwise the trains stood still. He claimed that he, like many others, had been living in the belief that it was safe to drive on the Røros line.

These examples also illustrate *decoupling of decisions that are related in their impact on safety*. For instance, the decision to implement a new departure procedure was not coupled to the installation of ATC, although the new departure procedure might lead to increased collision risk on railway sections without ATC.

8.11 Conflicting objectives and the Snorre A blow-out

Here are some examples of conflicting objectives that are mentioned in the reports on the Snorre A blow-out:

- The operational organisation of Snorre A was transferred from Saga to Norsk Hydro and then to Statoil within less than four years. These shifts created vulnerabilities in the organisation. People had to spend time an effort to adapt to new organisational structures and routines. They lost their networks with experts in other parts of the operator company. These effects were apparently not taken into account when top management in Norsk Hydro and Statoil made their deal concerning the operator responsibility for Snorre A (Wackers, 2006).

- The operational organisation of Snorre A expressed a desire to be "left alone" after the takeover by Statoil, in order to reduce the strains associated with organisational change. According to Schiefloe et al. (2005), this desire was to a great extent respected. This may have reduced the strain of the Snorre A operational organisation. However, the limited degree of integration of Snorre A may also have kept the operational organisation from utilising competence and experience from other parts of Statoil's organisation. Schiefloe et al. suggest that this led to a weakening of some of the "informal organisational safety barriers" (2005: 9).

- According to Schiefloe et al. (2005), Snorre A was turned into a money machine during the years preceding the blow-out. Emphasis on long-term planning and robustification of the platform was reduced, and preventive maintenance was deferred to the future.

- Statoil negotiated a new drilling contract immediately after taking over Snorre A. According to this contract, the drilling contractor was paid only for effective operational time (Wackers, 2006: 40). Wackers claims that this type of contract makes it more difficult for the drilling contractor's offshore personnel to voice their safety and reliability concerns during an operation: "If they demand an operation to be stopped because they do not trust the situation anymore, their employer will not get any payment during the downtime. If they turn out to be wrong the financial consequences for the company could even be greater." (2006: 41)

- According to Wackers (2006), the decision to recover slot P31 in spite of the complexity of the well was part of a strategy to improve and optimise the productivity of Snorre A.

- The decision to start the slot recovery operation without a final risk review meeting reflected a trade-off between safety and optimal utilisation of the drilling rig.

We have argued that the path from conflicting goals to an organisational accident often goes via uncoupled (uncoordinated) local optimisations. Various actors make their own tradeoffs without comprehensive knowledge about side effects and interactions with optimisations made by other actors. Wackers (2006:54) suggests that such decoupling occurred at different levels of aggregation. One example is the decoupling of the 1999 business deal concerning the shifts in operator responsibility for Snorre A from an exploration of its medium or long term consequences for safe and reliable operation of the installation. Another example is the decision to perforate the mechanical plug in the tail pipe before pulling the scab liner without considering the effects on the barrier status during the operation.

Wackers also argues that time is *not* money, but time can be made into money, for instance by means of contracts conditions, economic incentives and deadlines.

We have not identified a unified theory that gives a comprehensive grasp on the issues related to the handling of conflicting objectives. This chapter thus combines concepts and models from several authors. It may be too early to discuss the "strengths and limitations" of this perspective. In the future, we should not be satisfied just to note *that* some accidents may be related to the presence of conflicting objectives. Rather, we need to understand why some organisations handle conflicting objectives in a safer manner than others. This may enable us to propose *how* an organisation may survive in a competitive environment without unnecessarily compromising safety.

Safety scientists have been rather reluctant to use the concept of "power" until now. It may prove necessary to examine how power is built and exploited in safety-related decision in order to understand how conflicts between conflicting objectives are handled in a setting where different actors have different interests.

8.12 The Conflicting Objectives perspective – a summary

Safety is an objective that may conflict with other objectives. The conflicts are rarely conspicuous or distinct in terms of clear choices, but day-to-day adaptations will, directly or indirectly, be subject to pressures or gradients stemming from different objectives. From a safety viewpoint, the danger is that safety is gradually sacrificed in relation to other objectives.

Rasmussen's (1996) *migration model* frames the core of this perspective. Local optimisations of performance are contained by three different boundaries of acceptable performance, related to financial performance, workload and safety. The fundamental challenge is that the former two effectively enforce a gradual migration towards the safety boundary. The boundary of safety performance may be perceived as comprised of two steps; an inner boundary of *unconditionally* safe performance, and an outer boundary of *conditionally* safe performance. In a distributed decision making context, various actors can influence each other in complex ways. E.g., the actions of actor A can bring about that actor B, who conceives himself to be within the inner boundary of unconditionally safe performance, suddenly and unwittingly operates between the two boundaries, that is, in a mode of conditioned safety but unaware of the conditions. If a third actor then, either deliberatively or unwittingly, enters the conditioned mode without knowing about actor B, the risk level may rise even further. The practical relevance of the migration model

is conditioned by the possibility of making the safety boundaries visible and insistent at the individual as well as at aggregate levels. Administrative measures like *work permits* may be conceived as attempts to prevent and manage risky encounters with conditioned safety circumstances.

Interacting decisions that affect the control of risk take place in many different contexts, ranging from political systems to individual operators, and even technical systems. Two points are of special relevance concerning interacting decisions:

1. Decisions are conducted in diverse settings or contexts, differing with respect to dominant constraints, decision criteria and typical problem framings, as well as physical and causal distance to the physical hazard.
2. The stereotypical top-down, prescriptive command-and-control mode of interaction is rarely or never representative for interactive decisions. Local interpretation, adaptations etc generate differences that may make a difference.

8.13 Key questions for the applicability of the Conflicting Objectives perspective

- ⇨ Is safety affected by boundaries and gradients of other objectives?
- ⇨ Can the safety boundaries be made visible and insistent for a decision?
- ⇨ Is it possible to identify a set of typical decision contexts, and describe how safety boundaries are conceived and represented in these contexts?
- ⇨ Is it possible to foresee how safety can be "lost" in interacting decisions?
- ⇨ Is it possible to identify and institute additional safety-relevant decision constraints and criteria, e.g. by use of the migration model?

8.14 References

Argyris, C. and D. A. Schön (1978). *Organizational Learning*. Reading, Massachusetts: Addison-Wesley.

Bourrier, M. (1998). Elements for designing a self-correcting organisation: Examples from nuclear power plants. In A. Hale and M. Baram (eds.). *Safety Management. The Challenge of Change*. Oxford: Pergamon.

Brehmer, B. (1991). Distributed decision making: Some notes on the literature. I J. Rasmussen, B. Brehmer og J. Leplat (eds.). *Distributed decision making: Cognitive models for cooperative work.* Chichester: Wiley.

Kørte, J., Aven, T. and Rosness, R. (2002). On the use of risk analysis in different decision settings. Paper presented at ESREL 2002, Decision Making and Risk Management, Lyon, 19-21 March 2002.

LaPorte, T. R. and Consolini, P.M. (1991). Working in practice but not in theory: Theoretical challenges of "High-Reliability Organisations". *Journal of Public Administration Research and Theory, 1,* 19-47.

Lindblom, C. E. (1959). The science of "muddling through". *Public administration Review, 19,* 79-88.

Rasmussen, J. (1994a). High Reliability Organizations, Normal Accidents, and other dimensions of a risk management problem. Paper. *NATO Advanced Research Workshop on Nuclear Arms Safety.* Oxford, UK, August 1994.

Rasmussen, J. (1994b). Risk management, adaptation, and design for safety. In B. Brehmer and N.-E. Sahlin (eds). *Future Risks and Risk Management,* (pp 1-36). Dordrecht: Kluwer Academic Publishers.

Rasmussen, J. (1996). Risk management in a dynamic society. Presentation at the seminar *Safety and Reliability in Industrial Management,* Trondheim 29-30 May 1996. (Viewgraphs)

Rasmussen, J. (1997). Risk management in a Dynamic Society: A Modelling Problem, *Safety Science, 27* (2-3), pp. 183-213.

Rasmussen, J. and I. Svedung (2000). *Proactive Risk Management in a Dynamic Society* (Swedish Rescue Services Agency, Karlstad, Sweden).

Reason, J. (1990). *Human error*. Cambridge: Cambridge University Press.

Rosness, R. (2001). *"Om jeg hamrer eller hamres, like fullt så skal der jamres. Målkonflikter og sikkerhet."* [On conflicting goals and safety.] SINTEF Report STF38 A01408. Trondheim: SINTEF Industrial Management. Available at www.risikoforsk.no.

Schulman, P. R. (1993). The negotiated order of organizational reliability. *Administration & Society, 25* (3), 353-372.

Wagenaar, W. A. and Groeneweg, J. (1987). Accidents at sea: Multiple causes and impossible consequences. *International Journal of Man-Machine Studies, 27,* 587-598.

Woods, D. D., Johannesen, L.J., Cook, R.I., Sarter, N.B. (1994). *Behind Human Error: Cognitive Systems, Computers, and Hindsight.* State-of-the-Art Report 94- 01. Wright-Patterson Airforce Base, Ohio: CSERIAC

8.15 New references

Cook, R. & Rasmussen, J. (2005). "Going solid": a model of system dynamics and consequences for patient safety, *Qual Saf Health Care,* 14, 130-134. Downloaded from qhc.bmjjournals.com.

Hollnagel, E. (2009). *The ETTO Principle: Efficiency-Throughness Trade-Off.* Farnham: Ashgate.

Hopkins, A. (2008). *Failure to Learn. The BP Texas City Refinery disaster.* Sydney: CCH.

Klein, G. (1998). *Sources of Power. How People Make Decisions.* Cambridge, Mass.: The NIT Press.

Rosness, R., 2009: "A Contingency model of decision-making involving risk of accidental loss", *Safety Science, 47*, (6), pp. 807-812.

Snook, S.A. (2000). *Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq.* Princeton: Princeton University Press.

Starbuck, W. H. & Farjoun, M., (eds.) (2005). *Organization at the limit. Lessons from the Columbia Disaster.* Oxford, Blackwell Publishing

Vaughan, D. (1996). *The Challenger Launch Decision.* Chicago: The University of Chicago Press.

9 The Resilience Engineering perspective

It is not yet entirely clear what "Resilience Engineering" is or where it is going. We may think of Resilience Engineering as a sixth perspective on organisational accidents and resilient organisations, as a synthesis incorporating parts of the former five perspectives, as a new paradigm for risk control, as a tool box for building resilient organisations, and/or as a productive meeting place for researchers with related interests. Many central contributions to "Resilience Engineering" are elaborations (or more precisely, translations) of core topics from the other five perspectives, such as barriers, complexity, or the handling of conflicting goals. At the same time, by providing a new synthesis, Resilience Engineering points to new ways of thinking about resilient organisations and organisational accidents and new strategies for building resilience.

In this chapter, we will emphasise those aspects of Resilience Engineering which distinguish it from the previous five perspectives. As a consequence, some contributions to the Resilience Engineering literature have already been presented in the context of other perspectives. At the same time, we shall try to convey Resilience Engineering as a more or less coherent perspective or paradigm, encompassing underlying assumptions, concepts and theoretical notions as well as recommendations and tools for evaluating and building resilience.

We will start by reconsidering the meaning of 'resilience'. We will then give an overview of how aspects from other perspectives are translated into the RE context, and proceed with a *selection* of some key concepts and issues which characterize Resilience Engineering as of today.

9.1 Resilience and Resilience Engineering

A resilient system is a system with an inherent capability to adjust its functioning (Hollnagel 2007). This adjustment can be done both before and in response to changes and disturbances. These system amendments allow the continuity of operations, even in the face of major accidents or continuous stress. A resilient system is able to respond to regular and irregular threats in a way that is both robust and flexible, it is able to self-monitor its performance, and it is capable of anticipating disruptions and pressures, as well as their consequences. Hollnagel (2008) states that "*…a resilient system is… the intrinsic ability of an organisation (system) to adjust its functioning prior to or following disturbance to continue working in face of the presence of a continuous stress or major mishaps*"

At a more aggregate level, we can summarise Resilience as:

- a *mode of preparation* on the basis that unexpected trouble is ubiquitous and unpredictable;
- a *form of proactive control*, in terms of an ability of a system or organisation to anticipate the forthcoming, to minimize or eliminate unwanted variability, and to take advantage of productive variability;
- a quality of being *able to stretch and then return* to something resembling its former shape.

Resilience Engineering denotes the systematic attempt to provide ways of conceiving the problem of resilience as well as the solution(s), and the tools and methods to be applied.

9.2 Comparing RE aspects with aspects borrowed from other perspectives

RE is founded on many themes and aspects that also are addressed by other perspectives. By using the term translation, we emphasize that the overlapping themes have a distinct meaning related to the RE agenda that is related to, but not necessarily corresponding to their meaning and interpretation in the other perspectives.

9.2.1 Intractability and interactive complexity

In everyday language, the word "intractable" is used to characterise problems that are difficult to deal with or solve, diseases for which we lack an adequate treatment and persons that are strong-willed and resistant to outside influence. In this everyday sense, most socio-technical systems are complex, intractable, interdependent and constantly changing.

The notion of an intractable system strongly resembles Perrow's (1984) description of systems with high interactive complexity. On the other hand, distinct events can also be denoted intractable in the sense that it may be hard to predict that they may occur, to conceive what they mean, and what the possible implication is.

In vein with the HRO perspective, intractability is thus related to events that are the consequence of some unanticipated combination of the normal variability in socio-technical performance. Hence, adverse events and accidents are not necessarily related to some sort of collapse of the normal system components and functions, they may also result from intractable combinations of adaptive behaviour. Intractable events are thus also the flip side of the necessary adaptations to variability. Failures and successes alike are results of adjustments to cope with complexity. By implication, intractable events also represent opportunity.

Intractability also points back to the Information Perspective in a critical sense: is there such a thing as a "correct" interpretation of information about intractable events within reach at all?

9.2.2 Functional resonance and combined complex interactions

The notion of "functional resonance" appears to refer to the same phenomena that Perrow (1984) framed with the concept of combined "complex interactions" and "tight coupling". The contribution of RE is to provide additional metaphors to help us think about these phenomena, and to elaborate some of the implications for risk control.

The term "functional resonance" refers to the possibility that the variability of individual functions may combine and escalate in an unwanted and unexpected way. This is the result of functional couplings in the system. Any part of the system variability can be a "signal", and the "noise" is determined by the variability of the functions in the system. Thus the variations of a number of functions may resonate, i.e., reinforce each other and thereby cause the variability of one function to exceed its normal limits. This principle captures emergent system properties that only are understandable if the system is not decomposed in isolated components (Woltjer & Hollnagel, 2007; Macchi et al., 2008). The proneness of a system/organisation to experience the Normal Accident is not a "yes or no" question according to some predefined, static criteria. The conditions for "Normal accidents" may develop (emerge) slowly and "intractably".

A disturbing implication of the "functional resonance" metaphor is that it may be impossible to identify in advance the limit between acceptable and unacceptable variability for a given function. Functional resonance implies that variability which most of the time is unproblematic, may resonate suddenly and unexpectedly with variability in other functions and escalate to a dangerous level. The problem is that we may not know in advance when this will happen – i.e. how much variability the system can accommodate before functional resonance may occur. Rasmussen

(1996) suggested that attempts to control variability should focus on the limit between acceptable and unacceptable variability, for instance by making that limit “visible” to the actors and provide effective feedback when they approach or exceed the limit. Such measures may be impossible to implement if the limit can only be identified on hindsight, after the variability has run out of control.

Systems with functional resonance may not be captured by the binary logic of many reliability and risk analysis models. A fault tree, for instance, is based on the preconditions that we can define in advance what constitutes a failure for each of the components in the fault tree, and that the occurrence of a failure of the system as a whole is determined by the state of the components. The “functional resonance” metaphor suggests that both these preconditions may be invalid for many systems.

9.2.3 ETTO – Efficiency-Thoroughness Trade-Off and handling conflicting goals

The principle of efficiency-thoroughness trade-off (ETTO) refers to a natural part of human performance. Individuals and organisations must adjust to cope with their current working conditions. These adjustments are always approximate because there is always a limited amount of information, resources and time. Individuals and organisations therefore continually seek viable compromises between doing the job efficiently and doing it thoroughly.

ETTO is part of the individual’s behaviour and decision strategies in the work setting. Aspects of deliberate choice become more relevant in this context. Hollnagel (2009 p. 35) lists several “ETTO rules” that can be found in the workplace and which are examples of judgments that are recognisable in practice. A few examples are listed below:

- *'It looks fine' - so there is no need to do anything, meaning that an action or an effort can safety be skipped.*
- *'It is normally OK, there is no need to check' - it may look suspicious, but do not worry, it always works out in the end. A variation of this is 'I/we have done this millions of times before' - so trust me/us to do the right thing.*
- *'It will be checked later by someone else' - so we can skip this test now and save some time.*
- *'It has been checked earlier by someone else' - so we can skip this test now and save some time.*
- *'We always do it in this way here' - so don't be worried that the procedures say something else.*

The ETTO principle in many ways resembles some key points of the perspective of conflicting goals. ETTO is not limited to deliberate decision-making. On the contrary, ETTO is carried out more or less automatically much of the time, and the subject may not be aware fully aware of compromises he or she makes in order to reconcile efficiency and thoroughness requirements.

9.2.4 Barriers within RE and the other perspectives

Variability may be a result of the efficiency-thoroughness trade-offs made by one or more actors. In this context, it is conceivable that barriers may either dampen the unwanted variability or amplify variability that leads to continuous operation. *Barriers* thus need to be seen as hindrances or enablers. On one hand, these barriers may either prevent an unwanted event from taking place, or protect against the consequences of an unwanted event. On the other hand, they may enhance the capabilities to allow the system to continue in operation. As in the energy-barrier perspective, barriers can be described in terms of barrier systems (organisational and/or physical structure of the barrier) and barrier functions (the specific purpose of the barrier, e.g. “to prevent ignition of hydrocarbon leaks”). Hollnagel (2004) identifies four categories of barrier systems: (1) Physical

barrier systems, such as safety belts and fences, block the movement or transportation of mass, energy, or information, (2) Functional barrier systems, such as password protection and interlocks, set up pre-conditions that need to be met before an action (by human and/or machine) can be undertaken, (3) Symbolic barrier systems, such as signs and procedures, are indications of constraints on action that are physically present, and (4) Incorporeal barrier systems, such as ethical norms or laws, are indications of constraints on action that are not physically present.

9.3 Systemic proaction: an overarching paradigm of control

Resilience Engineering does not see safety as an absence of accidents but as a capability of the system to adjust and cope with current conditions. These adjustments are always approximate. Resilience Engineering is about increasing the ability of the organisation to make correct adjustments to avoid incidents and accidents, the latter also in the sense of worst-case resonance effects that resembles ”normal accidents”. Resilience Engineering also makes the claim that this will benefit the optimisation of both protection (safety) and production, on equal terms.

Before we proceed with some key concepts of Resilience Engineering, we will present what can be denoted a conception of control that gives meaning to many of these concepts. This paradigm of control, which we denote *systemic proaction*, is founded on some premises that will be summarised in the following paragraphs.

9.3.1 Underspecification and the variability that cannot be removed

Socio-technical systems are recognised to be so complex that work situations are always underspecified. Designers can not anticipate every contingency in advance. Functions cannot be assumed to be bimodal[37], and normal performance carries by implication an inherent variability. It is thus impossible to specify work operations exhaustively in advance, and organisations (as well as the people in them) are in a state of constant flux. Both organisations and their inhabitants are constantly changing and adjusting to the circumstances at hand. Adding to this is the fact that time and resources are scarce, something that forces adjustments to be approximate.

Hence, performance variability is inevitable - as well as *necessary*. This variability that precludes specification represents both a source for success and failure – it has a dual role. The dilemma and the challenge is that while risks emerge from non-linear, interactive combinations of performance variability (intractable events), safety can not be achieved simply by constraining or eliminating normal performance variability. Safety management must therefore employ a unified (dual) view of both success and failure, and find ways that reinforce variability that leads to success, and dampen variability that leads to adverse outcomes. Safety can thus not be maintained by removing variability at large.

A key feature of a resilient organisation is that it does not lose control, and is able to continue and recover. A system in control can minimise or eliminate unwanted variability, both in its own performance and / or in the environment. Loss of control relates to when the system fails to cope with this kind of variability

9.3.2 Unexampled events and loss of control

Westrum (2006) proposed a typology (classification) of threats that can be translated into a corresponding typology of events. The *regular* threats (events) are those that occur so often that the system/organisation learns how to respond. The *irregular* threats (events) are unexpected but

[37] That is, either functioning or not functioning, and nothing in between.

imaginable. Finally, the *unexampled* events are impossible to imagine and exceed the organisation's experience.

Irregular events can be retrospectively classified as *unexpected* due to insufficient emphasis on imagination, while unexampled events are unexpected by definition. An *intractable* system may display combinations of *both* regular and unexpected (irregular, unexampled) events. Its intractability manifests itself as the problem of interpreting the implication and what to expect in terms of the *next* event. In an intractable system, a regular event is not necessarily followed by another regular event.

As stated by Epstein (2008)*,"…uncertainty is not some noisy variation around a mean value that represents the true situation. Variation itself is nature's own irreducible essence*". The sources of variation, irregularities, deviations, unexampled, and intractable events are not necessarily within the system itself. In an open (sociotechnical) systems perspective, interaction with the environment is source of a *dynamism* that can lead to unexpected events.

There is a strong link between loss of control and unexpected events. Unexpected events are frequently considered a result of lack of control (e.g., Johnson, 1980; Kjellén and Larsson, 1981). The occurrence of unexpected events however, may well have its causes outside the system and its immediate context.

According to Epstein (2008), times have changed, but the methods have not. E.g. nuclear PRA models are so large that they are neither reviewable nor surveyable. Such risk models are (ibid.) "*not used for their insights, but for the quantitative results offered, thus never exploring novel failure modes of the facilities, totally missing the ability to postulate unexampled events and strange systems and extra-system influences/interactions/background.*" Epstein asserts that a second culture is needed, a culture that, "*to be prepared for the unexampled event, must play with the model, question assumptions, run scenarios, and understand the uncertainty*".

9.3.3 Systemic proaction

To be effective and efficient, safety management based on resilience thus cannot be based solely on hindsight, error tabulation, and failure probabilities. Intractable events demand a kind of proactivity that goes beyond the premise of linear, sequential modelling of failures, faults and their subsequent effects.

The uniqueness of the RE approach is not the focus on proactivity as such, but the ambition of being proactive in a *systemic* sense. The notion of a systemic view is an attempt to move attention beyond classical component and failure orientation in dealing with systems and anticipating behaviour at the system level. It is also aims to go beyond the traditional "level" orientation of e.g. "the technical", "the human" or "the organisational", seeking to grasp a larger, holistic reality of the conditions for both failure and success.

The systemic view enforces relatively less focus on intended behaviour of isolated components and defined deviances from "safe" norms, and correspondingly more awareness of possible unintended effects and propagations across different levels and framings of activities in a system. Possibly dangerous events and circumstances cannot be confined to their own "proper" sphere. Not only do extraneous events and conditions force themselves in, but the outcomes of decisions within any institutionalised framework constantly affect those outside.

Systemic proaction is, however, a level of ambition that implies a multitude of pitfalls. Cause-effect relations in a Human-Technology-Organisation perspective may be very hard to spot in advance (LeCoze 2005). The presence of resilience as a coping strategy introduces an additional

element of ingenuity and dynamism due to adaptive interventions. Perrow (1984) argued that the act of adding more technical barriers could increase system complexity and thus increase the potential for system accidents. In a similar manner, the flexibility and adaptive capacity that we introduce in order to build resilience may conceivably add to the intractability of the system. Such a dynamism carries a possible inherent challenge that actually goes beyond intractability of the *system* or the specific *events* in that sense that emergence means that the rules may be changed by the very act of playing the game. In other words, the intractability of the system can not be separated from the practice of being resilient. The notion of systemic hence carries the rather disturbing possibility that application of knowledge about a phenomenon may contribute to its unstable and mutable character (Giddens 1990).

Resilience Engineering hence attempts to respond to the challenge of *proactivity in a systemic sense* by 1) improving organisational abilities to establish robust and flexible processes, 2) monitoring and revising risk models within a systemic view, and 3) proactive use of resources in order to respond to disruptions in a context which encompasses dynamic production and economic demands.

A central premise for such an approach is to incorporate humans, technology and organisation on an equal basis in a functionally oriented, systemic perspective. However, this should be done without making the mistake of portraying humans as machines. *Resilience* as a concept is to a large degree rooted in the social sciences with respect to human and organisational factors. Hence, Resilience *Engineering* as an approach locates itself in the midst of a well known gap between available knowledge provided by researchers of the social sciences, and industrial practices in which engineering and managerial models and practices traditionally prevail. As pointed out by LeCoze and Dupré (2008), important recent models produced so far are based on theorizing perspectives founded in social sciences. We should therefore be very sensitive to the differences between prescriptive models (with management purposes) and descriptive models, as they target different actors and communities.

9.4 Some key concepts of Resilience Engineering

As indicated in Figure 1, Resilience Engineering can be conceived as being founded on a paradigm of systemic proaction, which in turn is based on consolidated premises that partly are translations of aspects covered by other perspectives. In this section, we present a selection of concepts that indicates a spectre of what RE comprises as of today, such as “emergent phenomena” and “proactive safety management systems”. All these concepts may be seen as key aspects of the paradigm of systemic proaction. As indicated on right side of the figure, RE also comprises tools to support systemic proaction. We will present some of these tools in Section Error! Reference source not found..

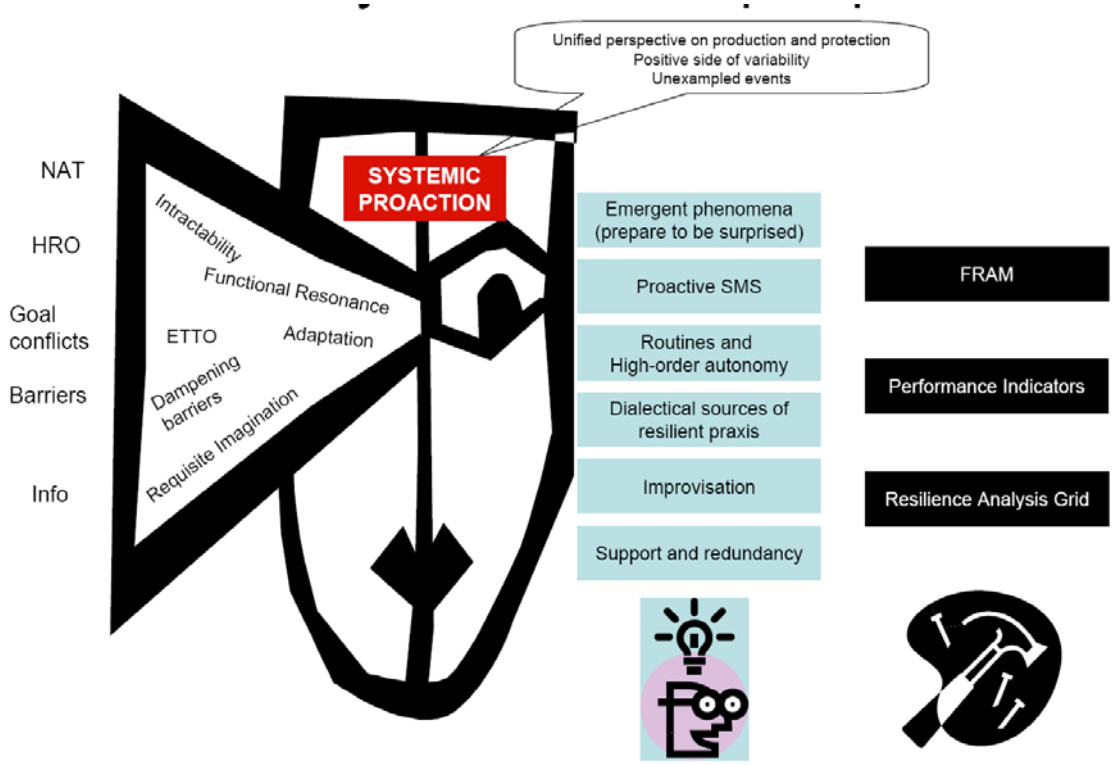

Figure 14. Resilience Engineering and its links to other perspectives.

9.4.1 Emergent phenomena ("prepare to be surprised")

This concept is very simple, but nonetheless foundational for Resilience Engineering. Due to the inherent variability and dynamism, fundamental surprises in the form of emergent phenomena must be expected. We must live with a lack of predictive models that can give hints on "what's next?" The resilient organisation must be *prepared to be surprised*.

9.4.2 Proactive Safety Management Systems targeting the coping ability of the system

According to Hollnagel (2008) traditional Safety Management System (SMS) are

- *Reactive* in the sense that improvements are based on correction of failures.
- *Proactive* in the sense that a reaction is triggered by the difference between the actual state and the target state (closed-loop feedback control). However, the difference can arise because of unanticipated internal and external disturbances. Therefore, the response may not be appropriate.
- Thus, also *proactive* in the sense of feed-forward control focussing on leading the system from an actual state to a desired future state. The model of the process is developed describing the process and the possible disturbances from the environment. The reaction is designed to react to anticipated disturbances, rather than the actual. As all models are approximations, it is easy to fail in relation to disturbances that are not foreseen. Hence, the limitation in this approach is that the response will not take place if disturbances have not been taken into account in the model. Feed-forward control may also result in unnecessary responses.

However, a successful, proactive SMS may experience the *fundamental regulator paradox* (Weinberg & Weinberg, 1979:250, Van Steen, 1996) of cybernetic theory. That is, if the number of events to correct against drops significantly because of the absence of "errors" and incidents, the process may be uncontrollable in face of a sudden disturbance. The lack of information may be misinterpreted to mean that the process is under control – while the fact is the opposite.

Hollnagel argues that from a control theory perspective, it makes more sense to use a definition of safety such that the output (the amount of essential information) increases when safety improves. The "target" of the control loop should not be to avoid or get away from something, but rather to achieve or get closer to something.

Resilience Engineering attempts to do exactly such a turn by *targeting the coping ability* of the system, that is, increasing the ability of the organisation to make correct adjustments. This target is pursued by a combination of feedback and feed-forward control, in which:

- The process model is the description of how safety is produced, and what is required to detect significant changes to be able to select appropriate adjustments.
- Disturbances can represent both threats and opportunities, and may originate from internal or external variability.
- The SMS should be able to handle the regular threats as well as events with serious adverse consequences that happen very rarely.

The output is related to safety and productivity performance that is monitored by performance indicators. A challenge is to find meaningful indicators. In addition to lagging indicators, leading indicators, showing what the state may be in the future, are needed.

9.4.3 Addressing systemic dynamics and dynamism

The variability, intractability and emergent properties of systems can be ascribed to some knowable dynamical aspects and patterns of a system that are hidden due to underspecification, but also to an inherent *dynamism* that produces novel patterns of behaviour. Proaction at a systemic level must aim to keep up with both, not at least because it will be difficult to make the distinction on the spot.

One way of enabling systemic proaction is to try to gain control by managing the *coupling points* of interactions between various functional parts of the system. These are the places or situations where subsystems interact, where variability in the output from one subsystem can be propagated or contained, amplified or dampened, or interact with other sources of variability in unforeseen manner.

The principle of managing coupling points can be illustrated by an example. Rules and routines can be conceived as coupling points of systemic interactions. Disturbances can create situations where workers find it necessary to adapt the rules to the necessities of the concrete situation. Disturbances can be amplified if these adaptations have side effects that were not foreseen by the rule followers. Systems with high levels of uncertainty require flexible use of rules, because it is impossible to foresee all possible contingencies when the rules are written. Procedures should not only specify "the one right way" to do the job. Grote (2008:99) proposes that the rules should also regulate the degree of flexibility that is allowed when applying the rules. Less flexibility should be allowed in tightly coupled systems than in loosely coupled systems. In this way, rules, including the rules on how to design rules ("meta-rules"), can be used to manage coupling points.

9.4.4 Improvisation

Resilience also inevitably requires a capacity to improvise, as a contribution to the ability to absorb strain and preserve functioning despite the presence of adversity, to recover or bounce back from untoward events, and to learn and grow from previous episodes of resilient action (Andresen et al., 2008). Properly addressed and facilitated within an organisation, improvisation could be made a booster for resilience, e.g. by allowing actors to take into account the actions of relevant others in "heedful interrelating" (Weick and Roberts, 1993). However, improvisation may always go wrong, thereby rendering plain and intelligible the inherent vulnerabilities in complex systems that cannot be avoided, whatever sophisticated methods we employ in order to reveal the most intricate secrets of their behaviour (Grøtan et. al 2008b).

9.4.5 Support and redundancy

Resilience Engineering as of today is predominantly occupied with the coping ability in terms of anticipating, attending to and responding to events, as well as learning effects. Some authors point at the need for decision support and redundancy in order to ensure that both people, groups as well as organisation endure resilience in the sense of not being exhausted or worn out in the act of meeting the demanding requirement of being resilient.
As suggested by the label Resilience *Engineering*, a central ambition of this community of researchers has been to develop practical tools and methods for building resilience. We shall illustrate this research effort with one example.

9.5 Functional Resonance Analysis Method

As suggested by the label Resilience *Engineering*, a central ambition of this community of researchers has been to develop practical tools and methods for building resilience. We shall illustrate this research effort with one example.

The Functional Resonance Analysis Method (FRAM[38]) is based on the functional resonance model as an explanation of accidents (Hollnagel, 2004, see Paragraph 9.2.2 above). Both the model and the method promote a systemic view to accident investigation and risk analysis. The purpose of the functional resonance analysis is to understand the characteristics of system functions and their couplings. This method takes into account the non-linear propagation of events based on the concepts of normal performance variability and functional resonance. The analysis consists of five steps:

1. Definition of the purpose of the analysis and description of the situation. At this point it is necessary to define the system boundaries, including the interfaces.

2. Identifying essential system functions, and characterising each function. Functions are described through six aspects, in terms of their input (I, that which the function uses or transforms), output (O, that which the function produces), preconditions (P, conditions that must be fulfilled to perform a function), resources (R, that which the function needs or consumes), time (T, that which affects time availability), and control (C, that which supervises or adjusts the function), and may be described in a table and subsequently visualized in a hexagonal representation.

3. Characterising the (context dependent) potential variability through some common performance conditions[39]. The context affects the variability of functions. It is

[38] The acronym FRAM has been used to denote both the "Functional Resonance Analysis Method" and the "Functional Resonance Accident Model". The latter is part of the theoretical foundation for the method. We shall stick to the former usage, which is also more recent.
[39] Common conditions for successful performance

recognised that the variability can have positive as well as negative consequences. The interest is therefore on how to describe the conditions that may affect performance variability. Conditions that may affect performance variability are named "Common Performance Conditions" (CPCs) and are based on those used in CREAM (Cognitive Reliability and Error Analysis Method; Hollnagel, 1998). These CPCs address the combined human, technological, and organisational aspects of each function. Eleven common performance conditions (CPCs) that are identified in the FRAM method may be used to elicit the potential variability: 1) availability of personnel and equipment, 2) training, preparation, competence, 3) communication quality, 4) human-machine interaction, operational support, 5) availability of procedures, 6) work conditions, 7) goals, number and conflicts, 8) available time, 9) circadian rhythm, stress, 10) team collaboration, and 11) organisational quality. Domain specific conditions may also be identified. Recent developments of the method include interpretation of the conditions as organisational functions, i.e. from training to management competence. After identifying the CPCs, the variability needs to be determined in a qualitative way in terms of stability, predictability, sufficiency, and boundaries of performance i.e. adequate, inadequate or unpredictable.[40]

4. Identify the potential for functional resonance based on possible dependencies/couplings among functions and the potential for functional variability. The output of the functional description of Step 1 is a list of functions each with their six aspects. The description of the aspects defines the potential links among the functions. The output from one function may, for instance, be the input to another function. Depending on the conditions at a given point in time, potential links may become actual links; hence produce an instantiation of the model for those conditions. The potential links among functions may be combined with the results of Step 2, the characterisation of variability. That is, the links specify where the variability of one function may have an impact, or may propagate. This analysis thus helps to reveal how a (stochastic) resonance can develop among functions in the system.

5. Identifying barriers for variability (damping factors) and specifying required performance monitoring. Besides recommendations for barriers, FRAM is aimed at specifying recommendations for the monitoring of performance and variability, to be able to detect undesired variability. Performance indicators may thus be developed for every function and every link between functions.

The method still needs improvement in order to provide further guidance to the analysts regarding how the method is applied and how results can be communicated to a wider audience. The applicability of the method seems very large, as functional analysis is applicable to socio-technical systems that are intractable. One main difference between FRAM and other functional analysis methods, i.e. structured analysis and design technique (SADT), is that FRAM takes into account the influence of the context of operation. For the time being, other proposals for systemic analysis models include Systems-Theoretic Accident Modeling and Process (STAMP, Leveson, 2004) and Core Task Analysis (Nuutinen and Norros, 2009).

[40] Recently, it has been proposed to distinguish between two types of functions when performing safety assessment: foreground and background functions. Foreground functions represent the focus of the analysis and background functions represent the context in which foreground functions are performed. (Macchi, 2010)

9.6 The Snorre A blow-out from a resilience engineering perspective

We have argued that Resilience Engineering can be viewed as a synthesis of other perspectives discussed in this report. As a consequence, many aspects of the Snorre A blow-out discussed in previous chapters are also relevant from a Reliability Engineering point of view. We will not repeat these discussions here. Instead, we will consider what we regard as the most remarkable aspect of the incident: The capacity of the platform crew to improvise and implement a viable plan to control the well in spite of the complexity of the situation, the imminent danger, and the lack of essential resources such as drilling mud and electric power.

Capacity for improvisation is not a prominent topic in the resilience engineering literature. Wackers (2006:65f) emphasises the importance of trust for the successful recovery of the Snorre A blow-out. This is in accordance with Weick's (1993) analysis of the Mann Gulch fire, where he argued that successful improvisation in a group faced with an imminent threat depends on a positive interplay between sense-making and trust in the leadership of the group. Wackers also emphasised the willingness of the platform manager to break rules when this was necessary, as well as the rich knowledge that enabled to crew to do this in a relatively safe manner.

Wackers (2006) points to a paradox which has also been suggested by Schiefloe et al. (2005): The Snorre A crew may have built their capacity to improvise through exposure to the installation in frequent corrective maintenance jobs that were due to the emphasis on cost reduction and deferral of preventive maintenance. "[Operating] Snorre A as a money machine maintained the improvisatory skills that saved the day in the recovery of the blow-out" (Wackers, 2006:67).

9.7 The Resilience Engineering (RE) perspective – a summary with special emphasis on the relation to other perspectives

The resilience of a system can be characterized as a *mode of preparation* for surprise, a *form of control* in terms of coping with the unexpected, and an *ability to stretch and return* to something resembling its former shape. Resilience Engineering (RE) denotes the systematic attempt of engineering resilient properties of a wide scale into a system. As such, RE is not as clear cut and focussed as the preceding five perspectives. It is more like a synthesis constituting a composite perspective, trying to absorb and translate a diversity of aspects that we have seen in the other perspectives into a unity of its own terms. Moreover, as RE is evolving at the time, this unity is definitely not closed.

As for the HRO perspective, the central question is *what may go right* despite disturbance and surprise, and the answer resides in the realm of preparedness, foresight and flexibility. Compared to HRO, RE however comprises a more fundamental orientation towards *adaptation* as a normal state of affairs, and (comparatively) less emphasis on redundancy and spontaneous reconfigurations emerging under exceptional or trying conditions.

RE is justified by the notion of *intractability* which resembles the normal accident theory (perspective, termed NAT in this section) notion of unpredictability and non-linearity due to (high) interactive complexity. RE, however, positions intractability not solely as a problem. There are also strong (and more positive) connotations to the inevitability and necessity of adaptive behaviour. A central premise is that failure and success stem from the same sources (adaptation), and that intractable conditions/events also represent *opportunities* for adaptation and improvement. There is also a possible demarcation line between NAT and RE in terms of dynamics versus dynamism. Accordingly, NAT can be interpreted as to focus on the intractability of interaction due to a dynamic potential that does not presume that the interacting agents themselves are changing. It is primarily the speed of propagation (tight coupling) that disables coping. The claims of NAT can thus be attributed to non-intuitive results from System Dynamics,

or “chaos” due to tiny differences in leverage points. The RE perspective, due to its strong focus on adaptation and emergence, may be *interpreted as* aiming for a grasp of the additional dynamisms that stem from rules of interaction and agents themselves changing as the interaction unfolds. RE can thus be attributed to a much broader theory of complex adaptive and responsive systems in which agents as well as their relations are continually changing as a result of interaction, and in which these changes are emergent rather than resultant – i.e. the outcome of many changes is different from the “sum” of the changes.

Moreover, the *functional resonance* metaphor of RE clearly resembles Perrow’s notion of the normal accident stemming from interactive complexity boosted by tight coupling, but makes an important distinction also here. RE labels these dynamics as *variability* (of interactivity). Part of this variability is inherently about *functional coupling*, which in turn is partly resulting from successful adaptation. This poses a signal versus noise kind of problem in dealing with (high) interactive complexity, as opposed to a binary choice that can be evaded by design (as of NAT). Rather, the issue for RE is to find out which combinations that can escalate in unwanted directions, and which are actually productive of adaptation. Hence, interactive complexity is not an irreducible basic dimension of the system, but a potentially dangerous quality of the necessary variability and functional couplings. Still, in accordance with NAT, the functional resonance metaphor does not preclude the “normality” of productive variability eventually going out of hand, e.g. boosted by tight coupling. For the time being, RE has not developed specific or rigorous criteria to distinguish between “good” or “bad” functional couplings, that is, NAT-like criteria. RE and NAT can, however, be combined in the view that the conditions for the “normal” accident may develop slowly and intractably.

While the Information perspective addresses misinterpretation of existing information, RE raises the question whether there really exists something like a “correct” interpretation about intractable systems/events, except by hindsight. In relation to the Conflicting Objectives perspective, e.g. Rasmussen’s recommendation of making variability limits visible to the operator, RE implies that the functional couplings and co-variability may be more important than the amplitude of a singular variability. RE also challenges the assumption that it is possible to identify a static limit that distinguishes safe and unsafe variability. The Efficiency-Thoroughness Trade-Off (ETTO) principle is also very close to Rasmussen’s migration model. ETTO claims to address generic conditions and constraints for adaptation that are conducive to the actual migration towards performance boundaries. However, the various (conflicting) goals are not the major driving force behind the actual migration, as the ETTO dimensions (efficiency, thoroughness) attempt to be generic and independent of specific decision contexts and goal preferences. RE can also be combined with the energy-barrier perspective, as barriers can be seen as dampening devices that are hindrances or enablers of propagation of variability.

Hence, RE aims for more than adaptation and coping at the sharp end. It also aims for proaction as an overarching paradigm of control for a system as a whole. The degree of proaction is ambitious in the sense that it defies to be locked into formalized or institutionalised decision contexts, and attempts to transcend traditional distinctions between technological, human and organisational aspects. RE aims for a degree of proaction that is *systemic* in the sense of looking for functional couplings unhindered by the aforementioned borderlines, and also in the sense of being sensitive to unusual or extraneous couplings in and between systems. A number of approaches to identifying and controlling the coupling points are proposed, e.g. facilitating higher-order autonomy in the execution of routines, and maintaining a dialectical relation between prescription and practice. In that sense, RE has implications for safety management. The fundamental regulator’s paradox is employed to direct management attention from counting errors and deviations, to a more proactive focus on measuring the coping ability of the organisation.

It is, however, unavoidable that attempts to implement resilience as a safety strategy introduces an additional element of ingenuity and dynamism due to adaptive interventions targeted at functional couplings. The intractability of the system is not exogenous to the practice of being resilient – we may think of intractability and the practice of being resilient as two sides of the same coin. To illustrate this point, we may paraphrase Giddens (1990) in micro terms; the application of knowledge about a system in order to cope with its intractability, contributes to its mutable and unstable character.

9.8 Key questions for the applicability of the Resilience Engineering perspective

- ⇨ (Similar to HRO) Is it interesting to investigate and strengthen the organisation's (assumed[41]) ability to cope with circumstances that "normally" may lead to accidents?
- ⇨ Is the organisation able to adapt to changing circumstances?
- ⇨ Is the organisation able to transform surprise into opportunity?
- ⇨ Is the organisations self-understanding based on stereotypical roles and behaviours that are unaffected by change and adaptation?
- ⇨ Is the organisation able to deal with equivocality of data and information, without being paralyzed?
- ⇨ Can the (safety) challenges of organisation/system be depicted in terms of functional variability and functional couplings?
- ⇨ Is the safety management system ready to focus on coping ability (paying less attention to error and deviation)?

9.9 References

Adamski, A. J. & Westrum, R. (2003) Requisite imagination: The fine art of anticipating what might go wrong. In Hollnagel, E (ed.) *Handbook of cognitive task design.* New York: Lawrence Erlbaum Associates

Andresen, G., Rosness, R. and Sætre, P.O. (2008). Improvisasjon – tabu og nødvendighet. In R.K. Tinmannsvik (ed.). *Robust arbeidspraksis. Hvorfor skjer det ikke flere ulykker på sokkelen?* Trondheim: Tapir akademisk forlag.

Dekker, S. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety. *Applied Ergonomics*, 34(3), pp. 233-238.

Epstein, S. (2008). Unexampled events, resilience and PRA. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives*, Aldershot: Aldershot

Foster, H.D. (1993). Resilience theory and system evaluation. In J.A. Wise, V. D. Hopkin and P. Stager (eds). *Verification and Validation of Complex Systems: Human Factors Issues*. Berlin: Springer, 35-60.

Giddens, A. (1990). *The Consequences of Modernity.* Cambridge: Polity Press.

[41] Such an assumption must be based on a realistic intention, that is, acknowledging that resilient capabilities does not come for free

Grote, G. (2008). Rules management as source for loose coupling in high-risk systems. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives,* Aldershot: Aldershot.

Grøtan, T.O, Størseth, F., Rø, M & A. B. Skjerve (2008a). *Literature review of Resilience and Improvisation*. The Building Safety project web. http://sintef.org/Projectweb/Building-Safety

Grøtan, T.O, Størseth, F., Rø, M & A. B. Skjerve (2008b). *Resilience, Adaptation and Improvisation – increasing resilience by facilitating for successful improvisation* . In. Ed. (Hollnagel, Pieri, Rigaud) Proceedings 3rd symposium of resilience engineering. Juan les Pins. France.

Gunderson, L.H., Holling, C.S., eds. (2002). *Panarchy: Understanding Transformations in Human and Natural systems*. Washington D.C.: Island Press.

Hale, A. and Heijer, T. (2006). Defining Resilience. In: E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts*. Aldershot: Ashgate Publishing Company, pp. 35-40.

Herrera, I., Hovden, J. (2008). Leading indicators in the framework of resilience: a conceptual approach. In. Ed. (Hollnagel, Pieri, Rigaud) Proceedings 3rd symposium of resilience engineering. Juan les Pins. France.

Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method.* Oxford, UK: Elsevier Science.

Hollnagel, E. (2004). *Barriers and accident prevention.* Aldershot: Ashgate.

Hollnagel, E. & Woods, D.D. (2006). Epilogue: Resilience Engineering Precepts. In: E. Hollnagel, D.D. Woods, and N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts.* Aldershot: Ashgate, pp. 347-358.

Hollnagel, E. (2007). IO07 presentation: Resilience Engineering and Proactive Safety Management, presentation held at the *IO07, The 3rd international conference on integrated operations in the petroleum industry*, Trondheim, Norway, October 2 - 3, 2007.

Hollnagel, E. (2008) "Preface" and "Safety management, looking back or looking forward" In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilient Engineering Perspectives*, Aldershot: Ashgate.

Hollnagel, E. (2009). *The ETTO Principle: Efficiency-Thoroughness Trade-Off*. Farnham: Ashgate.

Kjellén, U. and Larsson, T. (1981). Investigating accidents and reducing risks: a dynamic approach. *J. Occupational Accidents, 3* (2), 129-140.

Leveson, N., Duplac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., Barrett, B. (2006) "Engineering Resilience into Safety-Critical Systems." In: E. Hollnagel, D.D. Woods, and N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts.* Ashgate Publishing Company, pp. 95-123.

Leveson, N.G. (2004). A new accident model for engineering safer systems. *Safety Science, 42*(4), 237-270.

Macchi, L. (2010). *A Resilience Engineering approach to the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for Air Traffic Management safety assessment.* Ph.D. Thesis. École Nationale Supérieure des Mines de Paris, France.

Macchi, L., Hollnagel, E. & Leonhardt, J. (2008). *A systemic approach to HRA: A FRAM modelling of Control Overflight activity*. 4th Eurocontrol Annual Safety R&D Seminar. Southampton, UK.

Mendoça D. (2008) Measures of Resilient Performance. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives*. Ashgate, Aldershot, USA.

Nuutinen, M. and Norros, L. (2009). Core task analysis in accident investigation: analysis of maritime accidents in piloting situations. *Cognition, Technology and Work, 11*, 129-150.

Pavard, B., Dugdale, J., Saoud, N., Darcy, S., Salembier, P. (2008). Underlying concepts in robustness and resilience and their use in designing socio-technical systems. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives*, Aldershot: Ashgate.

Perrow, C. (1984). *Normal Accidents: Living with High-risk Technologies*, New York: Basic Books.

Reason, J. (1990). *Human error,* New York: Cambridge University Press.

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot: Ashgate.

Reason, J. & Hobbs, A. (2003). *Managing Maintenance Error*, Aldershot: Ashgate

Reason, J. (2008). *The Human Contribution. Unsafe acts, accidents and heroic recoveries*. Aldershot: Ashgate.

Renn, O. (2008). *Risk Governance. Coping with Uncertainty in a Complex World*. London: Earthscan.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K. & Herrera, I.A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives*. SINTEF report (STF38 A 004403), ISBN: 82-14-02724-1.

Van Steen, J., ed. (1996). *Safety Performance Measurement*. Rugby : Institution of Chemical Engineers

Wackers, G. (2006). *Vulnerability and robustness in a complex technological system: Loss of control and recovery in the 2004 Snorre A gas blow-out.* Working paper no. 42/2006. Oslo: Center of Technology, Innovation and Culture, University of Oslo.

Weick, K., Sutcliffe, M. (2001) *Managing the unexpected. Assuring High Performance in the Age of Complexity.* University of Michigan Business School Management Series San Francisco: Jossey-Bass.

Weick, K., Sutcliffe, M. (2007) *Managing the unexpected*. Resilient Performance in the Age of Uncertainty. Second Edition. San Francisco, Calif. : Jossey-Bass

Westrum, R. (1993). Cultures with Requisite Imagination. In J. Wise, D. Hopkin, and P. Stager, eds. *Verification and Validation of Complex Systems: Human Factors Issues*, New York: Springer-Verlag, pp 401-416.

Westrum, R. (2006). A typology of resilience situations. In *Resilience Engineering Concepts and Precepts* edited by Hollnagell, E., Woods, D., Leveson N., Aldershot: Ashgate

Woltjer, R. and Hollnagel, E.(2007). The Alaska airlines flight 261 accident: a systemic analysis of functional resonance. *Proceedings of the 2007(14th) International Symposium on Aviation Psychology*, April 23-26, Dayton, OH.

Woods, D.(2006). Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making. Testimony on *The Future of NASA* for Committee on Commerce, Science and Transportation, John McCain, Chair, October 29, 2003

Woods, D.D. (2006). Essential Characteristics of Resilience. In: N. Leveson, E. Hollnagel, and D. D. Woods, *Resilience engineering: concepts and precepts*. Aldershot: Ashgate, pp. 21 – 34.

Woods, D.D. & Hollnagel, E. (2006). "Prologue: Resilience Engineering Concepts." In: E. Hollnagel, D.D. Woods, & N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts*. Ashgate Publishing Company, pp. 1-6.

Woods, D.D., Johannesen, L.J., Cook, R.I., and Sarter, N.B. (1994). *Behind Human Error: Cognitive Systems, Computers, and Hindsight (State-of-the-art report).* Wright-Patterson Air Force Base, OH: Crew System Ergonomics Information Analysis Center.

Woods, D. and Wreathall, J. (2003). *Managing Risk Proactively: The Emergence of Resilience Engineering*. Columbus: Ohio Universtity, 2003.

10 Summary and comparison of the perspectives

In the previous chapters, we discussed one perspective at a time. It may not be quite clear how much the perspectives have in common, or to what extent they are contradictory or complementary. We will therefore compare the perspectives with regard to a few central issues. The comparison is summarised in Table 5.[42]

10.1 Notions of immediate causes of accidents

The energy and barrier perspective provides an explicit view on the immediate causes of accidents: Accidents occur when objects are affected by harmful energy out of control, in the absence of effective barriers between the energy source and the object. This view of accident causation seems to be explicitly or implicitly accepted by most people that are occupied by accident prevention and risk analysis.

Proponents of the other perspectives do not explicitly contradict the energy view of accident causation. However, it is elaborated in different ways. In Normal Accident Theory, Perrow (1984) restricts attention to systems accidents, which are caused by unanticipated interactions of multiple errors. Researchers in the HRO tradition tend to say little explicitly about the nature of accident causation, but their implicit idea seems to be that accidents are triggered by errors that have not been recovered in time. Turner's theory of man-made disasters explicitly associates accidents with a breakdown in the flow and interpretation of information within an organisation. In the perspective of conflicting objectives, accidents may be seen as the results of actors transcending the operational envelope of the systems they operate. From a Resilience Engineering point of view, accidents occur when various sources of variation, such as Efficiency-Thoroughness Trade-Offs are amplified through interactions and functional resonance. At this level, the perspectives are complementary, rather than contradictory.

10.2 Notions of "root causes" of accidents

With the term "root causes" we refer to system attributes or processes that are used to explain why the immediate causes of accidents occur. Proponents of the energy perspective tend to focus on failures to establish and maintain adequate barrier functions. They may also point to dependencies among barriers, since such dependencies may increase the likelihood that several barriers may fail simultaneously.

[42] We have not included a comprehensive discussion on research needs in this report. However, we identified a few areas in the first version of the report:
The research on resilient organisations has been conducted on aircraft carriers and in the nuclear industry. These types of industries have a lot of resources and military organisations do not have to consider profit to operate. We need more studies from other industries to examine whether the findings can been found in other areas. And it is particularly important to study industries with fewer resources than aircraft carriers and nuclear industry.
We need more field studies of decision-making in normal settings. What is actually happening in complex environments concerning decision making? Are organisations in the oil and gas industry able to reconfigure in response to emergencies or periods of extreme demand?
One important lesson after the terror attacks on September 11, 2001 is that the risk and safety community will have to pay more attention to the danger for terror attacks and sabotage. We need to assess the extent to which the perspectives outlined in this memo can be fruitfully applied to issues related to intentional harm.

Normal Accident theory finds an underlying problem in a mismatch between the properties of the system and the control strategy. Such a mismatch occurs if a centralised control regime is applied to system with high interactive complexity, or if a decentralised control regime is applied to a tightly coupled system. A tightly coupled system with high interactive complexity is inherently vulnerable, since a mismatch is bound to occur, irrespective of whether a centralised or a decentralised control strategy is applied.

The theory of High Reliability Organisations does not say much explicitly about root causes of accidents. By turning around their findings from organisations with very reliable performance, one may suggest that less reliable organisations may be characterised by a failure to build organisational redundancy and by a failure to adapt the organisational structure in the face of demanding situations.

In Turner's theory of Man-made disasters, accidents are viewed as the culmination of a process in which the prominent perceptions and interpretations in the organisation gradually diverge from the realities manifested by danger signals and warnings from the outside. This process may often includes decoy effects, where a less important problem distracts the attention form the problems that actually cause trouble

In the perspective of conflicting objectives, several mechanisms may contribute to accidents. High-level decision-makers may deliberately *take a risk*, or they may *run a risk*, i.e. make a decision (or non-decision) which affects the risk level without considering the impact of that decision. The impact of such decisions may be indirect. For instance, a high-level decision-maker may fail to provide the resources that are needed for safe operation of a system. Unforgiving systems, with "invisible" and/or "untouchable" boundaries, may lead to systematic erosion of safety margins or to episodes where actors inadvertently break the envelope of safe operations. Opaque systems where safety-critical decisions are highly distributed may lead to situations where some actors influence the operational boundaries of other actors in ways that are not noticed by the latter.

Resilience Engineering is more a theory about coping ability than a theory about accidents. We may, however, propose a possible "construction" of a Resilience Engineering view of root causes of major accidents: Major accidents arise when the coping capacity of an organisation is insufficient to handle the emerging dangerous interactive patterns of the technology. Resilience Engineering is strongly influenced by Normal Accident theory in this respect.

Table 5. Comparison of the perspectives on resilient organisations.

Issue	Energy and barrier perspective	Normal accident perspective	HRO perspective	Information processing perspective	Conflicting objectives, adaptation and drift	Resilience Engineering perspective
Notion of immediate causation of major accidents	Object affected by harmful energy which is out of control in the absence of effective barriers between energy source and object	System accidents characterised by unexpected interaction of multiple errors, some of which are usually latent	There seems to be an implicit understanding that accidents are caused by un-recovered errors.	A breakdown in the flow and interpretation of information which is linked to the physical events.	Actors cross boundaries towards unacceptable risk in effort to locally optimise behaviour.	Accidents may occur when various sources of variation (e.g. Efficiency-Thoroughness Trade-Offs) are amplified through interactions and functional resonance.
Notion of root causes of major accidents	Failure to establish and maintain adequate barrier functions Dependencies among barrier functions	System accidents are caused by a mismatch between system properties (complexity, coupling) and control strategy. Contradiction between demand for decentralised control and centralised control in complex, tightly coupled systems.	Not discussed explicitly.	Disasters develop as a process in which the prominent perceptions and interpretations in the organisation gradually diverge from the realities manifested by danger signals and warnings from the outside.	High level decision makers taking risks and running risks. Unforgiving systems (invisible and "un-touchable" boundaries). Distributed decision making in dynamic and opaque systems.	A mismatch between the coping capacity of the organisation and the emerging dangerous interactive patterns ("intractability") of the sociotechnical system.
Critical assumptions	All accidents involve energy flow out of control as the immediate cause of harm. Effective risk control strategies can be found by focussing on energy flows.	Systems with high interactive complexity require decentralised control. Tightly coupled systems require centralised control. Organisations can not be centralised and decentralised at the same time.	"Human errors are here to stay". However, it is possible to achieve nearly faultless performance through organisational redundancy. Organisations can change and adapt to different situations.	A disaster is almost always associated with recognition of a disruption or collapse of the existing cultural beliefs and norms about hazards.	Activities tend to migrate towards the boundary of acceptable performance as actors' search viable trade-offs between such considerations as workload and productivity.	Sociotechnical systems are always changing. Variation and non-linear interaction effects are not only inevitable, but also necessary. It is possible to anticipate, attend and respond to even intractable systems.

Issue	Energy and barrier perspective	Normal accident perspective	HRO perspective	Information processing perspective	Conflicting objectives, adaptation and drift	Resilience Engineering perspective
What is the relationship between minor and major accidents?	Minor and major accidents have the same basic causes. However, major accidents tend to involve failure of more than one barrier.	Minor accidents are often caused by a single failure. Major accidents are caused by multiple failures and are related to the structural properties of the system (complexity, coupling, and control).	Not explicitly discussed. In a HRO, one would expect major accidents to involve failure of one or more recovery mechanisms.	Many smaller accidents can be indicators for disasters (large-scale accidents), but they do not necessarily have the same root causes - failures in information processing.	Major accidents tend to arise through a pattern of distributed decision-making and conflicting objectives, more often than minor accidents do.	Minor accidents occur so often that the organisation learns how to respond (regular threats). Major accidents are often either unexpected but imaginable (irregular threats) or even impossible to imagine and exceed the organisation's experience (unexampled events).

10.3 Critical assumptions

In order to focus on the contrasts among the perspectives, we have tried to identify critical assumptions underlying each perspective (Table 5).

The energy and barrier perspective seems to entail two critical assumptions. The first one is that all accidents involve energy flows out of control as the immediate cause of harm. The second assumption is that effective risk control strategies can be derived from this energy view. We discussed these assumptions in Section 4.7.

Perrow's (1984) Normal Accident Theory makes three assumptions related to structural properties of socio- technical systems: (1) Systems with high interactive complexity can only be effectively controlled by a decentralised organisation. (2) Systems with tight couplings can only be effectively controlled by centralised organisations. (3) An organisation cannot be centralised and decentralised at the same time.

The following three claims are central to HRO Theory: (1) It is not feasible to totally eliminate erroneous actions. (2) However, it is possible to achieve nearly faultless performance by developing organisational redundancy, so that nearly all-erroneous actions are recovered before lead to severe harm. (3) Some organisations adapt to extreme demands by changing to an informal, competence based organisational structure and by adopting an informal interaction style.

The basic assumption of Turner's theory of man-made disasters is that there is a close link between the physical events involved in major accidents and the way the organisation handles information on hazards.

The perspective on conflicting objectives, as presented here, entails one central assumption: Human activities tend to migrate toward the boundary of acceptable performance as the actors search viable trade-offs between such considerations as workload and profitability.

As mentioned above, Resilience Engineering seems to resemble Normal Accident theory in its understanding of the origin of major accidents. However, Resilience Engineering Resilience Engineering is based on the assumption that social systems are always in a state of flux. Variation and non-linear interaction effects are seen not only as inevitable, but also as necessary. Many researchers in this tradition seem to share a tacit assumption that it is possible to anticipate, attend and respond to even intractable systems.

At this level, the perspectives clearly point in different directions. No perspective explicitly contradicts the idea that accidents involve uncontrolled flows of energy. However, the other perspectives tend to entail a claim that organisational structure or processes must be included if we are to give a fruitful account of major accidents. Some researchers (e.g., Sagan, 1993) view Normal Accident theory and HRO theory as contradictory, whereas others (e.g. Rasmussen, 1994a) view them as complementary.

10.4 The relationship between major and minor accidents: The popular version of the iceberg theory

Few principles have been cited more often by safety practitioners than the iceberg theory. This principle was proposed by Heinrich (1931)[43]. For a given activity he compared the ratios between:

1. The number of disabling insurance claim injuries (e.g. workers crossing the rail tracks to get to work between rail wagons get caught as two wagons moved together),
2. Minor accidents from different scenarios related to the same activity (e.g. workers tripping over rails or stumbling on the uneven ground), and
3. The number of opportunities for an accident to occur (e.g. the number of times people crossed tracks). The "no injury" category was thus a measure of exposure, and not a frequency of near misses.

Heinrich found that the ratios were very variable, depending on the activity. The published ratios shown in (Figure 15) should therefore be interpreted as averages across a broad range of activities. Later versions of the triangle referenced by Hale (2000) are based on other classes of events and give different ratios.

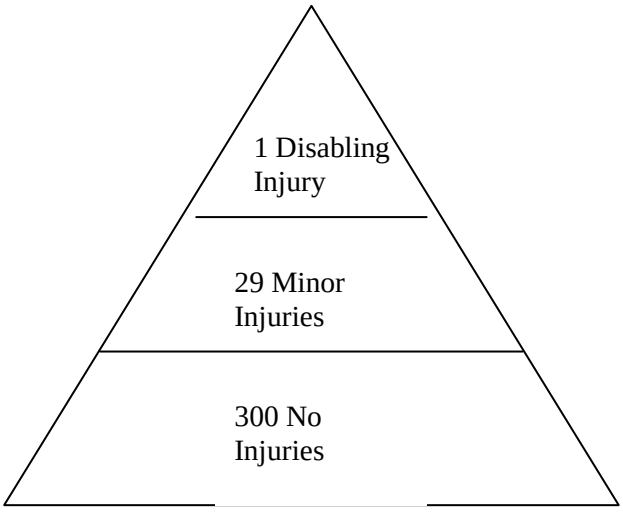

Figure 15. The Iceberg theory. Adapted from Heinrich (1931), cited in Hale (2000).

Hale (2000) identified two reasons why the inventors published this triangle. They wanted to argue that there were many precursors to disabling accidents. Prevention did not have to wait until an accident had happened. The other purpose was to find a shorthand way of estimating accident costs based on incomplete accident records or a sample of the relevant accidents. The objective of this exercise was to motivate senior managers to invest in prevention.

Heinrich did *not* claim that the underlying causes for each degree of seriousness were the same. The original statements of the iceberg theory thus made no strong claims concerning the relationships between major and minor accidents. However, a rather different version of the

[43] Our presentation of Heinrich's original version of the iceberg model draws heavily on a paper by Andrew Hale (2000).

iceberg model came into fashion among some managers, consultants and safety practitioners during the eighties and nineties. According to this popular version, near misses, minor accidents and major accidents (including those with many fatalities) stem from the same causes. Moreover, according to this popular version, the ratios between major accidents, minor accidents and near accidents are constant. This implies that a preventive measure that successfully reduces the frequency of minor accidents will reduce the frequency of major accidents by a similar proportion. Another implication of the popular version is that low LTI[44] rates can be taken as a trustworthy indicator of the risk of major accidents.

Hale (2000) bluntly labelled the popular version of the iceberg theory an urban myth. He concluded that the available empirical evidence strongly indicates that major and minor injuries differ systematically with regard to locations, activities, amounts of energy released and the number and types of barriers or recovery opportunities that were bypassed in the event.

The perspectives outlined in this report may be used to further illuminate why the popular version of the iceberg theory is not plausible when it is extended to major accidents involving several fatalities. This amounts to asking what the perspectives have to say about the similarities and differences between major and minor accidents.

According to the energy and barrier perspective, minor and major accidents are both caused by uncontrolled energy releases. However, major accidents usually involve larger amounts of energy and the failure of multiple barrier functions, whereas minor accidents may arise from a single failure. The energy sources are also often different. Minor accidents are typically caused by people tripping, falling, being hit by falling objects, or loosing control of hand tools. Major accidents are typically caused by fires, explosions, collisions and collapsing structures. Finally, the barriers failing in major accidents are often different from the barriers failing in minor accidents.

In Normal Accident theory, this contrast is captured by the distinction between component failure accidents and system accidents. Normal Accident theory goes one step further, by relating system accidents to structural problems – either a highly interactive system controlled by a centralised organisation, or a tightly coupled system controlled by a decentralised organisation.

We are not aware of explicit discussions of this issue among HRO theorists. Their position seems to imply that a major accident in a HRO would typically involve a failure of organisational redundancy, i.e. of the mechanisms that usually recover errors before they lead to a catastrophic outcome. A minor accident might occur because recovery mechanisms were not established in the first place.

Neither are we aware of explicit discussions of this issue in Turner's work on Man-made disasters either, since his discussions concentrate on major accidents. He implies that many smaller accidents can be indicators for disasters. He does not seem to imply that minor accidents arise from a long-term process of deteriorating information processing. Major accidents tend to come as fundamental surprises (Woods, 1990), whereas most minor accidents resemble earlier accidents experienced by the organisation. Prevention of minor accidents can thus be based on epidemiological approaches, whereas the prevention of major accidents requires analytic or evolutionary strategies (Rasmussen, 1997).

From the perspective of conflicting objectives, minor and major accidents are both related to the tendency of human activities (including decision-making) to migrate towards the boundary of

[44] LTI – Lost Time Incidents.

acceptable performance (Section 8.2). However, the adaptation processes leading to migration may take place under different conditions (Rasmussen, 1994b). In manual activities, which are often associated with minor accidents, adaptation often takes place in a feedback loop with a single operator and his equipment, tools or materials and their environment (e.g. a car driver adapting the speed to the environment, based on cues such as speedometer readings, speed limit signs, the quality of the road, traffic density and feedback from the vehicle). Organisational accidents in distributed systems typically involve several actors, each seeking local optimisation based on an incomplete view of the system. Major accidents thus tend to arise from situations where separated adaptation processes interact in a way that was not foreseen by the actors.

From a Resilience Engineering perspective, minor and major accidents entail different learning and coping challenges. Minor accidents occur so often that the organisation can learn how to respond by experience. Major accidents are often unexpected but imaginable (irregular threats), or they may even be impossible to imagine and exceed the organisation's experience (unexampled events). The learning and coping capacities that are needed to cope with the risk of major accidents are thus fundamentally different from the learning capacities needed to prevent minor accidents.

Taken together, these perspectives present several reasons why one should not expect major and minor accidents to arise from very similar patterns of safety problems. A company that displays excellent LTI records could be heading for a disaster, since some of the factors that contribute to major accident risk have little impact on the LTI frequency.[45]

Another important implication is that prevention of major accidents requires measures that go beyond those needed to prevent minor accidents. One of the most dangerous misunderstandings related to the iceberg theory is the idea that safety culture programs that are directed at the prevention of minor accidents will be sufficient to control the risk of major accidents. At worst, this idea may be used as an excuse for not providing adequate barriers against major accidents. The potential consequences of this fallacy are demonstrated in the Texas City disaster, where 15 workers were killed (CSB, 2007). In Section 9.4 of their report on Texas City, the U.S. Chemical Safety and Hazard Investigation Board demonstrate that BP failed to respond effectively to known process safety problems and that management and resources attention were diverted towards disciplining workers that were caught breaking the rules concerning personal safety (CSB, 2007:168).

As a consequence, we need to consider the implications of these perspectives for prevention of major accidents. This is the topic of the next chapter.

[45] See Hopkins (2000b) for an example.

11 From theory to practice: Implications for risk control and accident prevention

We concluded the previous chapter with a claim that preventive strategies that work well with minor accidents may fail to provide effective control of major hazards. In this chapter we will summarise practical implications of the perspectives presented the previous chapters: How can we monitor major hazards? What risk reduction strategies can we derive from the perspectives? How can we learn the right lessons from disasters, minor accidents and near misses? What are the impacts of organisational change on major accident risks?

11.1 Monitoring the risk of organisational accidents

Effective safety management in complex and dynamic organisations is inconceivable without adequate feedback mechanisms (Kjellén, 2000:114). This is not only a matter of providing managers with appropriate information to support rational decision-making. Persistent feedback helps attract the attention of managers and employees to safety. Compelling feedback can also be necessary to "unfreeze" a rigid and unrealistic set of shared assumptions associated with the incubation period preceding a disaster (see Section 7.1). In this section we will discuss how the risk of organisational accidents can be monitored, with a view to the five theoretical perspectives.

The most straightforward way to monitor the risk of *minor* accidents in a stable system is to use loss-based performance indicators such as Lost Time Incident rates or Severity rates[46]. However, we should not confuse monitoring of risk with monitoring of loss. When speaking about risk, we usually refer to a *potential* for unwanted events in the future.[47] In contrast, the loss-based performance indicators express experienced loss in the past. Still, given a reliable reporting system, it makes good sense to interpret a statistically significant trend in experienced loss related to minor accidents as an indication of a corresponding change in the risk of minor accidents. Even a non-significant deterioration in a loss-based performance indicator may lead us to take action if we consider it better to react on a "false alarm" than to wait for enough aversive data to confirm a significant trend.

It is less straightforward to monitor the risks of major accidents. Major accidents are rare events, even if we consider highly aggregated data (e.g. "all accidents with more than five fatalities in the Norwegian petroleum industry"). The time needed to detect a significant trend in major accident frequency is generally far too long to provide useful feedback in a safety management context. Major accidents are also too rare to attract continuous management attention.

A common answer to this problem is to devise safety performance indicators based on information about contributing factors and root causes (Kjellén, 2000:248ff). One approach is to rate the elements of a company's safety management systems with reference to a model of an ideal safety management system. This approach is used by the *International Safety Rating System*

[46] The Lost-time injury rate is the number of lost time incidents per 10^6 employee-hours. A lost-time injury is an injury due to an accident at work where the injured person does not return to work on the next shift. The Severity rate (S-rate) is the number of working days lost due to lost-time injuries per 10^6 employee-hours. Fatalities and 100 per cent permanent disability are usually counted as 7500 days lost (Kjellén, 2000).

[47] A thorough discussion of the risk concept is beyond the scope of this report, but it may be worth noting that risk may be viewed in two fundamentally different ways: (1) as a property of the world, which exists independently of the person who makes statements about the risk, and (2) as an expression of uncertainty of observable quantities of the world. See Aven (2003) for a discussion advocating the latter position.

(Bird and Germain, 1990), the Safety Element Method (Alteren, 1999) and Tripod Delta (van der Want, 1997). Can the perspectives presented in this report help us identify relevant indicators or conditions that could be followed up in order to identify changes in the risk of organisational accidents?

The *energy and barrier perspective* emphasises the fact that barrier functions need to be monitored and maintained. Barrier elements can deteriorate and interdependencies between barriers may arise or increase. Risk monitoring could be performed by investigating attributes of each individual barrier function, and of the relationship between them:

- How can a specific barrier function be taken care of? What are the important barrier elements?
- How can barrier functions fail?
- Are there interdependencies with other barrier functions (common cause failures)?
- How can barrier functions deteriorate?
- How can barrier functions be maintained and monitored?
- Are there potential indicators to measure availability/ efficiency?

A major challenge in monitoring barrier functions is to handle the diversity of different ways a barrier function may be carried out, and the great number of barrier elements involved. A quantitative approach for risk monitoring is the use of risk indicators. These may be based on the causal models in Quantitative Risk Analyses (Øien, 2001). The total set of risk indicators (technical and organisational) can be used to estimate the total change in risk, in the time periods between updates of the QRA.

Table 6. Practical implications of the perspectives on resilient organisations.

Issue	Energy and barrier perspective	Normal accident perspective	HRO perspective	Information processing perspective	Conflicting objectives, adaptation and drift	Resilience Engineering perspective
How can major accident risk be monitored?	Monitor the quality / effectiveness of barrier functions	Monitor interactive complexity and tightness of coupling. Monitor compatibility between control structure and technology.	Monitor the structural and cultural preconditions for organisational redundancy.	Combine HazOps and holistic approaches that include human and organisational factors. Check the organisation's ability to follow up signs of danger, e.g. near-accidents.	Is the feedback between different levels (vertical) from government to the daily immediate and open? Measurements/ strategic tools like balanced scorecard taking account of risk can be of help.	Monitor the ability to cope with surprises (intractable events). Monitor normal performance variability, buffering capacity, balance between flexibility and stiffness and cross scale interactions.
Risk reduction strategies	Include barrier functions in the design of the system; strive for 'defence-in-depth'. Ensure that compensatory measures are taken when barriers are unavailable. Monitor and maintain barrier functions throughout system life.	Reduce complexity or "loose" couplings. Apply decentralised control in systems with high interactive complexity, centralised control in tightly coupled systems. Discard high-risk systems that are both complex and tightly coupled.	Build organisational redundancy Build cultures that combines requirement for fault-free performance with openness to the fact that errors do occur.	Make systematic efforts to collect and analyse information about hazards and keep important hazards on the agenda. Build a culture that promotes active search for signals of danger, and knowledge sharing across organisational boundaries.	Make boundaries to unacceptable performance visible and touchable. Train personnel in boundary handling. Establish "counter-pressures" that favour safe performance. Keep a focus on situations where each stakeholder has a limited overview over the overall situation.	Risk reduction is achieved by increasing coping ability rather than eliminating variability. Build and maintain the abilities to anticipate, attend, respond and learn. Maintain a "mute dialectic" between procedures and practice.

Issue	Energy and barrier perspective	Normal accident perspective	HRO perspective	Information processing perspective	Conflicting objectives, adaptation and drift	Resilience Engineering perspective
How can we learn from disasters and incidents?	We will see the effects of barriers and the barriers can be improved. Incidents can inform us about unexpected interactions or dependencies between barriers.	Incidents can provide information on unexpected interaction. However, single failure incidents provide little information on the structural problems that make a system prone to have system accidents.	Primarily, we learn from the daily operation and the normal procedure, but incidents/ accidents may demonstrate the absence of structural or cultural preconditions for organisational redundancy.	Arguing for use of several organisational learning approaches (e.g. Argyris & Schön [1978] double-loop learning where procedures for gathering signals about hazards are directly challenged). Focus on social learning, rather than individual learning.	Causal paths in an incident should be tracked beyond operator errors back to the normal operations in organisational units that contributed to create the incident scenario. Based on several incidents, one may create a work support system that makes decision-makers aware of the potential side effects.	Reveal interaction patterns that were not spotted and why, i.e. shortcomings in anticipation and coping. Incorporate (low fidelity) simulation to develop flexible and innovative responses. Do not expect an exact replay – the next disaster will be somewhat different.
How can technological and organisational change influence risk levels?	Increase of scale or speed may lead to increased accumulations of hazard sources. Maintenance and monitoring of barriers may deteriorate if requisite resources are no longer provided.	The degree of interactive complexity and coupling can change the preconditions for controlling the technology. Organisational change can cause incompatibility between control structure and technology.	Downsizing may affect the preconditions for organisational redundancy. HROs are capable of spontaneous reconfiguration in response to high demand or crisis.	Organisational change can make information flow more complex and indirectly influence risk. A problem solving process may be terminated because the relevant decision forum disappears.	Vertical communication lines can be weakened or disappear. Boundaries can be exceeded individually or by several actors at the same time. The systems of management and regulation may be unable to keep up with a fast pace of change in technology.	Intractability is inherent in all sociotechnical systems. Both organisations and technology are in constant change. Hence, work operations will always be underspecified to some degree. Technological and organisational changes may create discontinuities and new combinations that render the coping strategies (habits) less suitable than before.

According to *Normal Accident theory* (Perrow, 1984), the organisation should ensure that the control structures are compatible with the properties of the technology. For instance, in order to cope with a tightly coupled technology, an organisation needs to maintain a correspondingly tight control structure. This may prove a challenging task if tight controls are not instrumental to carrying out the primary tasks (e.g. production). In this case, performance is likely to drift away from prescriptions given in rules and regulations as local adaptations take place. Moreover, the centralised control structures that are needed to handle emergencies may fail to materialise if they are not prepared and reinforced, e.g. through emergency drills. On the other hand, an organisation that handles technology characterised by complex interactions may need to monitor its capacity to improvise in a safe and effective manner in case of disturbances in the production process. There is also a need to monitor the technical modifications, since such modifications may introduce increased complexity or tighter couplings.

Monitoring of major accident risks following the *HRO theory* might focus on organisational redundancy in safety critical tasks: (i) Are the structural (instrumental) pre-conditions of organisational redundancy present (at least two persons with overlapping competence, access to critical information, etc.)? (ii) Does the organisational culture contribute to organisational redundancy? These issues are of current interest in connection with downsizing of organisations, where the structural conditions of organisational redundancy may be vulnerable. In some cases, there may no longer be a second person present to build organisational redundancy, or expert support may be less available. Are the preconditions for adequate handling of normal operations, as well as handling of deviations and emergency situations present in the organisation? The cultural dimension of organisational redundancy is not easy to monitor directly. Possible approaches might be to analyse near misses, and to carry out a working environment survey, focusing on questions about loyalty, solidarity, frankness, authority gradient and communication.

HRO theorists also draw attention to the organisation's capacity to adapt to unforeseen situations. In this context Weick and Sutcliffe (2001) have devised a set of simple questionnaires devised to assess the degree of "mindfulness" in an organisation.

Risk monitoring, based on the *Information processing perspective* of accidents, may combine HazOps with holistic approaches that include human and organisational factors (Turner and Pidgeon, 1997). Turner and Pidgeon (1997: 187-189) emphasise the role of safety culture as a key for handling and continuously monitoring risk. They propose that the following issues should be focused in risk monitoring: i) senior management commitment to safety; ii) shared care and concern for hazards and their impact upon people; iii) realistic and flexible norms and rules about hazards; and iv) continual reflection upon practice through monitoring, analysis and feedback systems. A possible objective for monitoring efforts could be to assess the organisation's responses to signs of trouble, e.g.

- How does the organisation respond to concerns and warnings from outsiders (e.g. clients, contractors, media, regulatory authorities, NGOs)?
- What measures are decided and implemented in response to incidents and accidents? (None? Cosmetic fixes? Blaming the victim? Change of work practice or hardware? Change in managerial practices?)
- How are people voicing concern ("whistleblowers") treated? (Ignored? Ostracised? Celebrated?)

The perspective *Conflicting objectives, adaptation and drift* addresses the capacity to handle conflicting objectives without drifting into dangerous system states. Uncontrolled local

adaptations may lead to catastrophic and fundamentally surprising events in systems characterised by distributed decision-making. According to Rasmussen's "migration" model, the boundaries of safe performance should be made visible and touchable, so that the actors have a way to know when they approach or exceed the boundaries. In situations with conflicting demands, people may face incentives for taking short cuts. Rasmussen also emphasises the need for feedback between different levels, from governments to the shop floor. In addition to the vertical dimension, we may be faced with cooperation between different companies at the operational level (following outsourcing, use of contract work). This will demand monitoring directed at cross border activities. Risk monitoring, following this perspective, should emphasise the following questions: Is it possible for a single actor to know if he or she exceeds the boundaries for safe behaviour (does the system give distinct responses)? Will he/she be able to recover in case of exceeding the boundaries (or is the environment 'unforgiving')? Is the information level (e.g. the number of alarms) adapted to the human capacity? Other questions for review are about the relationship between safety and economy. Do managers follow up safety performance to the same extent as economy? Are high-level decision-makers held accountable for the accident risks associated with their decisions? Does risk monitoring include cross border operations when more than one enterprise is present (e.g. in the case of outsourcing)?

From a *Resilience Engineering* point of view, organisations should monitor their coping ability. There is a need to monitor the normal performance variability, but there is also a need to monitor the capacity of the organisation to handle the effects of this variability, including unexpected interaction effects.

We should realise that performance indicators are two-edged swords. A negative trend can alert the organisation to problems, whereas a positive trend can lead managers to conclude that safety has been taken care of, and that they can direct their attention to other issues. Reliance on a single indicator can lead managers to focus on one aspect of health and safety (e.g. lost time incidents) and at the same time pay less attention to other health and safety issues (e.g. potential for major accidents; see Hopkins, 2000b for an example). In general, the persons whose performance is monitored tend to adapt to their behaviour to the performance indicators that are used.

11.2 Risk reduction strategies

An important advantage of applying more than one perspective on organisational resilience is that each perspective contributes to possible risk reduction strategies. By combining several perspectives, we can thus build a larger repertoire of risk reduction strategies. To gain optimal effect from risk reduction measures we have to ensure that structural and cultural aspects of the risk reduction strategies are compatible. The structural basis for safety control may consist of rules, regulations and working procedures, authority and responsibility assignment, reporting systems, formal communication, risk assessments and routines for deviation control. Cultural aspects of safe work performance include activities like ensuring employee involvement, knowledge sharing and organisational learning.

The *energy and barrier perspective* focuses on limiting energy amounts and controlling energy flows, as illustrated by Haddon's ten strategies for loss reduction (Section 4.1). Barrier functions are designed into technical systems and operational procedures. Administrative barriers can be seen as a part of this tradition. One example is the work permit system. No single barrier is 100 % effective, because they may have weaknesses due to active failures or latent conditions. Therefore, one way to build more safety into a technical system is to introduce multiple barriers, or a 'defence-in-depth' strategy (Reason, 1997). To be effective, this approach requires that interdependencies between barrier functions are minimised. The approach also requires provisions for monitoring and maintaining barriers.

According to *Normal Accident theory,* the preferred risk reduction strategy is to modify the technology in ways that reduce interactive complexity and loosen the couplings. This is the only effective strategy with systems that are both highly interactive and tightly coupled. An alternative strategy is to adapt the organisation to the technology: Decentralise control with high interactive complexity, centralise with tight couplings. In this context, decentralisation implies more than just changing formal authorities. Local agents must be given the resources (e.g. information, competence, manpower) that are necessary to cope with the situations they may face.

The *HRO perspective* focuses on being proactive and to predict and prevent potential dangers as early as possible. A central risk reduction strategy is to build organisational redundancy. This strategy requires that a sufficient number of competent personnel are available, so that some overlap in competence, responsibilities and possibilities for observation is achieved. Workplace design should allow, and even encourage, seeking counsel from a colleague, observation of other people's work, and intervention in case of an erroneous action. Moreover, it is necessary to build a culture that encourages questioning and intervention. Another strategy is to build organisations with a capacity for spontaneous, adaptive reconfiguration. Among other things, this involves building a *flexible culture* (Reason, 1997, Chapter 9).

The *information processing perspective* puts a strong focus on the gathering, interpretation and dissemination of information. One aspect of this is the systematic collection, analysis and dissemination of information about hazards, and actively trying to find out what we do not know. Another aspect is the building of "cultures with requisite imagination", i.e. cultures which encourage sharing of information, innovation and learning (Westrum, 1993). Reason (1997, Chapter 9) conceptualised these challenges in terms of building an *informed culture*, a *reporting culture*, and a *just culture*.

With regard to *conflicting objectives*, three risk reduction strategies can be derived from the migration model (Section 8.2, p. 80): The first is to make boundaries towards unacceptable risk visible to the relevant actors. This can be challenging in practice, since we tend to adapt to many kinds of warnings, so that the boundary can become "invisible" over time. The second strategy is to make boundaries touchable. This implies that the actor is given a chance to recover if he strays beyond the boundary to unacceptable performance. The third strategy is to provide a "counter-pressure" that favours safe actions, e.g. through follow-up and feedback. In situations with *distributed decision making,* when a lot of activity is taking place and each stakeholder has a limited overview, there is a possibility that decisions perceived as safe by each local actor may interact in unforeseen ways and trigger an accident. Such situations may in principle be avoided by giving the actors access to more information, thus improving their situation awareness. This strategy presupposes that the actors have the capacity to handle the increased information load. Alternatively, one may try to program the decisions to be made, i.e. specify in advance the action to be taken by each actor so as to make their actions predictable. The latter approach is characteristic of railway operations. Many actors (e.g. train drivers) have a very restricted view of the total system, but their actions are tightly controlled through regulations, orders and signalling systems so as to avoid conflicts.

The responsibility for safety must be clearly communicated. If a strategic decision is perceived to cause trouble, in let us say the maintenance department, this uncertainty and perception must be immediately communicated back to the management level. This will make it easier to see the relationship between decisions and the risk level, and will also serve as a tool to establish counter pressure. It is an important management task to seek feedback on one's own decisions.

The adaptation perspective also alerts us to the possibility that some risk-reducing measures may lead to behavioural change ("compensation") that reduces the risk-reducing effect (Wilde, 1982).

In extreme cases, a person may overestimate the effect of a risk-reducing measure and change his/her behaviour to a point where the risk is greater than it was before the risk-reducing measure was introduced.

According to the *Resilience Engineering* perspective, risk reduction is achieved by increasing the coping ability of the organisation. The organisation should be prepared to handle events that can be foreseen as well as unexampled events. It is neither feasible nor desirable to eliminate performance variability, but this does not imply that performance variability can be ignored. The organisation thus needs to find acceptable and realistic ways to handle the tensions between procedures and practice. The first step in this direction is to identify the tensions and reflect on the relationship between practice and procedures (Nathanael and Marmaras, 2008).

The risk reduction strategies derived from the different perspectives tend to be complementary, with some overlaps. There is, however, one noteworthy tension. Uncritical application of the energy and barrier perspective might lead us to combine numerous physical, technical and organisational barriers in order to contain a hazard source. According to Normal Accident theory, this strategy could fool us into designing a system with high interactive complexity. A safety system may under adverse circumstances camouflage the source of a disturbance and cause operators to diagnose a problem incorrectly.

In some cases, a search for risk-reducing measures is triggered because a quantitative risk analysis (QRA) produces results that are not compatible with the acceptance criteria of the activity. In such situations, the search for risk-reducing measures is often restricted to factors that are explicitly modelled in the QRA. For instance, if an unacceptable risk level is identified in the QRA of an offshore installation, a common response is to propose a modification of the design and recalculate the risk, using the same QRA approach. Measures to reduce the frequency of hydrocarbon leaks in the first place are often not considered, because such measures will usually not have any impact on the calculated risk if standard QRA procedures are used.

11.3 Learning from disasters and precursors

The perspectives contribute concepts and directions that may help us to describe and explain accidents and incidents. They may also contribute some insight into the preconditions for learning from accidents.

The *Energy and barrier perspective* focuses on effects of barriers and examines how barriers could be improved, or if new barriers should be established. From this perspective, the organisation should use information on disasters and precursors to identify weak points and problems related to barrier functions. It should also use such information to identify and resolve problems related to the monitoring and maintenance of barrier functions. Organisations should, for instance, pay close attention to incidents related to their work permit systems. Work permit systems can be safety critical because they often replace several technical barriers. Finally, one may ask whether the hazardous energy source is really necessary, whether the amount of energy could be reduced, and whether the hazard source is adequately controlled.

The *Normal Accident perspective* leads us to ask whether the presence of interactive complexity or tight couplings contributed to the accident. Incidents could also give the organisation information on how well its control structures are adapted to the properties of its technology. For instance, in the case of an organisation handling a tightly coupled technology, an incident or accidents may reveal gaps in the control structure. Information from incident investigations can thus be used to reduce complexity, loosen couplings, or at least to prepare the organisation to handle the problems created by complexity and tight coupling.

The *HRO perspective* covers both structural and cultural aspects of the organisation. LaPorte and Consolini (1991) stressed that normal situations and precursors, and not only disasters, are important sources for learning. Weick (1987) showed that some HROs (nuclear submarines) use story-telling to build a resilient culture. Stories about accidents and critical incidents have an important place in this socialisation process.

The *information processing perspective* invites us to look for deficiencies in the organisation's information handling prior to the incident or accident. Did someone have the pieces of information that were necessary to foresee and avert the accident? Why was this information not acted on? In some cases, the information that is needed to identify and assess a sign of danger is distributed among several disciplines or organisational units. The focus after accidents must be on social learning, rather than individual learning. People in the organisation should be trained to ask critical question and investigate assumptions in what is termed as "public testing" by Argyris and Schön (1978).

The *conflicting objectives perspective* proposes that systems may drift towards greater risk as performance and decision processes are shaped by competitive pressure. Decision-makers in distributed systems may be running risks because they are not aware of how their decisions interact with the decisions made by other actors. Investigators of accidents and incidents should pay attention to human-system-interaction at the boundary of acceptable performance. They should also examine the way decisions are distributed among decision-makers and decision fora, looking for cases where decisions which interact strongly in their impact on risk are taken in different fora. Rasmussen and Svedung (2000) argue that causal paths in an incident should be tracked beyond operator errors and hardware failures, back to the normal operations in the organisational units that contributed to create the accident scenario. Based on several incidents one may create a work support system that makes decision-makers aware of potential side effects.

According to the *Resilience Engineering* perspective, most major accidents occur because the organisation was taken by surprise by a pattern of interaction. The main point is not to learn how to respond to that pattern of interaction the next time it occurs, since the next accident will probably be somewhat different. It is therefore more to the point to ask *why* the organisation failed to anticipate and prepare for this pattern of interaction. Such an investigation could be a starting point for improving the organisation's anticipation and coping ability. Another point is to learn from successful coping, for instance in incidents where a major disaster was averted through successful improvisation. Again, the point is not only to learn how to cope with one particular scenario, but also to develop a capacity to cope with other unanticipated events.

Accident investigators need to apply several perspectives in order to raise critical questions, since there is always a danger that you will find only what you are looking for. Important questions are:

- Who is represented in the accident investigation group? Does the composition of the group provide for knowledge sharing and the application of multiple perspectives?
- How do experts and lay persons understand the accident?
- What perspectives are used and why?
- Are we able to draw generic lessons from the specifics of a particular incident?
- How can we improve our ability to learn from incidents (second order learning)?

Two common pitfalls should be kept in mind. Organisations often focus too much on the idiosyncratic or atypical aspects of an accident. This may lead to measures that only apply to a specific activity in a specific place under specific circumstances, whereas similar problems in similar situations remain uncorrected. The other pitfall is to tighten procedures and rules to a point where they are not compatible with efficient performance of work. Unrealistic procedures and

rules are not only ineffective. They also tend to produce discrepancies between word and action, and to foster a culture where such discrepancies are tacitly accepted.

11.4 Resilience and change

We noted in the introduction that risk management efforts currently face a very fast pace of change in technology, which is associated with increasing scales of industrial installations and high degrees of integration and coupling of systems. At the same time, organisational structures change dramatically in response to a very aggressive and competitive environment. Finally, the political and regulatory environment changes in various directions; sometimes leading to more elaborate demands for risk control (e.g. the Seveso directive). In this section we will consider organisational and technical change that has been initiated in order to achieve other goals than safety improvements.

The effects of change are obviously complex. At the organisational level, one needs to distinguish between the immediate effect of the change process as such (e.g. employee anxiety about loosing their jobs), and the long-term effect of the changed characteristics of the organisation (e.g., lower manning levels, new control structures). Pfeffer (1998) argued that, while the short terms effect of a downsizing in saved costs are quite easy to achieve and measure, the long-term effects are more uncertain. Lee Marks (1993) has surveyed the consequences of downsizing in US industry, see Table 7.

Table 7. Effects of downsizing (Lee Marks, 1993).

Consequence	Percent of firms reporting
Lower morale among remaining work force	61
More need for retraining remaining employees	41
More use of retraining remaining employees	36
More use of temporary workers and contractors	35
Increased retiree health care costs	30
Entire functions contracted out	25
Wrong people lost	20
Severance costs greater than anticipated	16
Too many people lost	6

These numbers are averages across many industries, and thus hide variations. However, they demonstrate some of the typical effects on downsizing. The high percentages of firms reporting lower morale and retraining needs are noteworthy.

How can technological and organisational change affect the resilience of organisations? From the *energy and barrier perspective* we may note that increases of scale or speed may be associated with increased accumulations of hazard sources (e.g. vehicles that carry more kinetic energy; plants with larger repositories of dangerous substances). However, change may also go in the opposite direction. Efforts to reduce consumption of input factors may, e.g., lead to intensification of processes so that smaller amounts of dangerous substances need to be handled (Kletz, 1991). Inventories of dangerous substances and goods may be reduced to reduce inventory costs. The number of people exposed to a hazard may be reduced as a consequence of reduced manning levels.[48] Change can also affect the resources needed to effectively monitor and maintain barriers,

[48] The impacts of reduced manning level on risk can be complex. The expected number of injuries and fatalities associated with the activity may decrease because fewer persons are exposed to the hazard. The individual risks of the remaining workers may remain unchanged, or perhaps increase somewhat if fewer persons have to perform the same

such as competent manpower. From this perspective, one may want to monitor the backlog on preventive maintenance of safety barriers.

Normal Accident Theory directs attention to changes in technology as well as control structure. Technological change may affect the degree of interactive complexity or lead to tighter coupling. Organisational change may lead to either more or less centralised control structures. As a consequence, the degree of compatibility between technology and control structures may change. Change sometimes leads to reduced risk levels. For instance, Perrow (1984: 159ff) argues that safety in the U.S. system of airways (including Air traffic control) was improved during 1960s and 1970s due to reduced coupling and complexity. However, it seems plausible that the dominant trends in most industries are towards tighter coupling and more interactive complexity. Indeed, Beck (1992, 1999) claims that such changes are part of major transformation of society ("reflexive modernisation"). New risks, such as those related to the greenhouse effect and the nuclear power industry, are global and can strike everyone.

Many of the organisations studied by researchers in the *HRO* tradition are stable and conservative (e.g. Bierly, 1995). This research tradition thus provides limited empirical evidence on the effects of change. However, HRO theory directs attention to possible effects of downsizing on organisational redundancy (Rosness et al., 2000). The instrumental preconditions for redundancy may, e.g., be threatened as a result of reduced manning levels. Going from two control room operators to one may imply that nobody may be there to intervene in case the remaining control room operator responds inadequately to an alarm. Outsourcing may lead to cultural barriers in the organisations, and in some cases weaken the cultural preconditions for organisational redundancy. Organisational change may, on the other hand, be associated with a reduction of authority gradients and thus facilitate communication and cooperation.

The *information processing* perspective emphasises impacts of technological change on the flow of safety-relevant information. This includes the quality of communication channels – the impact of face to face communication is sometimes very different from that of an e-mail or a memo (Weick, 1987). Adoption of information and communication technology thus may have profound impacts on organisational resilience. Organisational change may also affect ongoing problem solving processes. For instance, a decision forum may disappear during a change process, and thus leave some safety issues unresolved. Moreover, organisational change may affect the resources and status of personnel serving as "watchdogs" representing safety interests. These tasks are often associated with staff functions, and may be seen as "non-productive" in organisations undergoing a business process reengineering process.

The *conflicting objectives* perspective emphasises the potential for drift: Many small changes may accumulate and gradually cause a system to migrate beyond the boundary of safe operations. Decision processes that interact strongly in their impact on safety may be allocated to different decision arenas, leading to the possibility of conflicting decision outputs. The pace of technological and organisational change may exceed the speed of information handling in regulatory and safety management processes. A high pace of technological change renders retroactive control strategies ineffective, since experience becomes obsolete at a correspondingly high pace. A common regulatory strategy is to replace detailed prescriptive regulation with goal-oriented legislation (Hopkins and Hale, 2002). This strategy allows enterprises to develop and implement new means to accomplish given safety objectives without waiting for new legislation to approve the new solutions.

---

set of hazardous tasks. The over all effect for society depends on what happens to the persons that are made redundant – e.g. whether they enter new jobs that are less risky. These are only the impacts of changes in exposure. The over all impact will also depend on whether risk control improves or deteriorates as a result the organisational change.

Based on experience from the Norwegian oil industry, Serck-Hansen and Steinum (2001) maintain that the quality of the change process is essential for its safety outcome. They emphasise the quality of participation, founded on trust and a common understanding of the situation. Focus should be kept on tasks in the design phase. They call for patience in implementation and warn against too early focus on the final results.

Taken together, the perspectives show the diversity and complexity of the possible impacts of organisational and technological change on safety. We have to realise that it is not feasible to predict all safety impacts of a major change process. This situation calls for robust safety management strategies, where proactive evaluations of the proposed change process and its proposed outcome are combined with continuous monitoring of the effects of the process. For instance, a normative safety management model such as the SMORT questionnaire (Safety Management and Review Technique; Kjellén et al., 1987; Kjellén, 2000) may be used upfront to detect instances where the proposed organisation fails to provide the resources and routines that are needed to take care of safety. SMORT also contains checklists pertaining to the planning and execution of projects. During and after the process, interviews and questionnaires may be used to monitor its effects. Moreover, incident and accident investigations may focus on the impacts of organisational change on safety. In order to succeed, this approach requires top management commitment to safety. Top management must be willing to change their plans, moderate their ambition level, postpone the process and even reverse some of the modifications if this is necessary to achieve the company's safety objectives.

11.5 Epilogue

At this point, some readers may miss a tight and elegant synthesis of the diverse perspectives and ideas on organisational accidents and organisational resilience. Why not put everything into a neat little model, or at least compile a handy checklist, so that people can use the ideas without bothering about six different perspectives?

Our answer is that the six perspectives, with all their associated concepts and propositions, do not fit into a neat little model. The concepts and ideas of one perspective cannot always be readily expressed using the concepts of a different perspective. Neither do we believe that it is simply a question of pitting the perspectives against each other, devising empirical tests, and deciding which perspective most adequately reflects the realities of organisational life[49].

Moreover, we do not believe that simplification and reduction is always a good thing in the life of organisations. This brings us back to Westrum's notion of requisite imagination and Schulman's argument in favour of conceptual slack (Section 7.3 above; see also Westrum, 1993; Weick, 1987; Schulman, 1993). We suggest that complex organisations in dynamic and ambiguous environments thrive on open-minded controversies, rather than single-minded consensus. Open-minded organisations with room for divergent opinions may respond more effectively to signs of trouble than organisations with less tolerance for divergent interpretations of reality.

Finally, we contend that a rich repertoire of perspectives is a great asset to the safety practitioner. It is extremely difficult to get attention to the same message year after year. With a broad array of perspectives at his or her disposal, the safety practitioner is in a much better position to bring out new messages, to surprise and to provoke interest.

[49] The reader may have noted that Sagan (1993) tried to do something along these lines in book "Limits to safety". Although his results are interesting in their own right, they hardly provide a refutation of HRO theory; see Section 6.9 above and Rasmussen (1994a).

12 References

Adamski, A. J. & Westrum, R. (2003) Requisite imagination: The fine art of anticipating what might go wrong. In Hollnagel, E (ed.) *Handbook of cognitive task design.* New York: Lawrence Erlbaum Associates

Alteren, B. (1999). Implementation and evaluation of the Safety Element Method at four mining sites. *Safety Science, 31*: 231-264.

Andresen, G., Rosness, R. and Sætre, P.O. (2008). Improvisasjon – tabu og nødvendighet. In R.K. Tinmannsvik (ed.). *Robust arbeidspraksis. Hvorfor skjer det ikke flere ulykker på sokkelen?* Trondheim: Tapir akademisk forlag.

Argyris, C. and D. A. Schön (1978). *Organizational Learning*. Reading, Massachusetts: Addison-Wesley.

Ashby, W.R. (1981). Self-regulation and requisite variety. In F.E. Emery (ed.). *Systems Thinking. Volume One.* Harmondsworth: Penguin Education, 100-120. Earlier published as Chapter 11 in W.R. Ashby (1956). *Introduction to Cybernetics,* Wiley.

Aven, T. (2003). *Foundations of Risk Analysis – A knowledge and decision oriented perspective.* Chichester: Wiley.

Bainbridge, L. (1987). Ironies of automation. In J. Rasmussen, K. Duncan and J. LePlat (eds.). *New Technology and Human Error.* Chichester: Wiley (271-283).

Beck, U. (1992). *Risk Society: Towards a New Modernity.* London: Sage.

Beck, U. (1999). *World Risk Society.* Cambridge: Polity Press.

Bierly, P.E. and Spender, J.-C. (1995). Culture and High Reliability Organizations: The case of the nuclear submarine. *Journal of Management, 21* (4), 693-656.

Bird, F.E. and Germain, G.L. (1985). *Practical Loss Control Leadership.* Institute Publishing, Division of International Loss Control Institute, Loganville, Georgia.

Bolman, L.G. and Deal, T.E. (1986). *Modern approaches to understanding and managing organizations.* San Francisco: Jossey-Bass.

Bourrier, M. (1998). Elements for designing a self-correcting organisation: Examples from nuclear power plants. In A. Hale and M. Baram (eds.). *Safety Management. The Challenge of Change*. Oxford: Pergamon.

Brehmer, B. (1991). Distributed decision making: Some notes on the literature. I J. Rasmussen, B. Brehmer og J. Leplat (eds.). *Distributed decision making: Cognitive models for cooperative work.* Chichester: Wiley.

Burns, T. R. and G. M. Stalker (1961). *The Management of Innovations*. London: Tavistock.

Clarke, L. and Perrow, C. (1996). Prosaic Organizational Failure. *American Behavioral Scientist, 39* (8) 1040-1056.

Cohen, M., March, J. and Olsen, J. (1988). A garbage can model of organisational choice. In March, J. (Ed.). *Decisions and Organisations*. Oxford: Blackwell, 294-334.

Cook, R. & Rasmussen, J. (2005). "Going solid": a model of system dynamics and consequences for patient safety, *Qual Saf Health Care,* 14, 130-134. Downloaded from qhc.bmjjournals.com.

CSB (2007). *Investigation Report. Refinery Explosion and Fire. BP Texas City, Texas.* Report No. 2005-04-I-YX. U.S. Chemical Safety and Hazard Investigation Board.

Cullen, L. (1990). *The Public Inquiry into the Piper Alpha Disaster*. London: HSO.

Dekker, S. (2003). "Failure to adapt or adaptations that fail: contrasting models on procedures and safety." *Applied Ergonomics*, 34(3), pp. 233-238.

Epstein, S. (2008) " Unexampled events, resilience and PRA." In: Hollnagel E, Nemeth CP, Dekker S, editors. Resilience Engineering Perspectives, Aldershot: Aldershot

Foster, H.D. (1993). Resilience theory and system evaluation. In J.A. Wise, V. D. Hopkin and P. Stager (eds). *Verification and Validation of Complex Systems: Human Factors Issues.* Berlin: Springer, 35-60.

Gibson, J. J. (1961). The contribution of experimental psychology to the formulation of the problem of safety – a brief for basic research. In *Behavioral Approaches to Accident Research,* New York: Association for the Aid of Crippled Children, pp. 77-89. Reprinted in W. Haddon, E.A. Suchman and D. Klein (1964). *Accident Research: Methods and Approaches.* New York: Harper & Row.

Giddens, A. (1990). *The Consequences of Modernity.* Cambridge: Polity Press.

Grøtan, T.O, Størseth, F., Rø, M & A. B. Skjerve (2008a). *Literature review of Resilience and Improvisation*. The Building Safety project web. http://sintef.org/Projectweb/Building-Safety

Grøtan, T.O, Størseth, F., Rø, M & A. B. Skjerve (2008b). *Resilience, Adaptation and Improvisation – increasing resilience by facilitating for successful improvisation* . In. Ed. (Hollnagel, Pieri, Rigaud) Proceedings 3rd symposium of resilience engineering. Juan les Pins. France.

Gunderson, L.H., Holling, C.S., eds. (2002). Panarchy: Understanding Transformations in Human and Natural systems. Washington D.C.: Island Press.

Guttormsen, G., Randmæl, S. and Rosness, R. (2003). *Utforming av regelverk for togframføring.* Report STF38 A03408. Trondheim: SINTEF Industrial Management. (Design and formulation of operational rules for railways. In Norwegian.)

Haddon, W. (1970). On the escape of tigers: An ecological note. *Technological review, 72* (7), Massachusetts Institute of Technology, May 1970.

Haddon, W. (1980). The Basic Strategies for Reducing Damage from Hazards of All Kinds. *Hazard prevention,* Sept./ Oct. 1980.

Hale, A. (2000). Conditions of occurrence of major and minor accidents. 2me séance du séminaire "Le risque de défaillance et son contrõle par les individus et les organisations", 6-7 novembre, Gif sur Yvette.

Hale, A. and Heijer, T. (2006). "Defining Resilience." In: E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts*. Aldershot: Ashgate Publishing Company, pp. 35-40.

Heinrich, H. W. (1931). *Industrial Accident Prevention.* New York: McGraw-Hill. (Cited by Hale, 2000).

Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method.* Oxford, UK: Elsevier Science.

Hollnagel, E. (1999). *Accident analysis and barrier functions.* Halden, Norway: Institute for Energy Technology.

Hollnagel, E. (2004). *Barriers and Accident Prevention*. Aldershot, UK: Ashgate.

Hollnagel, E. & Woods, D.D. (2006). "Epilogue: Resilience Engineering Precepts." In: E. Hollnagel, D.D. Woods, and N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts.* Aldershot: Ashgate, pp. 347-358.

Hollnagel, E. (2008). Risk + barriers = safety? *Safety Science, 46,* 221-229.

Hollnagel, E. (2008) "Preface" and "Safety management, looking back or looking forward" In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilient Engineering Perspectives*, Aldershot: Ashgate.

Hollnagel, E. (2009). *The ETTO Principle: Efficiency-Throughness Trade-Off*. Farnham: Ashgate.

Hopkins, A. (1999). The limits of Normal Accident theory. *Safety Science, 32* (2-3), 93-102.

Hopkins, A. (2000a). An AcciMap of the Esso Australia Gas Plant Explosion. Paper presented at t he 18th ESReDa seminar Risk Management and Human Reliability in Social context. Karlstad, Sweden, June 15- 16, 2000.

Hopkins, A. (2000b). *Lessons from Longford: The Esso Gas Plant Explosion.* Sydney: CCH.

Hopkins, A. (2008). *Failure to Learn. The BP Texas City Refinery disaster.* Sydney: CCH.

Hopkins, A., ed. (2009). *Learning from High Reliability Organisations*. Sydney: CCH.

Hopkins, A. and Hale, A. (2002). Issues in the regulation of safety: Setting the scene. In B. Kirwan, A. Hale and A. Hopkins (eds.). *Changing Regulation: Controlling Risks in Society.* Oxford: Pergamon.

Hovden, J. and Steiro T. (2000). The effects of cost- cutting in the Norwegian petroleum industry. Presented at *ESREL 2000, Foresight and Precaution*. In Cottam, Harvey, Pape & Tait (eds), Balkema, Rotterdam, ISBN 90 5809 140 6, P. 601-605.

Johanson, J. (2009). Vision Zero – Implementing a policy for traffic safety. Safety Science, *47*, 826-831.

Johnson, W. G. (1980). *MORT Safety Assurance Systems.* New York: Marcel Dekker.

Kjellén, U. 2000: *Prevention of Accidents Through Experience Feedback.* Taylor & Francis, London and New York.

Kjellén, U. and Larsson, T. (1981). Investigating accidents and reducing risks: a dynamic approach. *J. Occupational Accidents, 3* (2)*,* 129-140.

Kjellén, U., Tinmannsvik, R.K., Ulleberg, T., Olsen, P.E., Saxvik, B. (1987). *SMORT: Sikkerhetsanalyse av industriell organisasjon. Offshore-versjon.* [MORT. Safety analysis of industrial organisations. Offshore version.] Oslo: Yrkeslitteratur.

Klein, G. (1998). *Sources of Power. How People Make Decisions.* Cambridge, Mass.: The NIT Press.

Kletz, T. (1991). *Plant design for safety: A user friendly approach.* New York : Hemisphere Publ.

Kørte, J., Aven, T. and Rosness, R. (2002). On the use of risk analysis in different decision settings. Paper presented at ESREL 2002, Decision Making and Risk Management, Lyon, 19-21 March 2002.

LaPorte, T. R. and Consolini, P.M. (1991). Working in practice but not in theory: Theoretical challenges of "High-Reliability Organisations". *Journal of Public Administration Research and Theory, 1,* 19-47.

LaPorte, T.R. and Rochlin, G. (1994). A Rejoinder to Perrow. *Journal of Contingencies and Crisis Management, 2,* (4), 221-227.

Lee Marks, M. (1993). Restructuring and downsizing, In: Mirvis, P. H. (ed.). *Building the Competitive Workforce* (New York: John Wiley, 1993).

Leveson, N.G. (2004). A new accident model for engineering safer systems. *Safety Science, 42*(4), 237-270.

Leveson, N., Duplac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., Barrett, B. (2006) "Engineering Resilience into Safety-Critical Systems." In: E. Hollnagel, D.D. Woods, and N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts.* Aldershot: Ashgate, pp. 95-123.

Lindblom, C. E. (1959). The science of "muddling through". *Public administration Review, 19,* 79-88.

Macchi, L. (2010). *A Resilience Engineering approach to the evaluation of performance variability: development and application of the Functional Resonance Analysis Method for Air Traffic Management safety assessment.* Ph.D. Thesis. École Nationale Supérieure des Mines de Paris, France.

Macchi, L., Hollnagel, E. & Leonhardt, J. (2008). *A systemic approach to HRA: A FRAM modelling of Control Overflight activity*. 4th Eurocontrol Annual Safety R&D Seminar. Southampton, UK.

March, J. G. and Olsen, J. P. (1976). *Ambiguity and Choice in Organizations.* Bergen: Universitetsforlaget.

Mendoça D. (2008) Measures of Resilient Performance. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives*. Ashgate, Aldershot, USA.

Nathanael, D. and Marmaras, N. (2008). Work practices and prescription: A key isesue for organizational resilience. In E. Hollnagel, C.P. Nemeth and S. Dekker, eds. *Resilience Engineering Perspectives. volume 1: Remaining Sensitive to the Possibility of Failure.* Aldershot, UK: Ashgate.

NOU 2000: 30: *Åsta- ulykken, 4. januar 2000. Hovedrapport.* [The Åsta accident, January 4, 2000. Main report.] Justis- og politidepartementet. Statens forvaltningstjeneste, 2001. Electronic version available at http://odin.dep.no/jd/norsk/publ/utredninger/NOU/012001-020007/index-dok000-b-n-a.html

NOU 2001:9: *Lillestrøm-ulykken 5. april 2000.* [The Lillestrøm accident, April 5, 2000]. Justis og politidepartementet. Statens forvaltningstjeneste, 2001.

Nuutinen, M. and Norros, L. (2009). Core task analysis in accident investigation: analysis of maritime accidents in piloting situations. *Cognition, Technology and Work, 11*, 129-150.

Pavard, B., Dugdale, J., Saoud, N., Darcy, S., Salembier, P. (2008). Underlying concepts in robustness and resilience and their use in designing socio-technical systems. In: Hollnagel E, Nemeth CP, Dekker S, editors. *Resilience Engineering Perspectives*, Aldershot: Ashgate.

Perrow, C. (1984). *Normal Accidents.* New York: Basic Books.

Perrow, C. (1986). *Complex Organizations. A Critical Essay.* New York: Random House.

Perrow, C. (2007). *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters.* New Jersey: Princeton University Press.

Petroleumstilsynet (2005). *Investigation of gas blowout on Snorre A, Well 34/7-P31A, 28 November 2004.* Report. Stavanger: Petroleumstilsynet.

Pfeffer, J. (1998). *The Human Equation: Building profits by putting people first.* Boston: Harvard Business School Press.

Pidgeon, N. and O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science, 34,* 15- 30.

Rasmussen, J. (1986). *Information processing and human-machine interaction. An approach to cognitive engineering*. New York: North-Holland.

Rasmussen, J. (1994a). High Reliability Organizations, Normal Accidents, and other dimensions of a risk management problem. Paper. *NATO Advanced Research Workshop on Nuclear Arms Safety.* Oxford, UK, August 1994.

Rasmussen, J. (1994b). Risk management, adaptation, and design for safety. In B. Brehmer and N.-E. Sahlin (eds). *Future Risks and Risk Management,* (pp 1-36). Dordrecht: Kluwer Academic Publishers.

Rasmussen, J. (1996). Risk management in a dynamic society. Presentation at the seminar *Safety and Reliability in Industrial Management,* Trondheim 29-30 May 1996. (Viewgraphs)

Rasmussen, J. (1997). Risk management in a Dynamic Society:
A Modelling Problem *Safety Science, 27* (2-3), pp. 183-213.

Rasmussen, J. and I. Svedung (2000). *Proactive Risk Management in a Dynamic Society* (Swedish Rescue Services Agency, Karlstad, Sweden).

Reason, J. (1990). *Human error*. Cambridge: Cambridge University Press.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.

Reason, J. (2008). *The Human Contribution. Unsafe acts, accidents and heroic recoveries*. Aldershot: Ashgate.

Renn, O. (2008). *Risk Governance. Coping with Uncertainty in a Complex World*. London: Earthscan.

Roberts, K.H. (1993). *New Challenges in Understanding Organizations.* New York: Macmillan Publishing Company.

Rochlin, G. I., LaPorte, T. and Roberts, K. H. (1987). The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review 40*(4), 76-90. Also available on the Internet site:
http://www.nwc.navy.mil/press/review/1998/summer/art7su98.htm

Roe, E. and Schulman, P.R. (2008). *High Reliability Management. Operating on the Edge.* Stanford, California: Stanford Business Books.

Rosness, R. (2001). *"Om jeg hamrer eller hamres, like fullt så skal der jamres. Målkonflikter og sikkerhet."* [On conflicting goals and safety.] SINTEF Report STF38 A01408. Trondheim: SINTEF Industrial Management. Available at www.risikoforsk.no.

Rosness, R. (2004). *Ti tommeltotter og null ulykker?: Om feiltoleranse og barrierer*. Trondheim: SINTEF.

Rosness, R., (2009). A Contingency model of decision-making involving risk of accidental loss, *Safety Science, 47*, (6), pp. 807-812.

Rosness, R. (2009b). Derailed decisions. In C. Owen, P. Béguin and Ger Wackers (eds). *Risky Work Environments*. Farnham: Ashgate.

Rosness, R., Håkonsen, G., Steiro, T. and Tinmannsvik, R.K. (2000). The vulnerable robustness of High Reliability Organisations: A case study report from an offshore oil production platform. Paper presented at the 18th ESReDA seminar *Risk Management and Human Reliability in Social Context.* Karlstad, Sweden, June 15-16, 2000.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K. & Herrera, I.A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives*. SINTEF report (STF38 A 004403), ISBN: 82-14-02724-1.

Sagan, S. D. (1993). *The limits to safety. Organizations, accidents, and nuclear weapons.* Princeton, New, Jersey: Princeton University Press.

Schulman, P. R. (1993). The negotiated order of organizational reliability. *Administration & Society, 25* (3), 353-372.

Serck-Hansen, C. and Steinum, T. (2001). Methodology for change: Results from a workshop on safety and organisational change. In E. Serck-Hansen (ed.). *Safe Change. Methodology on Change in Norwegian Oil Industry.* Høvik: Det Norske Veritas.

Schiefloe, P.M., Vikland, K.M., Ytredal, E.B., Torsteinbø, A., Moldskred, I.O., Heggen, S., Sleire, D.H., Førund, S.A., Syversen, J.E. (2005). *Årsaksanalyse etter Snorre A hendelsen 28.11.2004.* Stavanger: Statoil

Sklet, S. (2006). *Safety Barriers on Oil and Gas Platforms. Means to Prevent Hydrocarbon Releases.* Trondheim: Doctoral Theses, NTNU.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494-506.

Snook, S.A. (2000). *Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq.* Princeton: Princeton University Press.

Starbuck, W. H. & Farjoun, M., (eds.) (2005). *Organization at the limit. Lessons from the Columbia Disaster.* Oxford, Blackwell Publishing

Statens jernbanetilsyn (1999). Forskrift om " Krav til styring og oppfølging....". [Regulations concerning “Requirements for control and follow-up…]

Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis, 11* (3) 499-507.

Turner, B. A. (1978). *Man-made disasters.* London: Wykeham Science Press.

Turner, B. A., Pidgeon, N. F. (1997). *Man-made disasters*. 2nd Edition. London: Butterworth-Heinemann.

Van der Graaf, G. (2001). Hearts and minds. Paper presented at *Sikkerhetsdagene 2001,* Trondheim 30-31 October 2001.

Van der Want, P.D.G. (1997). Tripod incident analysis methodology. In: J. van Steen (ed.). *Safety Perormance Measurement.* Warwickshire, UK: Institution of Chemical Engineers

Van Steen, J., ed. (1996). *Safety Performance Measurement*. Rugby : Institution of Chemical Engineers

Vaughan, D. (1996). *The Challenger Launch Decision.* Chicago: The University of Chicago Press.

Wackers, G. (2006). *Vulnerability and robustness in a complex technological system: Loss of control and recovery in the 2004 Snorre A gas blow-out.* Working paper no. 42/2006. Oslo: Center of Technology, Innovation and Culture, University of Oslo.

Wagenaar, W. A. and Groeneweg, J. (1987). Accidents at sea: Multiple causes and impossible consequences. *International Journal of Man-Machine Studies, 27,* 587-598.

Wagenaar, W. A., Groeneweg, J., Hudson, P.T.W. and Reason, J.T. (1994). Promoting safety in the oil industry. *Ergonomics, 37*, 1999-2013.

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review, 29,* (2) 112-127.

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management, 16* (3), 571-593.

Weick, K.E. (2001). *Making sense of the organization*. Oxford: Blackwell.

Weick, K.E. and Sutcliffe, K.M. (2001). *Managing the Unexpected.* San Francisco: Jossey-Bass.

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the unexpected: Resilient Performance in an Age of Uncertainty.* San Francisco: Jossey-Bass.

Westrum, R. (1993). Cultures with Requisite Imagination. In J.A. Wise, V. D. Hopkin and P. Stager (eds). *Verification and Validation of Complex Systems: Human Factors Issues.* Berlin: Springer, 401-416.

Westrum, R. (2006). A typology of resilience situations. In *Resilience Engineering Concepts and Precepts* edited by Hollnagell, E., Woods, D., Leveson N., Aldershot: Ashgate

Wilde, G.J.S. (1982). The theory of risk homeostasis: Implications for safety and health. *Risk Analysis, 2* (4). 209-225.

Woltjer, R. and Hollnagel, E. (2007). The Alaska airlines flight 261 accident: a systemic analysis of functional resonance. *Proceedings of the 2007(14th) International Symposium on Aviation Psychology*, April 23-26, Dayton, Ohio.

Woods, D. D. (1990). Risk and human performance: Measuring the potential for disaster. *Reliability Engineering and System Safety, 29,* 387- 405.

Woods, D.(2006). Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making. Testimony on *The Future of NASA* for Committee on Commerce, Science and Transportation, John McCain, Chair, October 29, 2003

Woods, D.D. (2006). Essential Characteristics of Resilience. In: N. Leveson, E.

Hollnagel, and D. D. Woods, *Resilience engineering: concepts and precepts*. Aldershot: Ashgate, pp. 21 – 34.

Woods, D.D. & Hollnagel, E. (2006). "Prologue: Resilience Engineering Concepts." In: E. Hollnagel, D.D. Woods, & N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts*. Ashgate Publishing Company, pp. 1-6.

Woods, D. D., Johannesen, L.J., Cook, R.I., Sarter, N.B. (1994). *Behind Human Error: Cognitive Systems, Computers, and Hindsight.* State- of- the- Art Report 94- 01. Wright-Patterson Airforce Base, Ohio: CSERIAC

Woods, D. and Wreathall, J. (2003). *Managing Risk Proactively: The Emergence of Resilience Engineering*. Columbus: Ohio University, 2003.

Yin, R. K. (1994). *Case Study Research. Design and methods.* Second edition. Thousand Oaks: Sage.

Øien, K. (2001). *Risk control of offshore installations. A framework for the establishment of risk indicators.* Ph.D. Thesis. Department of Production and Quality Engineering. Trondheim: NTNU.

Trondheim
Address: NO-7465 Trondheim, Norway
Phone: +47 73 59 30 00
Fax: +47 73 59 33 50

Address: P.O. Box 124, Blindern, NO-0314 Oslo, Norway
Phone: +47 22 06 73 00
Fax: +47 22 06 73 50