

Master's thesis

Inger Lise Johansen

# Foundations of risk assessment

Trondheim, June 14th, 2010

NTNU  
Norwegian University of  
Science and Technology  
Faculty of Engineering and Technology  
Department of Production and Quality Engineering



# The foundations of risk assessment

Inger Lise Johansen

June 13, 2010

## Preface

This report represents the master thesis in TPK 4900 Production and Quality Engineering. The master project is executed spring 2010 at the Norwegian University of Science and Technology, Department of Production and Quality Engineering. The thesis is titled *Foundations of risk assessment*. Readers unfamiliar with the subject are guided by an appendant list of abbreviations and acronyms.

I wish to thank Professor Marvin Rausand (NTNU) and Professor Mary-Ann Lundteigen (NTNU) for invaluable advice and inspiring discussions throughout the project. I would also like to thank David Jønsson and Ketil Johansen for patiently proof reading the final version. Special gratitude is directed to Vivi Moe for allowing me to use her piece *Baller i lufta* in fronting this report.

Inger Lise Johansen  
Stud.techn.  
Trondheim, Norway, 14<sup>th</sup> June 2010

## Abstract

The purpose of this study is to shed light on the foundations of risk assessment. By exploring the polysemantics of basic concepts and their influence on the process and results of risk assessment, the thesis endeavors to clarify the words of risk assessment and promote reflection among practitioners and scholars. The findings are derived from integration and critique of pioneering and state of the art literature.

Risk is a characteristic of the future concerning the uncertain consequences of decisions and contingencies. Understanding risk urges contemplation on fundamental issues of ontology (is risk a real-world property?) and epistemology (what can we know about risk?). The many-faceted concept has been differently interpreted across time, cultures and disciplines. Numerous definitions coexist in dissonance and concordance, caricaturing risk singly or as a combination of events, consequences, probability or uncertainty. The quantitative definition of Kaplan and Garrick (1981) embeds all elements, defining risk as the answer to three questions: 1) What can happen? 2) How likely is it? 3) If it does happen, what are the consequences? In comparison with contending definitions, this triplet definition gains in comprehensibility and relevancy to risk assessment. The defining questions are, however, very capacious and render significant interpretative freedom. Focal to this study is the first question, whose associated terminology is particularly vague and on which focused discussions remain most disturbingly few.

An alternative means for grasping the concept of risk is to examine its related counterconcepts. Uncertainty not only makes a central component of risk, it also has a complementary meaning as lack of confidence in the results of risk analysis. Safety is often conceived as freedom from unacceptable risk or the antonym of risk. The conceptually sensitive coupling between risk and safety reveals that the rightness of this claim depends on whether uncertainty is considered part of the second question of Kaplan and Garrick (1981). Security is the equivalent of safety in situations of intentional harm. The moral and analytical complexities of security outdo those of safety since the first question becomes how someone can *make* something happen. Vulnerability is the lacking ability of a system to resist the impact of an unwanted event and to restore to its original function. The relation between risk and vulnerability is not commutative. A counterconcept to vulnerability is resilience, meaning a system's ability to bounce back to a reference state after a disturbance. Complementing the negatively connoted concept of risk with resilience offers a positive perspective for mastering the dynamics of future uncertainties.

Risk analysis is the process of answering the triplet definition of risk, whereas risk assessment refers to the wider process of risk analysis and risk evaluation. Neither the analytical process nor its results should be considered in isolation from the purpose of risk assessment, which is to inform decision making about risk. Decisions shall be risk-informed, not risk-based, meaning that risk assessment is never the sole input to decisions. The plurality of stakeholders and the prevalence of uncertainties represent two major challenges to risk-informed decision making. Framing analysis by deliberation and informing deliberation by analysis presupposes that decision makers understand the words and results of risk assessment.

Hazard is a source of potential harm. Whereas risk pivots on the future realization of this potential, hazard exists presently and solely at the source. Closely related is the concept of threat, which is conceptually reserved to sources of intentional damage. There is a plethora of terms marking the intersection between prevention and mitigation in the realization of a hazardous potential. Hazardous event is pro-

moted as the least ambiguous denotation, defined as an event confined to the first significant release of a hazards that will result in harmful exposure if not controlled. Triggering event and safety issues are promising concepts for bridging hazards and hazardous events. Triggering events are the most immediate causes of hazardous events, while safety issues are one or more hazards in combination with local triggering events. Both concepts reflect the calculability and controllability of risk and should thus be used with caution.

Accident scenario is promoted as the answer to the question of what can go wrong. It is a uniquely defined path in an event tree, confined by an initiating event and a corresponding end state. Unfortunately, both the concept itself and the terms that confine are circularly defined. Initiating event is a vague descriptor that in principle can be placed anywhere in the bowtie-diagram. End states are pragmatically conditioned on the purpose of analysis; implicitly through the selection of consequences and explicitly in the relevancy of pivotal events. A principal advice is that any accident scenario shall be terminated in the absence of discrete ramifications. Contrasting the scenario approach to risk assessment with the conventional approach in Norway shows that accident scenario is not imperative to the triplet definition of risk. A revised definition of accident scenario is suggested in initiative to further discussion: An accident scenario is a sequence of events from the hazardous event to a uniquely determined end state of relevance.

The study has demonstrated the importance of striving for a clear and consistent terminology. Researchers, practitioners and regulators use the words of risk assessment differently and inconsistently. Not only does this preclude communication internally and across analysis teams, it also leads to erroneous applications of methods and inexpedient use of results. This urges terminological vigilance of every practitioner, as well as further academic and standardization efforts towards a unifying nomenclature. A key challenge is to reconcile the analyst's need for pragmatic procedures with the decision maker's call for consistent and communicable results. Ultimately, this is a matter of finding the optimal fit between analysis and deliberation in risk-informed decision making.

# Contents

<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Objectives . . . . .	2
1.3 Limitations . . . . .	2
1.4 Structure . . . . .	3
<b>2 Understanding risk</b>	<b>5</b>
2.1 Introduction . . . . .	5
2.2 Characterizing risk . . . . .	6
2.3 Theorizing risk . . . . .	9
2.4 Defining risk . . . . .	11
<b>3 Counterconcepts to risk</b>	<b>18</b>
3.1 Introduction . . . . .	18
3.2 Uncertainty . . . . .	18
3.3 Safety . . . . .	23
3.4 Security . . . . .	26
3.5 Vulnerability . . . . .	29
3.6 Linking vulnerability and resilience . . . . .	32
<b>4 Risk assessment</b>	<b>34</b>
4.1 Introduction . . . . .	34
4.2 The contents of risk assessment . . . . .	34
4.3 The purpose of risk assessment . . . . .	40
4.4 The limitations of risk assessment . . . . .	43
4.5 Using risk assessment in decision making . . . . .	46
<b>5 What can go wrong?</b>	<b>58</b>
5.1 Introduction . . . . .	58
5.2 Hazard . . . . .	58
5.3 Threat . . . . .	65
5.4 On the concepts of event and causation . . . . .	68
5.5 Hazardous event . . . . .	72
5.6 Reason's events of causation . . . . .	76
5.7 Safety issues . . . . .	83

<b>6 Accident scenario</b>	<b>87</b>
6.1 Introduction . . . . .	87
6.2 Initiating event . . . . .	88
6.3 The termination of an accident scenario . . . . .	92
6.4 Is accident scenario a sound concept? . . . . .	97
6.5 A refined definition of accident scenario . . . . .	105
<b>7 Epilogue</b>	<b>107</b>
<b>Bibliography</b>	<b>109</b>
<b>A Abbreviations and acronyms</b>	<b>122</b>

# List of Figures

2.1	Demarcating risk (adopted from Rosa, 1998).	8
2.2	Assessing risk retrospectively.	9
2.3	Risk according to (a) Rosa (1998) and (b)Aven and Renn (2009) (adopted from Aven and Renn, 2009).	14
2.4	(a)A single and (b)family of risk curves (adopted from Kaplan and Garrick, 1981).	16
3.1	Six levels of quantification in the treatment of uncertainty in risk analysis according to Paté-Cornell (1996).	21
3.2	Safety is a function that decreases with the probability of harm, the severity of harm and our ability to foresee this with confidence. $x$ , $y$ and $z$ are levels of safety such that $x>y>z$ (adopted from Möller et al., 2006).	24
3.3	Components of the vulnerability framework of Turner et al. (2003).	31
3.4	The different scope of vulnerability and risk analysis (adapted from Einarsson and Rausand, 1998).	32
4.1	Contents of risk management and risk assessment according to ISO 31000 (2009).	35
4.2	Contents of risk analysis and risk assessment according to NORSOK Z-013 (2001).	36
4.3	Bowtie-representation of risk assessment (adapted from Rausand and Høyland, 2004).	37
4.4	Simplified fault tree (adopted from NASA, 2002a).	38
4.5	Example of event tree (adopted from USCG, 2000b).	39
4.6	The socio-technical system involved in risk management (adopted from Rasmussen, 1997).	45
4.7	Conceptual framework for including organizational actors in risk analysis.	46
4.8	Comparing the results of risk assessment, $R$ , with a predefined set of risk acceptance criteria, $\bar{R}$ (adapted from Breugel, 1998).	48
4.9	Framework for risk-informed decision making (adapted from Aven, 2003).	52
4.10	Risk analysis is the sole analytical input to risk-based decision making.	53
4.11	Strategies and actors in the risk management escalator of Klinke and Renn (2002).	54
5.1	The framework for organizational accidents of Reason (1997).	60
5.2	The multi-faceted nature of hazards.	63



5.3	Hazard is existing only as a source. . . . .	64
5.4	Safeguarding against hazards. . . . .	64
5.5	The motivational threat classification of Vidalis (2004) suggests that cyber threats may be unintentional. For most other purposes, <i>threat</i> is reserved for intentional harm. . . . .	68
5.6	The cloudy events of risk analysis. . . . .	72
5.7	Trying to escape a hazardous event. . . . .	75
5.8	Different hazardous events for the same scenario. . . . .	76
5.9	General accident progression according to Wagenaar et al. (1990). . . .	78
5.10	Latent and active failure pathways (adopted from Reason, 1995). . . . .	79
5.11	Fictitious example of failure state profiling (taken from Wagenaar et al., 1994). . . . .	80
5.12	Integrating general failure types and triggering events in the bowtie- diagram. . . . .	82
5.13	Integrating general failure types, triggering events and safety issues in the bowtie-diagram. . . . .	84
5.14	Safety issue is a combination of triggering events and hazard. . . . .	85
6.1	An accident scenario is a single path in the event tree. . . . .	88
6.2	Depiction of the success scenario $S_0$ (adopted from Garrick, 2008). . . .	89
6.3	Identifying initiating events (adopted from Garrick, 2008). . . . .	89
6.4	An initiating event may ramify into a range of end states. . . . .	90
6.5	Initiating event can in principle be placed anywhere in the bowtie- diagram. . . . .	91
6.6	Different interest horizons following a hazardous event. . . . .	93
6.7	Risk acceptance criteria as determinative to scenario end state. . . . .	94
6.8	Cutting of the event tree at the point where specific modeling expertise is required. . . . .	96
6.9	Consequence spectrum following a hazardous event. . . . .	99
6.10	Comparing (a) the scenario approach to risk assessment with the frame- work of (b)NORSOK Z-013 (2001). . . . .	101
6.11	Comparing (a) the scenario approach to risk assessment with the frame- work of (b)NORSOK Z-013 (2001). . . . .	102

# List of Tables

2.1	The risk table (adopted from Kaplan and Garrick, 1981). . . . .	15
4.1	Summary of the strengths and limitations of deterministic and probabilistic approaches to safety (Extracted from Niehaus and Szikszai, 2001). . . . .	50
5.1	Checklist of type, origin and potential consequences of hazards (extracted from ISO 14121, 2007). . . . .	61
6.1	Presentation format of risk relative to a set of hazardous events (adapted from Rausand and Høyland, 2004). . . . .	100

# Chapter 1

## Introduction

### 1.1 Background

Risk is an intuitive concept that complicates and spices up our daily lives. Perhaps now more than ever, the headlines of the recent spring have demonstrated the omnipresence of risk in modern society. The risk of encountering volcano ash clouds has pushed airline systems on the edge of bankruptcy and stranded state and industrial affairs. Whereas these are consequences of excessive caution, the blowout of an oil rig in the Gulf of Mexico in April 2010 has alerted the world to the costs of recklessness. This and similar catastrophes of the past exert considerable influence on how we think about forthcoming decision problems. A topical example is the issue of future oil and gas production at the newly drawn dividing line in the Barents Sea. The alchemy of risk assessment is to transform experience into foresight, in order to ensure that such decisions are informed by the best available technical knowledge.

Risk assessment is a many splintered thing. It is a discipline of numerous methods, scholars and fields of application. This diversity has led the words of risk assessment into a bewildering land of ambiguity and confusion. Notably contentious is the fundamental concept of risk, over which theorists have fought to define since the rise of the scientific risk literature in the late 1960s. Commonly accepted is the quantitative definition of Kaplan and Garrick (1981), defining risk as the answer to three questions:

1. What can happen?
2. How likely is it?
3. If it does happen, what are the consequences?

In a talk given to a plenary session at the Society for Risk Analysis, Kaplan (1997) notes that the scientific community is still discussing how we should interpret this triplet definition of risk. This attention has by and large been directed at the second question. Representative is Aven's (2003) preoccupation with the interpretation of probability and uncertainty in quantitative risk assessment. Few have yet sought to clarify the first of these questions or contemplate the variety of terms sustaining our conception of risk. An attempt of the latter is made by Christensen et al. (2003), who compare a selection of definitions on the central terms of risk assessment. Albeit elucidating, this contribution is more collocating than reflective, hence failing to

provide rudimentary insights. The nomenclature of risk assessment is still ambiguous after more than forty years of application. Since this leads to communication problems, erroneous applications of methods and so on, there is a call for enhanced understanding and shared awareness of the foundational concepts of risk assessment.

## 1.2 Objectives

The purpose of this study is to shed light on the foundations of risk assessment, discuss the basic concepts and how their interpretation influences the analysis process and the understanding of results from risk assessment. From this overall goal, five lower level objectives are deduced:

1. Perform a literature survey and discuss the main definitions (or interpretations) of the term *risk*- and also discuss how the term risk is related to concepts like safety, security, vulnerability and so on.
2. Discuss the concept of *accident scenario*. Suggest a “suitable” definition and especially discuss the extent of a scenario. What is the initiating event of the scenario and where should the development of the scenario be terminated?
3. Discuss the concepts of *hazard* and *threat*- and triggering events. Do we need to distinguish between these concepts? The aviation organization ICAO has suggested to focus on so-called *safety issues*. What are the benefits and limitations of this approach?
4. How can we measure and compare consequences to various types of assets? -and how can we obtain a single measure for different degrees of harm to one type of assets (e.g., fatalities, injuries, permanent vs. non-permanent disabilities)?
5. Discuss risk assessment as basis for decision-making. What are the pros and cons related to risk-based decision making and risk-informed decision making?

Following agreement with the supervisor, task 4 will not be covered in this study.

## 1.3 Limitations

The thematic coverage is confined to four out of five tasks in approaching the overall objective. Omitting the fourth issue of consequent measurement is not considered depriving to the remainder. It does, however, remain a cardinal aspect in risk-informed decision making that requires examination in its own right. The same holds for the concept of probability, whose interpretation affects both the derivation and understanding of the results of risk assessment.

The study is limited to considerations of accident risk. It does not cover continuous, gradual or long-term development, as is typical for analysis of health and environmental risk. Nor is vulnerability analysis considered, albeit the concept of vulnerability is thoroughly discussed as a counterconcept to risk. The reader should beware that all findings are not directly transferable beyond applications of accident

risk. Accident scenario, for instance, is a meaningless descriptor of risk from continuous emissions. The first half of the report is by and large concerned with generic insights relevant to all domains of (bodily) risk.

A second limitation concerns the study's adherence to the traditional way of thinking about risk analysis. Novel perspectives and methods, like resilience engineering and dynamic modeling approaches, are left out of consideration. This is because the overall objective calls for elaboration of basic concepts rather than presentation of advanced models or contending paradigms. The reader is not required any previous knowledge on the subject, although advised to consult additional references on scarcely covered topics.

The findings are derived from integration and critique of pioneering and state of the art literature. The study is hence purely theoretical. During the literature selection process, emphasis has been placed on conceptual contributions, but also on mapping the variety of terms and definitions across applications and guidelines. A challenge that follows is the difficulty of reconciling pragmatic concerns with a quest for generic insights. Some terms are amenable to general definition, while others are necessarily pragmatically conditioned. In the latter case, the most valuable findings are the nuances and contrasts of the various conceptions, calling for terminological vigilance of practitioners and scholars of risk assessment.

## 1.4 Structure

Chapter 2 explores the many facets of risk. Broad characteristics of the concept are presented, followed by a philosophical briefing on contentious ontological and epistemological interpretations. Abstraction is finally sought by discussing a handful of definitions with emphasis on conceptual content and clarity. The quantitative definition of Kaplan and Garrick (1981) is adopted for the study, while stressing the importance of clarifying foundational ambiguities in the respective questions.

The following chapter seeks to clarify what risk is *not* by relating it to central counterconcepts. First, uncertainty is examined as a constituent yet complementary concept to risk. A discussion on the antonymous concept of safety follows thereafter, along with the related, but more complex concept of security. The feasibility of extending and complementing risk analysis is lastly discussed by contrasting risk with the concepts of vulnerability and resilience.

Chapter 4 examines the contents and role of risk assessment in mastering technological risk. Risk assessment is briefly described with the visual aid of the bowtie-diagram and an introduction to logic modeling. Contemplation follows on the purpose of risk assessment, leading to a discussion on its prevalent strengths and limitations. Most attention is devoted to the use of risk assessment in decision making, particularly aided by the decision making framework of Aven (2003).

Subsequently, chapter 5 seeks to tidy up the toolbox of concepts for answering the first question of Kaplan and Garrick (1981). The concepts of hazard and threat make the starting point of inquiry, while a philosophical discussion on event and causation lays the foundation for entering the jungle of terms relating a hazard to events of cause and realization. Central are the concepts of hazardous event and triggering event as conceived in the framework of Reason (1990b). ICAO's concept of safety issues is eventually considered in light of the remaining terminological knobs.

Chapter 6 examines Kaplan and Garrick's (1981) conception of accident scenario. The extent of a scenario is problematized by exploring the terms of initiating event

and end state. A final discussion pulls the threads together by questioning the conceptual soundness of accident scenario and contrasting the scenario approach to risk assessment with the approach of NORSOK Z-013 (2001). The chapter is closed by suggesting a refined definition of accident scenario in initiative to further reflection.

Commentary conclusions and recommendations for further work are given in the epilogue of chapter 7.

## Chapter 2

# Understanding risk

### 2.1 Introduction

If you ask ten persons what they mean by the word *risk* you will, most likely, get ten different answers. Not only are the conceptions of lay people and professionals prone to differ, disparities are striking also within those communities. The polysemantics of risk are aptly captured by Garland (2003, p.49):

Today's accounts of risk are remarkable for their multiplicity and for the variety of senses they give to the term. Risk is a calculation. Risk is a commodity. Risk is a capital. Risk is a technique of government. Risk is objective and scientifically knowable. Risk is subjective and socially constructed. Risk is a problem, a threat, a source of insecurity. Risk is a pleasure, a thrill, a source for profit and freedom. Risk is the means whereby we colonize and control the future. 'Risk society' is our late modern world spinning out of control.

Against this backdrop of ambiguity, risk has become the buzzword of today. It is the subject of debate and analysis, anxiety and speculation. Christensen et al. (2003) assert that its manifold interpretations lead one not only to doubt if discourses structure around the same thing, but also whether individual sciences have a clear conception of what they are investigating. Whether equipped with the techno-scientific objective of estimation, or the socio-culturalists' aim of contextual explanation (Lupton, 1999), misconceptions are likely to propagate if the basic object of analysis is encapsulated with confusion. When analyzing and debating risk, it is rudimentary to clarify what we actually mean by *risk*.

This chapter explores the many facets of risk. First, broad characteristics of the concept are presented, followed by a philosophical briefing on the ontology and epistemology of risk. Abstraction is subsequently sought in the representation of a handful of risk definitions. The definitions are discussed with respect to conceptual content and clarity, before finally emphasizing the importance of elucidating foundational issues in risk assessment.

## 2.2 Characterizing risk

### 2.2.1 The remarkable history of risk

Equipped with the title *Against the Gods*, Bernstein (1996) entertainingly maps the remarkable history of risk. The word *risk*, he introduces, stems from the Italian *risicare*, meaning “to dare”. At the very heart of the risk concept is the ability to define what may happen in the future and to choose among alternatives. Central to Bernstein’s story telling is how quantitative breakthroughs over the past 450 years have shaped the trajectory of progress into a modern society uniquely characterized by its mastery of risk. Anthropologist Lupton (1999) tells the story from a different perspective, mapping the changing conceptions of risk through time. The premise of Lupton is that our understanding of risk takes place in a specific socio-cultural and historical context. Risk in its early, 16th century use denoted unfortunate events beyond the scope of human intervention. The emergence of modernity and with it the disciplines of probability and statistics, readjusted the notion to what could be measured, calculated and prevented. In the everyday parlance of contemporary western societies, the term is loosened. Today, risk seemingly characterizes any hazardous, misfortunate, or simply annoying event. We speak of nuclear accidents, terrorism attacks and delayed departure of trains using the same notion of risk.

An extensive expert apparatus proliferated in the 20th century with the aim of understanding, measuring and controlling risk. A band of scientists have of this reason caricatured our postmodern society as preoccupied with risk. Among the most influential is the dystopian Beck (1992), postulating that we currently live in a *risk society* that is undermining its own preconditions. In remarkable contrast is Bernstein (1996), who positively portrays a society that has broken down the barriers for mastering risk. Modern conceptions of risk, he concludes, goes hand in hand with opportunity for gain and historical progress. Either one sides with Beck (1992) or Bernstein (1996), it can be concluded that risk is a defining characteristic of contemporary society. According to Lupton (1999), there are at least six pressing risk domains in the present socio-cultural, political and economic context of western societies:

- *Environmental risk* related to global warming, pollution, radiation, chemicals and floods.
- *Lifestyle risk* in consumption of food and drugs, sexual activities, driving practices, stress and leisure.
- *Medical risk* of drug therapy, surgery, childbirth and diagnostic tests.
- *Interpersonal risk* from engaging in intimate relationships, social interactions, love, sexuality and parenting.
- *Economic risk* of under- or unemployment, loan, investment and bankruptcy.
- *Criminal risk* of participating in or being the victim of illegal activities.

A seventh group of *technological risk* may be added, capturing the accidental side effects of technological innovations that preoccupy technical risk assessors and theorists like Perrow (1984) and Beck (1992).

The preponderant domains in which *risk* now applies are very diverse. What are common to these situations, rendering them explainable by one single word? Broad



qualitative features of the risk concept are presented in the following. These can be summarized as:

**Risk** is a characteristic of the future concerning the uncertain consequences of decisions and contingencies.

### 2.2.2 Uncertainty about future consequences

Intuitive to the notion of risk is that something is at stake. It might be the loss of life or limb, freedom, enterprise or biodiversity. According to Fischhoff et al. (1984), the most defining aspect of risk is the attribution of consequences to future events. Lupton (1999) observes that contemporary conceptions of risk almost exclusively relate to undesirable consequences. An important exception is the parlance of economic speculation, where one speaks of “good” and “bad” risk as the anatomy of making money. Attempting to generalize this view, economist Holton (2004) promotes a sole requirement in that someone must care about, that is, be exposed to the consequences. Luhmann (1991) elaborates that one can speak of risk only if able to draw certain distinctions; between good and bad outcomes, advantages and disadvantages and the probability and improbability of occurrence.

The latter division brings us to the second major characteristic of risk; the consequences are probable to a varying degree, but never certain. If an outcome is certain to happen, one does not face a risk (Adams, 1995). This is because risk is exclusively concerned with consequences of a future that is draped in uncertainty. Although omitting the word *risk*, Lindley (2006) preaches that the future is inherently incapable of following logic’s rules of falsity and truth. When contemplating the future, one must thus always prescribe probabilities that are neither 0 nor 1. The theory of probability is of this reason at the mathematical heart of the risk concept (Bernstein, 1996).

Accepting this tenet is conceptually quite challenging. Does it mean that an unprotected person who jumps out of an airplane at 10 000 feet above ground does not face a risk, since he is almost certain to die? Or if he does, is he facing high or low risk? Most people would presumably agree that few activities involve greater risk than this hypothetical extreme. The principal issue is that a probability close to, but not equal to one, implies a high risk (Campbell, 2005). Whether we are certain that this probability is correct is, however, a different but significant issue which will reappear in Section 3.2.

While future consequences and their uncertain realization are central to both lay people and experts’ conceptions of risk, they are also a primary source of discord. Philosopher Adler (2003) explains this by reference to probabilistic and non-probabilistic conceptions of risk, characterizing the weight people place on probability and consequence severity when contemplating risk. There is an extensive body of literature on the subject that lies beyond the scope of this study. The interested reader may consult for instance Ball and Floyd (1998) or Tversky and Kahneman (1974). For now, we will continue our exploration of the risk concept by abstract attribution.

### 2.2.3 Fighting contingency

Luhmann (1991) conceives risk by causal attribution to decisions. Decisions, he claims, are what binds time, making us turn the page from past to future by project-

		Uncertainty	
		YES	NO
Stakes	YES	Indeterminacy (Quantum Mechanics)	Determinism (Celestial mechanics)
	NO	Risk (Decision Science)	Fate (Myth)

Figure 2.1: Demarcating risk (adopted from Rosa, 1998).

ing essential aspects of a described future onto the present. Accepting the premise of Luhmann, we speak of risk only if we can identify a decision without which the consequences could not have occurred. The consequences are hence avoidable, that is, within the influential scope of one or several decision makers. Rosa (1998) promotes a similar position when demarcating *risk* from *fate* as depicted in Figure 2.1. While this implies the exclusion of some situations from the risk concept (like meteorite destruction of earth), the exceptions are fascinatingly few in number. In contemporary society, nearly all events are within the influence of humans. Instead of passively accepting the future, we actively engage in it in pursuit of control. The paradox is that we can never fully manage the future, not even the one we generate by means of our own decisions. In the context of risk, one is never emancipated from the gap between possible and chosen action; reality and possibility. Renn (2008) explains this as contingency; the future is neither predetermined, nor independent of today's activities. Embracing the disturbing conclusions of Perrow (1984), Luhmann maintains that the more we seek to control, the more contingencies are introduced and risk proliferates. The gap between the past and future grows, and with it society's dependency on decision making.

The argumentation of Luhmann is deeply philosophical, and serves to support a conclusion explaining societal processes in terms of risk rather than vice versa. Nonetheless, it points to a crucial characteristic which simple conceptualizations of risk as consequence and uncertainty seem to miss. When striving to understand risk, we must also understand the decisions that make up our very conception of it.

#### 2.2.4 Past futures

Accepting that risk is related to future contingencies begs the question if one can speak of past risk. Is it sound to claim that the risk of swine flu was high in 2009? And if so, what considerations underly this statement; that over 900 000 Norwegians caught the flu during 2009 (FHI, 2010) or the uncertain predictions at its very onset?

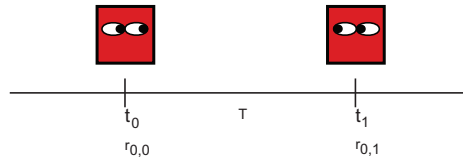


Figure 2.2: Assessing risk retrospectively.

The Norwegian Petroleum Safety Authority (PSA) publishes an annual report titled *Trends in risk levels* (RNNP). RNNP endeavors to measure risk levels by collocating a range of relevant indicators, like reported accidents during the year of interest (PSA, 2010). A conclusion is drawn regarding the risk level as *observed*. Is this a proper use of the term risk? Rhetorically, one can ask what to conclude if there were zero reported accidents during the period. Does that mean that the risk was zero? Consulting the risk literature, the advice is an unanimous no. Risk can never be zero, unless we stop performing the activity in question (Adams, 1995). More importantly, looking back at the past, one is able to say with certainty that an accident has or has not happened. Since certainty has got nothing to do with the concept of risk, it is the opinion of this author that PSA should consider rephrasing their publication to, for example, *Trends in safety performance levels*.

Monitoring trends in risk levels is not an unreasonable objective. The crucial point is that in order to speak of past risk, one must recapture the future as conceived in the past and not the past outcomes as such. Figure 2.2 illustrates that considerations made today,  $t_1$ , of risk for a previous interval  $T$ , must be made by moving the point of observation to a time  $t_0$ . If no assessments at  $t_0$  are documented, the problem becomes one of separating reasonable foresight from hindsight. The Norwegian research institute SINTEF is currently struggling with this problem, retrospectively mapping so-called *risk influencing factors* (RIF) in a research project on trends in helicopter safety (see, Kråkenes et al., 2009).

Closing with the words of Luhmann (1991, p.42), one can state that a main difficulty of risk is that the way it is evaluated varies in time:

With hindsight, we evaluate risk in terms of whether a loss has occurred or not. When we look back, we no longer understand why in a present now belonging to the past we had been so cautious or, as the case may be, why we had made such a risky decision. And from out of the future another present stares us in the face, in which we will in retrospect certainly come to a different appraisal of the risk situation we are experiencing in this present. But how we will see it remains uncertain.

### 2.3 Theorizing risk

Risk is an intuitively appealing concept. Perhaps paradoxically, it is also a concept that is difficult to contemplate. Consulting the risk literature, one is bewildered by diametrically diverging opinions on what risk really *is*. In her quest for rationality, Shrader-Frechette (1991) critically reviews theoretical extremities on the subject. Focal in the conflict among risk philosophers is the very existence of risk and what methodological norms, if any, guarantee the rationality of evaluation. The positions are arrayed on a spectrum from *cultural theory* to *naive positivism*. Exponents of the

former stance are Douglas and Wildavsky (1983), while the latter has traditionally been occupied by risk analysts like Starr (1969). The positions are briefly presented in the following, adopting the advice of Rosa (1998) of separating issues of *ontology* from those of *epistemology*:

- **Ontology** asks “What is out there?”. It deals with what exists, the nature of existence and states of the world.
- **Epistemology** inquires “How do we know what’s out there?” It refers to the acquisition of knowledge, the thoroughness of that knowledge and its justification.

### 2.3.1 Ontology

Ontological *realism* makes the bedrock of naive positivism. Risk is considered an objective state of the world that exists independently of human observation (Rosa, 1998). A risk is a risk, regardless if anyone has recognized it as such. In contrast is ontological *relativism*, which is fundamental to the cultural theory of Douglas and Wildavsky (1983). Risk is interpreted as a cultural, rather than physical phenomenon; nothing is a risk in itself. While the realist position holds a promise of an *actual risk* of a certain state or quantity, relativism denies that risk is anywhere but in our minds. *Perceived risk* is a meaningful complement in the former case and an unnecessary given in the latter (Adams, 1995).

While otherwise concordant in their critique of naive positivism and cultural theory, Shrader-Frechette (1991) and Rosa (1998) disagree over the issue of ontology. Rosa alleges that there are certain states of the world that can be objectively defined as risk. Some risks are undeniably real, regardless of our perception of them. Shrader-Frechette (1991, p.84) on the other hand, asserts that “(..) there are no risks except perceived risk”. Many risks are real as they bring real consequences, but until their manifestation, risk is purely perceived. Although appealing to the recognition that risk is a property of a never observable future, this exposition invites unanswerable philosophical questions. Does it imply that dangers we do not know about are not representing a risk? And may two people experiencing a similar situation have different risk? According to Kaplan and Garrick (1981), the answer to the latter question is yes. Risk depends on what you do and what you know and is thus relative to the observer. But this is a matter of epistemology.

### 2.3.2 Epistemology

Epistemology is closely related, but conceptually far from ontology. According to Rosa (1998), there need not be an isomorphic relationship between the world and our understanding of it. Both naive positivism and cultural theory fuse the ontology and epistemology of risk into a reductionist philosophical purée. This diverts our attention from asking the most important question of what our *knowledge* of risk is, with theoretical obsession of what risk *is*.

Naive positivists believe that risk may be objectively identified and estimated, devoid of bias and sociological shaping. In the seat of honor are technical risk assessors, whose claims are considered completely objective, neutral and value free. True knowledge is provided of a risk that is real, hence guaranteeing rational risk management (Shrader-Frechette, 1991). An early advocate is Starr (1969, p.1237), announcing that:

The principal point is that the issue of public safety can be focused on a tangible, quantitative, engineering design objective.

At the other end of the epistemological spectrum are Douglas and Wildavsky (1983, p.80), asserting that all knowledge is a social construct. And because nothing is a risk in itself, any claim about risk is as imperfect as the other:

Everyone, expert and layman alike, is biased. No one has a social theory above the battle. Knowledge of danger is necessarily impartial and limited: judgments of risk and safety must be selected as much on the basis of what is valued as on the basis of what is known.

Due to our limited perceptual and cognitive capabilities, Rosa (1998) agrees that knowledge claims are always subjective. That we can never generate perfect knowledge about the world does not, however, mean that all claims are equally fallible. Although never absolutely true, knowledge claims admit to varying degrees of approximation. Shrader-Frechette (1991) clings to this argument when launching *scientific proceduralism* as an epistemological middle position. Some claims, like those of technical risk assessors, are recognized as more explanatory than others. But above that, thinking rationally about risk presumes intelligible and democratic debate in a balanced consideration of facts and values. Such a middle position is in line with most contemporary approaches to risk management (see, e.g. Renn, 2008) and will serve as the underlying epistemology of this thesis. Whether risk exists outside our perception is considered minor to the question of how we best can produce knowledge to reduce our uncertainty about the future.

## 2.4 Defining risk

Risk assessment guru Kaplan (1997) opens his speech to the Society for Risk Analysis by reminiscing how an expert committee gave up after four years struggling to define risk. Maybe it is better not to define risk, the final report concluded, and let each author define it in his own way. And so he did. In a recent paper, Aven (2010b) navigates through a vast number of risk definitions. Some are diametrically distinct, while others wordily nuanced. Little consensus is ostensibly achieved since Fischhoff et al. (1984) early recognized that defining risk is a manifold and inherently controversial task. According to this trio, the choice of definition affects the outcomes of decision problems and is thus an exercise in power. As put by Slovic (1999, p.699);

(..) whoever controls the definition of risk controls the rational solution to the problem at hand.

Both contributors search a flexible definition, contending that no definition is suitable for all problems. Notwithstanding that definitions are never entirely true or false, they provide useful tools for abstraction and clarification of focal points (Rosa, 1998). A selection of common risk definitions are discussed in the following with emphasis on conceptual content and clarity. The review of Aven (2010b) serves as explanatory inspiration, characterizing definitional elements in the form:

$$\mathbf{Risk} = (A, C, P, U) \quad (2.1)$$

$A$  represents events,  $C$  denotes consequences and  $P$  and  $U$  designate probability and uncertainty.

### 2.4.1 The traditional engineering approach

A conventional definition in engineering contexts is fronted by Wilson and Crouch (1982, p.9):

$$\text{Risk} = \text{Probability} \otimes \text{Severity} \quad (2.2)$$

This definition may be conceptualized as  $R=(C,P)$ . It is rooted in the ontology of realism, assuming that risk is an objective state of the world as future events with associated consequences and probabilities of occurrence. For decision making, Wilson and Crouch admit that the terms represent perceptions only. The definition is appraised as superior in applications of risk/benefit analysis. It provides a compound measure that is unambiguous, easy to handle and enables ranking of alternatives. When multiple events are considered, the measure is commonly referred to as *expected loss* or *expected value*.

Aven (2010b) is clear when dispelling this type of definition. The pressing problem is that improbable events of potentially large consequences are equated with frequently occurring events of minor consequences. Haimes (2009) elaborates that the relative importance of both probability and consequence is distorted, hence masking the criticality of extreme events like dam failure or airplane crashes. Since such situations require different management strategies than, for example, car accidents, the definition of Wilson and Crouch (1982) is likely to preclude effective risk management.

### 2.4.2 The international standard

The most recent international standard on risk management, ISO 31000 (2009, p.1), defines risk as:

**Risk** is the effect of uncertainty on objectives.

Risk is in this definition conceived as  $R=(U)$ . With reference to Section 2.2, this insufficiently captures that risk is concerned not only with uncertainty, but also consequences. Regardless of the potential consequences, all objectives seemingly represent a risk. This is because their fulfillment is a property of the future and is thus uncertain. Does the uncertainty tied to the objective of reducing national sickness absence qualify it as a risk? And if so; is it the attainability objectives that represents a risk or the uncertainty itself? Recalling the words of Luhmann (1991), it may be argued that *objectives* implies consequences of some sort, since it allows one to draw distinction between realizing the objective or not. Yet, the locus of attention is not the goodness of the objectives as such, but how they are affected by uncertainty. How is one then to prioritize between different objectives that are equally affected by uncertainty?

The most evident weakness of the ISO 31000 (2009)-definition is simply its vagueness. What is an effect and how is it measured? Is it something that is in my head or is it a state of the world? What is an objective and what separates it from other concepts and eventualities? ISO 31000 (2009, p.1) attempts to clarify some of these issues via five notes:

NOTE 1: An effect is a deviation from the expected-positive and/or negative.

NOTE 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3: Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the likelihood of occurrence.

NOTE 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

On the positive side, the notes convey that risk is a many-faceted concept. It is recognized that outcomes can be both positive and negative, reflecting that an outcome can be positive for some stakeholders while negative for others (Aven and Renn, 2009). On the negative side, the risk concept is not only expanded into definitional inertia, embedded are also contending definitions like that of Wilson and Crouch (1982). In the pursuit of abstraction and clarification, we are therefore better served continuing our definitional search elsewhere.

### 2.4.3 Consequence-orientation according to Klinke and Renn

Klinke and Renn (2002, p.1071) defines risk as:

The possibility that human actions or events lead to consequences that harm aspects of things that human beings value.

In contrast to the ISO 31000 (2009)-definition, Klinke and Renn emphasize consequences rather than uncertainty. Their definition may thus be caricatured as  $R=(C)$ . By choosing the loose term *possibility*<sup>1</sup> instead of *probability*, focus is seemingly on the consequences that might occur rather than our uncertainty of this happening.

Klinke and Renn are specific, yet general, in defining the consequences of interest. Unless something human beings value might be harmed, we do not speak of risk. An epistemological middle position is indicated in which risk is a real world, but value-dependent concept of selection. The definition captures the necessity of exposure to potential outcomes as postulated by Holton (2004). However, combined with its peripheral account of uncertainty, it may erroneously lead you to think in certainties when contemplating risk. Given that a consequence occurs, do you care? Owing to this, risk considerations may be biased towards catastrophic, but unrealistic outcomes. The result may be excessive precaution, along with neglect of less severe, but more probable consequences. What is more, decision making is likely precluded as one cannot conclude whether a risk is high or low or compare different outcomes. According to Aven (2010b) and as demonstrated in the previous sections, this holds for all definitions conceiving risk in terms of  $R = (C)$ ,  $R = (U \text{ or } P)$  or  $R = (A)$ .

---

<sup>1</sup>The reader should note that possibility has a distinct meaning within *possibility theory*, which deals with certain types of uncertainty as an alternative to probability theory (Lindley, 2006). This specific meaning is, however, hardly the intention of Klinke and Renn (2002).

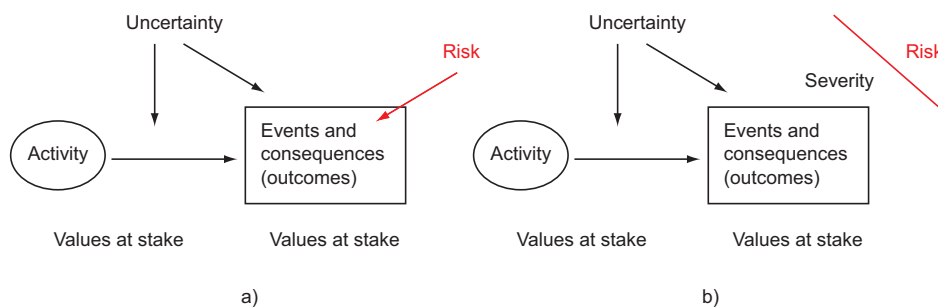


Figure 2.3: Risk according to (a) Rosa (1998) and (b) Aven and Renn (2009) (adopted from Aven and Renn, 2009).

#### 2.4.4 Event-orientation: Rosa vs. Aven and Renn

An example of the latter category is Rosa (1998, p.28):

**Risk** is a situation or event where something of human value (including human themselves) has been put at stake and where the outcome is uncertain.

Three elements found in nearly all conceptions of risk are, according to Rosa, captured in this definition; a state of reality of human interest, a possible outcome (positive or negative) and the notion of uncertainty. Unfortunately, Rosa refrains from concretizing what lies at the very heart of his definition. What is an event? His only specification is the plausible, but in the context of risk assessment too general, demarcation scheme of Figure 2.1. Consider the case of car driving ending in a fatal accident. Is the event of interest the choice of not using seat belt, being distracted by a fly, entering the opposite lane or crashing into another car?

In a thorough critique of the Rosa (1998)-definition, Aven and Renn (2009) agree that it offers a sound foundation for risk management as it diverts attention to uncertainty instead of probability, and outcome stakes instead of specific consequences. This is in line with Aven's contributions on the insufficiency of probability calculus in expressing uncertainty (see, e.g. Aven, 2003). Probability-centered risk definitions, he asserts, are too narrow. Aven believes that probability assignments mask critical assumptions and suppositions made in the assessment, truncating important aspects of uncertainty. This is, however, not a generally accepted convention. Consulting leading statisticians like Lindley (2006) and risk assessors like Garrick (2008), probability is our only and perfect tool for quantitatively expressing uncertainty.

The main flaw of Rosa's definition is according to Aven and Renn the granting of ontological realism to risk as an event. Uncertainty is not real, they claim, but a construct of human imagination to cope with future outcomes that can become real. Without incorporating the epistemological component of uncertainty in the risk concept, conceptual difficulties are allegedly induced as one is unable to appraise a risk as high or low. Owing to this, they suggest a slightly refined definition that is conceptualized in Figure 2.3. Risk is no longer described as  $R = (A)$ , but as  $R = (A, C, U)$  (Aven and Renn, 2009, p. 6):

**Risk** refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value.



Table 2.1: The risk table (adopted from Kaplan and Garrick, 1981).

<i>Scenario</i>	<i>Likelihood</i>	<i>Consequence</i>
$s_1$	$p_1$	$x_1$
$s_2$	$p_2$	$x_2$
$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$
$s_n$	$p_n$	$x_n$

The argumentation of Aven (2009) is not only intricate, but does also seem to twist the very point of Rosa (1998). Believing that certain states of the world are possible, that is, objectively real, does not exclude epistemic considerations of uncertainty from the risk concept. If our ability to understand risk is very uncertain, risk appears less like an objective state and more like a mental construction. Notwithstanding that, the conclusion of Aven (2009) remains plausible when discarding the Rosa-definition as incompatible with practical risk assessment. It is of this reason considered unsuitable for our purpose. Also the uncertainty-centered conception of Aven and Renn (2009) and Aven (2010b) is forsaken, if only on the grounds of conceptual complexity.

#### 2.4.5 The quantitative definition of Kaplan and Garrick

Consulting the reference tracker SCOPUS, one of the most cited definitions of risk is the *quantitative-*, or *triplet definition* of Kaplan and Garrick (1981, p. 13). Risk is defined as the answer to three questions:

1. What can happen? (i.e. what can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

To answer these questions, Kaplan and Garrick suggest the making of a list as in Table 2.1. Each line,  $i$ , is a triplet of a scenario description,  $s_i$ , the probability,  $p_i$ , and consequence measure,  $x_i$ , of that scenario. Including all imaginable scenarios, the table is the answer to the questions and therefore the risk. Formally, risk is defined as a set of triplets:

$$R = \{ \langle s_i, p_i, x_i \rangle \} \quad (2.3)$$

Acknowledging uncertainty in consequence and probability estimations, the definition may be further refined into:

$$R = \{ \langle s_i, p_i(\phi_i), x_i \rangle \} \quad (2.4)$$

$p_i(\phi_i)$  and  $p_i(x_i)$  are the probability density functions for the frequency and consequence of the  $i$ th scenario. In our simplified framework, Equation 2.3 and Equation 2.4 corresponds to  $R = (A, P, C)$  and  $R = (A, P, C, U)$ . Arranging the scenarios in order of increasing severity and damage, Equation 2.3 and Equation 2.4 can be plotted as a single or a family of curves as shown in Figure 2.4. In contrast to the definition of Wilson and Crouch (1982), Kaplan and Garrick stress that it is not the mean of the curve, but the curve(s) itself that is the risk. Since risk by definition

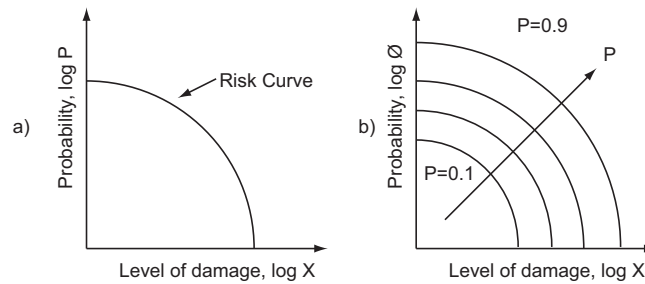


Figure 2.4: (a) A single and (b) family of risk curves (adopted from Kaplan and Garrick, 1981).

is given by the totality of curves over the entire consequence spectrum, it is in the opinion of this author that referring to risk in plural is somewhat superfluous. At the risk of insulting the great many scholars who frequently speak of *risks*, it appears a modest correction that this is rarely imperative.

### Comprehensibility and content

The definition of Kaplan and Garrick (1981) has gained wide acceptance both within the scientific community and among practical risk assessors (Haimes, 2009). A reasonable explanation is its direct relevance to risk assessment. Not only do the three questions offer simple clarification of what the risk concept is, provided is also procedural guidance for risk assessment. Moreover, unlike some of the above definitions, all elements of  $A$ ,  $P$ ,  $C$  and  $U$  are included and apparently given equal considerations. The following recommendations are thus not biased towards extreme events as in the definition of Klinke and Renn (2002), nor is the relative importance of consequence and probability distorted like in the case of Wilson and Crouch (1982). Compared to the entangling definitions of ISO 31000 (2009) and Aven and Renn (2009), the triplet definition gains in comprehensibility.

### Constraints and ambiguities

Paradoxically, the plainness of Kaplan and Garrick's definition may also be claimed its weakness. As a foundation for risk assessment, it opens up for many interpretations. In fact, the scientific community is still discussing how the individual questions shall be interpreted. Aven (2010b) is harsh in his critique, claiming that Kaplan and Garrick's focus on probability as an expression of uncertainty is too narrow. By jumping directly into probabilities, potential surprises could be left unconsidered since one cannot accurately express what is extremely uncertain. This is a typical misinterpretation according to Garrick (2008), replying that the commonly added question of *what are the uncertainties?* is already embedded in the second question. Haimes (2009) sees the necessity of adding a different question, which is *over what time frame?* Garrick's response to this suggestion would probably be that the question of time is already embedded as a significant constraint in all three questions. What is interesting is that all contenders are right in their own means. While the definition may embed all contents of the risk concept, this ultimately depends on the interpreter. Since the understanding influences the choice of analytical methods,

the following results and their use in the decision making process, there is a need for making clear the foundations of risk assessment in terms of these three questions.

The definition of Kaplan and Garrick (1981) is adopted for this study, premising clarification of the following conceptual ambiguities:

1. *What can happen?* To foresee a future of endless possibilities, we must structure our imagination. What do we refer to when contemplating what can happen? Is it an accident scenario, an event or a set of consequences? Precisely what *is* an accident scenario and what distinguishes it from notions of initiating event, hazardous event and accidental event? Do the notions yield different analytical logics and results? When does a scenario start and when is it terminated? What is a hazard and what triggers it into a scenario? How can we assess scenarios of malicious acts? And what about the scenarios we cannot foresee?
2. *How likely is it?* According to Garrick (2008), the choice of the word *likely* is a well-considered one. Likelihood, he claims, is a general, intuitive expression that may be further specified as either *frequency*, *probability*, *credibility* and *probability of frequency*. This is problematic, since likelihood is a unique term in its own right, expressing a certain kind of statistical function that is not synonymous with any of the above mentioned terms (Lindley, 2006). More importantly, probability is far from a simple concept *per se*. Is it an objective property or does it only exist in our heads? Will two people, given the same background knowledge, assign the same probability? To what help is the past? Do we need to express our confidence in the assigned probabilities, that is, our uncertainty about the uncertainty?
3. *If it does happen, what are the consequences?* Imagine that we are to perform a risk assessment before the start-up of the nuclear power plant in Chernobyl in 1977. What do we mean by consequences? If it only comprises things that human beings value, as suggested by Klinke and Renn (2002), whose values shall we consider? Need the consequences be measurable? How do we compare consequences to life and limb, the environment and state economy? At what point in the accident scenario do we measure the consequences? Shall we model recovery operations and socio-political responses? How can we assess long-term consequences that will prevail twenty years ahead?

The present study is devoted to clarifying the first of these questions. Not only is the inquiry of *what can happen?* the most fundamental, it also appears as the most capacious. Paradoxically, it is also the issue on which focused discussions remain most few. An example of the contrary is the second question of *how likely is it?*, which has been subject to heated academic disputes since the mid 1980s. This is not to say that the debate is settled by any means; the interpretation of probability in risk analysis still enjoys a focal role in current contributions (see, e.g. Aven, 2010b). It is, however, in the opinion of this author that the first question is most in need for theoretical maturing.

Although the second and the third question, *what are the consequences?*, urge elaborate considerations in their own right, they still have implicit appearances in the present study. This is because the first question forms the basis of the remaining triplets in a definition that is utterly compound.

## Chapter 3

# Counterconcepts to risk

### 3.1 Introduction

An alternative means to grasping an intricate concept is to clarify its related counterconcepts. That is, to explain a concept based on what it is *not*. According to Luhmann (1991), it is a widely held belief that risk is a counterconcept to the German word *Sicherheit*. This is a very broad term that can be translated to either *safety*, *security* or *certainty*. In the risk literature, safety and security have distinct meanings, which interestingly, differ especially with respect to the third meaning of *sicherheit*. In this chapter, risk is discussed in light of the related concepts of safety, security and vulnerability. At first, the most central yet blurry concept to risk is examined, that is, *uncertainty*.

### 3.2 Uncertainty

Risk is tied to uncertainty. Removing the component of uncertainty transmutes risk into consequences that are destined to happen, hence emptying the concept of intrinsic value. The two notions are, perhaps of this reason, interchangeably used in everyday parlance. Within the scientific community, the interconnectedness of risk and uncertainty yields dissensions that are both linguistic and conceptual. Are risk and uncertainty complementary, synonymous or constituent concepts? Ground-breaking to this exposition is the demarcation of risk and uncertainty introduced by economist Knight (1921), which is discussed after first considering uncertainty in its own right.

#### 3.2.1 Uncertainty is a counterconcept to certainty

Webster (1978) defines uncertainty as:

**Uncertainty:** Something not certainly and exactly known.

According to this definition, uncertainty is a trivial term applicable to all situations where certainty is absent. Uncertainty is therefore ubiquitous and inescapable. Lindley (2006) introduces his book *Understanding uncertainty* by clarifying that some statements may be known to you as true and others false, but the vast majority of statements you know as neither true nor false. You are uncertain. In Lindley's view

is uncertainty a general, but precise term that speaks the language of probability. To measure your uncertainty of an event, Lindley invites you to compare your beliefs with a standard of drawing a specific number of favorable balls from an urn. If you assign a 0.6 probability that it will rain tomorrow, this equals the random drawing of a ball from an urn consisting of 60 favorable out of 100 balls. Reviewing the terminology in core references of risk assessment, Christensen et al. (2003) observe that uncertainty is usually considered self-explanatory. Without elaboration they posit that this is unfortunate, as uncertainty and its associated terminology is just as controversial as that of risk. Although a sensible claim, it is in the opinion of this author that at least on an abstract level, uncertainty is a less compound and more easily understood notion than risk. This is because it is labeled by its very counterconcept of certainty. The interpretation of uncertainty in risk assessment is, however, a complicated issue indeed. The suggested definition of Christensen et al. (2003, p.194) is adopted for clarification:

**Uncertainty:** Imperfect knowledge about the individual aspects of a system as well as the overall inaccuracy of the output determined by the system.

Uncertainty in the context of risk assessment is as much about the confidence we have in the process and results of risk analysis as it is about the uncertain outcomes as such.

### 3.2.2 Two manifestations of uncertainty

Consulting the guidance of NUREG (2009) on treatment of uncertainties in probabilistic risk assessment (PRA), uncertainty is something that impacts the robustness of results. When documenting the conclusions of PRA, it is thus necessary to take into account the associated uncertainties. Helpful is in this regard the distinction between two manifestations of uncertainty:

- **Aleatory uncertainty** stems from intrinsic randomness in a known population. For instance, this may be the height of an arbitrary child in a specific kindergarten. There is only one type of aleatory uncertainty, that is, *parameter uncertainty* related to uncertainty in computation of input and output parameter values.
- **Epistemic uncertainty** comes from lack of knowledge about fundamental phenomena. An example is the effect of  $SO_2$ -discharges on global warming. There are three types of epistemic uncertainty; *model uncertainty* due to the inaccuracy of models in representing real world phenomena, *completeness uncertainty* stemming from the risk contributors not considered in the analysis and *parameter uncertainty*.

Whereas aleatory uncertainty is inherently irreducible, epistemic uncertainty may be reduced with acquisition of knowledge. Uncertainty can thus be characterized as epistemic if there is a possibility to reduce it by gathering more data or refining models or approaches. Faber (2005) finds it interesting that these classifications are time dependent, noticing that phenomena which first have been conceived as a mixture of aleatory and epistemic uncertainty, may become purely epistemic with the progress of time and science. Kieureghian and Ditlevsen (2009) accordingly ask

if there is nothing but epistemic uncertainty. In conclusion, they assert that the advantage of classification is mostly pragmatic, as it becomes clear which uncertainties are prone to reduction at least in the short term.

### 3.2.3 Uncertainty and the interpretation of probability

The distinction between aleatory and epistemic uncertainty is valuable also in the sake of transparency. Paté-Cornell (1996) worries that epistemic uncertainties tend to be under-reported and often ignored in analyses of politically sensitive issues. As an example, she points to the conservative hypotheses of the International Panel on Climate Change (IPCC). Aleatory uncertainties is generally more acknowledged and integrated in mathematical models. According to Paté-Cornell (1996), this is rooted in the historical conflict over the meaning of probability.

Probability has traditionally been interpreted from two competing stances; the frequentist and the Bayesian school of thought. Scholars of frequentist conviction conceive probability as an objective property, defined by the limiting frequency of an independent set of identically distributed observations. Following the Bayesian interpretation, probability is a measure of your degree of belief and therefore only a mental construct (Watson, 1994). Whereas aleatory uncertainties may be treated by classical frequentist methods, epistemic uncertainties can only be addressed through Bayesian methods and expert opinions. Paté-Cornell (1996) presents six levels of increasing sophistication for treating uncertainty in risk analysis. Figure 3.1 shows that these range from purely qualitative to probabilistic assessments of aleatory and epistemic uncertainty. The topmost level invites the debated issue on whether to express uncertainty about uncertainty in terms of “secondary probabilities”. In Norway, Aven (2003) has been influential in arguing that such treatment of uncertainty only induces confusion in decision making. Moving across the Atlantic, NUREG (2009) is clear in requiring both a qualitative statement of confidence and a quantitative expression of the associated uncertainties. At the heart of this issue is the sufficiency of probabilities in expressing uncertainty, as was early questioned by Apostolakis (1989).

### 3.2.4 On Knight's distinction between risk and uncertainty

Although uncertainty forms the bedrock of the risk concept, the above discussion demonstrates that it is also complementary to risk in the sense of confidence. Influential, yet contrasting to this exposition is the much debated distinction between risk and uncertainty of Knight (1921). In his groundbreaking contribution *Risk, uncertainty, and profit*, Knight posits that risk and uncertainty represent two fundamentally distinct concepts (Knight, 1921, p.19):

But Uncertainty must be taken in a sense radically distinct from the familiar notion of Risk, from which it has never been properly separated. [...] It will appear that a measurable uncertainty, or ‘risk’ proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effects an uncertainty at all. We shall accordingly restrict the term ‘uncertainty’ to cases of the non-quantitative type.

According to Langlois and Boulder (1993), early scholars interpreted Knight's distinction such that risk applies to situations where probabilities can be assigned,

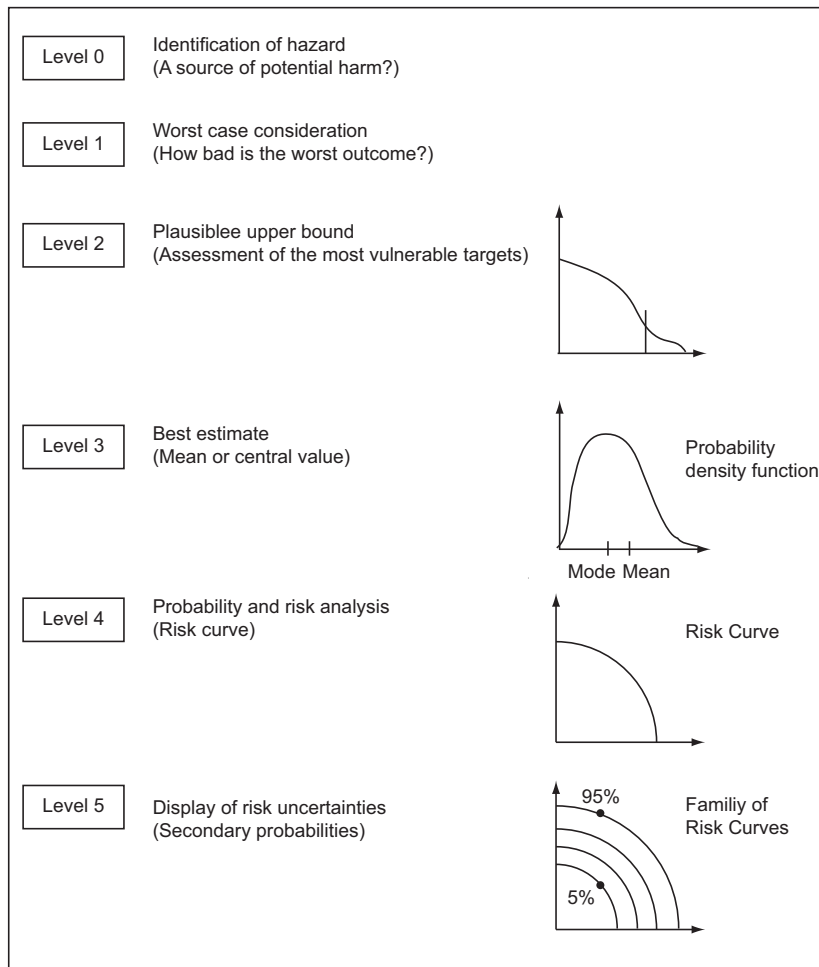


Figure 3.1: Six levels of quantification in the treatment of uncertainty in risk analysis according to Paté-Cornell (1996).

whilst uncertainty is reserved for situations in which one cannot. This interpretation has according to Tversky and Fox (1995) grown deep roots in decision theory, where decisions under uncertainty are known to promote a different approach than decisions under risk. While offering a sensible perspective in decision theory, this exposition appears conceptually confusing in the context of accident risk (as found in, e.g. Douglas, 1985).

Another common interpretation is fronted by Holton (2004), maintaining that risk owes to objective probabilities, while uncertainty concerns subjective such. Although this is central to Knight's argumentation, it appears somewhat outdated in light of today's conventional acceptance of Bayesian probabilities. Taking a different perspective, Langlois and Boulder (1993) find neither of the interpretations correct. The main and misinterpreted message of Knight, they claim, is that risk is related to situations of identifiable outcome states, whereas uncertainty rises with the impossibility of exhaustive outcome classification.

### 3.2.5 Uncertainty is a wider concept than risk

The reader should note that Knight wrote from a frequentist perspective on probability. Albeit pioneering in his critique of this stance, he is still convinced that the concept of probability rests solely within that paradigm (Bernstein, 1996). What is more, the preface leaves no doubt that Knight primarily appeals to the financial audience. It does not serve us to rest with the nuances of a contested perspective aimed at a different domain in the first place. Nevertheless, the many interpretations of Knight (1921) demonstrate the necessity of being vigilant when using the term *uncertainty*.

Uncertainty is a wider concept than risk. Not only does it make a constituent part of the latter concept, it also manifests itself on many levels. We have uncertainties about our values, what scenarios to expect and options to consider, the assigned probabilities and our very capabilities of considering these (Hansson, 1996). Hence pragmatically, it appears more useful to divert our attention to differentiating types of uncertainty. It is in this regard interesting to note that the second interpretation of Knight closely corresponds to the terms of aleatory and epistemic uncertainty (Paté-Cornell, 1996). This shows the interconnectedness of the concepts of risk, uncertainty and probability with respect to ontological realism. Whereas the prefix of *your* uncertainty expressed through *your* probabilities is fundamental to Lindley (2006), the notion of aleatory uncertainty implies the objective existence of some *the* uncertainty and a ditto risk.

The critique of Langlois and Boulder (1993) offers a fruitful perspective to the limitations of our conceptualization of risk. Consider the game of Russian roulette, in which you know the chance of firing a bullet and you know that if it does go off, you will most certainly die. Then, imagine you are Buzz Aldrin in the year of 1969, contemplating the risk of the world history's very first manned moon landing. You can barely imagine what awaits you in space, and the possible outcomes are anything but exhaustive. Do the two situations equally well subscribe to the notion of risk? According to the general criteria of Section 2.2, the answer to this question must still be yes. Having said that, how we conceive the conceptual relation between risk and remaining concepts is clearly influenced. Most conspicuous is the conception of safety.



### 3.3 Safety

Safety is for most people equated with freedom from risk (Reason, 1997). While it is intuitively appealing that safety means the absence of risk, this conception runs into difficulties confronted with the recognition that zero risk is utopia. More plausible is therefore the technical convention of safety as defined in ISO/IEC Guide 51 (1999, p.2):

**Safety:** freedom from unacceptable risk.

Implicit in this definition is that safety is a state of low risk. It need not be zero, but must be below a certain level. From this it appears that safety is a binary variable; something is either safe or unsafe. Brown and Green (1980) contemplate this position, reasoning that just as risk, is safety a dimension of continuous scale. While it might be true that the adjective *safe* is misplaced in situations of unacceptable risk, we may still talk of different degrees of safety or safe.

The main problem of the ISO/IEC Guide 51 (1999)-definition is that it urges contemplation on what is acceptable risk. Paraphrasing HSE (1992), acceptable risk can be understood as the level of risk we are willing to live with in order to secure certain benefits. The recent discussion of Johansen (2010) demonstrates that this is a very complex issue. In the pursuit of a clear understanding of safety, we thus seem better served consulting yet another source.

#### 3.3.1 Safety is a concept of relatives, not absolutes

Much research has been devoted to studies of safety. The concept in itself, however, is under-theorized and most often taken for granted (Möller et al., 2006). An exception is the International Civil Aviation Organization (ICAO, 2009, p.2-2), who clarifies safety as the outcome of organizational processes which have the objective of keeping risk under control:

**Safety:** The state in which the possibility of harm to persons or of property damage is reduced to, and maintained below, an acceptable level through a continuing process of hazard identification and safety risk management.

Also ICAO conceives safety with reference to acceptable risk, while providing a richer description by emphasizing the element of control. ICAO reasons that most connotations of safety have one underlying commonality in the possibility of absolute control. Since absolute control is an unachievable goal in dynamic operational contexts (Rasmussen, 1997), safety must encompass relative rather than absolute control. This reflects the flaws of the common interpretation as observed by Reason (1997). The reader should, however, note that there need not be an isomorphic relation between absolute freedom from risk and absolute control.

Möller et al. (2006) extend the argument by distinguishing between absolute and relative concepts of safety. The former covers interpretations of safety as freedom from risk, while the latter reflects the definitions of ISO/IEC Guide 51 (1999) and ICAO (2009). In contrast to ICAO (2009), Möller et al. (2006) contend that there is no need to add control to the notion of safety, as it is implicitly included through its influence on the risk dimensions of probability and severity. This claim can be challenged by referring to the studies of Slovic (1987), which reveal the significance

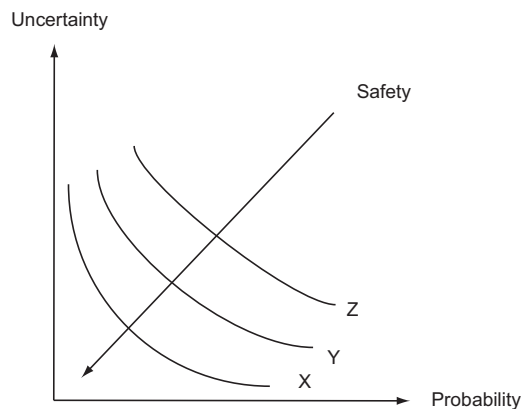


Figure 3.2: Safety is a function that decreases with the probability of harm, the severity of harm and our ability to foresee this with confidence.  $x$ ,  $y$  and  $z$  are levels of safety such that  $x > y > z$  (adopted from Möller et al., 2006).

of voluntariness and personal control to risk perception. While it is true that enhanced control need not yield reduced risk (Perrow, 1984), it seems unreasonable to exclude the component of control from safety on the grounds that it influences through other variables.

The latter discussion brings us to a second distinction, which Möller et al. (2006) draw between objective and subjective concepts of safety. As long as safety is conceived with reference to risk, this is inextricably tied to the relativity of the risk concept and thus equally debatable. While Brown and Green (1980) believe that safety is a purely personal construct, it is interesting to note that ICAO (2009) refer to safety as some seemingly objective state. Möller et al. (2006) reconcile this with an *intersubjective* perspective of safety, which resembles the epistemological middle position to risk of Shrader-Frechette (1991).

### 3.3.2 Is safety more than the antonym of risk?

The definitions of ICAO (2009) and ISO/IEC Guide 51 (1999) conceive safety as some antonym of risk. There is an inverse relation between risk and safety; the lower the risk, the higher the safety. According to Möller et al. (2006), this is a too narrow conception because it disregards the significance of epistemic uncertainty. Safety, they claim, is a function that decreases with the probability of harm, the severity of harm and our decreasing ability to foresee it with confidence. This is depicted in Figure 3.2. The proposition can be traced back to the ideas of Ellsberg (1961), observing that many people violate certain axioms of decision theory when faced with ambiguity<sup>1</sup>. Even if the expected outcome is less favorable, people show a strong tendency to choose the option associated with the lowest ambiguity. The significance of asking “what is the worst to be expected?” is thus lessened when two options of differing ambiguity are compared (Ellsberg, 1961, p.668).

In a thorough critique of Möller et al. (2006), Aven (2009) agrees that epistemic uncertainty is central to the concept of safety. Aven too, conceives probability, harm

<sup>1</sup>Ellsberg uses the notion ambiguity in characterizing situations of scanty, unreliable or conflicting information, which makes a central part of our term epistemic uncertainty.

and uncertainty as the three major components of safety. What he does not accept, is the alleged link between risk and safety. The flaw in the reasoning of Möller et al. (2006) as Aven sees it, is the way risk is conceptualized in the first place. If probability and harm are defined as the major components of risk, safety is undoubtedly more than the antonym of risk. If, on the other side, one adopts Aven's risk definition in which epistemic uncertainty is already included as a central component of risk, the relation between safety and risk is affirmatively antonymous.

Alternatively, safety can be constructed without any reference to risk. Hollnagel et al. (2006) scrap the idea of safety as the inverse of risk as outdated. Fundamental to their paradigmatic framework, *resilience engineering*, is the conception of safety as the ability to succeed under varying conditions. Resilience engineering emphasizes adaption instead of control (cf. ICAO, 2009). This transfers safety from a question of risk to one of resilience, which is a concept to be examined in Section 3.6.

### 3.3.3 Coupling risk and safety

The academic correspondence between Möller et al. (2006) and Aven (2009) shows the conceptually sensitive coupling between risk and safety. This calls for conscious application of the two terms. Risk and safety are interchangeably used. While the American nuclear industry employs the notation of *probabilistic risk assessment* (PRA) (NUREG, 2009), the International Maritime Organization (IMO, 2002) denotes what is basically the same thing *formal safety assessment* (FSA). Discussions on acceptable risk are repeatedly framed as a question of "how safe is safe enough" (see, e.g. Jongejan, 2008). Considering the ambiguity surrounding both terms, a minimum requirement must be to clarify the meaning placed in whatever one chooses to apply. Furthermore, it raises the question of whether we are actually served having both these words in our vocabulary.

Brown and Green (1980) argue that safety is a less ambiguous term that is preferable to risk. In contrast, ISO/IEC Guide 51 (1999) goes as far as advising against using the word safety, on the grounds that it introduces no extra information and will only lead to confusion. It is in the opinion of this author that both terms convey useful information in their own means. On one hand, risk is a broader concept than safety, as it is concerned not only with consequences of harm (Möller et al., 2006). On the other hand, it might be argued that safety is a more capacious concept than risk as it is not so restricted to future outcomes. It appears more meaningful to talk of past safety than past risk. Following the argumentation of ICAO (2009), safety is also a more compound concept, due to its strong connotations with the concept of control. Depending on the interpretation of Kaplan and Garrick's (1981) triplet definition of risk, the component of epistemic uncertainty also makes a quintessential additive to safety as the antonym of risk.

Recall the distinct examples of traveling to space and engaging in the games of Russian roulette. Epistemic uncertainty makes safety a relevant complement to risk in the former situation, while somewhat misplaced in the latter. There is, however, another reason for this, namely that the two situations differ with respect to agency. While the risk of Buzz Aldrin is primarily accidental, participants in Russian roulette deliberately engage in the game of risk. They might be forced into participation, you may argue, but even in this situation the term safety seems misplaced. Instead, we describe the situation as one in lack of *security*.

On the grounds that it appears a less compound concept, *risk* is principally preferred over *safety* in the present study. This is in line with the vast majority of theoret-

ical contributions on the subject. Notwithstanding this, safety serves an important role as an *adjective* describing risk. For distinguishing between risk of accidental and intentional origin, the notations of *safety risk* and *security risk* are used respectively.

### 3.4 Security

It seems like all the words of the risk discourse are fraught with a fuzziness that must be initially recognized. Security is no exception. Within the engineering community, the concept had been granted little attention before 2001 and the shocking events of 9/11 (Apostolakis and Lemon, 2005). Consulting the political sciences, security has since the onset of the cold war been connoted with external threats to state sovereignty (Bilgin, 2003). Social scientists, like Buzan et al. (1998), have construed the concept around threats to societal identity, while law scholars, like Zedner (2003a), problematize security as some counterconcept to crime. The semantics of security are, according to Zedner (2003b), as obscure as those of risk. It is conceived as a state of being and a means to an end, a positive or negative presence, a material or symbolic good and a private or public service. Since its meanings are various, conflicting and politically contested, Zedner argues that the concept of security defies simple definition. In remarkable contrast to the numerous definitions on risk, security is left undefined even by those engaged in clarifying the concept. For illustration, the risk lexicon of the US Department of Homeland Security (DHS) DHS (2008a) defines 73 terms of which their most focal notion of security is not one. Rather than trampling this undiscovered ground, the focus of this examination is on what distinguishes the security concept from those of safety and risk.

#### 3.4.1 Security is characterized by intention to do harm

Safety and security are, although dictionary synonymous, conceived as two disparate concepts within the risk discourse. What separates them is the defining characteristic of agency. While safety is conceptually reserved for accidental risk, security is the counterconcept to deliberate risk from human intentions to do harm (Comfort, 2005). Substantial to security is the adversary intent and capability of a perpetrator, that is, a *threat agent* (Garrick et al., 2004). Information about the intent and capability of possible agents is denoted *intelligence*. These terms are defined and discussed in Section 5.3, in connection with a thorough examination on the concept of *threat*.

Based on the main feature of intentionality, a range of situations fall under the domain of security. There are mundane criminal events like burglary, sexual assaults or identity theft, as well as extraordinary situations of terrorism, war and sabotage (Zedner, 2003b). While the focus of law scholar Zedner is on the mundane, central to the risk assessment collective of Garrick et al. (2004) is by far the extraordinary.

#### 3.4.2 The borderline between safety and security

The demarcation between safety and security is in some cases blurry. A prominent example is the issue of insider threat from employees. DHS (2008b) addresses the problem of trusted individuals exploiting their access to knowledge about an organization, which is clearly a security problem given the will to cause harm. Yet in most cases, harm is caused not due to hostile intention, but from deliberate or routine

violations of rules. Far from causing harm, the will of such everyday perpetrators is simply to optimize their effort within organizational and individual constraints (Battmann and Klumb, 1993). Is this a problem of security or safety? As maintained by Reason (1990a), it is believed that violation of rules is a problem that can and shall be confronted under the domain of safety. A less clear-cut problem is intentional drug abuse at hazardous work-places, which may unintentionally cause slips and mistakes resulting in accidents.

### 3.4.3 Security after September 11

The American Department of Homeland Security was established in 2001 in response to the disastrous events of 9/11. Its initiative objective was to prepare a national strategy for homeland security for protecting the US from terrorism. The appeal, signed G.W Bush, goes as following (DHS, 2002, p. VI):

Our enemy is smart and resolute. We are smarter and more resolute. We will prevail against all who believe they can stand in the way of America's commitment to freedom, liberty and our way of life.

Interestingly, this line reveals that security is as much about preserving the American identity of liberty as it is about protecting Americans from physical harm. Not only does it give resonance to the reflections of Buzan et al. (1998) on societal identity, it also captures how the analytical and moral complexities of security outdo those of safety at once an enemy is appointed.

A momentous shift in the discourse of security followed the terrorist attacks in New York. Nearly all collected articles in the deadlock of these events contemplate how 9/11 has dramatically altered our conception of security. Slovic (2002) sets the agenda, prophesying terrorism as a new species of trouble that strains the capacity of quantitative risk analysis. What is the role of risk analysis, he asks, when the stakes are high and the uncertainties enormous?

### 3.4.4 Security beyond risk

Collective efforts have subsequently been initiated to extend the analysis of risk to deliberate acts of terrorism. A notable contribution is in the comprehensive work of Garrick et al. (2004). Central is a joint focus on threats and infrastructure vulnerability, which is a concept later to be defined in Section 3.5. Because intelligence information is more dispersed, guarded and limited than information on vulnerability, the main source of uncertainty lies in the assessment of threats. Assessing threats changes the first question of Kaplan and Garrick (1981) into how someone can *make* something happen. Although acknowledging the remarkable uncertainties associated with assessing risk of intentional origin, Garrick et al. (2004), Deisler (2002) and Aven (2007a) defend that the traditional risk sciences have the potential for dealing adequately with terrorism. After all, limited data and catastrophic consequences was the precise background against which qualitative risk assessment was developed.

Among the opponents to this position are Aradau and van Munster (2007), contending that terrorism post-9/11 represents a double infinite of uncertainty and

consequence that calls for a precautionary approach to risk management<sup>2</sup>. De Goede (2008, p.166) similarly argues that combating terrorism requires one to “think the unthinkable” in a fashion that exceeds the logic of risk calculation. While the risk disciplines are centered on predicting an uncertain future, anticipating the threats of terrorism lies closer to the creative work of the entertainment industry in visualizing the wildest plurality of extreme futures. Referring to this contribution, Salter (2008) maintains that the crucial difference between matters of safety and security is incalculability. In his case against quantification of aviation security, Salter protests that in contrast to aviation safety, there are no reliable data on aviation security. This author will neither defend nor contest this claim, but inform that there is an extensive expert apparatus around ICAO known to be world-leading in the development of security assessment (ICAO, 2010). Recognizing the risk of sabotage, hijackings and terrorist use of civil aircrafts as well as technical failures, civil aviation is a field where both safety and security uniquely come across.

### 3.4.5 Amplification of security risk

The link between security, risk and safety is challenged not only by the overarching presence of uncertainties. Also the question of ontology is left more difficult. It is hard to imagine that something residing within human will can be anything but subjective, while at the same time admitting the objective danger of an airplane that is about to crash into a skyscraper.

Zedner (2003b) asserts that security is both an objective and subjective condition. As an objective condition, security is predicated on the presence of what threatens it. The subjective state of security is described by feelings alone as freedom from anxiety. Zedner remarks that it is a deep irony that the subjective feeling of insecurity increases when averted to security risk. More than in the case of safety, an anonymous mismatch between risk and subjective security therefore arises. An interesting lens for viewing this phenomenon is the framework of *social amplification of risk* launched by Kaspersen et al. (1988). In essence, Kaspersen and his coworkers assert that dissemination of risk information amplifies risk above the inherently dangerous properties of a threat alone. This is exploited by terrorists, whose very mission is to nourish a fundamental sense of insecurity with respect to future attacks (Burgess, 2007).

Salter (2008) takes a further constructivist position in voicing that terrorism risk is made real only through its assessment. According to Salter, quantifying security produces risk in the sense of promoting new nightmares that neither targets nor agents might have otherwise imagined. Unfortunately yet comforting, limited information can be sought on behalf of ICAO, since their publications on aviation security are sealed with restricted access. Perfectly paradoxical, this is of security reasons. As information about the assessment and management of security risk is transformed into increased capability in the hands of threat agents, also “objective” security risk increases with dissemination of information. Contrasting this with the openly shared safety manual of ICAO (2009), highlighted is another complicating distinction between security and safety.

---

<sup>2</sup>In very uncertain or vulnerable situations, relying on precaution is believed a more suitable strategy than attempting to quantify risk based on highly uncertain parameters. The difference between precautionary- and risk-based approaches to risk management is presented in Section 4.5.

### 3.4.6 Means to the end of security

A final troubling characteristic of security is that attempts to control it invites severe moral questions. In the context of general crime prevention, Zedner (2003b) postulates that there are attendant costs to pursuing security that stand counter to its purported goal. The greatest paradox, she claims, is that the means to the end of freedom from security risk has the strong tendency to infringe individual liberties. Although philosopher Næss (1985) finds this true also for matters of safety, intentional attribution necessarily calls for a different control of thought.

## 3.5 Vulnerability

The massive disruptions following the earth quake at Haiti January 2010 is a tragic reminder of the concept of vulnerability. Not only was the country characterized by weak government, poor infrastructure and lacking emergency preparedness in the first place; the rescue operations were also hampered as existing critical functions were severely disabled by the quake (Aftenposten, 2010). The stronger, but less damaging earthquake that consecutively hit the more prosperous Chile, indicates that a fair share amongst the 230 000 lost lives might have been saved had Haiti been less vulnerable to this natural event.

### 3.5.1 Attributes of vulnerability

*Vulnerability* appears in a number of disciplines, from economics and anthropology to psychology and engineering. As a scientific branch, it originated in the field of ecology. According to Adger (2006), this is the only area in which it has a common, though contested, meaning. Einarsson and Rausand (1998) substantiate that for technological applications, vulnerability has not yet sought a generally accepted definition. Consulting the Norwegian Directorate for Civil Protection and Emergency Planning (DSB), vulnerability is defined by reference to the Norwegian Standard NS 5814 (2008, p. 6):

**Vulnerability:** the lacking ability of an object to resist the impacts of an unwanted event and to restore to its original state or function following the event. (Translated)

A slightly different interpretation is provided by the powerful assemblage of Turner et al. (2003, p.8074):

**Vulnerability** is the degree to which a system, subsystem, or system component is likely to experience harm due to exposure to a hazard, either a perturbation or stress/stressor.

Common to both definitions is that vulnerability is a property of the object of analysis. While the former is adopted for this study, the latter provides valuable insight in that vulnerability is a matter of degree that acts on different levels of a system. The system under analysis may be socio-ecological (see, e.g. Turner et al., 2003), socio-technical (see, e.g. Einarsson and Rausand, 1998) or societal (see, e.g. Apostolakis and Lemon, 2005). In line with all applications are three attributes of vulnerability (Adger, 2006):

1. *Exposure* to stress (e.g., an earthquake or terrorism attack).

2. *Sensitivity* as the degree to which a system is affected by this stress (e.g., the susceptibility of Haitian houses to trembling ground).
3. *Adaptive capacity* as the ability of a system to accommodate change (e.g., the effectuation of rescue operations and reconstruction).

All attributes influence the *disruption time*, which marks the time interval from an event occurs until a new stable situation is established (Einarsson and Rausand, 1998).

### 3.5.2 What make us vulnerable?

“Our free society is inherently vulnerable” it is stated in DHS (2002, p.7). The American way of living and the large, diverse and highly mobile population is claimed the nation’s greatest strength, but also its vulnerability. What is it that makes something vulnerable? The above definitions make it clear that one is vulnerable with respect to a certain type of stress. In the case of DHS (2002), this is terrorists hiding within the American midst. Regarding the event of an earthquake, the mobility of the American population is a poor determinant of vulnerability. More important in this case is land use planning. This is reflected in a comment of philosopher Jean-Jacques Rousseau, following an earthquake in Lisbon in 1755: “Why have we accumulated 20 000 houses with six to seven floors in a notably seismic location?” (Reproduced in Hovden, 2003, p.1). In contemporary institutions like the Norwegian Directorate for Civil Protection and Emergency Planning (DSB, 2010) and the UK Health and Executive office (HSE, 2009), land use planning is conceived as a central determinant of vulnerability to stresses of natural, technological and intentional origin.

Einarsson and Rausand (1998) categorize generic factors that influence the vulnerability of industrial systems as either internal or external. Internal factors are system attributes, like the complexity of interactions and tightness of couplings, technical reliability and organizational factors. Typical external factors are environmental, financial and societal conditions and infrastructure criticality. If broadening the scope to societal systems, the latter is of exceptional importance. *Critical infrastructures* are physical and information technology facilities, assets and networks so vital that their incapacitation will have debilitating effect on health, safety, security or economic well-beings of citizens or the effective functioning of governments (European Commission, 2004). Among these are energy installations and networks, communications and information technology, health care, finance and water supply.

Our extensive use of technology makes possible the rapid exchange of goods, services, people, information and knowledge (Comfort, 2005). Meanwhile, as the critical infrastructures become increasingly complex and interdependent, modern society is rendered extremely vulnerable. Infrastructure vulnerability is especially critical to terrorism risk. This owes to terrorism’s exact aim of maximizing social disruption (Apostolakis and Lemon, 2005). The devastating effects of the Haiti earthquakes demonstrate that also natural events may strain infrastructures like those of health care and food supply. It also illustrates that in most (but not all) cases, there is a link between lack of endowments and vulnerability (Turner et al., 2003).

### 3.5.3 Separating risk and vulnerability

Conceiving vulnerability as a property that influences the effect of an unwanted event, implies that it makes a central determinant of the third question of Kaplan



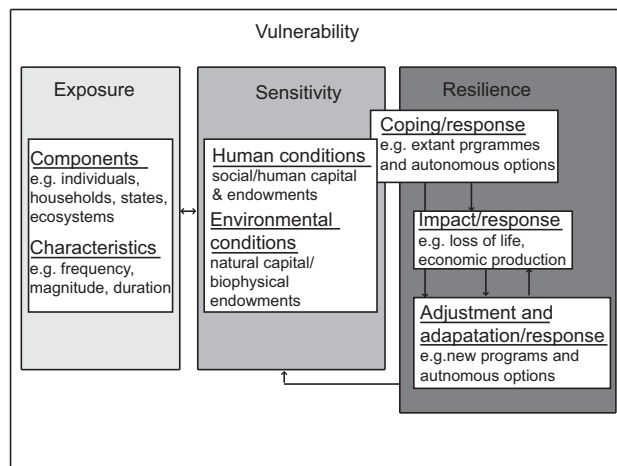


Figure 3.3: Components of the vulnerability framework of Turner et al. (2003).

and Garrick (1981). Is vulnerability simply a pillar of the risk concept or is it a concept entitled analysis in its own right? Einarsson and Rausand (1998) observe that in some references, vulnerability is considered similar to or a slightly broader concept than risk. An example is Aven (2007b), asserting that vulnerability is merely a part of the broader concept of risk. Vulnerability, he claims, is the combination of possible consequences and uncertainties given a source, while risk is the combination of this source and the related vulnerabilities. Einarsson and Rausand (1998) contend that vulnerability complements and extends the concept of risk. Vulnerability and risk analysis are believed to offer necessary and complementary information. This is in line with the guidelines of DSB (2010). Figure 3.3 illustrates that in comparison with traditional risk analysis, vulnerability analysis regards the whole disruption period until a stable situation is obtained. A second distinction is that vulnerability analysis deploys open system models, whilst risk analysis mostly operates within the physical boundaries of a system.

The advantage of separating risk and vulnerability both in concept and analysis is convincingly formulated by Sarewitz et al. (2003, p.809):

*The relation between vulnerability and risk is not commutative: reduced vulnerability always means reduced outcome risk, but reducing the outcome risk does not always reduce vulnerability.* (Original emphasis)

Instead of striving for reducing the probability of an unwanted event, Sarewitz et al. (2003) recommend reducing a system's vulnerability to this event. Regardless of the improbability of an event, unfortunate outcomes may still occur. Reducing vulnerability on the other hand, will always attenuate risk through reduced consequence severity. Especially important is this in cases of great epistemic uncertainty, as is demonstrated in the difficulty of assessing terrorism threat compared to infrastructure vulnerability (cf. Garrick et al., 2004). Great challenges are, however, present also in vulnerability analysis. Most pressing are the difficulty of measuring the dynamics and coupled complexities of societal and socio-ecological systems. There is also a call for reconciling the gap between objective and perceived vulnerability (Adger, 2006). Framing the problem as one of vulnerability instead of risk may be

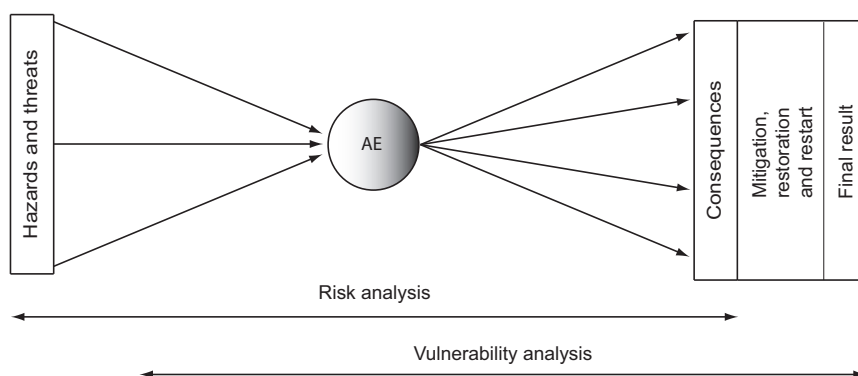


Figure 3.4: The different scope of vulnerability and risk analysis (adapted from Einarsson and Rausand, 1998).

more critical with respect to ontology, since “objective” vulnerability (as observed or analyzed) by and large depends on how people perceive and act upon it.

Equipped with the clever title *The vulnerability of science and the science of vulnerability*, Cutter (2003) posits that our ultimate vulnerability is the shortcomings in our knowledge about the world we live in. Our greatest source of vulnerability as Cutter sees it, is the lacking ability of vulnerability science to anticipate surprise, capture uncertainty and accept changes in our understanding. This is recognized by DHS (2002), promising that the more we know about our vulnerability, the more resilient we become.

### 3.6 Linking vulnerability and resilience

The nearest we come to a counterconcept of vulnerability is allegedly that of resilience. Yet, within their original field of ecology, vulnerability and resilience subscribe to different research traditions which have just recently began to converge (Adger, 2006). Paraphrasing Turner et al. (2003, p.8075), resilience can be defined as:

**Resilience:** A system’s ability to bounce back to a reference state after a disturbance.

According to Carpenter et al. (2001), resilience has the following attributes:

1. *The amount of change* a system can undergo and still retain the same controls on structure and function.
2. The degree to which the system is capable of *self-organization*.

3. The degree to which the system can build the capacity to *learn and adapt*.

Only wordily nuances and a negative sign seem to separate the main attributes of resilience and vulnerability. Of special junction is the third attribute of resilience, capturing that both resilience and vulnerability are concepts of dynamics. In contrast to the closely related, but static concept of robustness, resilience means the ability to tackle new and unexpected situations (Einarsson and Rausand, 1998). Recalling the concerns of Cutter (2003), this is precisely what makes resilience quintessential to vulnerability. In the proposed framework of Turner et al. (2003) in Figure 3.4, resilience is portrayed as the key to reducing socio-ecological vulnerability.

The framework also illustrates that vulnerability is more than some opposite of resilience, as it is additionally conditioned on exposure and sensitivity. Resilience, on the other hand, is a pervasive property that influences a system's response to *various* stressors. This is what makes resilience such an attractive concept, but also what complicates its means of achievement. Resilience engineering (as exposed by Hollnagel et al., 2006), may be criticized precisely of such pragmatic cloudiness. Nonetheless, complementing the negatively connoted concept of risk with a positive focus on resilience offers a promising perspective for mastering the dynamics of future uncertainties.

# Chapter 4

## Risk assessment

### 4.1 Introduction

Long before the time of Christ, Mesopotamian priests regularly assessed the impacts of proposed technological projects. Despite like practices of our ancestors, the rise of scientific risk assessment is claimed less than half a century old (Shrader-Frechette, 1991). Some references (e.g. Kates and Kasperson, 1983) draw a line at 1969 with the groundbreaking publication of Starr (1969) on comparative analysis of technological hazards. Most reviewers, however, date the birth of risk assessment to 1975 with the so-called *Wash-1400 report* of USNRC (1975) on nuclear reactor safety (Apostolakis, 2004). Since then, methodologies have advanced and the fields of application broadened into probabilistic risk assessment (PRA) of space systems (see, e.g. NASA, 2002a), quantitative risk assessment (QRA) in the offshore oil and gas industry (see, e.g. HSE, 2008) and assessment of human and environmental risk from chemicals (see, e.g. EU, 2000), to mention a few.

This chapter presents the contents and role of risk assessment in mastering technological risk. First, risk assessment is briefly described with the visual aid of the bowtie-diagram and an introduction to logic modeling. Contemplation follows on the very purpose of performing a risk assessment. This leads to a discussion on the strengths and limitations of risk assessment. Final attention is devoted to clarifying the main features of risk-based and risk-informed decision making and discussing the implications on risk assessment by way of communicability, relevancy and conceptual clarity.

### 4.2 The contents of risk assessment

In the risk management vocabulary of ISO guide 73 (2009, p.5), risk assessment is defined as:

**Risk assessment:** overall process of risk identification, risk analysis and risk evaluation.

ISO 31000 (2009) adopts this definition and conceptualizes risk assessment as shown in Figure 4.1. Risk assessment is in this figure put in the wider context of *risk management*, which ISO guide 73 (2009, p.2) defines as:

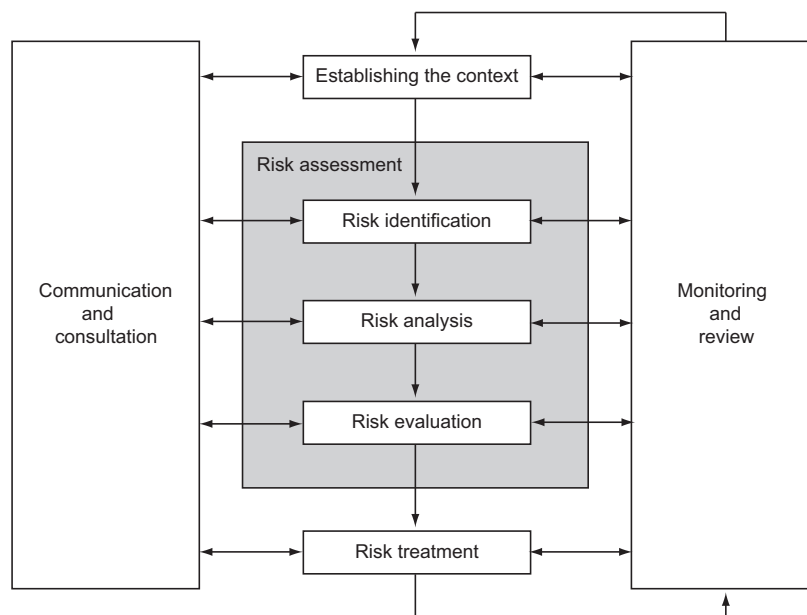


Figure 4.1: Contents of risk management and risk assessment according to ISO 31000 (2009).

**Risk management:** coordinated activities to direct and control an organization with regard to risk.

Risk management lies beyond the scope of this study and is not further examined. Having said that, the context in which risk assessment is placed influences the assessment in significant matters. Figure 4.1 models the dominant influence of communication and consultation with external and internal stakeholders throughout the entire assessment process.

ISO 31000 (2009) complements the framework of NORSOK Z-013 (2001) as is represented in Figure 4.2. What differs is mainly the locus of attention. While ISO 31000 (2009) is a generic standard on risk management, NORSOK Z-013 (2001) offers detailed guidance on analysis of risk and emergency preparedness. Risk assessment is slightly differently conceived as a collective process of *risk evaluation* and *risk analysis*, which in turn consists of *hazard identification* and *risk estimation*. In a review of generic and specific standards on engineering and chemical risk assessment, Christensen et al. (2003) report similar conceptual nuances. They reconcile that there is no need to seek a unified definition on the contents and distinction between risk analysis and risk assessment. Notwithstanding that demarcating hazard identification from risk analysis/risk estimation is mostly wordily quibbling, it is in the opinion of this author that separating risk assessment from risk analysis is expedient. In this study, risk analysis is conceived as the process of answering the three questions of Kaplan and Garrick (1981), while risk assessment covers the wider process of both risk analysis and evaluation, as is held by both ISO guide 73 (2009) and NORSOK Z-013 (2001).

Leaving definitional quibbles aside, risk assessment can be thought of as a structured, logical process of estimating the magnitude of risk, followed by a judgment of the significance of results (HSE, 2003b). Depending on the required level of detail,

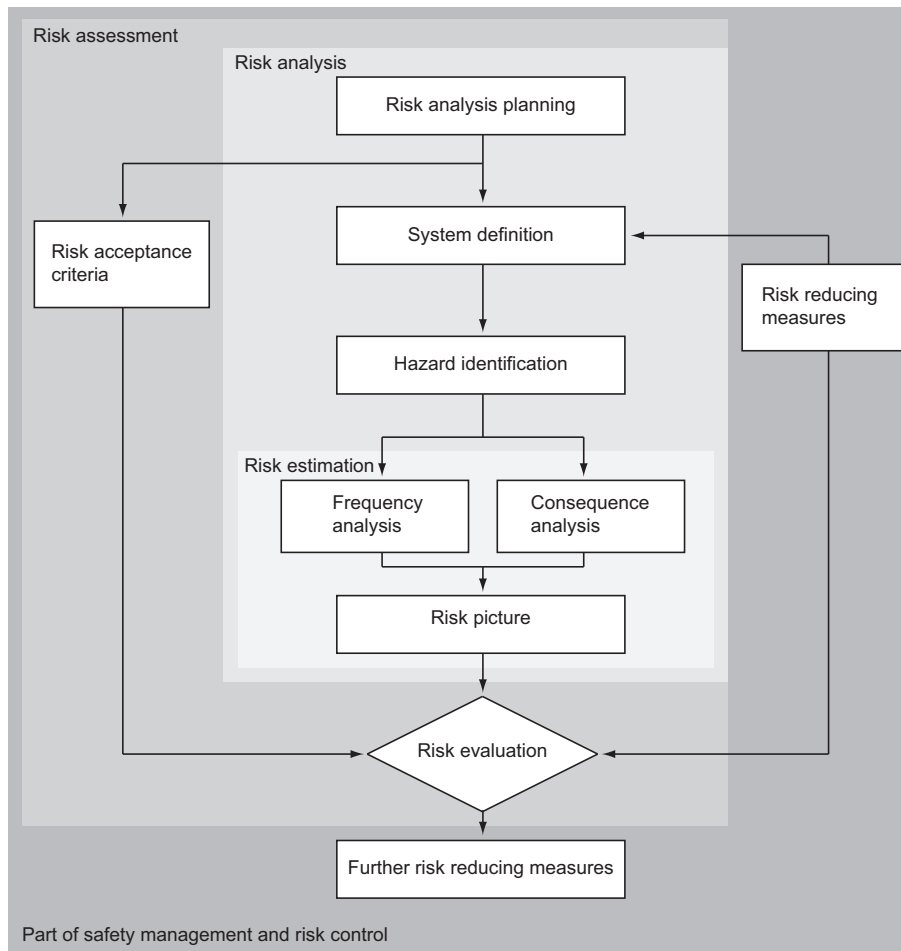


Figure 4.2: Contents of risk analysis and risk assessment according to NORSOK Z-013 (2001).

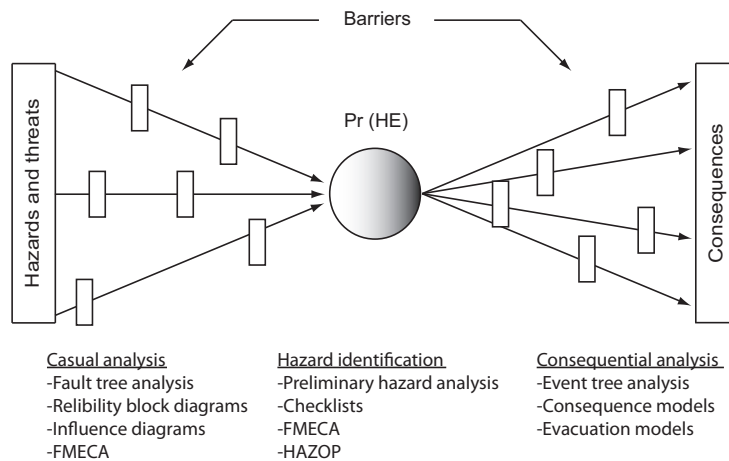


Figure 4.3: Bowtie-representation of risk assessment (adapted from Rausand and Høyland, 2004).

this can be a qualitative, semi-quantitative or quantitative process. The choice of method is affected by the problem at hand, the availability of resources, risk acceptance criteria, data availability and the risk management strategy (NS 5814, 2008).

#### 4.2.1 Inductive and deductive analysis of risk

Risk analysts are equipped with various tools, models and approaches. Among the distinctive characteristics are their structure, scope and underlying assumptions (NUREG, 2009). The essentials of risk analysis are aptly captured in the so-called *bowtie-diagram* of Figure 4.3. This presentation format, originally developed within the oil and gas-company Shell, is a popular feature in educational books (see, e.g. Rausand and Utne, 2009b) and guidances (see, e.g. HSE, 2006) on the subject. A bowtie-diagram represents the possible causes and consequences of a particular event, together with the safety barriers that are in place for prevention, control and mitigation.

Analyzing the left, midst and right part of the bowtie-diagram requires different techniques of modeling as is indicated in Figure 4.3. This owes to the distinctiveness of two paradigms of analytical reasoning; induction and deduction. Induction means drawing general conclusions from individual cases, whereas deduction is the reasoning from the general to the specific. In analogue with crime investigation, deductive analysis is the tool of all great detectives faced with a specific event of uncertain cause. Inductive reasoning on the other hand, attempts to ascertain the possible effects of a particular event (USNRC, 1981).

Induction and deduction perfectly complement each other in the consequential and causal analysis of risk. To determine *what* system states are possible, inductive methods like event tree analysis (ETA), failure mode and effect analysis (FMEA) and

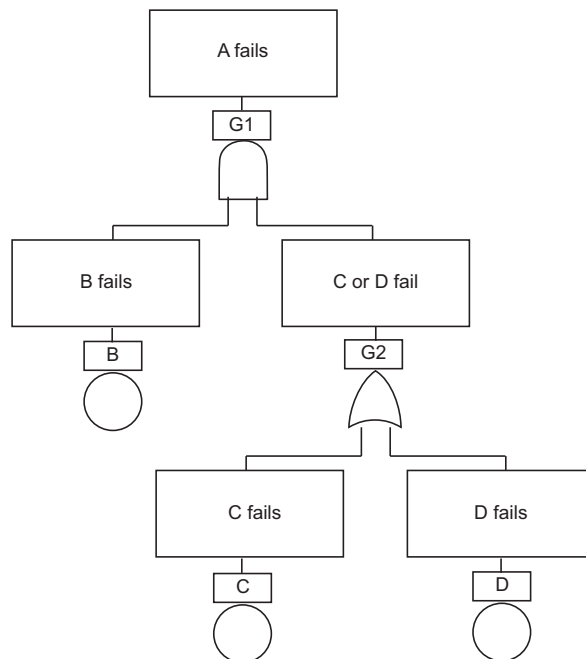


Figure 4.4: Simplified fault tree (adopted from NASA, 2002a).

preliminary hazard analysis (PHA) are most suitable. To determine *how* a given system state can occur, fault tree analysis (FTA) is our superior deductive tool (NASA, 2002a).

PHA and FMEA are but a few of many methods principally applicable to hazard identification. The interested reader may consult for instance HSL (2000) or DOE (2004) for a comprehensive overview on hazard identification techniques. These are *procedurally* structured, in contrast to the *logic* models of FTA and ETA. The logics of FTA and ETA offer in combination a communicable basis for answering the three questions of Kaplan and Garrick (1981), and are therefore sketched in the following.

### Fault tree analysis

Fault tree analysis is basically an analytical technique for identifying all credible ways in which a specified, undesired system state can occur (USNRC, 1981). Figure 4.4 illustrates that a fault tree is a graphic model. It consists of parallel and sequential combinations of faults leading up to an undesired top event, for instance, gas rupture. The faults can be associated with hardware or software failures, human errors or other pertinent events. These are binary events of either success or failure, connected by a complex of entities, called *gates*. The gates serve to permit or inhibit the upwards passage of fault. The reader is referred to NASA (2002a) for an elaboration on the numerous symbols. What is important in this context is to understand that a fault tree is always tailored to its top event, and is therefore not a model of all possible system failures or all causes of system failures. A vast number of fault trees must thus be generated in risk analysis of complex industrial systems. The reader should also note that covered are only the most credible faults as conceived by the



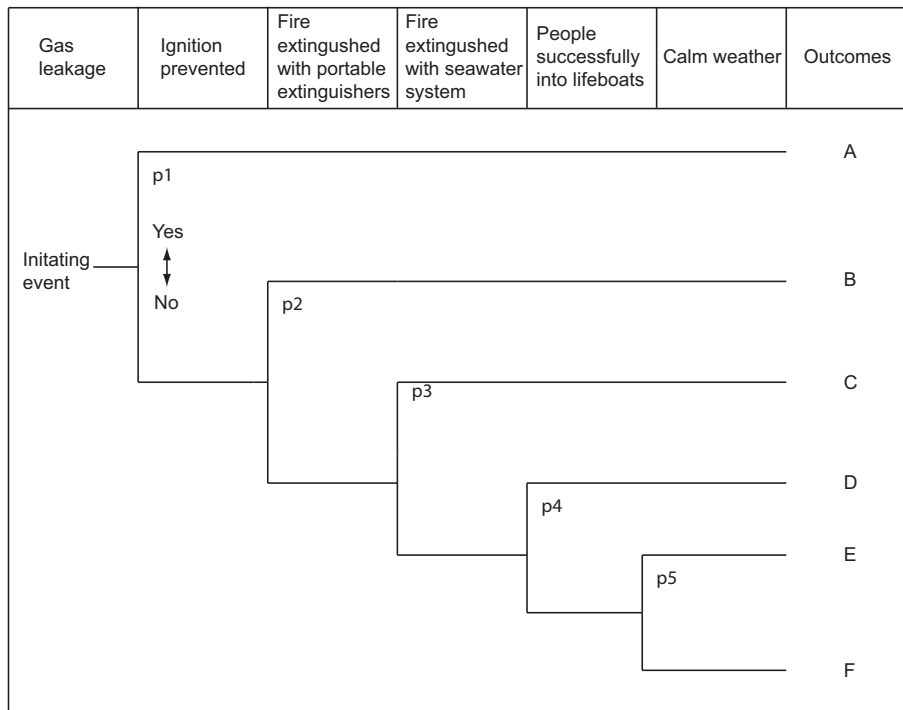


Figure 4.5: Example of event tree (adopted from USCG, 2000b).

analyst (USNRC, 1981).

While some refer to it as a probabilistic model (see, e.g. NUREG, 2009), Siu (1994) makes it clear that a fault tree is deterministic and of static structure. NASA (2002a) emphasizes that a fault tree is a principally a qualitative model that can be both quantitatively and qualitatively evaluated. By assigning probabilities to each basic event, the top-event probability can be mathematically derived from the logic structure of the tree. FTA thus provides significant input to Kaplan and Garrick's (1981) second question of *how likely is it?*

### Event tree analysis

Event tree analysis is a technique for modeling the range of possible outcomes following an initiating event. Figure 4.5 shows that an event tree is structured as a decision tree. The branches represent different plant responses and external influences (USCG, 2000b). These are the systems, equipment, human actions, procedures and processes that can impact the consequences of an initiating event, for instance, terrorist attack or gas rapture. Given the success or failure of such *lines of assurance*, the accident trajectory is either mitigated or continues as a downward line from the branch point until a final consequence is reached (Garrick, 2008). The probability of each consequence is calculated by associating each branch point with a probability of occurrence. It is important to beware that these are *conditional* probabilities, meaning that the probability of success or failure for a line of assurance is conditioned on the success or failure of the preceding. This is both a challenge and

a strength. It urges caution in constructing the logical progression of events, while enabling efficient accounting of timing, dependence and domino effects among various contributors (USCG, 2000b). A particular challenge is to take account of subtle system dependencies, like common components, operators and utility systems, when assigning the branch probabilities. According to USCG (2000b), this is one of two main limitations of event tree analysis. The other is that like FTA, is ETA limited to one initiating event only. The brilliance of it is that this event is what connects the causal analysis of a fault tree with the consequential analysis of an event tree (Svedung and Rasmussen, 2002). This is visualized in the bowtie-diagram of Figure 4.3.

### 4.2.2 Risk evaluation

ISO guide 73 (2009, p. 8) defines risk evaluation as:

**Risk evaluation:** process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

According to this definition, risk evaluation is seemingly a mechanistic process of determining whether a calculated risk falls above or below some predefined level. Radically different is the conception of Shrader-Frechette (1991), who sees risk evaluation as a political process that demands procedural inclusion of democratic and ethical principles. Tantamount to her contribution is the proper balancing of values and scientific “facts” in risk assessment.

Shrader-Frechette (1991) continues pursuing the heritage of Fischhoff et al. (1981). The mighty quintet discards common evaluation methods as ethically and pragmatically insufficient for capturing that risk acceptance is a complex phenomenon of accepting options, not risk. Since the adequacy of risk acceptance criteria (RAC) to this have been thoroughly discussed elsewhere (see, e.g. Johansen, 2010), risk evaluation is only superficially covered in the present study. What should be carried forward from the findings of Johansen (2010) is the need for understanding that risk acceptance criteria are fraught with severe limitations. Especially in problems of great risk, epistemic uncertainty or multiple affected parties, should risk evaluation never be reduced to a process of mechanistic comparison as implied in the definition of ISO guide 73 (2009). An alternative philosophy is discussed under the topic of risk-formed decision making in Section 4.5, which first urges contemplation on the purpose and limitations of risk assessment.

## 4.3 The purpose of risk assessment

The aim of risk assessment is according to HSE (2003b) to identify significant risk to the environment, health and safety of employees and any others who may be affected by an undertaking. But what is the very *purpose* of performing a risk assessment? The only reason for undertaking a risk assessment is, according to Bley et al. (1992), to understand a risk in order to *do something about it*. Such a view, in which risk reduction is considered the main objective of risk assessment, is a typical misconception according to Aven (2010a). Risk reduction is never a goal in itself. This owes to the recognition that creating value necessitates risk taking. The purpose of risk assessment is thus not principally to facilitate risk reduction, but to

provide input to a particular decision in a larger context. The vast majority of references confirm this position, unanimously stating that risk assessment is a tool to inform decision making in management of risk (HSE, 2001; NASA, 2002a; NUREG, 2009; NORSOK Z-013, 2001; IMO, 2002). Typical decision situations are:

- Accept a new project, activity or technology.
- Prioritize between concepts.
- Initiate improvements or relocate risk reducing measures.
- Verify new or existing regulations.

Common to all situations is the decision maker's need for reducing his uncertainty regarding the outcome of a decision. At a deeper level, risk assessment can thus be seen as a tool to address and a language to express our uncertainty about the future (Bley et al., 1992). Accepting this implies that risk assessment shall never purport to justify past decisions (HSE, 2003b), nor shall it be used as an advocacy tool (Paté-Cornell and Murphy, 1996). Rather, it is a *management* tool with the primary function of providing information pertinent to a forthcoming decision (USNRC, 1981).

#### **4.3.1 The intrinsic value of risk assessment**

It is not unreasonable to conclude that the main objective of risk assessment is to inform decision making. However, adopting this view raises the question of whether risk assessment has an intrinsic value beyond that of decision making. Is it reasonable to seek understanding simply for the sake of understanding alone? According to IAEA (1998), risk assessments have traditionally been performed by regulatory agencies to gain generic insights, or by licensees to demonstrate compliance with regulatory requests and for understanding key plant vulnerabilities. Arguably, these cases need not be related to a particular decision. In the case of demonstrating compliance, the purpose of risk assessment may simply be seen as a matter of duty for licensees. And as for the aim of gaining generic insights, one can suggest that knowledge acquisition is a purpose as good as any other. The principal point is that even the purpose of gaining generic insights is tied to one or more decisions. Do we need to gain even more knowledge? And how are we to act upon the acquired insights? Without such stated purposes, risk assessment can hardly provide useful results. Principally, this is because the decision context shall dictate the results of risk assessment rather the other way round (Aven, 2010a).

#### **4.3.2 Decision makers, stakeholders and objectivity**

Recalling the viewpoints of Luhmann (1991), it is extremely rare that risk cannot be traced back to one or more decisions. And if risk assessment, as risk, is always attributable to a decision, it is also attributable to a decision maker. What follows is that risk assessments are principally intended for someone in pursuit of influence. This has severe implications for risk assessment as well as the ontological riddle of risk subjectivity. Is it ultimately the perception of the orderer that matters?

What would complicate such an inference is the diversity of stakeholders involved in great questions about risk. Some are in the position to directly exert influence, while others have little or implicit influence in contributing with data, perspectives or values on selected topics. Yosie and Herbst (1998) report that there is no

agreed upon definition of a stakeholder. This is unfortunate, as it not only complicates the task of identifying relevant stakeholders, but also induces inconsistencies regarding their role and relative influence. Narrowly defining stakeholders as parties who want to be involved in the decision, may exclude affected parties not currently aware of the activity. Conceiving stakeholders simply as affected parties may, on the other hand, exclude parties that could significantly impact the decision. Yosie and Herbst (1998) sketch the following stakeholder categories:

- People who are directly affected by a decision to take action on an any issue or project.
- People who are interested in a project or activity, want to become involved in the process and seek an opportunity to provide input.
- People who are more generally interested in the process and may seek information.
- People who are affected by the outcome of a decision but are unaware of or do not participate in stakeholder processes.

All these are comprised by the definition of ISO 31000 (2009, p.4), which is adopted for this study:

**Stakeholder:** Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

The controversy surrounding the ongoing construction of a storage tank for liquefied natural gas (LNG) at Risavika, Norway, illustrates the difficulty of identifying, prioritizing and involving direct and indirect stakeholders. Vatn (2009) reports significant resistance amongst neighbors of the facility, although the localization is approved by local authorities. Authorization from DSB to store and treat inflammable goods was based on preliminary risk analysis in 2007, while updated risk analysis is required for obtaining final authorization. While it is the responsibility of the local energy supplier Lyse to provide these analyses, the decision of approval rests entirely within DSB. Does this reduce the purpose of risk assessment to matter of duty for Lyse? And may the external locus of decision making encourage bias towards approval? In order to influence the decision, also neighbors, workers and potential investors were interested in the results of risk analyses. What is problematic is that the interests of these stakeholders are ostensibly quite distinct. While the neighbors are likely concerned with major accidents that may harm their children and local environment, investors may share this concern but of different reasons, be it loss of property or declining stock prices. Workers at Lyse, on the other hand, may have principal interest in occupational accidents and emergency preparedness. Depending on whose questions you serve to answer, the focus and execution of risk assessment must necessarily differ. Recapturing the epistemological conviction of Rosa (1998), this implies that risk assessment is never entirely objective, no matter how real the risk under study might be.

What can be concluded from this discussion is that risk assessments are performed for a reason, and that neither the analytical process nor its results should be considered in isolation from that reason.

## 4.4 The limitations of risk assessment

If the purpose of risk assessment is to inform decision making, Bley et al. (1992) make a disturbing observation in that many decision makers are uncomfortable using the results of risk analysis. Apostolakis (2004) reports similar tendencies, noticing that only in the fewest of domains has risk assessment come to earn the confidence of decision makers. What does this reveal about the usefulness of risk assessment? Momentarily leaving the realm of risk, Lindley (2006) finds an unrecognized paradox in that you always expect your uncertainty to decrease with the acquisition of data, albeit the opposite might actually occur if the data contradicts your current information. Does this imply that risk assessment might actually *increase* uncertainty?

### 4.4.1 The flaws of risk assessment according to Beck

The usefulness of risk assessment has been questioned from many stands. Most trenchant is probably the slaughtering of Beck (1992), who dismisses risk analysis as entirely incapable of reacting adequately to contemporary risk. This owes to a failure in the techno-scientific rationalities that is “systematically grounded in the institutional and methodological approach of the sciences to risk”, allegedly serving to *increase* risk in contrary to its purported aim (Beck, 1992, p.51). Although Beck (1992) represents a landmark in the risk discourse, this author finds his accusations far-fetched and poorly substantiated. This is in line with the critique of Campbell and Currie (2006), sentencing Beck’s understanding of risk analysis as badly flawed. Campbell and Currie (2006) secrete the objections of Beck in that (1) risk analysts have vested interests in underestimating risk and are (2) unable to fulfill the impossible scientific standards of proving causal links. Moreover, probability assignments are accused for (3) being irrefutable and (4) displacing the focus from catastrophic potential, which is disastrous since Beck alleges that (5) even low-probability events are inevitable in the long run. As none of these objections stand up to scrutiny, Campbell and Currie (2006) conclude that risk assessment- although not flawless- earns a legitimate role in contemporary society.

### 4.4.2 Historical data, values and expert opinions

In contrast to the poorly articulated attack of Beck, risk assessment has also encountered well-founded critique among theorists and practitioners. HSE (2003b) has devoted a constructive report to counter the pitfalls of risk assessment, in which inappropriate use of historical and statistical data is a recurring theme. Aven (2009) substantiates that the scientific quality of risk analysis by and large depends on how probabilities are derived. Only when a large amount of relevant data is available, do traditional statistical methods meet the criteria of reliability and validity. Also concerned with problems of validity, Shrader-Frechette (1991) takes a different perspective in calling for redefinition of conventional accounts of scientific rationality. The main concern of Shrader-Frechette (1991) is the often neglected inclusion of values in risk assessment. Especially conspicuous is this at the stage of risk evaluation. However, also the process of risk analysis is pervaded by value judgments regarding what method to choose, what events and consequences to consider and so on. The problem relates to the use of expert opinions, which is one of three problems Bley

et al. (1992) find to create discomfort among decision makers. One of the most common criticisms leveled at risk assessment is over reliance on expert opinions in the absence of “objective” evidence. Instead of asking experts of their opinion, the trio replies, one shall ask for their evidence.

A second critique addressed by Bley et al. (1992) is the difficulty of analyzing human reliability. Human reliability analysis (HRA) attempts to predict the impact of human interactions on system reliability in terms of probability of successful performance (NASA, 2002b). Despite the numerous efforts made in this pursuit is HRA still considered an overly complex field.

#### **4.4.3 The inclusion of organizational factors**

The third limitation encountered by Bley et al. (1992) is the inability of traditional risk assessment to model the impact of organizational factors. This is certainly a severe defect, considering that the vast majority of major accidents are attributed to such factors (Reason, 1997). Responding to the challenge, Paté-Cornell and Murphy (1996) have developed a framework titled SAM (system-action-management). SAM structures and describes human and management effects on risk by a set of conditional probabilities. The aim of SAM is to improve risk assessment as a tool for managing and reducing risk.

Inspired by the same objective, Svedung and Rasmussen (2002) present a set of graphical representations to account for the dynamics of organizational decision making in structuring the analysis of socio-technical accidents. Their work builds on the pioneering article of Rasmussen (1997), *Risk modeling in a dynamic society*. Rasmussen models the hierarchical levels of decision making involved in risk management and regulatory rule making as shown in Figure 4.6. An alternative means for relating this model to risk assessment is suggested in Figure 4.7. The vertical levels of Rasmussen (1997) are rotated and merged with a bowtie-diagram. This presentation format depicts the influence of organizational actors in causal modeling, and carries the promise of well-directed recommendations to risk management decisions.

#### **4.4.4 The deeper issue of uncertainty**

What is striking with the limitations addressed by Bley et al. (1992), is that all emanate from the single, deeper issue of uncertainty. The reason why human performance, organizational influences and expert opinions create discomfort among decision makers, is that they are sources of substantial uncertainty. This takes us back to the initial query of whether risk assessment is an adequate tool for dealing with uncertainty in decision making.

Risk in complex systems transcends the realm of ordinary experience. Of this reason, does risk assessment occupy a unique niche that is difficult to disprove (Kates and Kasperson, 1983). Notwithstanding its limitations, the bulk of critics ultimately seem to agree that risk assessment is a powerful tool that provides decision makers with a platform for understanding, communicating and prioritizing actions (Apostolakis, 2004). Ironically, since risk assessment offers a language for addressing uncertainty beyond the perceptual, it may also deliver an increased sense of uncertainty. According to Aven (2003), this hinges on the communication of epistemic uncertainty. Resonance is given to an alternative explanation of Bley et al. (1992), suggesting that all limitations represent problems of communication. The key to

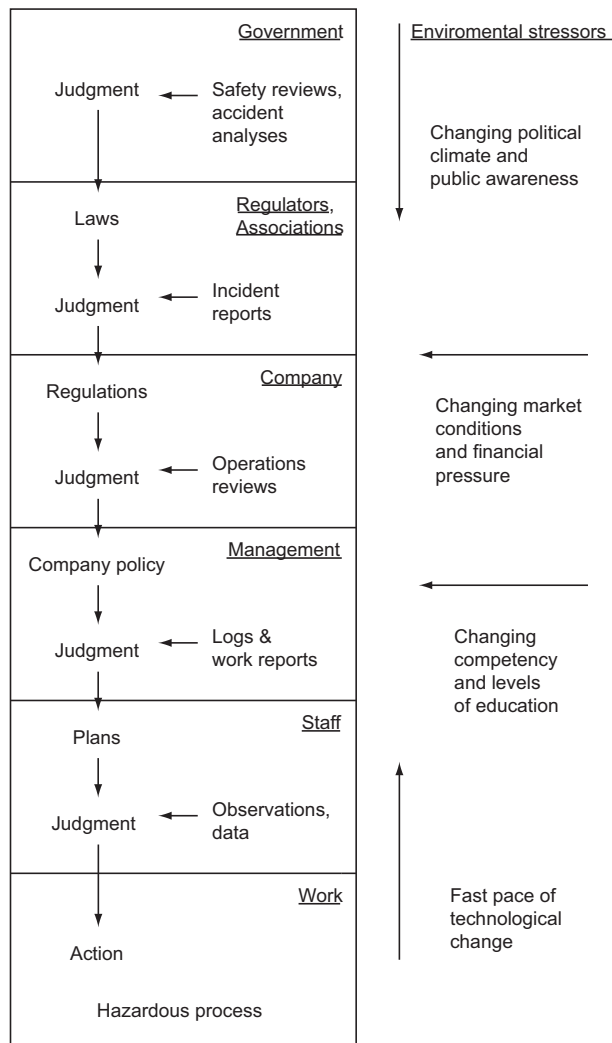


Figure 4.6: The socio-technical system involved in risk management (adopted from Rasmussen, 1997).

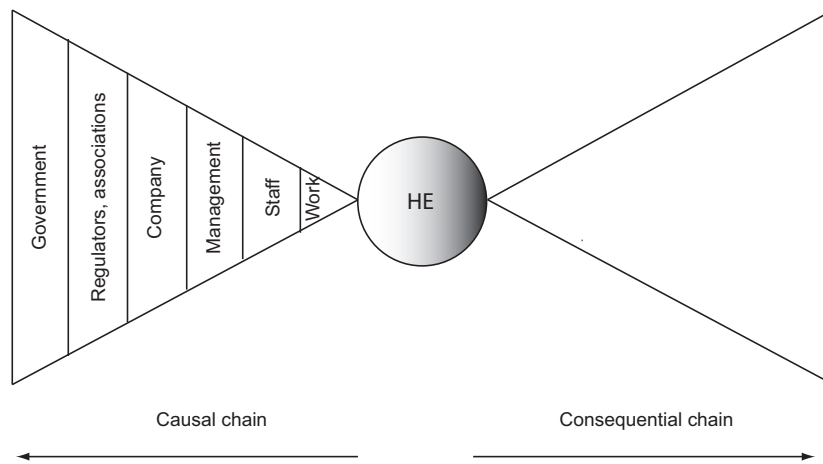


Figure 4.7: Conceptual framework for including organizational actors in risk analysis.

successful management as they see it, is to convey clarity in the expression of uncertainty both internal and external to the analysis team. Grasping the problem as one of communication carries an important implication, namely the criticality of having a clear and consistent language of risk assessment. Otherwise yet another source of uncertainty is introduced, that is, one of *linguistics*.

## 4.5 Using risk assessment in decision making

The plurality of stakeholders and the prevalence of uncertainties represent two major challenges for implementing risk assessment results in decision making (Amenola, 2001). Not only do they call for elaboration on the role of risk assessment in decision making, but also on how this reflects back by way of requirements to risk assessment. USNRC (1998) distinguishes between two philosophies of application:

**Risk-based decision making:** The decision is solely based on the results of risk assessment. USNRC (1998) applies the notion of *risk insights* when referring to the results of risk assessment. This may be dominant accident scenarios, estimations of core damage frequency, expected number of fatalities or importance measures like Fussel-Vesely (see, e.g. Cheok and Sherry, 1998). The option is chosen that have the lowest risk, fulfills some predefined requirement or scores best one an importance measure, without reference to other attributes or constraints.

**Risk-informed decision making:** The decision is based on joint consideration of risk insights and other relevant factors. Technically, USNRC (1998) describes this as an integration of probabilistic and deter-



ministic approaches to safety. The former refers to a pure risk-based philosophy, whereas the latter represents traditional engineering principles of redundancy, diversity and safety margins (Niehaus and Szikszai, 2001). Examples are the *defense in depth-philosophy* and the requirements to *architectural constraints* in IEC 61508 (1998). The latter was introduced to avoid that quantitative assessments alone determine hardware integrity (see, e.g. Lundteigen and Rausand, 2009). Contextually, risk-informed decision making spans beyond the incorporation of different perspectives on safety, to a philosophy of balancing safety with other attributes, for example, costs and economical benefits (Christou et al., 2000).

Albeit the distinction between risk-based and risk-informed decision making is fairly recognized, many authors use the terms interchangeably or in a contradictory sense. A prominent example is USCG (2000a), who lets the notation *Risk-based decision making guidelines* front a series of guiding documents on risk assessment and risk management. This is an obvious misnomer, since USCG (2000a, p.6) in fact stresses that “In risk-based decision making, all of the identifiable factors that affect a decision must be considered”, which is further claimed to be “more than just risk”. Bohnenblust and Slovic (1998) similarly characterize a proposed framework for integrating technical aspects and public concerns as “risk-based decision making”. From this it appears that many who allegedly embrace a risk-based approach are in fact promoters of the contrary. Also those who consciously apply the scheme of USNRC (1998) express an almost unanimous preference for the risk-informed approach. Representative is Apostolakis (2004, p.518), postulating that:

I wish to make one thing very clear: QRA results are never the sole basis for decision making by responsible groups. In other words, safety-related decision making is *risk-informed*, not *risk-based*. (Original emphasis)

Apostolakis reflects a current attitude within regulatory decision making. This has evolved from a traditional deterministic perspective, via a risk-based philosophy to an integrated, risk-informed approach (Niehaus and Szikszai, 2001). What is interesting is that despite the general and spoken preference for risk-informed decision making, many experts and managers tend towards a risk-based approach in practice (Aven, 2010a). Resolving this tension urges understanding of the practical and conceptual implications of both approaches.

#### **4.5.1 Risk-based decision making**

The perhaps greatest advantage of the risk-based approach is its simplicity of use on behalf the decision maker. This is because risk assessment provides direct input to the decision as such, and not simply the process of decision making (Aven, 2010a). Since the numbers are required to speak for themselves, the decision is in principle given before reaching the hands of the decision maker. All the decision maker is required to do, is to choose the risk insight most relevant to the decision and pick the option that best fulfill this measure. Alternatively, the results can be compared with a predefined set of risk acceptance criteria as depicted in Figure 4.8. For a thorough discussion on the merits and disadvantages of this approach, the reader is referred

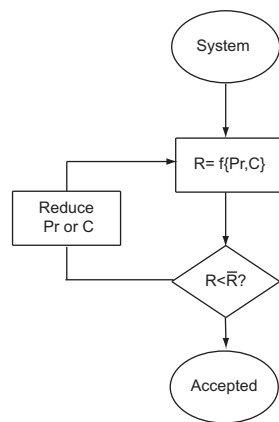


Figure 4.8: Comparing the results of risk assessment,  $R$ , with a predefined set of risk acceptance criteria,  $\bar{R}$  (adapted from Breugel, 1998).

to Johansen (2010). An attractive feature is that consistency is sought across decisions in the establishment of a clearly defined decision rule. Such coherence is according to Lindley (1985) a cardinal quality in any decision context.

### Optimization of neither safety nor development

The reader should note that risk acceptance criteria do not generally foster a risk-based approach in the strict sense of USNRC (1998). A risk acceptance criterion only serves as an upper constraint. Even if one or more options fall below this requirement, NORSOK Z-013 (2001) evokes the ALARP-principle<sup>1</sup> by requiring other factors, like costs and sound engineering principles, to be considered in addition to risk. This ensures effective expenditure on risk reduction measures along with a balanced consideration of options (HSE, 2001).

Mechanical compliance with risk acceptance criteria is indeed a risk-based approach. Such application has been repeatedly criticized by, for example, Ersdal and Aven (2008). Ersdal and Aven reinforce the ideas of Fischhoff et al. (1981), clarifying that there is much more to risk acceptability than risk. This pinpoints the most fundamental deficiency of risk-based decision making. In a world where exploration opportunities and limited resources enable and confine the progress of mankind, risk-based decision making optimizes neither safety nor development. Although it may yield pragmatic and fast solutions (Bohnenblust and Slovic, 1998), they are thus hardly very *good* solutions.

### The numbers are given an authority that cannot be justified

The more emphasis that is put on risk insights, the more stringent become the requirements to the quality, level of detail and scope of risk assessment (Caruso et al., 1999). Quality refers to the adequacy of modeling, while scope reflects the completeness of identified scenarios. What is discomfoting is that along with level of

<sup>1</sup>ALARP is the acronym for *As low as reasonably practicable*. ALARP is the British risk acceptability framework, providing conditional rather than absolute risk acceptance criteria. A suite of guiding documents are offered by HSE, see for instance, HSE (2001) and HSE (2003a).

detail and model complexity also comes increased uncertainty (Niehaus and Szikszai, 2001). A second deficiency of risk-based decision making is therefore the apparent paradox of requiring a more precise analysis while at the same time demanding more confidence in the results. This places great demand on the presentation and communication of uncertainties. In a continuation of her discussion on six levels of uncertainty treatment, Paté-Cornell (2002) worries that differing assumptions and presentations of uncertainty make a major source of inconsistencies in decision making. For two options to be meaningfully compared and ranked, they must be based on the same level of conservativeness. A plausible upper bound-estimate, for instance, cannot readily be compared with an estimation based on mean frequencies. And even if two options are treated on the same level of uncertainty, the problem remains if the results are to be compared against some predefined criteria. Ultimately, this not only diminishes our confidence in the ranking of results, but also the grounds on which risk assessment is granted overriding importance. The numbers are merely given an authority that cannot be justified (Aven, 2010a). In light of the subjectivity and imperfectness of risk assessment that is pinpointed in Section 4.4, this makes a compelling argument for dismissing a pure risk-based approach to decision making.

Admittedly, it must be noted that uncertainty is an issue that riddles both probabilistic and deterministic approaches to safety (Niehaus and Szikszai, 2001). An advantage of risk assessment in comparison with the latter is, in fact, its ability to quantify uncertainty. A summary of the strengths and limitations of deterministic and probabilistic approaches to safety is outlined in Table 4.1. Hence the principal flaw of risk-based decision making lies not in the flaws of risk assessment, but in the failure to compensate these weaknesses by considering more than one side of the same problem.

#### **4.5.2 Risk-informed decision making**

Simply flipping the above discussion reveals the advantages of risk-informed decision making. Principally, the risk-informed approach offers a more compound solution, since more than one factor is under consideration. As for the issue of safety, the integration of probabilistic and deterministic approaches serves to complement and compensate each other's weaknesses. From this a second advantage follows, in that the requirements to precision in risk assessment become somewhat lessened.

In a wider context, the above discussion dictates the benefit of considering not only different perspectives on safety, but also other factors that are relevant to risk acceptability. Hence conceptually and ethically, risk-informed decision making is supreme compared to the risk-based approach. The problem is that this comes with an operational prize.

#### **Separate layers of requirements or optimized decision making?**

One of the key challenges to risk-informed decision making is to reconcile probabilistic and deterministic insights (Niehaus and Szikszai, 2001). Often, these insights contradict each other. And in the absence of a method for reconciliation, the deterministic and probabilistic requirements will end up as separate layers of requirements, rather than a tool for optimized decision making. Caruso et al. (1999) agree to this position, admitting that there is currently no harmonized way for combining such insights, not to say the various accounts of uncertainty (cf. Paté-Cornell,

Table 4.1: Summary of the strengths and limitations of deterministic and probabilistic approaches to safety (Extracted from Niehaus and Szikszai, 2001).

	<b>Deterministic</b>	<b>Probabilistic</b>
<b>Strengths</b>	<ul style="list-style-type: none"> <li>-Principles of defense in depth, redundancy and diversity provide technically sound criteria.</li> <li>-Responsible for outstanding safety record.</li> <li>-Resulting requirements are expressed in pass/fail rules and are straightforward to implement and verify compliance.</li> </ul>	<ul style="list-style-type: none"> <li>-Accident frequencies and consequences are dealt with quantitatively based on realistic assumptions.</li> <li>-Quantitative approach to evaluating impacts of uncertainties on risk estimates.</li> <li>-Facilitates ranking of technical issues and events based on contribution to risk.</li> </ul>
<b>Limitations</b>	<ul style="list-style-type: none"> <li>-Deals with a limited set of uncertainties by use of conservative assumptions and safety margins. Combination of conservative assumptions tends to obscure understanding of realistic behavior</li> <li>-Limited to somewhat arbitrarily defined design basis. Protection for beyond design basis only implicitly provided.</li> <li>-Assurance that decisions create no undue risk to the public is made on a qualitative and subjective basis.</li> </ul>	<ul style="list-style-type: none"> <li>-Results highly dependent on and limited by state of knowledge; subject to change as knowledge evolves.</li> <li>-Uncertainties in risk estimates may be too large to support certain decisions.</li> <li>-Limited to accidents caused by randomly occurring failures; requires assumed validity of the deterministic basis of the plant.</li> </ul>

2002). Any such method would have to consider the nature of the decision problem, the risk insights to be used and the detail and quality of the risk assessment process. The problem multiplies when accounting for other factors beyond safety, as is demonstrated by Christou et al. (2000) in a case study on the integration of safety, local community and economic considerations in land-use planning.

### **Stakeholder involvement in risk-informed decision making**

Bohnenblust and Slovic (1998) provide a list of contentious issues concerning the use of risk assessment in decision making. Uncertainty and the combination of probabilistic and deterministic perspectives are central challenges. They are, however, only of secondary importance to this duo:

The actual point of discrepancy may not necessarily be related to safety. Often it turns out that controversies go back to basic disagreements between the different parties involved. Even the best safety analysis cannot solve such issues. (Bohnenblust and Slovic, 1998, p.151)

The main challenge as these authors see it, is the lacking of a framework for bringing technical information and public perceptions together in a normative sense in decision making. This pivots on the recognition that transition from risk-based to risk-informed decision making not only broadens the number of *factors* under consideration, but also the group of involved *actors*. This is not to deny the importance of stakeholder involvement in risk-based decision making. Their voices should nevertheless be heard in the specification of risk insights prior to risk assessment as

depicted in Figure 4.1. Yet since risk assessment makes the sole basis for decision making, there is neither need nor room for non-technical deliberation beyond this point. When other factors are allowed for consideration, the question becomes not only what risk measures to consider, but what other factors to include and their relative importance. The principal point is that different stakeholders are likely to have diverging opinions on both issues. Stakeholder involvement is thus a given companion in any risk-informed decision making process. This parallel development from risk-based to risk-informed decision making and the increasing focus on stakeholder communication is caricatured by Fischhoff (1995, p.138):

- All we have to do is get the numbers right
- All we have to do is tell them the numbers
- All we have to do is explain what we mean by the numbers
- All we have to do is show them that they have accepted similar risks
- All we have to do is show them that it's a good deal for them
- All we have to do is treat them nice
- All we have to do is make them partners
- All of the above

A *prima facie* challenge to risk-informed decision making is indicated in the latter item. That is, to elicit and integrate stakeholder opinions with scientific information in a just and practical way (Amendola, 2001). Adopting Apostolakis (2004)'s standpoint that risk decisions should never be risk-based, but risk-informed, urges a decision making framework that accentuates this feature.

### 4.5.3 A framework for risk-informed decision making

Figure 4.9 depicts a basic framework for risk-informed decision making. It is adapted from Aven (2003), who at the outset asks what is a *good* decision. Different stakeholders are likely to yield different answers to this question. What is further complicating is that the goodness of a risk-informed decision cannot principally be judged by the outcomes, since one is unable to observe the outcomes of anything but the chosen alternative. What is a good decision must instead be judged by the *process*. According to Aven (2003, p.97), there are two basic principles for reaching a good decision:

1. Establish an optimization model of the decision-making process and choose the alternative that maximizes (minimizes) some specified criteria.
2. See decision-making as a process with formal risk and decision analysis to provide decision support, followed by an informal managerial judgment and review process resulting in a decision.

The former covers, but is not restricted to, risk-based decision making. An optimization model may equally well incorporate other factors than risk. Examples are cost-benefit analysis (see, e.g. Wilson and Crouch, 1982), formal Bayesian decision analysis (see, e.g. Lindley, 1985) and multiattribute utility theory (see, e.g. Keeney

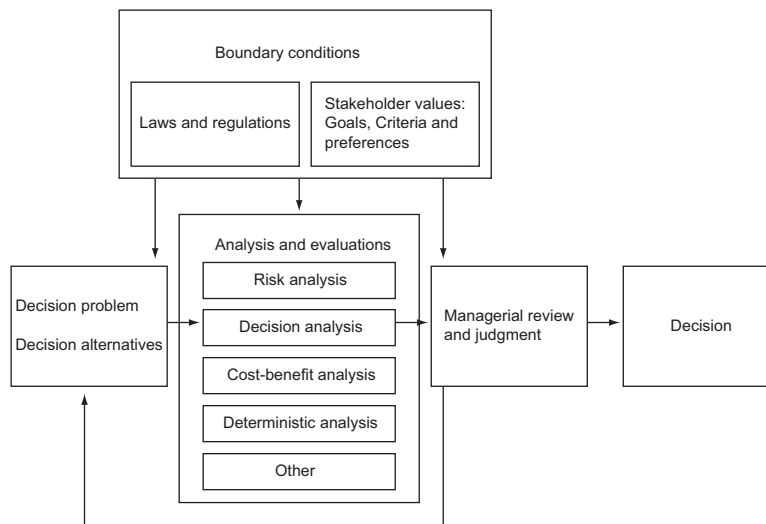


Figure 4.9: Framework for risk-informed decision making (adapted from Aven, 2003).

and Raiffa, 1976). The principal point of Aven (2003) is that although these models are (more or less) useful, they provide *support* to the decision maker rather than input to the decision as such. Only in the rarest of cases will such models provide all the answers that are important to a decision maker. The second of Aven's principles is therefore embraced and conceptualized as in Figure 4.9. The figure splits the process of decision making into four steps:

1. Identification of the decision problem, decision maker(s), options, relevant boundary conditions and stakeholders. This includes clarification of the goals and preferences of interested parties and the measures that best reflects these attributes.
2. Assessment of options by, for example, risk analysis, cost-benefit analysis and so on.
3. Managerial review and judgment of options, by evaluating and relating the results of analysis to the goals, criteria and preferences of interested parties.
4. Selection of options (decision).

The original figure of Aven (2003) is refined to pinpoint that risk analysis is never the sole analytical basis in risk-informed decisions. By splitting the fourth step into different types of analyses, the figure conveys that analysis of risk is accompanied by deterministic evaluations and analyses of costs, socio-economical impacts and so on. Figure 4.10 illustrates that if this is not the case, decision making is simply risk-based.

Even though the second and fourth steps have traditionally received most attention, are the remainder promoted as the key to truly good decisions. Predefining the

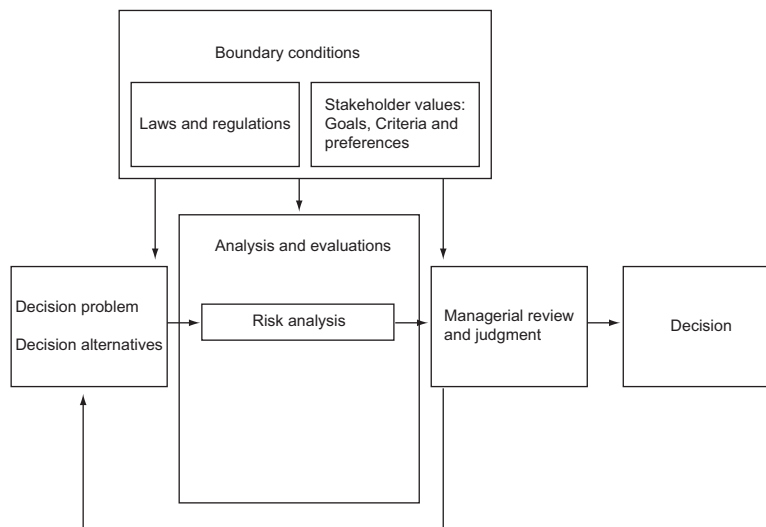


Figure 4.10: Risk analysis is the sole analytical input to risk-based decision making.

decision situation is cardinal for ensuring that analyses provide the required decision support. Managerial review ensures that all relevant factors are considered and that critical limitations, uncertainties and assumptions are addressed. Pervasive to both stages are the boundary conditions depicted in the upper box, reflecting the values and interests of relevant stakeholders. These may be formulated as organizational goals, criteria, standards, preferences or political and ideological views. The original figure of Aven (2003) is adapted to emphasize the variety of boundary constraints, ranging from laws and regulations to corporate and public opinions. Further refinement can possibly be achieved by indicating that there is a hierarchy of power among stakeholders. As an example, the air traffic control company Avinor has more influential power than commercial airlines in deciding whether to allow for air traffic in the presence of volcano ash clouds.

Figure 4.9 depicts that analysis is framed by deliberation and that deliberation is informed by analysis. This interactive approach is commonly referred to as *analytic-deliberative procedure* (Amendola, 2001). A fundamental recognition is that value judgments makes an inherent feature of decision making as well as expert approaches to risk assessment. Conceptually, the framework of Aven (2003) can be seen as an increased resolution of the framework of ISO 31000 (2009). Stakeholder communication is emphasized in both frameworks, as is also the importance of managerial review. A difference is that while ISO 31000 (2009) characterize the outcome in terms of risk treatment, does Aven (2003) describe it simply as a decision. This reflects the premise that risk-informed decision making is not necessarily about reducing risk, but a balancing act of values, risk factors and other attributes. Unfortunately but not accidentally, the framework restrains from prescribing the relative importance of these factors and the procedural inclusion of stakeholder opinions.

### Science against the people?

Two major challenges follow the inclusion of stakeholders in risk-informed decision making as this author sees it. The first is practical and concerns the means for iden-

		<i>Risk tradeoff analysis and deliberation necessary</i>
	<i>Risk balancing necessary</i>	Risk balancing necessary
<i>Scientific risk assessment necessary</i>	Scientific risk assessment necessary	Scientific risk assessment necessary
<b>Type of conflict:</b> cognitive	<b>Type of conflict:</b> cognitive, evaluative	<b>Type of conflict:</b> cognitive, evaluative, normative
<b>Actors:</b> agency staff, external experts	<b>Actors:</b> agency staff, external experts, stakeholders (industry, directly affected groups)	<b>Actors:</b> agency staff, external experts, stakeholders (industry, directly affected groups, representatives of the public)
<b>Discourse:</b> cognitive	<b>Discourse:</b> reflective	<b>Discourse:</b> participatory
Complex	Uncertain	Ambiguous

Figure 4.11: Strategies and actors in the risk management escalator of Klinke and Renn (2002).

tifying relevant stakeholders, eliciting their opinions and collocating this into useful information. It is beyond the scope of this study to explore the various approaches of participatory decision making. The reader is referred to Breakwell (2007) for a comprehensive overview. Common to all is that they are fraught with pragmatic and ethical constraints, as is concluded by Yosie and Herbst (1998) in a review on the use of stakeholder processes in environmental decision making. Many stakeholder processes are sentenced as badly managed, unfit to the relevant problem, excluding to relevant parties and for making ineffective use of scientific knowledge. The latter reflects the common apprehension that stakeholder-based and science-based decision making represent competing approaches. This is according to Yosie and Herbst (1998) a critical misconception, since there are no inherent reasons why the two processes cannot be mutually supportive as suggested in the framework of Aven (2003). Dictated is a second major challenge, which is the normative question of the how to balance stakeholder values and scientific evidence. In the scientific proceduralism of Shrader-Frechette (1991), this riddle is traced back to fundamental ontological and epistemological considerations. Risk assessment is considered an invaluable tool for making decisions about risk. It does, however, presuppose that one overcomes the naive positivist account to rationality, in which risk assessment is considered the perfect and only provider of truth. Calibration, peer reviews and ethical weights through deliberation are methodological suggestions for a more procedural account of rationality.

### The risk management escalator of Klinke and Renn

The seminal paper of Klinke and Renn (2002) extends and complements the contributions of Shrader-Frechette (1991). In response to five controversial themes regarding the legitimate role of risk assessment for regulatory decision making, Klinke



and Renn (2002) draw up a tripartite classification scheme for the optimal integration of analytic and deliberative processes. Essentially, this is determined by the prominence of three major challenges to risk management; complexity, uncertainty and ambiguity.

Problems characterized by complexity are prescribed a *risk-based* approach, in which risk assessment and cognitive deliberation among experts make the prime input to decisions. If epistemic uncertainty is the dominant characteristic, a *precaution-based* strategy is advised for resilience and reflexive discourse on the trade offs between competing extremes of over- and under-protection. Problems of high ambiguity necessitate a *discourse-based* approach, in which value-trade offs and stakeholder participation is the ruling principle.

The different strategies and associated actors are summarized in Figure 4.11. It should be stressed that the strategies are not mutually exclusive. In reality, making the right decisions is a matter of balancing the perspectives according to the dominant characteristic of the problem at hand. This promotes the general conclusion that risk-informed decision making must be tailored not only to the specific risk, but also the wider context in which decisions are taken. Not all decisions requires extensive stakeholder participation, in the same matter as risk assessment is granted less influence in situations of great uncertainty or conflicting values. This does not, however, mean that the scientific requirements to risk assessment decrease along the axis of deliberation. Rather, it places increased demands on the relevancy and communicability of results, in order to ensure that decision making is informed by the best available technical and scientific knowledge (Apostolakis, 2004).

#### **4.5.4 Implications on risk assessment**

Adopting the framework for risk-informed decision making in Figure 4.9 carries considerable implications on the process and use of risk assessment.

##### **Relevancy**

Firstly, any meaningful application of risk assessment in decision making presupposes that it produces relevant information. An inference that follows is the need for risk analysis to provide a much broader risk picture than is typically done today (Aven, 2010a). Figure 4.9 addresses this explicitly in the importance of clarifying stakeholder interests prior to risk assessment. Albeit obvious, neglecting this point represents a common contributor to poor utilization of risk insights in practice (Amendola, 2001). If the various stakeholders are not involved at this early point, it seems unrealistic to expect them to approve the outcome of risk analysis at stage 3.

##### **Communicability**

The production of relevant results makes a fundamental requirement to risk assessment. No guarantee is, however, provided that the results are *conceived* as relevant by the decision maker and interested parties. Regardless of the analyst's intentions, the results are of limited use if the receivers fail to relate the results to the problem at hand. Ultimately, this is an issue of communication. Required is not only a feasible presentation format, but also a clear and consistent use of words. In a case study on communication of risk assessment information to risk managers, Thompson and Bloom (2000), report that decision makers prefer simple charts and graphs that are

not overly busy or detailed. The information must be structured in such a way that central risk contributors and the impact of risk reduction measures are readily reflected. At the same time, the results should be extensive and detailed enough to convey multiple measures or attributes of risk. Reconciling this represents a fundamental challenge. Either, the decision maker receives an aggregate result in which value trade offs or risk contributors are hidden, or, he is overloaded with ambiguous information in demand for interpretation. A rule of thumb is that the results should be “as simple as possible and as complex as needed” (Leeuwen and Vermeire, 2007, p.24).

## **Confidence**

Communication of risk assessment is not simply about communication of results. Equally important is it to ensure that stakeholders have *confidence* in the results. On the practical side, this requires coherent presentation of key uncertainties (cf. Paté-Cornell, 2002) and honest communication of underlying assumptions and the amount of review the assessment has been through (Thompson and Bloom, 2000). From an epistemological viewpoint, it motivates continuous scientific improvement of risk assessment methodologies and more sophisticated means for understanding and representing uncertainties (Shrader-Frechette, 1991). Stakeholders must, however, also take their share of responsibility by improving their understanding of the fundamentals of risk assessment (Aven, 2010a). This reflects back on the risk assessment community through demands for harmonization of methodology, terminology and results.

### **4.5.5 A call for harmonization**

Decision makers are confronted with a variety of methodologies for assessing and presenting risk. Inconsistency in assessments performed by different analysts or for various end users is a significant barrier to the use of risk assessment in decision making (Niehaus and Szikszai, 2001; Kirchsteiger and Cojazzi, 2000). Amendola (2001) explains this in terms of *operational uncertainty*. Operational uncertainty reflects uncertainty introduced not from lack of knowledge, but from inconsistent use of it. Differences in operational background, choice and use of physical or logic models and misconception of fundamental concepts, are all factors which take risk assessment farther from the ideal of objectivity. This complicates communication across different parties in the risk assessment community and ultimately, the possibility of decision makers to get at proper understanding of the process and results of risk assessment. An attractive fix is technical harmonization of risk assessment and risk-informed decision making. The issue is promoted for future research by Niehaus and Szikszai (2001) and Amendola (2001), but is it feasible and realistic?

## **Necessary pragmatism**

The need for an internationally accepted, generic standard for risk-informed decision making motivated a workshop held by the European Commission in 2000. In the summary paper of Kirchsteiger and Cojazzi (2000), it is pinpointed that most existing standards are industry-specific and adopt different definitions, models and approaches to risk assessment. No existing standard was at that time found to satis-

factorily bridge these nonconformities. Notwithstanding the recent efforts of ISO 31000 (2009), this still seems to be the case ten years later.

Promoting risk assessment along harmonized procedures offers an attractive solution. Not only would it promote consistency and understanding across different domains and applications, it would also encourage a more transparent decision process in which all stakeholders can be involved. Despite these advantages, Kirchsteiger and Cojazzi (2000) conclude in disfavor of a harmonized, prescriptive approach to risk assessment and decision making. Somewhat paradoxically, this is precisely because the requirement of stakeholder involvement calls for pragmatic application of methodologies and measures to produce relevant results. Substantiation of this claim is provided by Amendola (2001), stressing that any attempts at procedural harmonization must take into account the decisional framework in which risk assessment is performed. As this ultimately depends on the time, activity, cultural and regulatory context, neither risk assessment nor consultation processes can be readily transposed across socio-economical contexts.

### **A minimum promise of coherence**

Although a universal, prescriptive standard is discarded as neither desirable nor realistic, Kirchsteiger and Cojazzi (2000) still see the necessity for linking the work of different international standardization organizations (e.g., CEN, ISO and IEC) on a generic, technical level. Such an effort would focus on generic aspects of risk-informed decision making (e.g. principles for setting risk acceptance criteria), while refraining from specifying low level, technical aspects (specific methodologies or decision criteria). Most fundamentally, Kirchsteiger and Cojazzi (2000) call for harmonization of central terms and concepts.

A consequence of the iterative link between process and results in Figure 4.9, is that different stakeholders may dictate conflicting indicators of risk. Notwithstanding that integrating these is challenging, this author believes that such diversity represents a true barrier to risk-informed decision making only when analysts, decision makers and stakeholders talk at cross purposes. Albeit perplexity cannot be removed by standardization of results or methodology, a conscious and clear use of terminology holds a minimum promise of coherence in risk-informed decision making.

## Chapter 5

# What can go wrong?

### 5.1 Introduction

Foundational to the risk definition of Kaplan and Garrick (1981) is the question *what can go wrong?* Since queried is virtually everything and anything, a set of terminological knobs is essential for piloting our analysis of risk. Kaplan and Garrick prescribe the word *accident scenario* for this purpose. Unfortunately, they refrain from defining it in anything but a circular manner; an accident scenario is simply the answer to the question of what might go wrong. It is in the opinion of this author that the latter inquiry necessitates a fundamental set of terms beyond the notion of accident scenario. Considering the widespread understanding that hazard- and scenario identification makes the most informative yet challenging part of risk assessment (Haimes, 2009), terminological consistency is especially critical at this step.

This chapter seeks to tidy up the toolbox of concepts for answering the first definitional question of risk. Focus is on the left and midst part of the bowtie-diagram, while the overarching concept of accident scenario is deferred to Chapter 6. The basic concepts of hazard and threat make a natural start of inquiry. As a foundation for entering the jungle of terms relating a hazard to events of cause and realization, a philosophical briefing on the concepts of event and causation follows thereafter. The midst of the bowtie-diagram is then clarified by stating a preference for *hazardous event*. In order to describe how hazardous events come about, *triggering event* is subsequently discussed in light of the ideas of Reason (1990b) and Wageenaar et al. (1990). An alternative perspective is presented in the concept of *safety issues* as fronted by ARMS (2009), which is finally contrasted and set in context with our remaining terminological knobs.

### 5.2 Hazard

Fundamental to risk is the comparatively plain concept of *hazard*. A closer examination confirms this assertion, while at the same time revealing that hazard by no means is exempted from difficult issues of demarcation and ontology.

### 5.2.1 A hazard is a source of potential harm

*Hazard* is in everyday parlance interchangeably used with its synonyms of *danger* and *peril* (Garland, 2003). In the language of risk scholars, hazard is by and large the preferred designation for something with possibility to cause harm (HSE, 2001). Unlike most other terms in the comparative analysis of Christensen et al. (2003, p.187), only nuances seem to separate the definitions under study. Their compound definition is as following:

**Hazard:** the inherent property/properties of a risk source potentially causing consequences/effects.

Common to all definitions is the potential or possibility of adverse effects. Slight disagreement appears on whether to distinguish *risk source* from *hazard*. The former is defined as (Christensen et al., 2003, p.185) :

**Risk source:** Activity, condition, energy or agent potentially causing unwanted consequences/effects.

From the two definitions, it appears that hazard is a more restricted term that constitute a part of the wider concept of risk source. Consulting ISO 31000 (2009), the opposite is apparent, as it is specified that a hazard can, but need not be a risk source. Since this author considers it unnecessarily confusing to separate the two notions, hazard is chosen as a collective term that simply describes, as is defined by ISO 14121 (2007, p.2):

**Hazard:** source of potential harm.

### 5.2.2 Situations as hazards

The ISO 14121 (2007)-definition is extended in IEC 60300-3-9 (1995, p.11), with the amendment “(.) or a situation with potential for harm”. Recall the Hillsborough tragedy in 1989, where 96 football fans were crushed to death (LFC, 2002). This was a situation of overcrowding that definitely brought potential of harm, hence clearly falling under the hazard definition of IEC 60300-3-9 (1995). Would it not be considered a hazard according to ISO 14121 (2007)? The answer is seemingly both yes and no. ISO 14121 (2007) differentiates between *hazard* and *hazardous situation*. The latter is described as a circumstance of exposure to hazard. In this manner, overcrowding may simply be seen be a situation of exposure to some other “true hazard”, for example, a poorly load bearing terrace.

A crowd of people can also be a source of harm in its own means. This was tragically demonstrated when nine festival participants died of suffocation during a Pearl Jam-concert at Roskilde in 2000 (BBC, 2000). Another borderline case is that of ergonomics, which leads you to think of a situation in which a dazed operator is doomed to loose control over a poorly designed device. Although ergonomics may not inflict harm in itself, it is even so an intrinsic property that has earned inclusion on ISO 14121 (2007)'s list on machinery hazards. From that it can be suggested that situations enter into the hazard definition when constituting a harmful potential in its own right. Since this basically means being a source of harm, it follows that the amendment of IEC 60300-3-9 (1995) is somewhat superfluous.



Figure 5.1: The framework for organizational accidents of Reason (1997).

### 5.2.3 Hazards as causes

In comparison with the proposition of Christensen et al. (2003), the definition of ISO 14121 (2007) gains in clarity by omitting the notation of *cause*. Although hazards certainly cause harm, this author believes that definition by explicit reference to cause may imply a simplistic causal relationship between hazard and effect. In reality, this link is shaped by how people and systems interact with the hazard. This is aptly captured in the conceptual framework of Reason (1997) in Figure 5.1. The figure also implies the existence of a set of underlying causes beyond the level of hazard, which are collectively termed *organizational factors*. Although crucial to the prevention of major accidents, considering remote causes as representing some “true hazard” is pragmatically unfeasible if the aim of analysis is to identify possible hazardous events (HSE, 2001). Precisely of this reason are hazard identification and causal analysis considered separate parts of risk assessment in the risk assessment framework of NORSOK Z-013 (2001) in Figure 4.2. Implied is the benefit of excluding cause from our definition of hazard, but so is also the blurry connection between the two modes of analysis. Are technical failures and human errors causes or hazards? Are we in need of a richer terminology to bridge the identification of hazards to their related causes and effects? These questions will, along with the framework of Reason (1997), reappear in section 5.6. For now, let us settle by accepting the purpose of *hazard* as to enable us to identify what can go wrong.

Table 5.1: Checklist of type, origin and potential consequences of hazards (extracted from ISO 14121, 2007).

<i>Type</i>	<i>Example of origin</i>	<i>Example of potential consequences</i>
Mechanical hazards	Acceleration, deceleration Falling objects Rotating elements	Crushing Shearing Stabbing or puncture
Electrical hazards	Arc Short-circuit Thermal radiation	Electrocution Burn Shock
Thermal hazards	Explosion Flame	Burn Dehydration
Noise hazards	Cavitation phenomena Scraping surfaces Whistling pneumatics	Permanent hearing loss Tinnitus Tiredness
Vibration hazards	Vibrating equipment Worn parts	Neurological disorder Vascular disorder
Radiation hazards	Ionizing radiation source Low frequency electromagnetic radiation	Damage to eyes and skin Effects on reproductive capability
Material/substance hazards	Aerosol  Fibre Oxidizer	Cancer  Infection Poisoning
Ergonomic hazards	Access	Fatigue

#### 5.2.4 Origin, characteristics and categories of hazards

Checklists are one of many approaches for identifying hazards. A checklist is a pre-defined list of possible hazards likely to prevail in a given domain, for instance, the process industry or offshore installations (HSL, 2000). Table 5.1 exemplifies a checklist of typical machinery hazards. Even though the original list is considerably larger, ISO 14121 (2007) stresses that its inherent lack of exhaustiveness urges analytical vigilance. While noticing that any assessment will only be as comprehensive as the list used, this is a disadvantage that holds for all checklists (HSL, 2000).

ISO 14121 (2007) divides hazards into eight categories as shown in Table 5.1. The hazards are further qualified according to their origin and nature of harm. Origin can, in a wider perspective, be seen as a dichotomy between natural and man-made hazards (Reason, 1997). Common natural hazards are lightning, earthquakes and avalanches. Man-made hazards are sometimes called technological hazards. Kates and Slovic (1983) apply the latter as a collective term for hazards originating from human needs and wants. In their early comparison of technological hazards, Kates and his partner identify 93 predominating hazards in contemporary life. These carry the potential for release of either *energy* or *material*. Within the former category are fireworks, handguns and dams, while the latter is exemplified by alcohol, asbestos and fossil fuels. Four differing characteristics are observed:

- Energy hazards persist for much shorter periods than those of materials.
- Energy hazards have immediate consequences, while the consequences of material hazards are typically delayed.
- Material hazards have transgenerational effects, in contrast to those of energy.
- Material hazards may significantly affect nonhuman mortality, while energy hazards do not.

Another and somewhat detached characteristic is that of intentionality (Kates and Slovic, 1983). Also Reason (1997) is concerned with this descriptor, noticing that although hazard usually means some inanimate danger, the hazard to be guarded against is in many situations other people. This is depicted in Figure 5.2, where the dichotomy between technological and natural hazards is broadened to include those originating from human will and powers. Mirrored with the dimension of harm *to what*, the grid draws attention to the multi-faceted nature of hazards. Albeit not erroneous, it is in the opinion of this author that the right quadrants in Figure 5.2 hold a matter too complex for the sole notion of hazard. Rather, the term *threat* applies, which is examined in the forthcoming section.

An interesting digression can be made in the notion of *moral hazard*. This is related to release of neither material nor energy, but of information (see, e.g. Homström, 1982). Moral hazard is, admittedly, of little relevance to studies of bodily risk. Yet it serves to remind us that just as risk, is hazard a capacious term which is connoted with hazardous systems, substances and technologies as well as people or situations. Demarcating hazard from risk is an important means for narrowing down both concepts.

#### 5.2.5 Hazard $\neq$ risk

Hazard is not the same as risk, although the notions are mixed both in dictionaries and everyday parlance. It is not uncommon that newspapers reveal that imported



Origin Victim	Technology	Nature	Humanity
Technology	×	×	×
Nature	×	×	×
Humanity	×	×	×

Figure 5.2: The multi-faceted nature of hazards.

toys, psychologically unstable people or unhealthy food are risks, although they in fact are hazards. According to Christensen et al. (2003), this is a common source of misunderstanding and poor communication. The principal difference is that hazard does not include the probability of adverse outcomes, as it exists simply as a source (Kaplan and Garrick, 1981, p.12). Risk, on the other hand, entails the probability of that source being converted into loss. This implies that the moment a hazard is realized, it is no longer a hazard but an event. Figure 5.3 illustrates this point by demarcating the situation of living under an escarpment after a winter of heavy precipitation from that of experiencing an actual avalanche. We may speak of risk in both situations, but of drastically different proportions. This leads us to a second distinction, which is illustrated by further refining the sketch in Figure 5.4. Although little can be done to reduce the potential energy of mammoth masses of snow, the risk of fatalities may be reduced by safeguarding the mountain hill as well as taking precautions like closing the road and the primary school nearby. While we may neither eliminate nor alter the particular hazard, we can still reduce the risk. Kaplan and Garrick (1981) express this symbolically in the form:

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}} \quad (5.1)$$

Albeit differently presented, this simple idea makes the foundation of Reason's (1997) perspective on organizational accidents. By illustrating the relationship between hazards, defenses and losses as in Figure 5.3, organizational accidents can be understood as the breaching of safeguards that separate hazards from vulnerable people or assets. Interesting is in this regard the taxonomy of Schupp et al. (2004), distinguishing between *primary hazards* of direct harmful potential and *functional hazards* that indirectly cause harm by adversely affecting safety barriers.

Resonance is given to the bowtie-representation of Figure 4.3, which aptly captures that risk is a concept of both hazard and vulnerability. Although a hazard has potential for causing great harm, the risk may be insignificant if either its probability of realization is negligible (or reducible by safeguards), or the system has multiple reactive safeguards in place. When hazards are communicated as risk, this asymmetrical relationship is likely disregarded and by that the (perceived) risk exaggerated.

Conceiving hazard as something existing only as a source is conceptually challenging. Does it rule out any meaningful comparison of the "hazardousness" of different hazards? After all, is it not the severity and nature of hazard realization that would allow such a ranking? Although Kates and Slovic (1983)'s grading of hazards

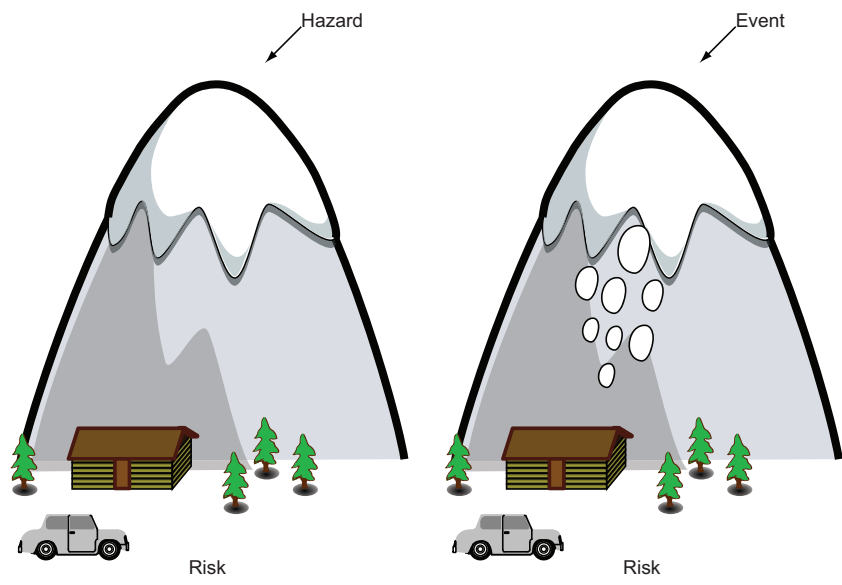


Figure 5.3: Hazard is existing only as a source.



Figure 5.4: Safeguarding against hazards.

is founded on a somewhat muddled distinction between hazard and risk, they make a principal point in that it is the probability of realization that is disregarded and not the realization itself. Although we may no longer consider a released hazard a hazard, it is still the consequences of this event we imagine when we identify and evaluate hazards. What does this imply for the ontology of hazards?

### 5.2.6 The realism of hazards

According to Garland (2003, p.51), dangers (which is his pronounced synonym for hazard) become dangers only when they relate to us in ways of carrying adverse effects:

Dangers are dangers for someone- for specific individuals or groups or species, under certain conditions- nothing is dangerous as such, not even floods and lightning. On the other hand, anything and everything has the potential to become a danger to something or someone.

It is admittedly true that just as risk, must hazard be identified as such in order to serve its designation. Yet this is the case also for potatoes, an extreme relativist might claim. And just as potatoes show certain characteristics, do many hazards have intrinsic properties or dispositions almost objectively recognizable as sources of harm (HSE, 2001). Hazards related to potential energy, for instance, carry the promise of pan cultural recognition (Rosa, 1998). Also the kinetic energy of a discharged bullet may be assumed similar recognition. While it is true that many hazards, like nanotechnology, carry dubious potential, it is in the opinion of this author that hazard is more easily claimed ontological realism than risk. The most pleading argument to this claim is that hazards are properties of the present, and may thus be observable (albeit many are not). Risk, on the other hand, is a property of the future and is hence inherently unobservable. It is no wonder then, that hazard identification makes up the most cardinal and tangible part of risk assessment.

## 5.3 Threat

In an annotation to the hazard definition of DHS (2008b), it is clarified that *hazard* differs from a *threat* in that hazards are not directed. A threat, on the other hand, relates to an entity, asset, system, network or geographic area. Myagmar et al. (2005) confirm this assumption when asserting that a threat cannot exist without a target. Threat is by DHS (2008b, p.33) defined as:

**Threat:** natural or man-made occurrence, individual or entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.

Apart from the specification of likely targets, the definition differs only marginally from that of hazard. The issue of potentiality is still in focus, as is also that of harm. Is threat simply a target-specific extension of the concept of hazard? It is not clear whether DHS (2008b), who is exclusively concerned with problems of security, subscribes to this position. If confronting those involved in assessment of both safety and security risk, it is most likely an insufficient specification. Credible representatives of this group are Garrick et al. (2004), who clarify that hazard and threat are primarily distinguished by intentionality. Their definition is adapted for this study (Garrick et al., 2004, p.136):

**Threat:** An expression of intention to inflict evil, injury or damage.

Before further examining this conception, the subject gains in comprehensibility by first exemplifying types and agents of threat.

### 5.3.1 Agents, types and strategies of threat

A *threat agent* is an individual or group that can manifest a threat. Vidalis (2004) suggests the following classification of threat agents:

- Hostile nations
- Terrorism and terrorist groups
- Corporations seeking competitive advantages
- Organized crime and criminals
- Empowered small agents motivated for ideological, political or religious reasons

Threat agents are also known as *threat sources* or *adversaries*. A threat agent in combination with a particular *threat type* form a *specific threat* (Baybutt, 2002). Baybutt, who is concerned with threats to process plants, exemplifies threat types in terms of on-site and off-site release of hazardous materials, interference with production and plant shut-down. Broadening the perspective, DHS (2008b) speaks of nuclear, biological, toxic or cyber attacks as *tactics* of threat. All these are relevant means to the strategy of terrorism. This can be seen as an element of yet a higher level threat typology. Terrorism enters into *The Issues Threat List* of the American FBI, as one of eight categories of *threat strategies* (represented in Roper et al., 2006):

- Terrorism
- Espionage of national defense information
- Proliferation of weapons of mass destruction
- Proliferation of advanced conventional weapons
- Economic espionage of sensitive financial, trade or policy information
- Targeting the national information infrastructure
- Targeting the government
- Perception management by manipulating or propagating deceptive information
- Other foreign intelligence activities

### 5.3.2 Motivation, capability, opportunity and impact

The threat-definition of Garrick et al. (2004) invites a range of concerns beyond those of hazard. Of interest is not only what inherent properties have the potential to cause harm, but also by whom, how, why and to whom or what harm is inflicted. These elements are all captured in the functional definition of Vidalis (2004):

$$\text{Threat} = \text{Function (Motivation, Capability, Opportunity, Impact)} \quad (5.2)$$

*Motivation* refers to the motivational drivers of a threat agent. These may be political, secular and religious, relate to personal gain, power and revenge or simply intellectual challenge. Synonymous is the term *intent*, meaning the desire to conduct an attack (DHS, 2008b, p.19):

**Intent:** Determination to achieve an objective

Intent (or motivation) is one of two elements commonly considered when estimating the likelihood of terrorist attacks. The other is *capability*, defined by DHS (2008b, p.16) as:

**Capability:** Means to accomplish a mission, function or objective

Capability expresses the degree to which an adversary is able to implement a threat (Vidalis, 2004). Included is the availability of tools and techniques to implement an attack, as well as the ability to use these correctly. To constitute a threat, an agent must thus be both motivated and capable. Baybutt (2002, p.271) reminds us of the saying “where there is a will, there is a way” and calls for conservative assumptions on capabilities. Having said that, neither capability nor motivation is sufficient should the conditions be unfavorable. For a threat agent to bring its capability to bear against a target, he must also have occasional *opportunity* to do so and the target must be vulnerable to attack. If motivation, capability and opportunity are present, the threat will reach the target and an *impact* will follow, potentially ranging from minor to catastrophic loss and disruption.

### 5.3.3 Hazard and threat- revisited

Let us concludingly return the distinction between threat and hazard. The above characteristics attest that threat is a broader concept than hazard. This is not only because it is composed by more attributes, but also because hazard itself must enter into the concept of threat. Admittedly, the list of FBI shows that not all threats directs at physical damage. Information security is a relatively well-matured field, in which traditional attributes are the availability, confidentiality and integrity of information (Myagmar et al., 2005). Creatively scanning the horizons up to 2017, HSE (2008) depicts that cyber-threats will vastly surpass bodily security issues in the future. Since the society has come to rely on increasingly dependent information systems, attacks on cyber networks can cause unimaginable consequences also to life and property (CIST, 1999). Yet in the case of direct bodily threat, one or more hazards must necessarily make a constituent part of the tactics and capability of a threat agent. The opposite does not hold, as something can be a hazard but not a threat given the absence of a target. What disturbingly follows is that all hazards have the potential of forming a threat. Not until recently has this been widely recognized by operators in hazardous industries. It calls for risk assessment not only of accidental releases,

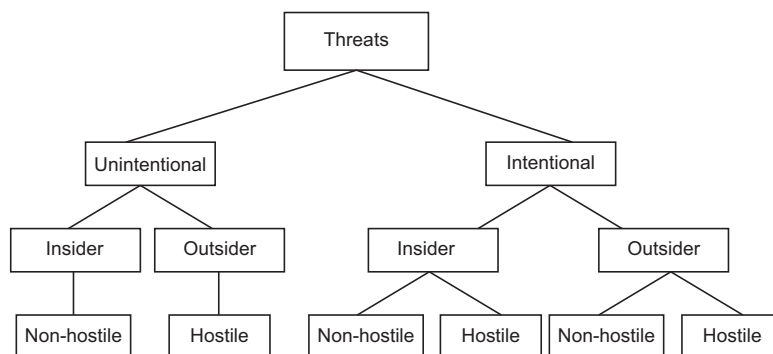


Figure 5.5: The motivational threat classification of Vidalis (2004) suggests that cyber threats may be unintentional. For most other purposes, *threat* is reserved for intentional harm.

but also of hazardous materials being exploited in malevolent acts of terrorism and crime (Baybutt, 2002).

Presupposed in the above discussion is that hazard and threat is distinguished by intentionality. In honest review, this is not a general convention. When searching for *threat* in any scientific database, a fair share of hits pertains to environmental harm that, albeit ostensibly man-made, cannot be assigned any motivational intention. As an example, both natural phenomena and developmental actions are by Salafsky et al. (2008) regarded as direct threats to biodiversity. Also in the field of information security are unintentional threats included, as is sketched in the motivational threat classification of Vidalis (2004) in Figure 5.5. Since inattentive users make a central contributor to breaches of data integrity, this does not appear unreasonable. Yet in the case of bodily harm, it seems feasible to let *threat* designate intentional origin alone. This is because analysis of security risk requires a term that uniquely captures the distinctive interconnectedness between motivation, capability and target. In conventional analysis of accidental risk, “threat” adds nothing but bewildering information. An example is Haimes (2009), who inconsistently applies the term in reference to hazard, initiating event and influencing conditions. In order to avoid such confusion, this section concludes with an appeal for reserving the concept of threat to the anatomy of security. Needed is rather a terminology for relating hazards to events of realization and causation. Before exploring this undulating ground, some words about events and causation offer an interesting basis for reflection.

## 5.4 On the concepts of event and causation

Hair dying, airplane crashes, birthdays and war have one thing in common in that they all may be thought of as events. But what is an event? In the science of classical statistics, event is simply conceived as a set of states (Savage, 1972). By example, we may estimate the probability that 1 egg in a dozen is rotten, which is an event consisting of 12 states. An event may hence be conceived as something we can assign a probability, as any subset of a sample space of possible outcomes (Tijms, 2007). Lindley (2006) represents a somewhat extreme conviction, claiming that we can assign a probability to the event that the capital of Cambodia is Phnom Penh. Admittedly, this conception hardly converges with everyday interpretations of *event*. The

principal difference is recognized by Savage (1972), pinpointing that the concept as formulated in the statistics is *timeless*. Since risk assessors are concerned with events of temporally defined starts and endings, it seems that more is gained from conferring scholars of philosophy.

#### 5.4.1 Something involving changes

An event may be narrowly conceived as something involving changes (Kim, 1973). The event of hair dying involves the changing of hair color, having birthday marks the transformation of age, while war and airplane crashes involve a variety of alterations of which termination of human lives is the most severe. Kim (1973) calls for an extension of this narrow view, conceiving events as concrete objects that are exemplifying a property at a certain point of time. An event thus comprises states and conditions, as a complex of objects and properties, time points and segments. Following this account, every event has a unique constitutive property in the sense that it subscribes to a generic event, for instance that of dying. What complicates this picture is that each individual event is usually thought to fall under many generic events, like the one and same event of dying may be the moving of a finger, the pressing of a trigger, a shooting and a mercy killing. Complicated is not only the conception of event, but also the relation between causal events and those of effect. To elaborate on this difficulty, Riker (1957) is invited to the panel, who admirably explains the event-concept in an easily understood and entertaining fashion.

#### 5.4.2 An event is bounded by subjective starts and stops

Riker (1957) begins his examination by admitting that a general term like event cannot be ostensively defined. Rather, it must thus be defined in context (e.g. war and chemical reactions are events) and genetically (the existence of some perceived motion or action, sometime, some place). On the basis of these specifications, Riker (1957, p. 58) constructs a formal definition:

**Event:** an event is any subjectively differentiated portion of motion or action.

While this definition is only preliminary to Riker, it is considered sufficient for the purpose of this study. Vital is the adverb *subjectively*, which denies the existence of any objective event. This is because the actions and motions under study are continuous; they are without beginning and end. Each temporally defined segment of motion or action succeeds a previous segment and precedes a latter, meaning that they are neither instantaneous nor eternal. Riker (1957, p.58) continues:

But, although reality is continuous, human perception is not. For a variety of reasons we are unable to comprehend the whole of this continuous reality (..) Faced with the complexity of continuous reality, humans understand it by breaking it up into pieces. Although a continuous reality cannot, by definition, consist of discrete motions and actions, *we imagine starts and stops*. What lies between the starts and stops we call events. (Added emphasis)

Events are thus created by the verbal imposition of boundaries that, regardless of the objective existence of the motions and actions, are entirely subjective. These starts and stops are by Riker (1957, p.61) called *situations*, which are:

**Situation:** an arrangement and conditions of movers and actors in a specified, instantaneous, and spatially extended location.

The *arrangement* (which is the spatial relation between movers and actors and the boundaries) and the *conditions* (meaning the previous history of motion and action) make the *form* of a situation. In contrast to events, which contain at least a portion of reality, are situations entirely artificial. It is also crucial to note that the initial and terminal situations are defined as such only in relation to the bounded event.

### 5.4.3 Ambiguous events and implications for causality

An event must according to Riker (1957) be bounded by situations that include all and only its movers and actors. This means that the movers and actors of the initial situation shall be included also in the terminal situation. If not, the event has either two or more beginnings or two or more endings. As this involves the self-contradiction that the initial situation is not the initial situation, Riker labels such affairs *ambiguous events*. An excellent manifestation is the First World War, over which historians still quarry to establish the triggering situation.

The great problem accompanying ambiguous events is the riddle of causation. If an event is understood as having two or more starts, it may also have two or more causes. What is troublesome is not the existence of multiple causes as such, but the assertion that any of these are sufficient and necessary conditions for the event to occur. Riker launches five canons for avoidance of ambiguity in events. Most relevant is the fifth advice of preferring small events to those of greater extent. This is because events of large extent and duration and many movers and actors are likely to be more ambiguous. Not only can small events be more precisely bounded, the remaining ambiguity may be resolved using statistical techniques that, based on the very assumption that a small slice of reality has a greater chance of occurring than a large one, are designed to cancel out the ambiguity in imprecisely bounded events. An example is the failure of a basic component, which can be adequately assessed using generic failure rate data from databases like OREDA (2004).

In the context of risk assessment, all events are ambiguous since they are hypothetical; neither the initial nor terminal situation is unique. Instead, logical fault- and event trees are applied to model the range of possible causes and consequences. Without ambiguity in the terminal situation of an event, the concept of risk loses its meaning indeed. Accepting that ambiguity cannot be eliminated, the beauty of minutely portioned events with well-defined starts and stops still offers a valuable canon for asking *what can wrong*. Along comes the recognition that mastering the boundaries of events is a subjective task, which further confirms the importance of a set of well-defined terminological knobs for enhancing consistency. Especially important is this according to Kim (1971), who maintains that only within a coherent framework of events is causal talk possible.

### 5.4.4 Causality

Closely related to the concept of event is that of causality. Most often we talk of events as causes or effects, although notions like conditions, states, phenomena and processes also engage us in causal talk (Kim, 1971). In a public lecture by one of the preminent researches on the field, Pearl (2000) explains causality as our awareness of what causes what in the world and why it matters.



## **The dual role of causality**

Throughout history, causality has served a dual role for mankind. On one hand, it has been used for targeting credit and blame for past events. On the other hand, understanding causality has enabled mankind to exert better control over future events. Accident investigation illustrates the former, while risk assessment makes a perfect example of the latter. Pearl notes that even if we by no means can practice control, deep understanding of causation may still yield sufficient sense of being in control. Recapturing the discussion in Section 4.3, this offers an intriguing perspective on the intrinsic value of risk assessment.

## **Riddles of causal inference**

Causality is, despite its prominence in human reasoning, a notion of mystery and controversy that many scientists and philosophers refrain from using. Pearl (2000) narrates that statisticians and physicists have been especially hesitant. This is notably due to the difficulty of defining when one event truly causes another. In the former field, the less stringent concept of correlation is by and large preferred over causation. What constraints the science of physics is the enigma of directionality. Although the sun is repeatedly observed to rise following the crow of the rooster, we all understand that it is not the rooster that causes the break of dawn. The problem, as observed by Pearl and many before him, is the impossibility of translating even this simplicity into a mathematical equation. Pearl (2000) is devoted to resolving this enigma, claiming that logical diagrams make a quintessential complement to the language of probability. The logics of a fault tree makes an excellent example, indicating that risk assessors have the necessary language for expressing causality at hand.

Pearl's account to causality is still threatened by two remaining problems of causation. These are inflicted by the ideas of the 1800th century philosopher Hume (Represented in Pearl, 2000). Causal connections are according to Hume the product of observations. This induces a first riddle regarding the learning of causal inference. How are causal connections established? And even if causal connections may be ever so correctly set, a second riddle follows when questioning: How can we make use of this information? Returning to the realm of risk, the first problem may be seen of as one of risk analysis, while the latter concerns the wider issues of risk assessment and risk management. The two problems are interconnected in that the latter necessarily influences how one is answering the first.

### **5.4.5 The focus of investigation**

Essential for solving both riddles as well as the enigma of directionality, is to recognize the significance of focus to your investigation. If the entire universe is chosen as the object of investigation, causality would disappear as there would be no such thing as intervention or circumscription. Instead, the scientist or risk analyst carves up a piece of the universe as the focus of investigation. The rest of the universe is considered as background or boundary conditions. According to Pearl (2000), it is this choice of ins and outs that creates the asymmetry that allows us to talk about causality and directionality of cause and effect. This is because causation basically means predicting the consequences of an intervention, be it the crowing of a rooster or the failure of a technical component. If we carve up the universe in a dif-

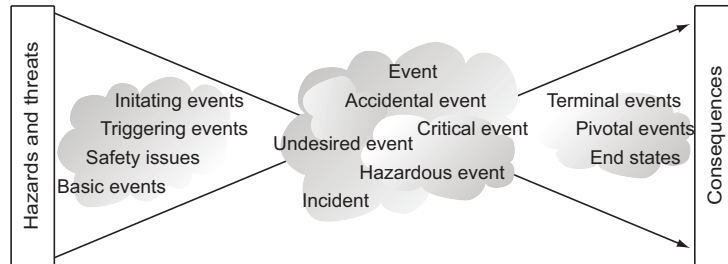


Figure 5.6: The cloudy events of risk analysis.

ferent manner, the inputs and outputs will correspondingly change, along with our understanding of causality. Reconsider the proposed rearrangement of the vertical model of Rasmussen (1997) in Figure 4.6. Depending on what levels we include in our causal analysis of risk, distinct root causes are revealed and with it the possible means of control.

Putting the pieces together, Kim (1971)'s claim that circumscriptions mostly take the form of events makes a powerful alliance with the assertion of Riker (1957) that events are confined by subjectively imposed situations. Demonstrated is not only the significance of boundary definitions to risk analysis, but also the subjective nature of both cause and consequence.

#### 5.4.6 The events of risk assessment

Having explored the concepts of hazard and event, the foundation is in place for considering events that involve hazards. Invaluable for maneuvering through the plethora of related terms is the bowtie-diagram of Figure 5.6. Suggested in the figure is the feasibility of a tripartite focus in separating events of initiation, release and escalation. The former relates to events of causation, for example, *triggering event* (TE) and *safety issues* (SU). Among the many candidates of the midst category are *hazardous event* (HE) and *accidental event* (AE). The third group follows the trajectory of a hazardous release and is occupied by more sporadically denoted intermediate and terminal events. The forthcoming sections endeavor to map the words of the two former. Since the center of the bowtie-diagram is centripetal to the analysis of risk, it makes a feasible starting point of our examination.

### 5.5 Hazardous event

In Section 5.2 it was stressed that a hazard exists simply as a potentiality or source. From that it followed that the moment this potential is realized, we no longer speak of hazard, but an event. Unlike the notion of hazard, there is no generally accepted term for this realization. The preceding section explains the added complexity. An

event is, in contrast to the ontological reality of hazards, bounded by subjectively imposed starts and stops.

In search of a designation that is as unambiguous as possible, this author believes that advantage is gained by explicitly relating it to the more objective concept of hazard. Instead of using ambiguous prefixes like *critical* or *accidental*, the node of the bowtie-diagram is preferably denoted *hazardous event*. This is in line with the practice of the RAMS-group at NTNU (see, e.g. Rausand and Utne, 2009a). Hazardous event is defined at the end of the section, after first presenting a selection of apparently synonymous contenders.

### 5.5.1 Events and incidents

In the vocabulary of ISO guide 73 (2009, p.6), *event* is applied without prefix and is widely defined as “the occurrence or change of a particular set of circumstances”. A set of explanatory notes establishes its location at the middle of the bowtie-diagram. Furthermore, it is specified that an event may consist of something not happening(!) and may be referred to as an *incident* or *accident*. According to this standard, incident is reserved for events without consequences, whereas accident denotes events of adverse outcomes. Contrasting is the nomenclature of DHS (2008b), conceiving incident as the single event-related term of any hazardous realization. Following this interpretation, ISO guide 73 (2009)’s notion of accident may be considered a subset of the wider notion of incident. There are, however, gray areas between these terms. Is there some lower threshold of adverse consequences for the designation of accident? It is in the opinion of this author that the definitions of ISO guide 73 (2009) and DHS (2008b) are both too vague for unambiguously serving the analysis of risk. This also holds for the notions of accident, incident and event.

Also Christensen et al. (2003, p.186) prefer the single notion of event, while defining it in a more confined manner:

**Event:** isolated incident or a number of interrelated circumstances/incidents resulting in release of agents and/or energy.

By specifying the realization of a harmful potential, this definition places itself in the center of the bowtie-diagram. Another observation is made in that an event may consist of many smaller events or circumstances. Recalling the advice of Riker (1957), this may pose a problem for the initial bounding of events. While the terminal situation is comparatively clear in the release of a potential, the starting point is left wide open to interpretation. It might be minutely portioned in close approximation to the end situation, but may also be located in the left part of the bowtie-diagram. Such indeterminacy is especially confusing when applied to define a capacious notion like *event*.

### 5.5.2 Accidental event

Like Christensen et al. (2003), does NORSOK Z-013 (2001, p.5) open up for multiple events in their term *accidental event* (AE):

**Accidental event:** Event or chain of events that may cause loss of life, or damage to health, the environment or assets.

The above problem of ambiguously defined initiation still holds. Vatn (1998) witnesses that some applications stretch AE back to the initiating event. Since section 6.2 demonstrates that initiating event is an equivocal term that goes far beyond the realization of a hazardous potential, this introduces unnecessary conceptual difficulties.

NORSOK Z-013 (2001) makes a valuable specification in that accidental events are acute, unwanted and unplanned. Excluded from analysis are thus hazardous releases occurring over longer time periods. Examples are occupational exposure to asbestos or continuous releases of toxic substance. Not only are such instances difficult to confine in time, required is also a distinctive analytical approach. The reader may consult HSE (1992) for an elaboration on the subject.

### 5.5.3 Undesired event

Consulting yet another standard, NS 5814 (2008, p. 6) employs the term *undesired event* (UE):

**Undesired event:** event that may lead to loss of values.(Translated from Norwegian)

An undesired event is described as the concretization of a corresponding hazard. This indicates its residence at the center of the bowtie-diagram. Depending on the purpose of analysis, the concretization is claimed further specification concerning time, place, scope and nature. A rough specification is exemplified as “fire”, while one of richer details is given as “fire in board no. 8”.

In the guidance of USNRC (1981), *undesired event* is understood as the topmost event in a fault tree. The concept has in this regard only implicit reference to hazard. UE is instead conceived as complete or catastrophic system failure, meaning failures that may lead to accidents of death or crippling injury. Since this need not be hazardous release, but an event located farther in the causal or consequence chain, the interpretation of USNRC (1981) lies somewhat beyond our current quest.

### 5.5.4 Critical event

Delvosalle et al. (2006) explicitly conceive *critical event* as the center of the bowtie-diagram. Also Svedung and Rasmussen (2002, p.405) prefer this term, specifying that a critical event:

(..) reflects the release of a well-defined hazard source, such as ‘loss of containment of hazardous substance’, or ‘loss of control of accumulated energy’.

Delvosalle et al. (2006) explain that loss of containment refers to the release of fluids in the process industry. For solids, critical events relate to loss of physical integrity, that is, a change in the chemical’s chemical or physical state. Examples of process-related critical events are the start of a fire and leak from a pipe. Both Delvosalle et al. (2006) and Svedung and Rasmussen (2002) stress that the definition of critical event must fit the purpose of analysis. Defined as neither too coarse nor specific, the set of critical events helps structuring the identification of relevant hazards as well as proactive measures.

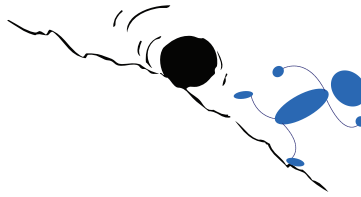


Figure 5.7: Trying to escape a hazardous event.

In bridging a situation of potential harm to one of realization, the conception of critical event falls close to the idea as initially advanced. There is one thing to indict though, which is simply the ambiguity embedded in the word *critical*. Depending on the interpreter, the term may refer to the severity of possible consequences, the cardinality of branches in the consequence chain or the relative impact on the overall functioning of a system. It seems like nothing but ambiguity is lost by relabeling the concept to *hazardous event*.

#### 5.5.5 Hazardous event

It is in the opinion of this author that *hazardous event* (HE) offers the most precise designation for the center of the bowtie-diagram. Unfortunately, the term is in most RAMS-publications only contextually defined, like by exemplifying gas leakages and high pressures as hazardous events (see, e.g. Lundteigen and Rausand, 2009). A generic definition is provided by Kjellén (2000, p.377):

**Hazardous event:** Loss of control of energy in the system or body movement, resulting in a potential for exposure of personnel (or the environment/material asset) to the energy flow.

Essential to Kjellén's conception of hazardous event is the loss of control of a source that may result in target exposure. This will serve as the basis for a refined definition. Two revisions are considered feasible, thereof to broaden the scope from loss of control of energy to the release of a hazard. Although Kjellén (2000) maintains that physical harm results from exposure to energy, Section 5.2 implies the feasibility of distinguishing between material and energetic releases, which both enter into the concept of hazard. The second specification is that the event not only has the *potential* for resulting in exposure, it *will* lead to exposure if not adequately controlled. The essential point is that the event is terminally bounded subsequent to hazard realization, but prior to reactive control. For illustration, let us return to the example of living under an escarpment in Figure 5.3. If still, the mammoth masses of snow remain a source of potential harm, that is, a hazard. When the masses are set in motion and the moment sufficient momentum is gained, a hazardous event occurs in the release of an avalanche. If an unprotected person stands in the middle of this trajectory, he will most certainly experience harm. However, whether he finds shelter in a nearby house or manages to run in a non-cartoonish matter (Figure 5.7), is conceptually excluded from the event of hazardous release.

Based on these annotations and the insights from the more or less synonymous concepts above, hazardous event is in this study defined as:

**Hazardous event:** Event confined to the first significant release of a hazard that will result in harmful exposure if not controlled.

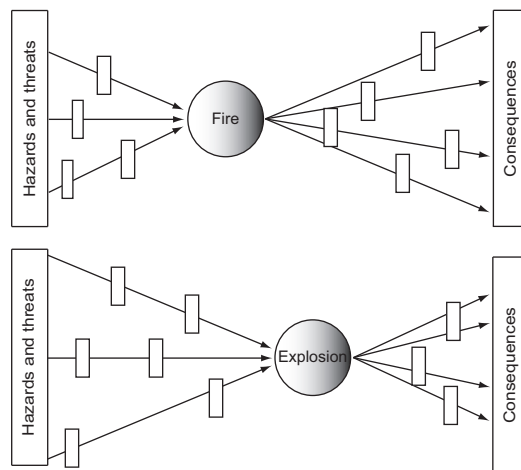


Figure 5.8: Different hazardous events for the same scenario.

The definition is intended for accidental releases as well as intentional threats to bodily harm. Excluded from consideration is the continuous release of harmful substances. This is implied by confining the event to initial and terminal situations of close approximation. Precisely how closely these are set is, however, not the principal object of inquiry. This owes to the recognition of ARMS (2009) that the mid event is more an imaginary concept than a real-life event, introduced to help the systematic assessment of accident trajectories and categorizing barriers as either preventive or reactive. More acknowledgeable is it that the analyst is left with considerable freedom in marking the limit between prevention and mitigation. For instance, the onset of a fire and an explosion may be two stages of the same accident trajectory that both account to our definition of hazardous event. The two imply different centers of gravity in the bowtie as sketched in Figure 5.8. What event to choose is pragmatically conditioned, but all the same heuristically guided by the first part of our definition.

Although the center of the bowtie obeys a variety of names and necessitates pragmatic interpretations, it remains a clear concept at least on an abstract level as the analytical crossover between prevention and mitigation. Neither the start nor the end of the diagram is blessed with such conceptual clarity.

## 5.6 Reason's events of causation

A listing of hazards marks the “start” of the bowtie-diagram in Figure 4.3. For illustrating the conceptual link between hazards, a hazardous event and its potential consequences, this representation is unproblematic. Nor does it fail to guide the identification of hazards and their related hazardous events. However, to enable us going back and answer *why* a hazardous event occurs and *how* it may be prevented,

the sketch is in need for refinement. There are two reasons for this. The first follows from our definition of hazard. Since hazard is conceived as a source of *potential* harm, it is neither an event nor a situation in the terms of Riker (1957). It is merely a condition. From that it follows that it cannot by *itself* mark the initiation of an event, but must enter into a triggering event or situation, that is, to form a cause.

A second rationale comes from the recognition that a hazardous event may always have several causes; each one necessary, but singly insufficient (Reason, 1997). In principle, these can all be traced back to the big bang. As a tragic example, Reason tells the story of the principal investigator of the Chernobyl accident, whose suicide letter is said to reveal that the true cause of the accident was the Union's dysfunctional economy since before 1917. Obviously, this recognition is of little preventive help as long as man is unable to travel back in time. A more topical example is a recent railway accident in Norway, where three persons were killed by a cargo ran amuck. Subsequently, the Norwegian National Rail Administration and the cargo operating company have both been blamed for long-term negligence in matters of maintenance and safety (TV2, 2010). Was this accident caused by organizational recklessness, operational errors or technical failures? By relating the incident to Figure 4.7, it becomes clear that the sole notion of hazard is insufficient to guide causal analysis of such situations. That is, unless one applies a very capacious hazard conception that also includes poor railway organization. Elucidated is not only the pragmatic challenge of demarcating hazards from their underlying causes, but also the significance of how we carve up our accidental universe in the sense of Pearl (2000). These considerations combine in the work of Reason (1990b) and the collaborative project of Wagenaar et al. (1990).

### 5.6.1 Triggering events

What is it that enables the realization of a hazard into a hazardous event? In the framework of Reason (1997) in Figure 5.1, losses and hazards are separated by a line of defenses that if all breached, may lead to an accident. Although Reason does not apply the concept of hazardous event, the triggering events that catalyze this transformation are the basis of his research. Or, to be more correct, they make a focal topic in demonstrating what *not* to focus on.

*Triggering event* is an informal and undefined term which Reason (1990b) interchangeably uses with the notion *local triggering factors*. For the purpose of this study, a triggering event can be understood as the most immediate cause of a hazardous event. This may be technical faults, atypical system conditions<sup>1</sup> or active failures. Reason, who is professor in cognitive psychology, is by and large concerned with the latter. *Active failures* are errors and violations committed at the sharp end of a system by train drivers, control room personal and like. They are characterized as active due to the immediacy of their adverse effects, which is the reason why such failures appear as the obvious instigators of hazardous events. This is implied by the downstream arrow of causal investigation in Figure 5.1 (active failures are in this figure labeled *unsafe acts*). In Reason (1990a)'s pioneering work *Human error*, unsafe acts are dissected into subgroups of slips, lapses, rule- and knowledge-based mistakes. The essential point is that these are neither random events nor

---

<sup>1</sup>In light of the discussions in Section 5.4, one may question whether system conditions can actually be considered events. But, the fact that they are atypical suggests that they are not normally present, and hence can be assigned a start, and end and a probability. Moreover, the notation of triggering events serves to prevent confusion with the related but dissimilar term *latent conditions*.

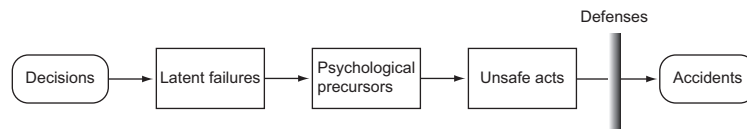


Figure 5.9: General accident progression according to Wagenaar et al. (1990).

causes, but consequences of a responding set of *psychological precursors* (labeled *local workplace factors* in Figure 5.1). The precursors are psychological processes that determine the actual behavior of workers on the shop floor (Reason, 1995). They are functions of the task, the local environment and the presence of hazards, and may be manifested as, for example, stress, unwanted attentional captures or inadequate tools. Psychological precursors are in an extensive collaboration project with Wagenaar and Hudson launched as the neglected link between active failures and their root causes. The generalized framework of Wagenaar et al. (1990) on accident causation is represented in Figure 5.9, showing how unsafe acts are promoted by psychological precursors which, in turn, are caused by *latent failures*.

### 5.6.2 Latent failures

Reason (1990b) explains latent failures in analogy with the resident pathogens of the human body. Rather than arising from single causes, cancer is brought about in the combination of resident pathogens and external stressors. The aetiology of organizational accidents follows the same logic. Like pathogens, latent failures lie dormant within the system, only to become fatal when combined with local triggering events or stressors. They are the result of bad management decisions, which have taken place well before the onset of a recognizable accident sequence. Their latency is thus not in the sense of being invisible, but due to their error generating capacity (Wagenaar et al., 1990).

Figure 5.10 depicts how latent failures propagate along what Reason (1995) denotes an *active failure pathway* to promote the occurrence of unsafe acts. A second causal pathway is the *latent failure pathway*, running directly from the organizational processes to the defenses that separate hazards from vulnerable people and assets. Poor design, for instance, may weaken the system responses by creating “holes” in its line of defenses. Latent failures not only increase the occurrence of hazardous events, but also enhance the possibility of adverse outcomes.

A source of confusion is that latent failures go under multiple names. In subsequent revisions, Reason (1997) uses the term *latent conditions* on the grounds that it is a more appropriate descriptor of causal indirectness. Reason still applies the synonym *general failure types* (GFT), which is a classifying notion introduced in the original work of Wagenaar et al. (1990). The term *type* was chosen to signalize that latent failures represent a set of phenomena and not individual tokens, as are the psychological precursors and unsafe acts. There is a many-to-many mapping between these types and tokens (Reason, 1990b). Deficiencies in, for example, training, may translate into a variety of precursors, like time pressure and inappropriate perception of hazards. On the other hand may undue time pressure be the product of several latent failures, for instance, poor scheduling and inappropriate procedures. In turn can a psychological precursor, alone or in combination with others, provoke an almost infinitely large set of unsafe acts. From this follows the critical



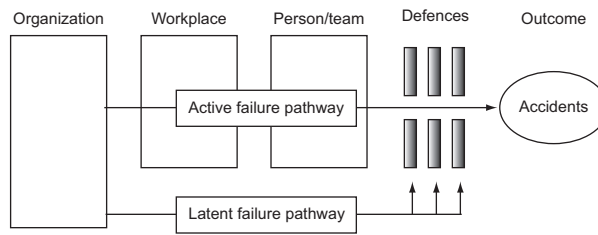


Figure 5.10: Latent and active failure pathways (adopted from Reason, 1995).

recognition that foreseeing all active failure pathways is impossible. Not only does this leave triggering events difficult to control, focusing on their elimination may even be counterproductive. This is because combating triggering events will only cure the symptoms and not the disease, with the result of concealment or exacerbation of the real root causes. The grand conclusion of Wagenaar et al. (1990) is the imperative of making latent failures the primary target for accident prevention. This forms the bedrock of motivation behind the *Tripod-Delta* approach, which aims at preventing the onset of accident scenarios before ever taking place.

### 5.6.3 Tripod

Tripod is a philosophy and a methodology developed by Wagenaar and his associates on commission of the petroleum company Shell. Since the project's beginning in 1988, Tripod has been cultivated via a suite of papers (see, e.g. Wagenaar et al., 1994), and is now a great selling trademark fronted by consultancy firms and a comprehensive manual. At the heart of Tripod lies the classification of 11 general failure types most likely to elicit precursors of unsafe acts:

- *Hardware* tools and equipment of poor quality and availability (HW).
- *Design* that promotes errors and violations (DE).
- *Maintenance management* yielding inadequate planning and inefficiency (MM).
- *Procedures* of poor quality, accuracy, relevance, availability and workability (PR).
- *Housekeeping* that neglects impending problems (HK).
- *Incompatible goals* leading to individual, group- and organizational goal conflicts (IG).
- *Communication* problems of misinterpretation, dysfunctional or absent communication channels (CO).
- *Organization* which allows warning signs to be overlooked (OR).
- *Training* that fails to provide workers with the necessary skills and knowledge (TR).
- *Defenses* that lack or fails in detection, warning, recovery and so on (DF). This is the only GFT that is specifically safety-related.

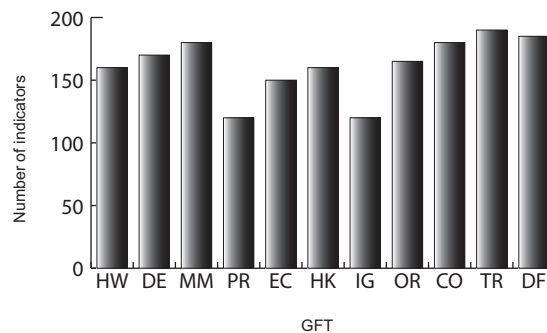


Figure 5.11: Fictitious example of failure state profiling (taken from Wagenaar et al., 1994).

- *Error enforcing conditions* as a compound of the remainder GFTs (EC).

In essence, Tripod is about controlling the controllable and disregarding what is not. And according to Wagenaar et al. (1994), what is controllable are the general failure types. For each GFT, a *failure state profile* is created as exemplified in Figure 5.11. The profile indicates the extent to which each GFT is likely to contribute to an accident. Failure state profiling may be performed either reactively or proactively, that is, as an accident investigation tool or for predicting the causal structure of future accidents. The respective methodologies are differentiated as *Tripod Beta* and *Tripod Delta*.

A major presumption of Tripod-Delta is that general failure types are amenable to measurement via psychological precursors. By combining the theoretical framework with an extensive, empirically derived database, the observed tokens are linked with the general failure types. For a particular operational context, profiles are then generated from comprehensive diagnostic checklists in assistance with advanced software tools. By indicating the most contributive GFTs, a practical means is provided for managing a limited set of latent failures in lieu of an infinite number of triggering events.

#### 5.6.4 Tools for auditing vs. decision support

Tripod-Delta has, according to Reason (1997), been successfully applied across a variety of continents, cultures and operations. A plausible explanation is the extreme variety of situations it is designed to encounter. Uniquely, it allows the transmission of local considerations into generic and manageable profiles (Wagenaar et al., 1994). Another explanation is its solid theoretical basis, which is developed by a venerable group of safety researchers.

The reader should note that the purpose and methodology of Tripod-Delta differs fundamentally from those of risk assessment. Whereas quantitative risk assessment chiefly purports to inform decision making in preoperational phases, Tripod-Delta is an *audit tool* designed for periodic measurement and control of operational risk. In the former case, GFTs cannot be measured as *is*, but if possible only as *intended*. Does the Tripod-framework still offer a useful perspective to our quest? Arguably, it forces us to contemplate our ability to foresee the ways in which hazardous events come about. Following the reasoning of Reason and his associates, only lim-

ited gains will follow an analysis of triggering events, as these are bound to reveal themselves in unprecedented ways. Emphasis should instead be on contextual diagnosis of organizational deficiencies. For illustration, let us return to the galloping cargo at Sjørøya, which may have been instigated by a variety of active failure pathways. With hindsight, it is tempting to claim that the actual pathway is of nothing but secondary importance to the organizational weaknesses that had been prevailing for years. Sooner or later, one might argue, an accident was bound to happen in one way or another. Notwithstanding that, Section 2.2 makes it clear that the concept of risk loses its meaning in retrospective. The important question is thus whether one could foresee that these deficiencies would combine with local triggering events to kill three people.

The very motivation behind Tripod is to understand the junction between latent failures and triggering events (Wagenaar et al., 1994). Looking back, Reason (1997) admits that focusing on latent conditions rather the combination *per se* has a logical defect. After all, latent conditions are present in all systems, even those of immaculate accident records. What discriminates between normal states and accidents is thus not the presence of latent conditions. Triggering events, on the other hand, are the ultimate determinants of whether or not a hazardous event occurs. Despite these objections, Reason still finds the above arguments compelling to why latent conditions are cardinal; in contrast to triggering events, they can both be identified and controlled. If we as risk assessors are to accept this inference, a second riddle comes forward. How can we integrate the concepts of Figure 5.9 into our bowtie-diagram?

### 5.6.5 Locating triggering events and latent conditions

Locating the concepts of latent failures, psychological precursors and triggering events in Figure 5.12 requires consistency with our proposed definition of hazard and hazardous event. Reason (1990b) leaves little doubt that triggering event takes place prior to and in close approximation to our concept of hazardous event. It is a crucial recognition that several events, for instance, technical failure and operator error, may combine to trigger the hazardous event. In order to serve its analytical purpose, our diagram must thus allow for multiple triggering events in an active failure pathway. An enigma the framework does not seem able to address, is how several hazards may combine into amplified hazardous events.

Wagenaar et al. (1990) stress the importance of distinguishing triggering events from mere error-enforcing conditions. It is, however, in the opinion of this author that psychological precursors are only of indirect importance to our depiction of accident causation. This is because they are individual tokens rather than types, which are vital to our understanding of organizational accidents, but only as an explanatory link between general failure types and unsafe acts. It is of this reason considered sufficient to include only the GFTs in our conceptual illustration.

Locating GFTs in Figure 5.12 is conditioned on our conception of hazard. Are the general failure types to be interpreted as hazards or are they external to our sketch? It appears that the former only complicates our conception of hazard, and by that also the process of hazard identification. Placing GFTs subsequent to hazard seems similarly inadequate, if only to entangle our identification of hazardous events. Yet, Section 5.2 suggests that there are borderline cases which fuse the notions of hazard and their underlying causes. Ergonomics, which is the suitability of design for human operation (Wagenaar et al., 1990), is an example of a general failure type close

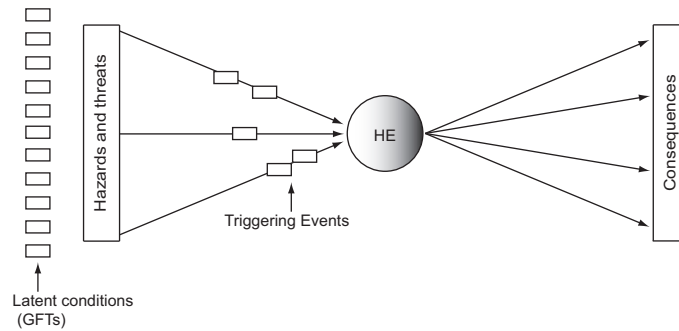


Figure 5.12: Integrating general failure types and triggering events in the bowtie-diagram.

to our notion of hazard. It is, however, worth to remember that none but one of the GFTs are specifically related to issues of safety. Rather, they are general processes underpinning both safety and quality. This indicates that GFTs are not hazards *per se*, but make a set of deeper underlying causes located to the left of the bowtie-diagram as suggested in Figure 5.12.

### 5.6.6 Complementing the concepts of hazard and hazardous event

In conclusion, let us return to the question of what the framework of Reason and his associates has to offer our terminological assessment of risk. It should be noted that its value is not merely the imperative of broadening the analysis to organizational factors. Promising methodologies for including organizational factors in risk analysis have been suggested elsewhere (see, e.g. Paté-Cornell and Murphy, 1996), as has also the added complexity of multiply involved organizations (see, e.g. Rasmussen, 1997). What our quest boils down to is the benefit of complementing the concepts of hazard and hazardous event. It is in the opinion of this author that extending the vocabulary is useful in two means. Firstly, placing general failure types outside the original bowtie-diagram offers an explanatory notion to the underlying causes of hazards. It also serves to remind us that by removing a hazard, the accident sequence may actually be stopped before it has even begun. This makes the first and most preferable out of ten strategies of accident prevention as first presented by Haddon (1973).

Yet, in many cases is the hazard the very reason for a company's existence. Eliminating the potential energy involved in commercial aviation, for example, certainly makes a preposterous suggestion. Deduced is a second yet contradictory rationale, which is that hazards relate to risk only in contemplation of their realization. Complementary to analyzing the hazardous substance inside a tank as in Figure 5.14, is thus envisioning the ways in which the substance might escape the tank. And to express these means of instigation, triggering event offers a communicable term.

The problem of adopting the concept is the peripheral role it is assigned by its own originators. If triggering events are as impossible to anticipate as claimed by Wagenaar et al. (1990), how can they be meaningfully included in the vocabulary of risk assessors? One possible solution is to follow the suggestion of ICAO's to focus on so-called *safety issues*. Before examining this concept, the present discussion on triggering events is closed by calling attention to its perhaps greatest value. That is, to serve as a necessary reminder of the inherent limitations of our causal extrapolation of future hazardous events.

## 5.7 Safety issues

Whereas Reason (1990b) carves up his causal universe in the combination of triggering events and latent conditions, ARMS (2009) makes a different cut in the alliance of triggering events and hazards. ARMS (Airline Risk Management Solutions) is a working group aiming at improving the methodology of operational risk assessment for aviation organizations. A key focus is the identification and assessment of *safety issues* (ARMS, 2009, p19):

**Safety Issue:** a manifestation of a hazard or combination of several hazards in a specific context. The Safety Issue has been identified through the systematic hazard identification process of the organization. A SI could be a local implication of one hazard (e.g. de-icing problems in one particular aircraft type) or a combination of hazards in one part of the operation (e.g. operation to a demanding airport)

This definition is somewhat imprecise and inert. The examples provided by ARMS (2009) reveal that safety issue is a concept of many manifestations: “wind shear at approach to xxx”, “operation into zzz in high altitude and short runway” and “fatigue on red-eye flights”. What they have in common is seemingly their context-specificity only. Due to the conceptual cloudiness introduced by its very originators, demarcating safety issues from those that are not seems hardly expedient. So is instead a short discussion on the merits and disadvantages of this perspective. For this purpose, re-definitional freedom is taken by interpreting safety issue as one or more hazards in combination with local triggering events.

### 5.7.1 Safety issues in principle and practice

Safety issues provide the starting point of risk estimation in ARMS. They are identified by analyzing recurring patterns in historical events, or may in the case of future changes be derived from conventional hazard identification methods (ARMS, 2009). Albeit the latter is claimed beyond the scope of the ARMS-process, it suggests that safety issues are applicable also to preoperational risk assessment.

Principally, safety issues serve to focus and localize the assessment of risk. The specification of safety issues is concretely and contextually defined. Each issue is subject to detailed risk assessment, allegedly based on the frequency of the initial hazard(!), the effectiveness of avoidance and recovery barriers and the severity of the most probable accident outcome. This implies that safety issue is not solely confined to hazard identification, but is also linked to the outcomes to the right of the bowtie-diagram. The rationale is provided by ARMS (2009), specifying that a safety issue usually links with several events. It is not a single event as those in the

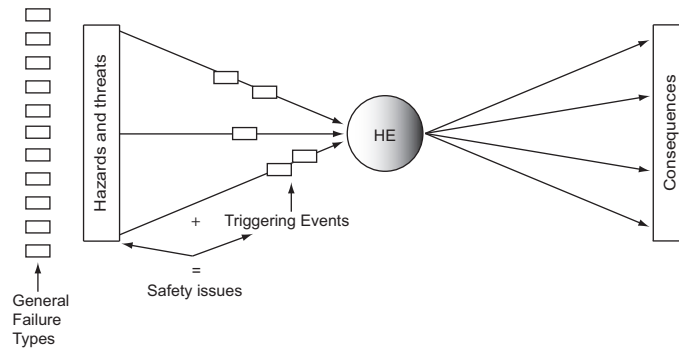


Figure 5.13: Integrating general failure types, triggering events and safety issues in the bowtie-diagram.

accident records, but a well-defined issue that is highlighted by several events. How this argument is to be interpreted appears unclear. Does a safety issue give rise to various hazardous events, or to one hazardous event with a range of outcomes? Is it possibly meant that each hazardous event or outcome links to a variety of safety issues? Considering the many-to-many relationship Reason (1990b) finds to characterize active failure pathways, neither of these interpretations seem logically flawed. The challenge is to account for this multiplicity in the bowtie-diagram.

Safety issues are in this study interpreted as in Figure 5.13. A hazardous event may rise from a variety of safety issues, which in turn can trigger a range of hazardous events. The latter point is, however, only expressible by drawing a multiple set of bowties.

### 5.7.2 Combating local factors

Focusing on safety issues will, according to ARMS (2009), result in a more scientific and objective risk assessment than the conventional approach of ICAO. It is promoted as a bridging solution between two evils in the traditional ICAO-methodology; the delusion of assessing past events and the subjectivity of projecting future events. Safety issues, one reads, can be adequately scoped and defined, leaving little room for subjectivity in risk assessment. Simplicity of use is a second advantage that holds for both assessors and managers of risk. Risk assessment is claimed easier due to the structuring of focus, while managing risk is reduced to a matter of managing your safety issues. The pleading argument of ARMS (2009, p.19) is that “you can do something about safety issues” since they are based on local implications rather than general assumptions. This stands in contrast to the underpinning ideas of Tripod-Delta. Would not the specific nature of safety issues yield the exact opposite conclusion had Wagenaar et al. (1990) been invited to the panel? Although the two perspectives seem diametrically distinct, they have a common denominator in acknowledging the prominence of local factors. Consulting Figure 5.13, it is also true

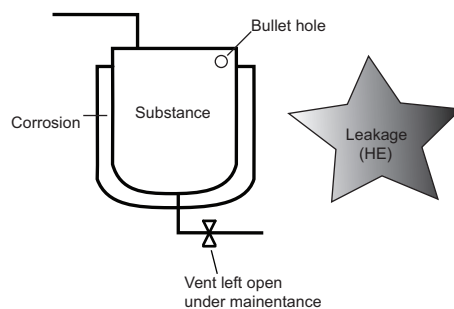


Figure 5.14: Safety issue is a combination of triggering events and hazard.

that both frameworks gain from reducing the occurrence of triggering events. The difference is that Reason and his coworkers believe that this battle can only be indirectly fought; by combating neither the triggering events nor the local factors, but the latent conditions. ARMS (2009) appears of a different conviction, claiming that it is the safety issues as such that should be managed. This is not to be interpreted as a quest for combating all triggering events; in focus are only those that combine with hazards to produce hazardous events.

The number of possible pairs must admittedly be as large as the infinite number of triggering events. This suggests that any list of safety issues is inherently incomplete. Paradoxically, this principal weakness may also be considered a pragmatic strength. In a universe of endless causal combinations, the concept of safety issues offers a just terminology for singling out those issues causing multiple or critical hazardous events. Let us return to the example of the tank in Figure 5.14. The tank may be subject to a vast number of triggers, for example, maintenance errors, corrosion or someone firing off a bullet. Instead of unilaterally asking what may trigger the substance into realization, safety issues help focusing the investigation by asking how the hazard may respond to common triggers. In comparison, also Tripod reduces the causal universe into a manageable few, but on an underlying level and without explicit reference to hazard.

### 5.7.3 Including safety issues in our vocabulary of risk assessment

The reader should note that the above reasoning is based on the conception of hazard and hazardous event as defined in the present study. In ARMS (2009), these concepts are somewhat differently conceived. Erroneous inferences are thus likely to haunt our conceptual discussion. The reason for taking such interpretative freedom is not only that safety issues is a relatively unexplored idea that is still under development, but also because the presentation of ARMS (2009) signifies a rather poor understanding of fundamental risk-related concepts. By example, the authors speak of risk assessment of historical events and the frequency of initial hazard. According to the discussions of Section 2.2 and Section 5.2, these are conceptually troublesome statements. Notwithstanding this, it is believed that safety issues offer an interesting perspective that is worthy of theoretical refinement.

## **A helpful, but subjective means for structuring hazard identification**

It appears as no coincidence that the concept of safety issues is developed for aviation organizations. In the aviation industry, the hazards are varied and numerous, as are also the events that may trigger their realization. Both potential and kinetic energy are given premises for flight operations. In turn, these may combine with natural hazards (e.g. lightning), intentional threats (e.g. hijacking) and triggering events (e.g. engine component failure). Faced with such diverse possibilities, safety issues offer a helpful means for structuring the process of both hazard identification and causal analysis. A detailed assessment is, according to ARMS (2009), relatively simple due to the concrete specifications of safety issues. The argument that the assessment is also rendered more objective and scientific is, however, more difficult to follow. Even if the process becomes more transparent, one cannot escape the fact that selecting the issues *per se* is a subjective matter. If these underlying assumptions are hidden, an “objective” assessment of safety issues may only serve to conceal the subjectivity Shrader-Frechette (1991) finds so important to reveal.

## **The grand question**

Safety issues have a more pragmatic appeal than the framework of Wagenaar et al. (1990). Rather than focusing on distant generic factors, safety issues shed light on tangible localities both operators and assessor can physically relate to. The argument of ARMS (2009) that you can do something about safety issues is therefore sensible. Yet, the grand question is not whether you can do something about safety issues, but whether doing something about your safety issues will affect the overall risk. If Reason (1990b) has taught us one thing, it is that combating accidents on this level is hardly sufficient. Does this imply that the concept of safety issues should be rejected? Safety issues, as presented in ARMS (2009), are definitely in need for both theoretical and methodological refinement. It is still in the opinion of this author that safety issues supplement our vocabulary of hazard and hazardous event, by uniquely describing the interplay between the former and triggering events. Especially relevant is this for contexts in which many hazards are likely to combine into hazardous events. Moreover, the concept makes a valuable complement to the proactive framework of Wagenaar et al. (1990). Whereas the latter assists in stopping the causal flow before entering the bowtie, safety issues offer a powerful alliance when recognizing the impossibility of full prevention. How to balance the two perspectives is, however, a matter of risk management that lies beyond the scope of this study.

Finally, it should be stressed that the two perspectives are compared on a conceptual level only. Tripod-Delta is an audit tool, whereas safety issues are intended for (operational) risk assessment. The latter would thus have been of superior relevance had our quest been one of methodology. On a conceptual level, both frameworks offer valuable descriptors for the initial extent of the bowtie.



## Chapter 6

# Accident scenario

### 6.1 Introduction

Kaplan and Garrick (1981) introduce *accident scenario* as the answer to *what can go wrong?* It is a peculiar recognition that the concept so dear to Kaplan and Garrick is left undefined both in the original source and the clarifying retrospect of Kaplan (1997). What is also disquieting is that so many theorists and practitioners have adopted the triplet definition of risk, while focused discussions on this fundamental concept remain rare. An attempt of definition is found in the appendix of Garrick (2008, p.246):

**Accident scenario:** a sequence of events, starting with an event known as the initiating event (..) or an initial condition, and then proceeds through a series of events until the system either corrects itself or the scenario of events is terminated at a damaged, degraded, or destroyed state.

A simpler means for conceiving *accident scenario* is to view it as a single path in an event tree. This is illustrated in Figure 6.1, showing that an accident scenario is uniquely determined by an *initiating event* (IE) and its path to a corresponding *end state* (ES) (Kaplan, 1997). The structuring of accident scenarios shows the logic of how a system responds to different types of events and conditions. An accident scenario is not an experienced, but a hypothetical sequence of possible events (Khan, 2001). Just like risk, is accident scenario hence a prospective term. For the purpose of describing an accident that has already occurred, *accident course* is considered more appropriate.

The concept of accident scenario is cardinal to the quantitative definition of Kaplan and Garrick (1981) and has remained so in the later work of both authors. It is foundational to what Garrick (2008) denotes *the scenario approach to quantitative risk assessment*. This is a methodology that embodies the triplet definition of risk. After identifying, categorizing and selecting a critical set of scenarios, the probability and consequence of each scenario are calculated and collocated in the representation formats of Table 1.1 and Figure 1.4. This is, however, not a general convention. An alternative approach is recommended by NORSOK Z-013 (2001), replacing accident scenario with the concept of accidental event (i.e. our preferred notion of hazardous event) as the focal point of analysis. Accident scenario is left undefined in

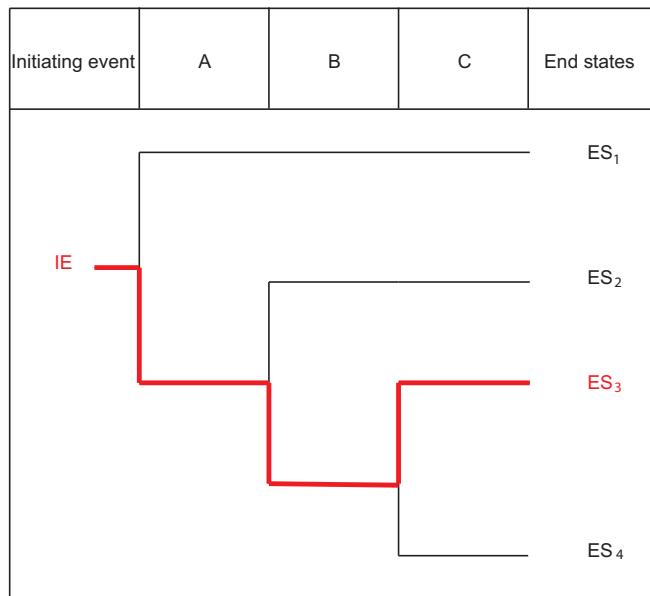


Figure 6.1: An accident scenario is a single path in the event tree.

this otherwise declarative standard, which is true also for the vast majority of other guides under study. Only in IMO (2002, p.4) is a proper definition sought:

**Accident scenario:** A sequence of events from the initiating event to one of the final stages

Due to its conciseness in capturing the distinctive features of accident scenario, the definition of IMO (2002) is adopted for the present study. Most importantly, it is considered true to the concept as presented in, for example, Kaplan (1997). This is not to say that the definition provides a sterling description on its own; required is an explanation of what is meant by “initiating event” and “final stages”. The importance of clarifying these boundaries is substantiated by Khan (2001), who reports wide variation in the portrayal of scenario extent in practice. The following sections endeavor to clarify what is meant by initiating event and end stages. Ultimately, this serves to further illuminate the concept of accident scenario. A final discussion pulls the threads together by questioning the soundness of accident scenario and contrasting the scenario approach to risk assessment with the approach of NORSOK Z-013 (2001).

## 6.2 Initiating event

A quick search in Kaplan and Garrick (1981) reports no matches to the term *initiating event*. In Kaplan (1997), it appears as a central yet undefined word, describing the point of departure for an accident scenario. Not until consulting Garrick (2008, p.246) is a concise explanation sought, defined in parenthesis as:

**Initiating event:** (an event that upsets an otherwise normally operating system)

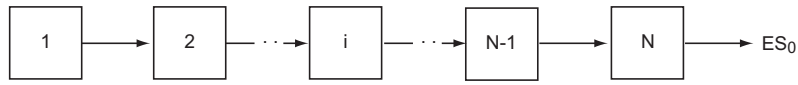


Figure 6.2: Depiction of the success scenario  $S_0$  (adopted from Garrick, 2008).

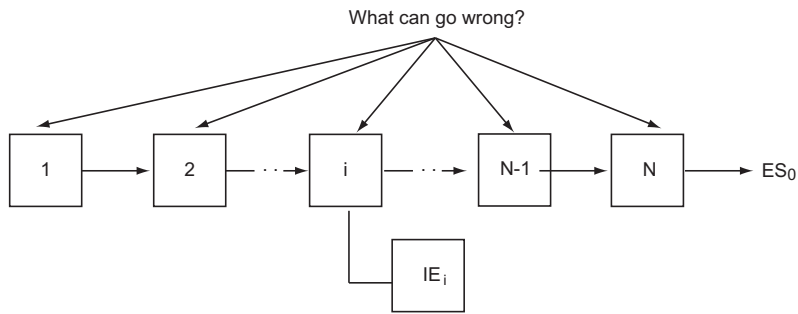


Figure 6.3: Identifying initiating events (adopted from Garrick, 2008).

### 6.2.1 Initiating event according to Kaplan and Garrick

Garrick (2008) explains initiating event both conceptually and methodologically by reference to Figure 6.2 and Figure 6.3. The first diagram depicts the *success scenario*,  $S_0$ , describing the functioning of a system when working as planned. After going through  $N$ , *as planned* events, this scenario leads to the successful end state,  $ES_0$ .

By asking *what can go wrong?* for every  $i; i = 1, 2, \dots, N$ , possible departures from  $S_0$  are identified and portrayed as in Figure 6.3. A prerequisite for answering this question is a proper understanding of the system and its interactions with the environment. Invaluable is also the aid of hazard identification methods like FMEA and HAZOP (Kaplan et al., 2001). The answers may range from equipment failure to natural events and intentional acts. What they have in common is that they all represent one or more initiating events. For some applications, *initial conditions* (IC) is considered a more appropriate term. A nuclear waste repository, for instance, is not so much threatened by initiating events as it is by a concurrent set of conditions, like annual rainfall.

The notation of initiating event signals that it initiates an accident scenario,  $S_i$ . Figure 6.4 illustrates that depending on the subsequent events, an initiating event may ramify into a range of possible end states,  $ES_i$ . Each path in this state space represents an accident scenario. Just as each IE can result in many end states, may different IEs end up at the same end state. Kaplan (1997) suggests that accident scenarios thus in principle can be identified either by inductive or deductive reasoning; by fault tree analysis of an end state or event tree analysis of an initiating event. The latter is by far the conventional practice according to Garrick (2008). Fault tree analysis serves in turn for quantification of IE-probabilities. IE thus constitutes the top event of the FTA and the initiating event in the ETA.

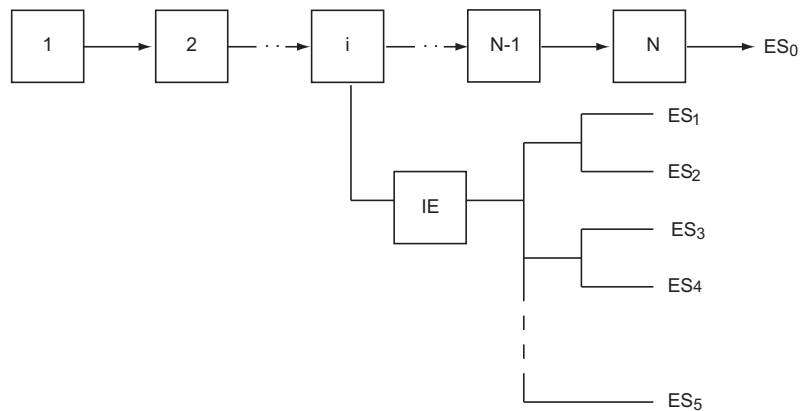


Figure 6.4: An initiating event may ramify into a range of end states.

### 6.2.2 Locating initiating events in the bowtie-diagram

Kaplan and Garrick's conception of initiating event is far from universal. An exceptional case is the methodology of ARAMIS (Delvosalle et al., 2006), reserving the term for the events farthest to the left in the fault tree analysis(!), that is, what is conventionally denoted *basic events* (USNRC, 1981). Following this nomenclature, initiating event denotes the most fundamental causes of a hazardous event. Consulting another source, Khan (2001) insinuates that initiating events are equivalent to our conception of hazardous event. Albeit these differences seem like terminological quibbling, they have distinct methodological implications.

The initiating events of Garrick (2008) are modeled in the event tree and may be stopped before they evolve into a hazardous event. For Delvosalle et al. (2006), they mark the most basic level of causal investigation and are thus excluded from the event tree. This is conceptually confusing, since what is denoted IE in the two frameworks may in fact be one and the same event, for instance, some operator error. Less ambiguity follows the practice of Khan (2001). This is because hazardous event is naturally situated at the center of the bowtie-diagram and not easily mistaken for events earlier in the event sequence. The problem is that Khan, like so many others, applies the notion of initiating event in subordinate clause and without further contemplation. Readers familiar with, for instance, Delvosalle et al. (2006) or Kaplan (1997) are thus likely to interpret the concept according to their own frame of references. This makes a certain recipe for inconsistency across analyses.

An obvious recommendation for ARAMIS is to replace *initiating event* by the term *basic event*. Khan (2001) is in the same manner advised to rather employ the term *hazardous event*. This is primarily to avoid confusion, but also because the above discussion implies that initiating event is a vague descriptor that in principle can be placed anywhere in the bowtie-diagram of Figure 6.5.

Further substantiation is given by Murphy et al. (2009) in a summary of their forthcoming guideline book on layer of protection analysis (LOPA). LOPA is a semi-quantitative tool for assessing the response of independent protection layers (IPL) to an initiating event in the process industry. The concept of initiating event is so central to LOPA that it makes the main topic of the coming book. According to Murphy et al. (2009), a key requirement is that the initiating event must be defined to lead to adverse consequences given the failure of all safeguards. From the examples

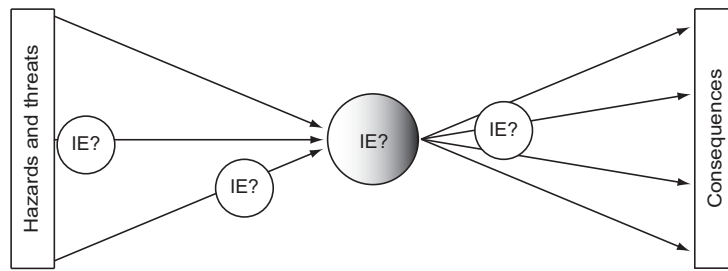


Figure 6.5: Initiating event can in principle be placed anywhere in the bowtie-diagram.

provided by the trio, it is clear that an initiating event may be either a hazardous- or a triggering event. Further clarification is sought in IAEA (1998), pinpointing that some initiating events might lead directly to a hazardous event, whereas a combination of subsequent events is needed if a number of barriers are in place for mitigation. Where in the bowtie-diagram the initiating event is located, is thus given by the nature of hazard and the safeguards under study.

### 6.2.3 Initiating event is a vague concept

If anything can be concluded from the above discussion, it is that initiating event is an analytical term that principally serves to mark the point of departure of your event tree analysis. To accentuate this point, it is tempting to redefine the concept in a circular manner; initiating is what marks the initiation of an accident scenario. This would be unfortunate, as the analyst is left with little guidance on where to start her analysis. In turn, it would also cloud our very conception of accident scenario. Nonetheless, it signals that for all other purposes but bounding an accident scenario, initiating event is a somewhat superfluous term. It is in the opinion of this author that the concepts of basic event, hazard, triggering event and hazardous event provide a less ambiguous terminology.

For the purpose of scenario structuring, initiating event remains a cardinal concept. Instead of merely mapping where it *might* be placed in the bowtie-diagram, one should thus ask where it *ought* to be. Garrick (2008) offers a principal advice in the point at which an otherwise normally operating system is upset. A problem is that this necessarily raises the question of what the “normal” sequence of events is. Not only does mapping the interactive operations of complex systems require extensive effort, but what is normal may in fact be departure from planned operations (Hollnagel et al., 2006). Adaptation to normal disturbances makes the paradigmatic basis of resilience engineering.

Putting these constraints aside, it seems a plausible inference that Kaplan and Garrick’s understanding of initiating event resembles Reason’s conception of triggering event. Where these are situated in the bowtie-diagram is pragmatically conditioned on the system and hazard under study. To suggest a more generic location, one is forced to question the very scenario approach to quantitative risk assessment. That prosecution is deferred to the concluding discussions of Section 6.4, while for now settling with initiating event as a concept given by departure from successful operation.

## 6.3 The termination of an accident scenario

The termination of an accident scenario is closely connected to the third definitional question *if it does happen, what are the consequences?* In Kaplan and Garrick (1981), the answer to this question is given in a measure of damage,  $X$ . This is not a single parameter, but a vector quantity that is both uncertain and time-dependent (Kaplan, 1997). The same  $X$  is by Garrick (2008) set equivalent to the end state of a scenario, which indicates that  $X$  and  $ES$  are actually one and the same thing. Even though this inference is disclaimed in the following, it certainly proves that the ending of a scenario depends on the consequences under consideration and *vice versa*. A key feature is the extent of which intervening, or *pivotal*, events to include in the event tree. This is intertwined with the issues of analytical purpose and what time frame to consider.

### 6.3.1 Adding a fourth question to the triplet definition of risk

Introductorily, it was noted that Haimés (2009) suggests adding a fourth question to the triplet definition of risk in *over what time frame?* Answering what can go wrong, he claims, has got everything to do with the timing of adverse effects. Haimés illustratively points to the diversity of consequences following the hurricane Katrina in 2005, ranging from loss of life, property and jobs to erosion of confidence in government and technology. Any meaningful assessment of future hurricane scenarios should according to Haimés include a similar vector of consequences. The challenge is that these outcomes not only differ in their temporal proximity to the initiating event, they also *continue* to evolve as a function of time and the vulnerability and resilience of the system. This can be illustrated by the recent tragedy at Haiti, where the number of reported fatalities continued to increase for many weeks after the initial earthquake. Whether one stops to measure the consequences immediately after the quake or when the last survivor is dug out four weeks later (Times, 2010), is thus decisive when assessing the risk of future disasters.

Kaplan and Garrick's conception of accident scenario is perplexed by the recognition that some consequences are revealed in considerable time after an initiating event. Does this mean that an accident scenario continues to evolve until the final consequences are manifest? The hurricane Katrina and the earthquake at Haiti indicate the justness of this supposition. Terminating an accident scenario without considering the timing of recovery actions would in the latter case be deluding, as many people died not in the initial quake but while waiting for help. A presumption is the existence of a certain point in time when survivors are no longer expected to be found, which serve as a natural endpoint of the scenario. In principle, this may be true also for damage to environment and property. Yet for more distant consequences, such as increased crime or loss of trust, the whole idea of setting a definite end state seems rather absurd. Not only may these in principle be of infinite regress, they also become less tangible (if ever) along with the temporal distance to a hazardous event. Although immaterial consequences are rarely considered in conventional risk assessment, they are determinative to authoritative priority setting on risk control (Hokstad and Steiro, 2006). More importantly, they raise a question that also concerns latent consequences to human health and the environment. Are scenarios of distant effects principally boundless?

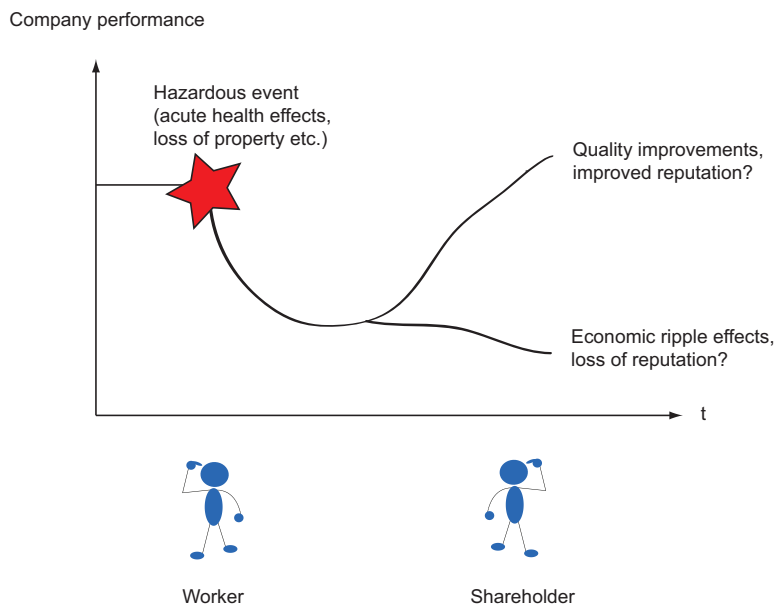


Figure 6.6: Different interest horizons following a hazardous event.

### 6.3.2 End states are not equivalent to consequences

The riddle of consequence timing encourages us to contest Garrick (2008) by demarcating end states from consequences. Following the recognition of Riker (1957), an end state is merely an *artificially* imposed situation that serves to bound an event or a sequence of events. A consequence on the other hand, is an ontologically realistic outcome to be measured from this state. The principal inference is that the timing of measurement need not coincide with that of the end state. Although a scenario is said to cease with the stabilization of an event sequence, the accounting of consequences may still take place at a later point of time. Especially important is this for hazardous events in potency of latent consequences. The increased rates of Thyroid cancer following the Chernobyl accident serve as a tragic reminder of this point (WHO, 2006). Notwithstanding the difficulty of envisaging the extent of distant outcomes, the tragedy demonstrates the importance of considering consequences subsequent to the stabilization of an identifiable sequence of events. Flipping the coin, one can suggest that the ending of a scenario is not principally a question of when to stop and measure the consequences, but what pivotal events are crucial to their undesired development.

### 6.3.3 Undesirability of outcomes and stakeholder interests

End states are in most literature described as a set of undesirable outcomes (see, e.g. USCG, 2000b; Rausand and Høyland, 2004). Due to the subjectivity inherent in the notion *undesirable*, this appears unfortunate at first glance. It does, however, perfectly coincide with the risk definitions of Rosa (1998) and Klinke and Renn (2002). If risk relates to consequences of what humans value, any modeling of consequences is necessarily determined by what is considered undesirable/desirable by *someone*. This is not to question the undesirability of, for instance, fatalities or financial loss,

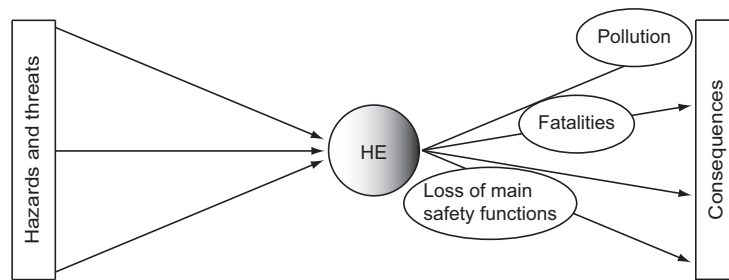


Figure 6.7: Risk acceptance criteria as determinative to scenario end state.

but a reminder of the importance of stakeholder interests to risk assessment. Figure 6.6 suggests that a worker might be most concerned with acute health effects, while a shareholder's prime concern are economic ripple effects. Many companies have gone bankrupt after experiencing a major accident, not necessarily due to immediate poverty loss but from loss of reputation (Hokstad and Steiro, 2006). Yet for other companies, liquidity might be improved in the long run as a result of reactive quality improvements or confident handling of crisis. In both cases is scenario extent decisive for judging the undesirability of an outcome. This implies that what end state to consider depends on the commissioning party, by virtue of setting the purpose of analysis.

### 6.3.4 The end state is given by the purpose of analysis

The objective of risk assessment is not only a function of a decision maker's interest, but also of regulatory requirements. The Petroleum Safety Authority in Norway, for instance, requires operators to compare the results of risk assessment with a pre-defined set of risk acceptance criteria (PSA, 2001). Among the required criteria are measures of fatality, pollution and loss of main safety functions. Since these are differently located in the progression of an accident scenario as suggested in Figure 6.7, the end points will differ accordingly (NORSOK Z-013, 2001). The most common measure for environmental pollution is damage duration, that is, the recovery time from a spill occurs until restoration has been completed. When calculating this measure, the end state is given at the point of complete restoration (Vinnem, 2007). For fatalities the picture is not so clear-cut, as no guidance is provided on which pivotal events to include in the counting of fatalities. Should one stop the analysis when people lie in the water or after a series of rescue operations?

USCG (2000b) offers a solution by modeling the succession of one and the same hazardous event over two event trees. The first models the onset and development of a fire. If not extinguished, the fire will lead to an end state of people in the water. From that state yet another tree is drawn, modeling events and conditions (e.g., water temperature and the presence of other vessels) that determine the success of rescue prior to Hypothermia. Whereas the former serves for evaluation of defenses against fire, the latter assesses the efficiency of the United States Coast Guard's rescue operations. The accident scenario can either be seen as a prolonged path from the beginning of the first diagram to the end state of the second, or as two or more scenarios determined by two different end states.

What this all boils down to is the necessity of choosing an end state relevant for



the study's purpose. As such, it appears a feasible suggestion that an accident scenario follows the entire sequence but can be partitioned in two parts. One follows a hazardous event through the lines of reactive barriers, and the other the subsequent recovery actions. The former normally lies within the scope of risk analysis, while the latter is covered by emergency and preparedness analysis (EPA) (NORSOK Z-013, 2001). An alternative division can be made between analyses of risk and vulnerability, as is suggested by Einarsson and Rausand (1998) in Figure 2.2. Where to draw the line might still be unclear, as all modes of analysis are closely interconnected. The interested reader may consult NORSOK Z-013 (2001) and DSB (2010) for guidance on performing risk analysis as basis for EPA and vulnerability analysis.

### 6.3.5 Maximum-credible accident scenarios

The U.S. Environmental Protection Agency recommends emergency plans to be based on *worst-case scenarios* (Khan, 2001). Considered are typically maximum short-term consequences of instantaneous release of a large amount of a chemical, assuming the failure of all mitigation systems. This is according to Khan (2001) an unfortunate confinement, as the approach not only de-emphasizes the probability of scenario occurrence, but also disregards possible domino effects over a longer time frame. As an alternative, Khan introduces the principle of *maximum-credible accident scenarios* (MCAS), requiring a scenario to be within the realm of possibility (i.e. have a probability higher than  $10^{-6}$  per year) and have potential to cause significant damage (i.e. at least one fatality). In order for emergency plans to be effective, they shall be based on the most realistic paths of escalation and address multiple parameters of damage. Khan admits a conceptual weakness in that scenario escalation is a hitherto neglected topic that lacks solid theoretical basis. One can furthermore speculate whether the MCAS-approach is basically a variant of the expected value-conception of risk. Although its ingeniousness can be contested, Khan (2001) offers a principal point in how scenario extent and selection influence the mode and use of risk assessment- and vice versa.

### 6.3.6 Uncertainty at the point of further ramification

Accepting that the end state must fit the purpose of analysis shatters the hope of any imperative termination of accident scenario. This recognition makes an important premise, but should not deter us from seeking general advice on the subject. One recommendation is offered by IAEA (1998), stating that event trees should be developed only up to the point where the nature of event sequence is uniquely determined. This implies that a scenario should not proceed in the absence of discrete pivotal events of clear sequential ordering. A contrary example is the scenario projections of IPCC (2007) on anthropogenic climate change. These are based on continuous emissions and distant human and natural responses, which would yield considerable uncertainties if modeled in an event tree. The scenarios are instead derived from advanced models of physical simulation.

Also Garrick (2008) is concerned with the issue of uncertainty, pinpointing that the farther one extends an accident scenario, the more uncertain are the results. This is one of the main reasons why *core damage frequency* (CDF) is the most common measure of nuclear power plant risk. Compared to calculating the probability of radiation health effects, one is much more confident if stopping the analysis at the point of core damage. Despite this obvious advantage, Garrick prescribes caution in

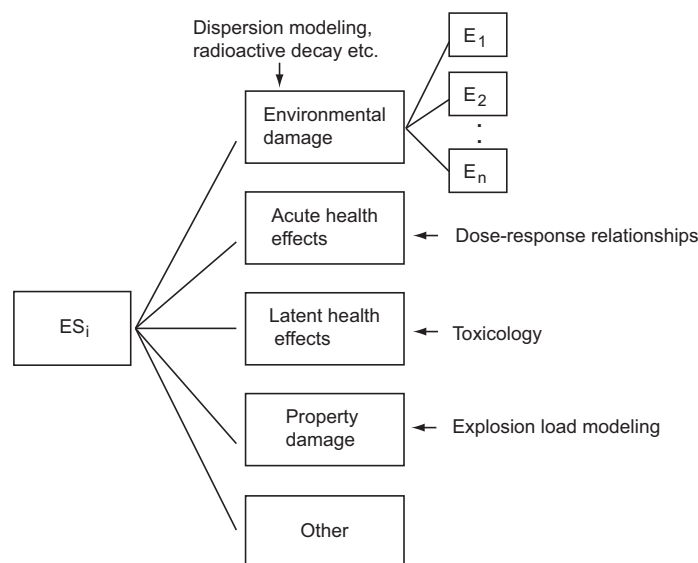


Figure 6.8: Cutting of the event tree at the point where specific modeling expertise is required.

letting surrogate endpoints like CDF reflect consequences further out in the event chain. The reason is that downstream risk measures might be inversely affected by a reduction in the precursor. Depending on the means by which core damage frequency is lowered, the frequency of secondary containment and fatalities might actually increase. This calls for a holistic approach in understanding the coupled processes between endpoints at different stages of scenario development. As such, Garrick (2008) finds it necessary to trade confidence with coherence in extending the scenario for further development. What further complicates the picture is that a whole treeful of end states reside within each category. Core damage actually includes a spectrum of damages, as do health effects in ranging from acute fatalities to latent injuries and cancer deaths. This not only challenges the logical construction of event trees, but also how different damage states are collocated and compared.

An attractive fix is presented in Rasmuson (1992), cutting of the scenario at the point at which specific modeling expertise is required for dispersion, dose-response relationships and so on. Ending the scenario within the competence radius of the risk assessor is a sensible idea, since extension beyond this point would introduce an obvious source of epistemic uncertainty. It will also improve the manageability of analysis, as the vector of consequences could possibly emanate from a common node as depicted in Figure 6.8. It should be noted that the modeling efforts exemplified in this figure enter into many of the same boxes; assessment of acute health effects, for instance, also requires dispersion modeling of the reach of exposure (Leeuwen and Vermeire, 2007). Rasmuson further recommends constructing event trees with enough detail to partition short-term and long-term damage sequences, while admitting that this is difficult to achieve in practice. Notwithstanding this, it is cardinal to note that any meaningful comparison across sets of scenarios presupposes that the end states are cut off at the same level.

### **6.3.7 Terminating the accident scenario**

Three main inferences can be drawn from the above discussion on scenario end states. The first is that if the concept of initiating event is ever so vague, the termination of a scenario is even more difficult to establish. Secondly, this owes to the inference that what end state to consider is ultimately a question of purpose. This can be seen to work at two levels; implicitly through the selection of relevant consequences and their timing, and explicitly in the relevancy of pivotal events. Central to the former are stakeholder interest and regulatory requirements. The latter is pragmatically determined by the system or unit under analysis and the hazardous event. For example, it may be adequate to model the efficiency of a technical system's response to a specific hazardous event up to the breaching of the final reactive barrier. Vulnerability or EPA analyses on the other hand, gain from extension to the very last recovery action or the point of final restoration. This is pinpointed in the illustration of Einarsson and Rausand (1998) in Figure 3.4. The figure also implies that it takes more than one bowtie-diagram to contrast varying end-states, as the bowtie's end by default marks the termination of the accident scenarios.

What further complicates the picture is the interconnectedness between all types of analyses. Especially trenchant is this when constructing scenarios of security threats, as the initiating event is in itself a complex of the adequacy and extent of anticipated responses and vulnerability (Garrick et al., 2004). In an ever uncertain future, this is restricted by our third and most general conclusion; any scenario should end when further development of the event tree is unfeasible. Adapting the recommendation of IAEA (1998), the reader is advised against developing a scenario beyond the point at which relevant branches may be uniquely identified and sequentially ordered. This is not to say that consequences beyond this point are disregarded. An end state is not a consequence in itself; it is the point from which consequences are measured- either instantaneous or in latency. Rather, it restrains us from introducing further uncertainty by extending the scenario beyond the knowledge of the risk assessor. It is nevertheless important to carry on the advice of Garrick (2008), stressing that sole reliance on surrogate endpoints may yield counterproductive measures. This calls for holistic and careful evaluation of consequences that ramify at different end points in the sequence of events.

## **6.4 Is accident scenario a sound concept?**

Accident scenario is an intuitive concept, which after closer examination rises as a complex of vaguely defined initiating events and pragmatic end states. Focus has hitherto been on the extent of a scenario, in search of a canonical starting point and a clear finishing line. Although a handful of advice and quite a number of cautions are promoted, the closest one comes to a grand conclusion is probably that accident scenario is not subject to universal bounding. While this need not be a bad quality, it certainly offers a pretext for questioning the necessity of employing this vague concept. The soundness of the concept of accident scenario is therefore contemplated in this final discussion, first from a conceptual standpoint and then in light of practical risk assessment and the understanding of its results.

### 6.4.1 Refining the triplet definition of risk

The task of finding, organizing and categorizing accident scenarios is according to Kaplan (1997) part science and part art. Subsequent to the seminal paper of Kaplan and Garrick (1981), this systematic process has been titled *Theory of Scenario Structuring* (TSS). Within it are well-known methods like FT, ET, FMEA and HAZOP, along with unconventional methods like Anticipatory Failure Determination (AFD) (see, e.g. Kaplan, 1997). TSS is thus not a specific method or theory, but a general perspective for envisioning and tracking the effects of hazards and threats on a system (Kaplan et al., 2001). One can say that accident scenario is the end, TSS the means and the triplet definition of risk the motivation. The concept of accident scenario makes a constituent part of the triplet definition of risk, which in turn guides the structuring and quantification of scenarios. Transferring this link into practice has shown that the concept of accident scenario is not without flaws.

A principal problem stems from the recognition that different methods within TSS can lead to different sets of scenarios for the same underlying problem. Kaplan et al. (2001) admit that this is conceptually awkward in light of the triplet definition of risk. To eliminate this awkwardness, the trio finds it necessary to refine the original definition of risk by making explicit three requirements that have formerly been implicit. That is, that the set of accident scenarios used in a quantitative risk analysis shall be:

1. Complete, in the sense that the set contains all possible scenarios.
2. Finite and denumerable, which is a presumption for making a table as in Table 2.1.
3. Disjoint, meaning that  $S_i \cap S_j = 0$ , in order to sum the probabilities over all scenarios.

The issue of completeness has haunted the triplet definition since it was originally introduced in Kaplan and Garrick (1981). Back then, the authors answer to a critique of the *Wash-1400 report*, objecting that since the listing of scenarios in reality is infinite, no risk analysis can ever be complete. To improve the formalism of risk analysis, Kaplan and Garrick introduce an “other” category,  $S_{N+1}$ , representing all scenarios not otherwise included. The set of scenarios is now logically complete as this remainder can be assigned a probability. This is not further pursued in Kaplan (1997), where an alternative solution is suggested by adding a  $c$  to the set of triplets:

$$R = \{ \langle s_i, p_i, x_i \rangle \}_c \quad (6.1)$$

The refinement is to emphasize that risk by definition is the complete set of scenarios. This signals the importance of identifying if not all, at least those that are most important. Kaplan et al. (2001) agree with this rationale, but find it incompatible with the variances seen in practical scenario structuring. How can the scenarios be complete if every man comes up with his own set to the same problem? The suggested solution is yet another refinement to the triplet definition of risk:

$$R = \{ \langle s_\alpha, p_\alpha, x_\alpha \rangle \}, \alpha \in A \quad (6.2)$$

In essence, the subscripts convey that the *actual* set of scenarios is neither finite nor denumerable as is implied in the original definition. Whereas the quality of completeness naturally holds, they are as continuous and non disjoint as any aspect of

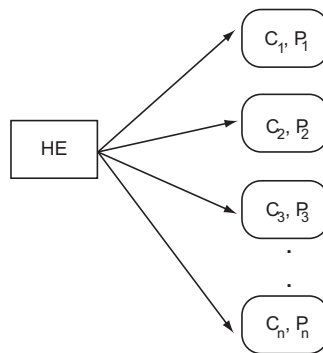


Figure 6.9: Consequence spectrum following a hazardous event.

reality (cf. Riker, 1957). The scenarios of risk analysis are only approximations to this *true* set of scenarios, which is partitioned into complete, finite and disjoint subsets. This takes the ontological troublesome idea of a finite set of scenarios out of the definition of risk. In the same turn, it justifies that different methods yield dissimilar scenarios, as they are simply different approximations to the same underlying truth. According to Kaplan et al. (2001), this is both conceptually and practically satisfactorily.

Although the refined definition of Kaplan et al. (2001) might be conceptually satisfactorily, it is ultimately a recognition of the omnipresent uncertainty in the scenarios you fail to envisage. The epistemological foundation of Kaplan and his associates resembles the position of Rosa (1998), where risk is interpreted as a real world phenomenon to be separated from our subjective knowledge of it. Rosa makes a crucial point in that all approximations are not equally good representations of the truth. Since any risk analysis is only as good as the set of identified set of scenarios, this implies the benefit of applying diverse techniques for scenario identification. Chiefly, this holds for the identification of initiating events, but also for what pivotal events are considered relevant for further ramifications (Garrick, 2008).

Kaplan and Garrick refrain from admitting any other weaknesses of the concept of accident scenario. Funnily enough, this is also true for the contrary; compelling arguments for why accident scenario is such a fundamental concept remain notably absent. Instead, it is launched as a given companion to the triplet definition of risk. What is further remarkable, is the scarcity of focused discussions amongst those who have adopted or disclaimed the triplet definition of risk, like the otherwise conceptually engaged Aven (2010b). One means for initiating such a discourse is to contrast the scenario approach to risk assessment with the practice of NORSOK Z-013 (2001).

#### 6.4.2 Contrasting the scenario approach to risk assessment

The conventional approach in the Norwegian petroleum industry is to calculate risk relative to a set of hazardous events. For referential purposes, this is denoted the *NORSOK Z-013 (2001)-approach* in the current study. NORSOK Z-013 (2001) lists a set of hazardous events<sup>1</sup>, which shall, as a minimum requirement, be considered to

<sup>1</sup>NORSOK Z-013 (2001) uses the term *accidental event*, which is equivalent to our conception of *hazardous event*. Following the argumentation in Section 5.5, the latter is consistently applied in the following, even when in direct reference to NORSOK Z-013 (2001).

Table 6.1: Presentation format of risk relative to a set of hazardous events (adapted from Rausand and Høyland, 2004).

HE	Pr(HE)	Loss of lives			Material damage			Environmental damage		
		Pr(C <sub>1</sub> )	Pr(C <sub>2</sub> )	Pr(C <sub>n</sub> )	Pr(C <sub>1</sub> )	Pr(C <sub>2</sub> )	Pr(C <sub>n</sub> )	Pr(C <sub>1</sub> )	Pr(C <sub>2</sub> )	Pr(C <sub>n</sub> )

the extent they are applicable. Amongst these are:

- Blowouts
- Process leaks, unignited and ignited
- Collisions
- Falling/swinging objects
- Structural collapse
- Loss of stability

For each hazardous event, a probability,  $\Pr(HE_i)$ , is assigned and a spectrum of consequences identified (Vatn, 1998). The consequences are uncertain and describable by a joint probability density function,  $\Pr(C_1, C_2.. | HE_i)$ , given the occurrence of a hazardous event. Alternatively, this may be written as a vector of consequences and their associated probabilities,  $[C_1, C_2..C_n]_{[p_1, p_2..p_n]}$ . The risk of each hazardous event can then be described as:

$$R(HE_i) = \Pr(HE_i) \cdot [C_1, C_2..C_n]_{[p_1, p_2..p_n]} \quad (6.3)$$

To get a description of the total risk picture, the risk associated with every hazardous event may furthermore be summarized and compiled. With reference to the discussion on expected value in Section 2.4, caution is urged when summing up risk in this manner. Another difficulty is that only consequences of similar dimensions are summarizable (Rausand and Utne, 2009b). Although summation is required for comparison with overall risk acceptance criteria (Vinnem, 2007), it is for many purposes satisfactory to view the consequence spectrum in its entirety as in Figure 6.9. A feasible presentation format is shown in Table 6.1. It is inspired by Rausand and Høyland (2004), portraying the consequence spectrum of each hazardous event and the associated probabilities. The consequences are, by example, split into three categories of  $n$  uniquely defined subcategories. Within the category “loss of lives” can, for instance,  $\Pr(C_1)$ , correspond to one fatality. The table perfectly answers the three questions of Kaplan and Garrick (1981) and is hence adequate at least from a definitional point of view.

### 6.4.3 Two main differences

Table 6.1 is not surpassingly different from Table 2.1 as presented in Kaplan and Garrick (1981). Principally, the approach of NORSOK Z-013 (2001) is nor very distant to

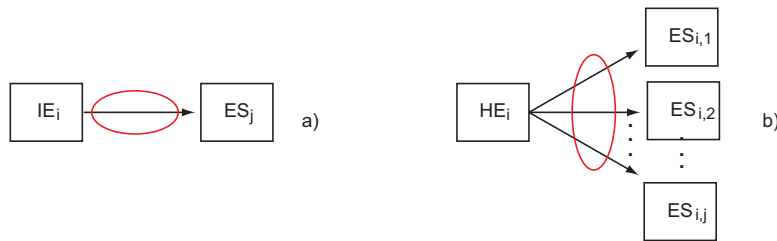


Figure 6.10: Comparing (a) the scenario approach to risk assessment with the framework of (b)NORSOK Z-013 (2001).

the scenario approach of Garrick (2008). Both derive a set of consequences from one or more initiating events, and for one and the other are pivotal events determinative to this purpose. Event tree analysis is central to both approaches. The single apparent difference is that the former considers each path individually, whereas the latter looks at the joint set of paths. There are, however, at least two principal dissimilarities as this author sees it.

### Pairs vs. sets of consequences

The first is that while the results of Garrick (2008) are given in *pairs* of initiating event and consequence, the approach of NORSOK Z-013 (2001) yields a *set* of consequences for each hazardous event. In the former, consequences are typically understood as events, while the latter represents consequences as random variables (Vatn, 1998). This is not to deny the multidimensionality of damage in the framework of Kaplan and Garrick (1981), but a representational difference in the linking of initiating events and end states. Figure 6.10 illustrates this in terms of one-to-one and one-to-many relations respectively. Whereas the former renders it easy both to calculate and track the probability of each pair, the latter yields a large and more intractable set of consequences and their associated probabilities. On the positive side, this will give a neater and more systematic list as each hazardous event is presented only once.

### Departure from normal operation vs. hazardous event

A second difference lies in the starting point of the event tree. The distinction is depicted in the bowtie-diagram of Figure 6.11. By following the practice of Garrick (2008) and starting the scenarios at departure from successful operation, some of the succeeding paths may not evolve into a hazardous event. It is also likely that different initiating events give rise to one and the same hazardous event. Both have the unfortunate implication that the identified sets of scenarios end up unnecessarily large.

Starting the event tree analysis at the point of hazardous event will avoid this problem, as one considers only those paths leading to damage if not controlled. What Kaplan (1997) denotes initiating events are instead included in the causal analysis of a fault tree, in a similar way, but with a different terminology than Delvosalle et al. (2006). This appears more conceptually and practically satisfactorily. Not only does it carve up a line between cause and effect (cf. Pearl, 2000), offered is also

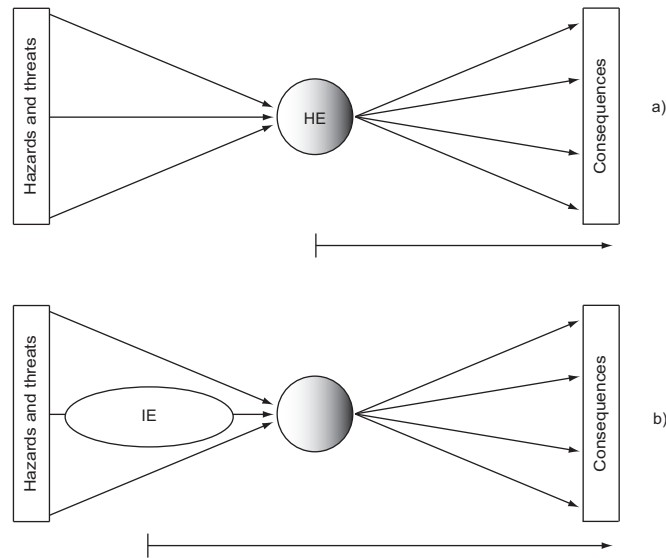


Figure 6.11: Comparing (a) the scenario approach to risk assessment with the framework of (b)NORSOK Z-013 (2001).

a more focused means for identifying hazardous events. Further substantiation is sought in the perspective of Reason (1990b). Since one and the same hazardous event can be triggered by a vast number of initiating events, a leaner analysis is achieved by banishing these sporadic causal factors to the causal analysis. It also indicates that scenario completeness can be easier claimed, as there are fewer means of hazardous realization than the almost indefinite variants of initiating events.

#### 6.4.4 Simple, but extensive calculus

Computationally, the scenario approach to risk assessment is comparatively straightforward. This is because one in principle arrives at only one probability per scenario, that is,  $Pr(AS_i)$  (Garrick, 2008). Since a scenario consists of a single initiating event and a corresponding end state, each pair is assigned a probability based on the initiating event and branch point probabilities (cf. Figure 6.1):

$$\Pr(AS) = \Pr(IE) \cdot \Pr(\bar{A} | IE) \cdot \Pr(\bar{B} | IE \cap \bar{A}) \cdot \Pr(C | IE \cap \bar{A} \cap \bar{B}) \quad (6.4)$$

Equation 6.4 is strikingly simple in comparison with Equation 6.3, due to the feature that only one end state is under consideration at the time. The approach of NORSOK Z-013 (2001) deals with a vector of end states that each has a different probability. To calculate the risk of each hazardous event, the various end state probabilities must thus be collocated. This is arguably a more arduous task. There are, however, at least two reasons why one should not jump to the conclusion that the scenario approach is computationally superior. Firstly, it necessitates a considerably longer list of issues to be quantified. Although each scenario is easily quantified, the list of scenarios undergoing this operation is contrastingly large compared to the approach of NORSOK Z-013 (2001). This is not only because each scenario calls for separate consideration, but also on the grounds that more and larger event trees are likely to follow when initiation is set prior to the level hazardous event. The paths not



leading to a hazardous event and/or undesirable end states are naturally screened out for calculation. Beyond that, little advice is offered for abridging the list of scenarios. This relates to a fundamental dissension within risk evaluation. Shall one prioritize the scenarios that are most severe or those that are most probable? Clear-cut advice is rendered difficult as these two dimensions are generally inversely related, ultimately displacing the issue from one of practicality to the realm of ethics (Shrader-Frechette, 1991).

Whether the prolonged list offsets the benefit of simple calculus is difficult to demonstrate, as it is likely to differ with the extent of both hazardous events and the range of possible end states. It can be suggested that few hazardous events combined with large spectra of end states favors a scenario approach. This is because the list of scenarios is left relatively short compared to the number of columns that would have to be included in Table 6.1. The more hazardous events, the more incalculable becomes the list of scenarios, and the more advantageous is the approach of systematic handling by each hazardous event.

A more perplex objection owes to the difference between end states and consequences as revealed in Section 6.3. Although it is conceptually unproblematic that each scenario is determined by a single end state, this is muddled by the observation that consequences and end states are treated as synonymous. This owes to the recognition that consequences are, as is repeatedly stressed by Kaplan and Garrick (1981), multidimensional vectors that are time-dependent and uncertain. As such, the authors render it unclear whether the second question of *how likely is it?* in fact refers to the probability of the aggregate consequences, a single consequence or even the initiating event. The approach of NORSOK Z-013 (2001) is still more comprehensive, as multiple end states are considered in addition to the issue of multidimensionality. Yet, this seems to reaffirm that none of the approaches can be acclaimed computational sovereignty.

#### 6.4.5 Disjointness

A challenge that seems to riddle both approaches is the requirement of disjointness. This is not troublesome to the purpose of identifying scenarios or consequences, but makes a fundamental premise for summarizing consequence probabilities (Kaplan et al., 2001). Probability theory tells us that the probabilities of two non-disjoint events cannot simply be added without considering the areas that overlap (Lindley, 2006). Hence if two or more paths in the event tree(s) coincide, simple summation of the probabilities will result in double counting in the overall probability. Typically, this occurs when single consequences are caused by several initiating or hazardous events (Gowland, 2006). The former is more easily avoidable within the scenario approach to risk analysis, as each end state is explicitly determined by a corresponding initiating event. Each pair is thus in principle a disjoint path in the event tree. The approach of NORSOK Z-013 (2001) is presumably more prone to double counting, as the various end states are not only grouped, but may also evolve from tangled hazardous events. A specific consequence may furthermore appear in several rows in Table 6.1, which urges caution if summarizing the risk over all hazardous events. The latter point holds, however, also for the approach of Kaplan and Garrick (1981). Although each path in a single set of scenarios (i.e., one event tree) is conceivably disjoint, may different *sets* of scenarios overlap. Not only can different sets lead to the same consequences, the single scenarios are in fact based on categories of initiating events that call for similar responses (Garrick, 2008). A likely result is that

nondisjointness is left hidden under a range of assumptions.

It should finally be remarked that although disjointness is a desirable feature, Kaplan et al. (2001) acknowledge that a modest amount of nondisjointness can be tolerated as its primary impact is conservativeness in the results.

#### **6.4.6 Presentation of results and central risk contributors**

The answers to the triplet definition of risk may according to Kaplan and Garrick (1981) be given in the format of Table 2.1. For pictorial representation, the risk curves of Figure 2.4 are recommended on the grounds that single numbers are insufficient for communicating the concept of risk. The curves (labeled *complementary-cumulative-distribution-functions*) are constructed by ordering the scenarios of increasing levels of damage and cumulating the respective probabilities. In the later work of both Kaplan (1997) and Garrick (2008), the tabular format is left unmentioned to the advantage of risk curves. To fully communicate a risk story, Garrick (2008) prescribes not only single curves or families of curves, but also different representations of families of curves. An extensive amount of modeling and analysis is integrated and assembled in the representation of risk curves. This is an obvious merit but also a pitfall, as it allows assumptions and major risk contributors to be buried in the presentation format.

It is not the intention of this author to evaluate the adequacy of risk curves in representing the results of quantitative risk assessment. This owes to the recognition that risk curves in principle can be employed also to the HE-based approach, and is hence not a distinguishing feature to the concept of accident scenario. If anything, this begs us to twist the argument and ask whether the approach of NORSOK Z-013 (2001) offers any distinct representational advantages.

Defining risk relative to hazardous events provides a unique means for identifying those hazards that contribute most to the overall risk picture. By summing the risk of each hazardous event as suggested in Equation 6.3, the relative contributions of, for example, process leaks and blowouts may be explicitly shown. Particularly advantageous is this for decision making on allocation of risk reduction measures, which lies at the core of risk management (Kjellén, 2000). The same does not hold for the approach of Kaplan and Garrick (1981), as each hazardous event may enter into a variety of scenarios without systematic consideration of its contribution to the overall risk. A possible variant is to compare the relative contribution of each initiating event. Yet, with reference to the above discussion and the framework of Wagenaar et al. (1990), this appears both cumbersome and counter-productive.

Garrick (2008) admits that risk curves in many cases obscure the relative effect of risk contributors. This is not, however, considered a major deficiency since most risk assessment software packages contain algorithms for ranking various contributors. It is still in the opinion of this author that the approach of NORSOK Z-013 (2001) has an advantage in the structured consideration of each hazardous event. Offered is not only a better basis for evaluating local risk, but also a well-arranged representation of the total picture. Both considerations are essential in decisions on risk acceptability (HSE, 2001).

#### **6.4.7 Conceptual soundness and practical superfluity**

Contrasting the scenario approach to risk assessment has indicated some few deficiencies of the concept of accident scenario. These are principally of pragmatic

character, such as the lacking of a systematic means for structuring results and displaying major risk contributors. A conceptual weakness is pinpointed in the initiation of a scenario at the level of triggering event. This not only implies that the event tree analysis becomes unnecessarily large, but also casts doubt upon our ability to achieve reasonable completion of the list of scenarios. On the positive side, the scenario approach gains in simple calculability. The probability of each scenario is easy to calculate and the corresponding end state simple to track. Disjointness is considered a more attainable quality following this approach, albeit caution is advised for summarizing the results of both approaches. Especially important is this when the sets of scenarios become numerous, which also makes the task of summarization almost insurmountable.

Summarizing these pros and cons yields no clear answer to whether accident scenario is a sound concept. The refinements to the triplet definition of risk suggest that the implicit requirement of the set of accident scenarios to be complete, finite and disjoint is conceptually challenging. Principally, this requirement should hold also for the approach of NORSOK Z-013 (2001), although the latter quality is somewhat difficult to conceive. Compared to this approach, it is in the opinion of this author that the concept of accident scenario gains in comprehensibility. It is perfectly suitable for communicating a critical course of events, like the possible developments following the recent blowout at an oil drilling platform in the Gulf of Mexico. This is, however, not to say that accident scenario is by default a communicable concept to decision makers. The longer the list of scenarios grow, the less do the numbers speak for themselves and the greater becomes the need for structural representation to provide meaningful input to decision makers.

The principal flaw of the concept of accident scenario remains in the diffuse definitions of initiating event and end state. When the analytical bounding is that vague, inconsistency across analyses is likely to follow. A promising refinement is to displace the start of each scenario to the point of hazardous event, as is inspired by the approach of NORSOK Z-013 (2001). Still, little inspiration is offered on where to stop the event tree.

Is the concept of accident scenario satisfactory and necessary for answering the triplet definition of risk? It is in the opinion of this author that the answer to this query is no. Also the approach of NORSOK Z-013 (2001) fits the definition of Kaplan and Garrick (1981) well, principally without ever having to employ the ambiguous notation of *accident*. It is, however, not the intention of this study to dismiss the scenario approach to risk assessment as extensively employed by disciples of Kaplan and Garrick (1981). Rather, it endeavors to call for awareness and discourse on the conceptual and practical implications of the concept of accident scenario.

## 6.5 A refined definition of accident scenario

As an initiative to further reflection, a refined definition of accident scenario is herewith suggested:

**Accident scenario:** A sequence of events from the hazardous event to a uniquely determined end state of relevance.

The definition of IMO (2002) is adapted to include a less ambiguous description of scenario extent. Firstly, the vague term *initiating event* is replaced with the more

conceptually clear notion of *hazardous event*. Scenario termination is then specified by compressing the most general advice of Section 6.3. It signals that the ending of a scenario is determined by the purpose of analysis, but should never be defined beyond the point of discrete ramifications. The latter makes a clarifying but disquieting specification, as it not only dismisses the concept of accident scenario for continuous or ambiguously defined event sequences, but also shakes the analytical bedrock of this study- the bowtie diagram.

## Chapter 7

# Epilogue

Numerous years of risk talk at cross purposes have led Stan Kaplan to formulate two theorems on communication (Kaplan, 1997, p.408):

- Theorem 1: 50 % of the problems in the world result from people using the same word with different meanings.
- Theorem 2: The other 50% come from people using different words with the same meaning.

When Kaplan finds himself in times of trouble, the theorems provide an effective means for focusing and draining out the emotions of any scientific dispute. The present study indicates that all risk scholars should follow the example of Kaplan and post the theorems on their office walls. An obvious case of the first theorem is the numerous conceptions of *risk*, while the second is demonstrated in the plethora of names referring to what this author denotes *hazardous event*. Researchers, practitioners and regulators use the words of risk assessment differently and inconsistently. Not only does this preclude communication internally and across analysis teams, it may also lead to erroneous applications of methods and inexpedient use of results. By shedding light on the following concepts and challenges, this study has demonstrated the importance of striving for a clear and consistent terminology on the foundations of risk assessment:

- *Risk*: A vast number of theorists and standards seek to describe and define risk. Some are contradictory, while others separated by wordily nuances. Defining risk urges contemplation on fundamental questions of ontology and epistemology, which in turn directs the understanding of results from risk assessment. Although the quantitative definition of Kaplan and Garrick (1981) is commonly accepted, it is very capacious and in need for interpretation. Each analyst's interpretation of the three questions conducts the risk assessment process in significant matters.
- *Counterconcepts to risk*: An alternative means to conceiving risk is to explore its related concepts of uncertainty, safety, security, vulnerability and resilience. Some are complementary or to some degree antonymous, while others are considered a constituent part of risk. Whether one considers, for example, uncertainty and vulnerability as embedded in the triplet definition of risk, influences the presentation of results and the modeling of scenario extent.

- *Risk-informed decision making*: The purpose of risk assessment is to provide decision support. Both the application and results of risk assessment shall be tailored to this purpose, through stakeholder involvement and managerial review. This presupposes good communication and that stakeholders and decision makers understand the principles and results of risk assessment. A diffuse nomenclature precludes deliberation and ultimately, the provision of relevant risk insights.
- *Hazards and events of release and causation*: A set of terminological knobs is essential for guiding the identification of hazards and the potential modes of release. The redundancy of terms describing the midst of the bowtie-diagram represent a clear case of Theorem 2. This is confusing to the analyst and hinders comparison across analyses. The choice of words in causal analysis reflects the aetiology of accidents and has significant implications both on the calculability and controllability of risk.
- *Accident scenario*: It is a true paradox that the perhaps most central term to Kaplan and Garrick (1981) is also the less elaborated. Both the concept itself and the terms that serve to bound it are somewhat circularly defined. The modeling of scenario extent is thus pragmatically conditioned in both directions. While analytical freedom is not necessarily a bad thing, it seems like nothing but vagueness is lost by confining the scenario by hazardous event and the point of no further ramifications.

A general search in ScienceDirect yields 1,504,020 replies to *risk*. These are not all of relevance to our quest, but they do reflect the central role the concept has come to earn in the scientific literature. Although this study has shown that risk is an utterly contested concept, it is all the same a mature topic. This is precisely due to the many definitional disputes and philosophical contributions of an eminent band of researchers. The same holds for the second question of Kaplan and Garrick (1981), which has been subject to intense academic debate regarding the proper interpretation of probability in risk assessment. Albeit contentious issues still remain, a broad understanding has accumulated on the characteristics and fallacies of these fundamental concepts. It is in the opinion of this author that we have come to a point where other issues urge the attentional capture of the scientific community.

The present study reveals that the common counterconcepts to risk are relatively well explored, as are also the concepts of hazard and triggering event in the framework of Tripod. This is not the case for the concept of accident scenario. Although many practitioners and researchers embrace the scenario approach to risk assessment, few have contemplated this foundational concept in a focused and constructive manner. The discussions indicate that the analyst's conception of accident scenario is utterly decisive to risk assessment. This should serve as a motivation and starting point for further scientific exploration. Especially trenchant is the need for theoretical maturing on the issue of scenario extent. Scenario extent is in this study discussed in light of the linear bowtie-model of accident risk. An interesting topic for further research is the relevancy and extent of accident scenario within recent paradigms of dynamic systems. Most imminent is, however, the need for reconciling the call for clear specification with the recognition that scenario extent is ultimately given by the purpose of analysis. At the heart of this enigma lies the challenge of balancing stakeholder concerns with the analyst's need for pragmatic procedures and the decision maker's call for consistent and communicable results. This is both

a normative and methodological issue. Arguably, it calls for contextual and ethical awareness on behalf of every risk analyst. Yet most important, it urges procedural improvements and further academic discourse on how analysis and deliberation best can be integrated in practice.

A harmonized terminology will facilitate in resolving the above challenges. Developing an agreeable conception of accident scenario necessitates clarification of central concepts of initiation, hazardous release and termination. In the same manner does focused deliberation presuppose shared understanding of central words and concepts. Sadly, if one overall finding stands out from the present study, it is that this is certainly not the case today. It must be admitted that striving for a unifying nomenclature seems overly ambitious at this moment. Although this author believes that semantic pragmatism is a nuisance that should be fought, the communication theorems of Kaplan (1997) are particularly important until we reach that point. Awareness to the fact that people associate similar words with different meanings provides a simple buffer to communication problems in deliberation and analysis of risk. Guarding definitional distinctions becomes a premise, but also a challenge as the decision maker is left with the task of final interpretation. The paralyzing risk of volcano ash clouds signifies that resolving these issues becomes increasingly important in a future of ever more complex decisions about risk.

# Bibliography

- Adams, J. (1995). *Risk*. UCL Press, London.
- Adger, N. (2006). Vulnerability. *Global Environmental Change*, 16:268–284.
- Adler, M. (2003). Risk, death and harm: The normative foundations of risk regulation. *Minnesota Law Review*, 87:1293–1446.
- Aftenposten (2010). *Chile var godt forberedt*. Available at <http://www.aftenposten.no/nyheter/uriks/article3543064.ece>.
- Amendola, A. (2001). Recent paradigms for risk informed decision making. *Safety Science*, 40:17–30.
- Apostolakis, G. (1989). Uncertainty in probabilistic safety assessment. *Nuclear Engineering and Design*, 115:179–179.
- Apostolakis, G. (2004). How useful is quantitative risk assessment? *Risk Analysis*, 24:515–520.
- Apostolakis, G. and Lemon, D. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, 25:361–375.
- Aradau, C. and van Munster, R. (2007). Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations*, 13:89–115.
- ARMS (2009). Operational risk assessment. Next generation methodology. In *Presentation by Nisula, J. Available at: <http://www.skybrary.aero/bookshelf/books/694.pdf>*.
- Aven, R. and Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12:1–11.
- Aven, T. (2003). *Foundations of risk analysis*. Chichester: Wiley.
- Aven, T. (2007a). On the ethical justification for the use of risk acceptance criteria. *Risk Analysis*, 27:303–312.
- Aven, T. (2007b). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering and System Safety*, 92:745–754.
- Aven, T. (2009). Safety is the antonym of risk for some perspectives of risks. *Safety Science*, 47:925–930.



- Aven, T. (2010a). *Misconceptions of risk*. Wiley, Chichester.
- Aven, T. (2010b). On how to define, understand and describe risk. *Reliability Engineering and System Safety*, IN PRESS.
- Ball, D. and Floyd, P. (1998). Societal risks, Final report. Technical report, Health and Safety Executive.
- Battmann, W. and Klumb, P. (1993). Behavioral economics and compliance with safety regulations. *Safety Science*, 16:35–46.
- Baybutt, P. (2002). Assessing risks from threats to process plants: threat and vulnerability analysis. *Process Safety Progress*, 21:269–275.
- BBC (2000). *The tragedy of Roskilde 2000*. Available at <http://www.bbc.co.uk/dna/h2g2/A442874>.
- Beck, U. (1992). *Risk society: Toward a new modernity*. Sage Publications, London.
- Bernstein, P. (1996). *Against the gods- the remarkable story of risk*. Wiley, New York.
- Bilgin, P. (2003). Individual and societal dimensions of security. *International Studies Review*, 5:203–222.
- Bley, D., Kaplan, S., and Johnson, D. (1992). The strengths and limitations of PSA: Where we stand. *Reliability Engineering and System Safety*, 38:3–26.
- Bohnenblust, H. and Slovic, P. (1998). Integrating technical analysis and public values in risk-based decision making. *Reliability Engineering and System Safety*, 59:151–159.
- Breakwell, G. (2007). *The psychology of risk*. Cambridge University Press, Cambridge.
- Breugel, K. v. (1998). How to deal with and judge the numerical results of risk analysis. *Computers and Structures*, 67:159–164.
- Brown, R. and Green, C. (1980). Precepts of safety assessment. *Journal of the Operational Research Society*, 31:563–571.
- Burgess, J. (2007). Social values and material threat: The European programme for critical infrastructure protection. *International Journal of Critical Infrastructures*, 3:471–487.
- Buzan, B., de Wilde, J., and Waever, O. (1998). *Security: A New Framework for Analysis*. Boulder, London.
- Campbell, S. (2005). Determining overall risk. *Journal of Risk Research*, 8:569–581.
- Campbell, S. and Currie, G. (2006). Against Beck: in defence of risk analysis. *Philosophy of the Social Sciences*, 36:149–172.
- Carpenter, S., Walker, B., Anderies, J., and Abel, N. (2001). From metaphor to measurement: resilience of what to what? *Ecosystems*, 4:765–781.

- Caruso, M., Cheok, M., Cunningham, M., Holahan, G., King, T., Parry, G., Ramey-Smith, A., Pubin, M., and Thadani, A. (1999). An approach for using risk assessment in risk-informed decisions on plant-specific changes to the licencing basis. *Reliability Engineering and System Safety*, 63:231–242.
- Cheok, M. and Sherry, R. (1998). Use of importance measures in risk-informed regulatory applications. *Reliability Engineering and System Safety*, 60:213–226.
- Christensen, F., Andersen, O., Duijm, N., and Harremoës, P. (2003). Risk terminology—a platform for common understanding and better communication. *Journal of Hazardous Materials*, 103:181–203.
- Christou, M., Mattarelli, M., and Nordvik, J. (2000). Land-use planning in the vicinity of chemical sites: Risk-informed decision making at a local community level. *Journal of Hazardous Materials*, 78:191–222.
- CIST (1999). Trust in cyberspace. Technical report, National Research Council (US).
- Comfort, L. (2005). Risk, security and disaster management. *Annual Review of Political Science*, 8:335–356.
- Cutter, S. (2003). The vulnerability of science and the science of vulnerability. *Annals of the Association of American Geographers*, 93:1–12.
- De Goede, M. (2008). Beyond risk: Premediation and the post-9/11 security imagination. *Security Dialogue*, 39:155–176.
- Deisler, P. (2002). A perspective: Risk analysis as a tool for reducing the risks of terrorism. *Risk Analysis*, 22:405–413.
- Delvosalle, C., Fievez, C., Pipart, A., and Debray, B. (2006). ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. *Journal of Hazardous Materials*, 130:200–219.
- DHS (2002). *National strategy for homeland security*. Department of Homeland Security, Washington DC.
- DHS (2008a). DHS risk lexicon. Technical report, Department of Homeland Security. Available at: [http://www.dhs.gov/xlibrary/assets/dhs\\_risk\\_lexicon.pdf](http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf).
- DHS (2008b). The insider threat to critical infrastructures. Technical report, Department of Homeland Security. Available at: [http://www.dhs.gov/xlibrary/assets/niac/niac\\_insider\\_threat\\_to\\_critical\\_infrastructures\\_study.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf).
- DOE (2004). Chemical process hazards analysis, DOE-HDBK-1100. Technical report, U.S. Department Of Eenergy, Washington D.C.
- Douglas, M. (1985). *Risk acceptability according to the social sciences*. Routledge, London.
- Douglas, M. and Wildavsky, A. (1983). *Risk and culture. An essay on the selection of technological and environmental dangers*. University of California Press, London.

- DSB (2010). Samfunnssikkerhet i arealplanlegging: Kartlegging av risiko og sårbarhet. Technical report, Directorate for Civil Protection and Emergency Planning.
- Einarsson, S. and Rausand, M. (1998). An approach to vulnerability analysis of complex industrial systems. *Risk Analysis*, 18:535–546.
- Ellsberg, D. (1961). Risk, ambiguity, and the Savage axioms. *The Quarterly Journal of Economics*, 75:643–669.
- Ersdal, G. and Aven, T. (2008). Risk informed decision-making and its ethical basis. *Reliability Engineering and System Safety*, 93:197–205.
- EU (2000). First report on the harmonization of risk assessment procedures. Part 1. Technical report, European Commission.
- European Commission (2004). *Critical infrastructure in the fight against terrorism*. Commission of the European Communities, Brussels.
- Faber, M. (2005). On the treatment of uncertainties and probabilities in engineering decision analysis. *Journal of Offshore Mechanics and Arctic Engineering*, 127:243–248.
- FHI (2010). Statusrapport om ny influensa A(H1N1), 7. januar 2010. Technical report, Folkehelseinstituttet. Available at: <http://www.fhi.no/dokumenter/f75b8a3bf1.pdf>.
- Fischhoff, B. (1995). Risk perception and communication unplugged: twenty years of process. *Risk Analysis*, 15:137–145.
- Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S., and Keeney, R. (1981). *Acceptable risk*. Cambridge University Press, New York.
- Fischhoff, B., Watson, S., and Hope, C. (1984). Defining risk. *Policy Sciences*, 17:123–139.
- Garland, D. (2003). *Risk and morality*. University of Toronto Press Incorporated, London.
- Garrick, B., Hall, J., Kilger, M., McDonald, J., O'Toole, T., Probst, P. S., Parker, E., Rosenthal, R., Trivelpiece, A. W., Arsdale, L., and Zebroski, E. (2004). Confronting the risks of terrorism: Making the right decisions. *Reliability Engineering and System Safety*, 86:129–176.
- Garrick, J. (2008). *Quantifying and controlling catastrophic risks*. Elsevier, Burlington.
- Gowland, R. (2006). The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment? *Journal of Hazardous Materials*, 13:307–310.
- Haddon, W. (1973). Energy damage and the 10 countermeasure strategies. *Human Factors*, 15:355–366.

- Haimes, Y. (2009). On the complex definition of risk: A systems-based approach. *Risk analysis*, 29:1647–1654.
- Hansson, S. (1996). Decision-making under great uncertainty. *Philosophy of the Social Sciences*, 26:369–386.
- Hokstad, P. and Steiro, T. (2006). Overall strategy for risk evaluation and priority setting of risk regulations. *Reliability Engineering and System Safety*, 91:100–111.
- Hollnagel, E., Woods, D., and Leveson, N. (2006). *Resilience engineering: concepts and precepts*. Ashgate Publishing Limited, Burlington.
- Holton, G. (2004). Defining risk. *Financial Analysts Journal*, 60:19–25.
- Homström, B. (1982). Moral hazard in teams. *The Bell Journal of Economics*, 13:324–340.
- Hovden, J. (2003). Theory formations related to the “risk society”. In *NoFS XV 2003, Karlstad, Sweden*.
- HSE (1992). The tolerability of risk from nuclear power stations. Technical report, HMSO, London.
- HSE (2001). Reducing risks, protecting people; HSE’s decision-making process. Technical report, HMSO, Norwich.
- HSE (2003a). Assessing compliance with the law in individual cases and the use of good practice. Technical report, The Health and Safety Executive. Available at: <http://www.hse.gov.uk/risk/theory/alarp2.htm>.
- HSE (2003b). Good practice and pitfalls in risk assessment. Technical report, Health and Safety Executive. Available at: <http://www.hse.gov.uk/research/rrhtm/rr151.htm>.
- HSE (2006). Guidance on risk assessment for offshore installations. Technical report, Health and Safety Executive. Available at: <http://www.hse.gov.uk/offshore/sheet32006.pdf>.
- HSE (2008). HSE scenario project: Boom and blame. Technical report, Health and Safety Executive, London.
- HSE (2009). PADHI - HSE’s land use planning methodology. Technical report, Health and Safety Executive. Available at: <http://www.hse.gov.uk/landuseplanning/padhi.pdf>.
- HSL (2000). Review of hazard identification techniques, RAS/00/02, HSL. Technical report, Health and Safety Laboratory. Available at: [http://www.hse.gov.uk/research/hs1\\_pdf/2005/hs10558.pdf](http://www.hse.gov.uk/research/hs1_pdf/2005/hs10558.pdf).
- IAEA (1998). *Guidelines for integrated risk assessment and management in large industrial areas*. International Atomic Energy Agency, Vienna.
- ICAO (2009). *Safety Management Manual: Doc 9859*. International Civil Aviation Organization. Available at: [http://www.icao.int/anb/safetymanagement/DOC\\_9859\\_FULL\\_EN.pdf](http://www.icao.int/anb/safetymanagement/DOC_9859_FULL_EN.pdf).

- ICAO (2010). Aviation security programme. Technical report, International Civil Aviation Organization. Available at <http://www2.icao.int/en/AVSEC/Pages/default.aspx>.
- IEC 60300-3-9 (1995). *Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems*. International Electrotechnical Commission, Geneva.
- IEC 61508 (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4*. International Electrotechnical commission, Geneva.
- IMO (2002). *Guidelines for formal safety assessment (FSA) for use in the IMO-rule-making process*. International Maritime Organization, London.
- IPCC (2007). Climate change mitigation. IPCC fourth assessment report from working group iii. Summary for policymakers. Technical report, Intergovernmental Panel on Climate Change. Available at <http://www.ipcc.ch/ipccreports/ar4-wg3.htm>.
- ISO 14121 (2007). *Safety of machinery- Risk assessment. Part 1: Principles*. International Organization for Standardization, Geneva.
- ISO 31000 (2009). *Risk management-Principles and guidelines*. International Organization for Standardization, Geneva.
- ISO guide 73 (2009). *Risk management- vocabulary*. International Organization for Standardization, Geneva.
- ISO/IEC Guide 51 (1999). *Safety aspects- guidelines for their inclusion in standards*. International Organization for Standardization, Geneva.
- Johansen, I. (2010). *Foundations and fallacies of risk acceptance criteria*. Project thesis NTNU, Trondheim.
- Jongejan, R. (2008). *How safe is safe enough? The government's response to industrial and flood risks*. PhD thesis, Technische Universiteit Delft.
- Kaplan, S. (1997). The words of risk analysis. *Risk Analysis*, 17:407–417.
- Kaplan, S. and Garrick, J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1:11–27.
- Kaplan, S., Haimes, Y., and Garrick, J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Analysis*, 21:807–819.
- Kasperson, R., Renn, O., Slovic, P., Brown, H. S., Emel, J. and Goble, R., Kasperson, J., and Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis*, 8:177–187.
- Kates, R. and Kasperson, J. (1983). Comparative analysis of technological hazards (a review). *Proceedings of the National Academy of Sciences US*, 80:7027–7038.
- Kates, R. and Slovic, P. (1983). The nature of technological hazards. *Science*, 220:378–384.

- Keeney, R. and Raiffa, H. (1976). *Decisions with multiple objectives: preferences and value tradeoffs*. Wiley and Sons, New York.
- Khan, F. (2001). Use maximum-credible accident scenarios for realistic and reliable risk assessment. *Chemical Engineering Progress*, 97:56–64.
- Kieureghian, A. and Ditlevsen, O. (2009). Aleatory or epistemic? Does it matter? *Structural Safety*, 31:102–112.
- Kim, J. (1971). Causes and events: Mackie on causation. *The Journal of Philosophy*, 68:426–441.
- Kim, J. (1973). Causation, nomic subsumption, and the concept of event. *The Journal of Philosophy*, 70:217–236.
- Kirchsteiger, C. and Cojazzi, G. (2000). Promotion of technical harmonization on risk-based decision making. Technical report, European Commission, Ispra.
- Kjellén, U. (2000). *Prevention of accidents through experience feedback*. Taylor and Francis, London.
- Klinke, A. and Renn, O. (2002). A new approach to risk evaluation and management: Risk-based, precaution-based and discourse-based strategies. *Risk Analysis*, 22:1071–1094.
- Knight, F. (1921). *Risk, uncertainty, and profit*. Percy Lund, Humphries.
- Kråkenes, T., Håbrekke, S., and Herrera, I. (2009). Risk influence modeling of recent developments in helicopter safety on the norwegian continental shelf. In *Reliability, Risk and Safety-theory and applications (contains papers presented at the 18th European Safety and Reliability Conference (ESREL 2009) in Prague, Czech Republic, September 2009*.
- Langlois, R. and Boulder, C. (1993). Frank Knight on risk, uncertainty, and the firm: a new interpretation. *Economic Inquiry*, xxxI:456–465.
- Leeuwen, C. v. and Vermeire, T. (2007). *Risk assessment of chemicals*. Springer Verlag, Heidelberg.
- LFC (2002). *The Hillsborough tragedy*. Available at [http://www.lfconline.com/feat/edb2/the\\_hillsborough\\_tragedy\\_69043/index.shtml](http://www.lfconline.com/feat/edb2/the_hillsborough_tragedy_69043/index.shtml).
- Lindley, D. (1985). *Making Decisions*. Wiley, London.
- Lindley, D. (2006). *Understanding uncertainty*. Wiley, Hoboken.
- Luhmann, N. (1991). *Risk: A sociological theory*. Walter de Gruyter, Berlin.
- Lundteigen, M. A. and Rausand, M. (2009). Architectural constraints in IEC 61508: Do they have the intended effect? *Reliability Engineering and System Safety*, 94:1609–1617.
- Lupton, D. (1999). *Risk*. Routledge, London.
- Murphy, J., Chastain, W., and Bridges, W. (2009). Initiating events and independent protection layers. *Process Safety Progress*, 28:374–378.

- Myagmar, S., Lee, A., and Yurcik, W. (2005). Threat modeling as a basis for security requirements. *Proc. 2005 ACM Workshop on Storage Security and Survivability (StorageSS05)*, New York, pages 94–102.
- Möller, N., Hansson, S., and Peterson, M. (2006). Safety is more than the antonym of risk. *Journal of Applied Philosophy*, 23:419–432.
- NASA (2002a). *Fault tree handbook with aerospace applications*. NASA Office of Safety and Mission Assurance, Washington D.C.
- NASA (2002b). *Probabilistic risk assessment procedures guide for NASA managers and practitioners*. NASA Office of Safety and Mission Assurance, Washington D.C.
- Niehaus, F and Szikszai, T. (2001). Risk informed decision making. Technical report, International Atomic Energy Agency. Available at: <http://www.iaea.org/worldatom/Meetings/2001/infcn82-topical1.pdf>.
- NORSOK Z-013 (2001). *Risk and emergency preparedness analysis (English version)*. Standard Norge, Oslo.
- NS 5814 (2008). *Krav til risikovurderinger*. Standard Norge, Oslo.
- NUREG (2009). *Guidance on the treatment of uncertainties associated with PRAs in Risk-informed decision making*. Office of Nuclear regulatory Research.
- Næss, A. (1985). Filosofiske betraktninger om lykke og ulykke. In *NOFS-85, SINTEF*.
- OREDA (2004). *Offshore Reliability Data Handbook. 4th Edition*. DNV, Høvik.
- Paté-Cornell, E. (2002). Risk and uncertainty analysis in government safety decisions. *Risk Analysis*, 22:633–646.
- Paté-Cornell, M. (1996). Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering and System Safety*, 54:95–111.
- Paté-Cornell, M. and Murphy, D. (1996). Human and management factors in probabilistic risk analysis: the SAM approach and observation from recent applications. *Reliability Engineering and System Safety*, 53:115–126.
- Pearl, J. (2000). *Causality. Models, reasoning, and inference*. Cambridge University Press, Cambridge.
- Perrow, C. (1984). *Normal accidents: Living with high risk technologies*. Basic books, New York.
- PSA (2001). *Regulations relating to health, environment and safety in the petroleum activities (the framework regulations) 2001*. Petroleum Safety Authority Norway, Norwegian Pollution Control Authority and Norwegian Social and Health Directorate.
- PSA (2010). *Trends in risk level in the petroleum activity. Summary report 2009*. Petroleum Safety Authority Norway. Available at <http://www.ptil.no/news/trends-in-risk-level-summary-report-2009-available-in-english-article6851-79.html>.

- Rasmuson, D. M. (1992). A comparison of the small and large event tree approaches used in PRAs. *Reliability Engineering and System Safety*, 37:79–90.
- Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27:183–213.
- Rausand, M. and Høyland, A. (2004). *System reliability theory. Models, statistical methods, and applications*. Wiley and Sons, New Jersey.
- Rausand, M. and Utne, I. (2009a). Product safety- principles and practices in a life cycle perspective. *Safety Science*, 47:939–947.
- Rausand, M. and Utne, I. (2009b). *Risikoanalyse- teori og metoder*. Tapir Akademisk Forlag, Trondheim.
- Reason, J. (1990a). *Human error*. Cambridge University Press, Cambridge.
- Reason, J. (1995). A systems approach to organizational error. *Ergonomics*, 38:1708–1721.
- Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate Publishing Limited, Aldershot.
- Reason, J. T. (1990b). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London, series B.*, 327:475–484.
- Renn, O. (2008). *Risk Governance. Coping with uncertainty in a complex world*. Earthscan, London.
- Riker, W. (1957). Events and situations. *The Journal of Philosophy*, 54:57–70.
- Roper, C. A., Grau, J., and Fischer, L. (2006). *Security education, awareness and training: From theory to practice*. Elsevier Inc, Burlington.
- Rosa, E. (1998). Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, 1:15–44.
- Salafsky, N., Salzer, D., Stattersfield, A., Hilton-Taylor, C., Neugarten, R., Butchart, S., Collen, B., Cox, N., Master, L., O'Connor, S., and Wilkie, D. (2008). A standard lexicon for biodiversity conservation: Unified classifications of threats and actions. *Conservation Biology*, 4:897–911.
- Salter, M. (2008). Imagining numbers: Risk, quantification and aviation security. *Security dialogue*, 39:243–266.
- Sarewitz, D., Pielke, R., and Keykhah, M. (2003). Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Analysis*, 23:805–810.
- Savage, L. (1972). *The foundations of statistics*. Dover Publications Inc, New York. Second revised edition.
- Schupp, B., Smith, S., Wright, P., and Goossens, L. (2004). Integrating human factors in the design of safety critical systems: A barrier based approach. In *Proceedings of IFIP 13.5 Working Conference on Human Error, Safety and Systems Development*.



- Shrader-Frechette, K. (1991). *Risk and rationality: Philosophical foundations for populist reforms*. University of California Press, Berkeley and Los Angeles, California.
- Siu, N. (1994). Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety*, 43:43–73.
- Slovic, P. (1987). Perception of risk. *Science*, 236:280–285.
- Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. *Risk Analysis*, 19:689–701.
- Slovic, P. (2002). Terrorism as hazard: A new species of trouble. *Risk Analysis*, 22:425–426.
- Starr, C. (1969). Social benefit versus technological risk. *Science*, 165:1232–1238.
- Svedung, I. and Rasmussen, J. (2002). Graphic representation of accident scenarios: Mapping system structure and the causation of accidents. *Safety Science*, 40:397–417.
- Thompson, K. and Bloom, D. (2000). Communication of risk assessment information to risk managers. *Journal of Risk Research*, 3:333–352.
- Tijms, H. (2007). *Understanding probability*. Cambridge University Press, Cambridge.
- Times (2010). *Haiti earthquake survivor Evan Muncie trapped under rubble for 27 days*. Available at [http://www.timesonline.co.uk/tol/news/world/us\\_and\\_americas/article7021168.ece](http://www.timesonline.co.uk/tol/news/world/us_and_americas/article7021168.ece).
- Turner, B., Kasperson, R., Matson, P., McCarthy, J., Corell, R., Christnesen, L., Eckley, N., Kasperson, J., Lures, A., Martello, M., Polsky, C., Pulsipher, A., and Schiller, A. (2003). A framework for vulnerability analysis in sustainability science. *Proceedings of the National Academy of Sciences US*, 100:8074–8079.
- TV2 (2010). *Jernbaneverket får skylda for Sjursøyaulykken*. Available at: <http://www.tv2nyhetene.no/innenriks/jernbaneverket-faar-ansvaret-for-sjursoeyaulykken-3173470.html>.
- Tversky, A. and Fox, C. (1995). Weighing risk and uncertainty. *Psychological Review*, 102:269–283.
- Tversky, A. and Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185:1124–1131.
- USCG (2000a). Risk-based decision making guidelines. Volume 2: Introduction to risk-based decision making. Basic principles. Chapter 1- Principles of risk-based decision making. Technical report, United States Coast Guard. Available at: [http://www.uscg.mil/hq/cg5/cg5211/docs/RBDM\\_Files/PDF/RBDM\\_Guidelines/Volume%202/Volume%202-Chapter%201.pdf](http://www.uscg.mil/hq/cg5/cg5211/docs/RBDM_Files/PDF/RBDM_Guidelines/Volume%202/Volume%202-Chapter%201.pdf).

- USCG (2000b). Risk-based decision-making guidelines. Volume 3: Procedures for assessing risks. Applying risk assessment tools. Chapter 12 - Event tree analysis (ETA). Technical report, United States Coast Guard. Available at: [http://www.uscg.mil/hq/cg5/cg5211/docs/RBDM\\_Files/PDF/RBDM\\_Guidelines/Volume%203/Volume%203-Chapter%2003.pdf](http://www.uscg.mil/hq/cg5/cg5211/docs/RBDM_Files/PDF/RBDM_Guidelines/Volume%203/Volume%203-Chapter%2003.pdf).
- USNRC (1975). *Reactor safety study, an assessment of accident risks in U.S Nuclear power plants, WASH-1400*. U.S. Nuclear Regulatory Commission, Washington DC.
- USNRC (1981). *Fault Tree Handbook, NUREG-0492*. U.S. Nuclear Regulatory Commission, Washington DC.
- USNRC (1998). *White paper on risk-informed and performance-based regulation*. United States Nuclear Regulatory Commission. Available at <http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1998/secy1998-144/1998-144scy.html>.
- Vatn, J. (1998). A discussion of the acceptable risk problem. *Reliability Engineering and System Safety*, 61:11–19.
- Vatn, J. (2009). Issues related to localization of an LNG facility. In *Reliability, Risk and Safety: Theory and Applications. Proceedings from ESREL 2009*.
- Vidalis, S. (2004). A critical discussion of risk and threat analysis methods and methodologies. Technical report, CS-04-03.
- Vinnem, J. (2007). *Offshore risk assessment. Principles, modeling and application of QRA studies*. Springer, London.
- Wagenaar, W., Groenewef, P., Hudson, P., and Reason, J. (1994). Promoting safety in the oil industry. The Ergonomics Society lecture presented at the Ergonomics Society Annual Conference, Edinburgh, 13-16 April 1993. *Ergonomics*, 37:1999–2013.
- Wagenaar, W., Hudson, P., and Reason, J. (1990). Cognitive failures and accidents. *Applied Cognitive Psychology*, 4:273–294.
- Watson, S. (1994). The meaning of probability in probabilistic safety analysis. *Reliability Engineering and System Safety*, 45:261–269.
- Webster (1978). *Webster's Encyclopedic Unabridged Dictionary of the English Language*. Random House, New York.
- WHO (2006). *Health effects of the Chernobyl accident: an overview. Fact sheet no. 303*. World Health Organization. Available at: <http://www.who.int/mediacentre/factsheets/fs303/en/index.html>.
- Wilson, R. and Crouch, A. (1982). *Risk/Benefit Analysis*. Ballinger Publishing Company, Cambridge.
- Yosie, T. and Herbst, T. (1998). Using stakeholder processes in environmental decisionmaking. Technical report, The Global Development Research Center. Available at <http://www.gdrc.org/decision/nr98ab01.pdf>.

Zedner, L. (2003a). The concept of security: An agenda for comparative analysis. *Legal Studies*, 23:153–176.

Zedner, L. (2003b). Too much security? *International Journal of the Sociology of Law*, 31:155–184.



# Appendix A

## Abbreviations and acronyms

AE	Accidental event
AFD	Anticipatory failure determination
AS	Accident scenario
ALARP	As low as reasonably practicable
BE	Basic event
CDF	Core damage frequency
CE	Critical event
DSB	Directorate for Civil Protection and Emergency Planning (NOR)
EPA	Emergency and preparedness analysis
ES	End state
ETA	Event tree analysis
FMEA	Failure mode and effects analysis
FSA	Formal safety assessment
FTA	Fault tree analysis
GFT	General failure type
HAZOP	Hazard and operability analysis
HE	Hazardous event
HSE	Health and safety executive(UK)
HRA	Human reliability analysis
IE	Initiating event
ICAO	International Civil Aviation Organization
IMO	International Maritime Organization
IPCC	International Panel on Climate Change
IPL	independent protection layers
LOPA	Layer of protection analysis
MCAS	Maximum credible accident scenario
LC	Latent conditions
PHA	preliminary hazard analysis
PRA	Probabilistic risk assessment
PSA	Petroleum Safety Authority(NOR)
QRA	Quantitative risk assessment
RAC	Risk acceptance criteria
RIF	Risk influencing factor
SAM	System-action-management
SU	Safety issue
TSS	Theory of scenario structuring
TE	Triggering event
UE	Undesired event

**MASTER THESIS**  
**2010**  
**for**  
**stud. techn. Inger Lise Johansen**

**FOUNDATIONS OF RISK ASSESSMENT**  
**(Grunnlaget for risikovurdering)**

If you ask ten persons what they mean by the word “risk”, you will, most likely, get ten different answers. To a slightly less degree, this also applies to professionals who are working with risk assessments. Quantitative risk assessments have now been applied for more than forty years, but still the terminology is ambiguous and confusing. This leads to erroneous application of methods, problems in communicating risk, and so on.

A commonly accepted definition of (accident) risk is that it is the answer of the three questions:

1. Which accident scenarios can happen (that may cause harm to some assets)?
2. How likely is each of these scenarios?
3. If a scenario does happen, what are the consequences?

The interpretation of this definition influences the choice of analytical methods, how the results from these methods are understood, and so on. The scientific community is still discussing how we should interpret the definition of risk, for example (i) what is an accident scenario, where does it start and where does it stop, what is the “initiator” of the scenario, (ii) what are the delimitations of accident scenarios, does it comprise only acute effects or also long-term effects, (iii) what do we mean by the term “likely”, is it a property of the scenario or only a social construct, (iv) what do we mean by “consequences”, when do we stop the accident scenario to “measure” the consequences, how can we include long-term effects and partial damage.

The objective of this master thesis is to shed light on the foundations of risk assessment, discuss the basic concepts and how the interpretation of these concepts influences the risk analysis process and the understanding of the results from the risk assessment.

As part of this master thesis the candidate shall:

1. Perform a literature survey and describe and discuss the main definitions (or interpretations) of the term *risk* – and also discuss how the term risk is related to concepts like safety, security, vulnerability, etc.
2. Discuss the concept of *accident scenario*. Suggest a “suitable” definition and especially discuss the extent of a scenario, what is the initiating event of the scenario and where should the development of the scenario be terminated?
3. Discuss the concepts of *hazard* and *threat* – and *triggering events*. Do we need to distinguish between these concepts? The aviation organization ICAO has suggested to focus on so-called *safety issues*. What are the benefits and limitations of this approach?
4. How can we measure and compare consequences to various types of assets? – and how can we obtain a single measure for different degrees of harm to one type of asset (e.g., fatalities, injuries, permanent vs. non-permanent disabilities)?
5. Discuss risk assessment as basis for decision-making. What are the pros and cons related to risk-based decision-making related to risk-informed decision-making?

Following agreement with the supervisor, the tasks may be given different weights – and additional tasks may also be included.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task’s content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfilment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

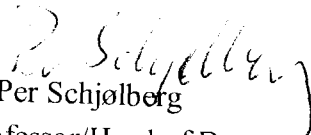
Deadline: June 14<sup>th</sup> 2010.

Two bound copies of the final report and one electronic (CD) version are required.

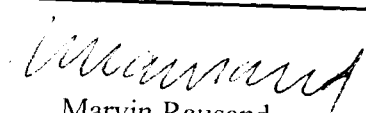
Responsible professor/Supervisor: Professor Marvin Rausand  
Telephone: 73 59 25 42  
E-mail: marvin.rausnad@ntnu.no

Supervisor: Mary Ann Lundteigen  
Telephone: 73 59 71 01  
E-mail: mary.a.lundteigen@ntnu.no

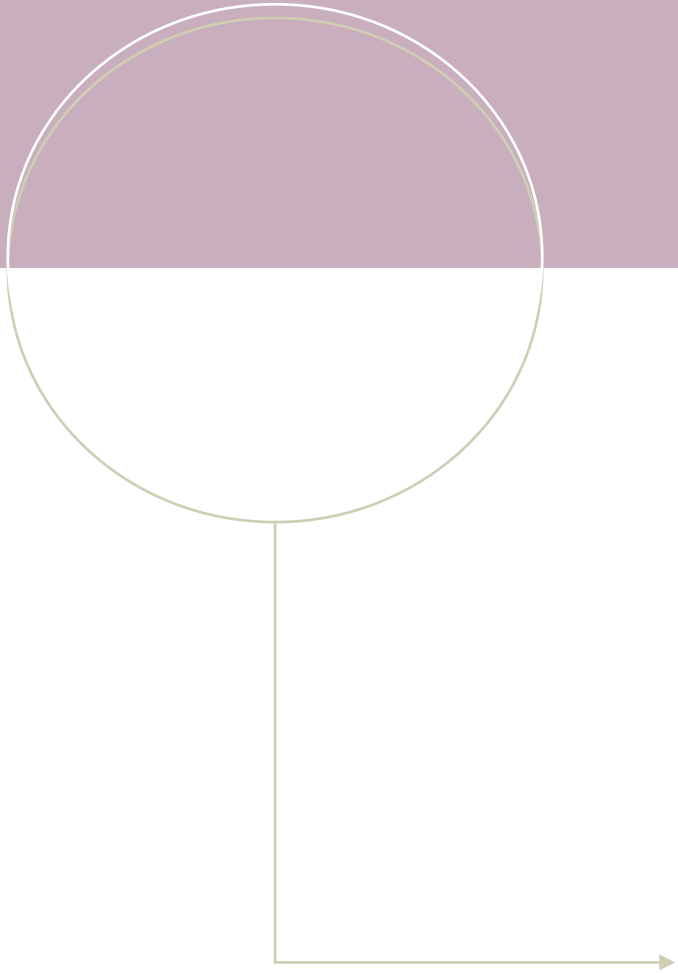
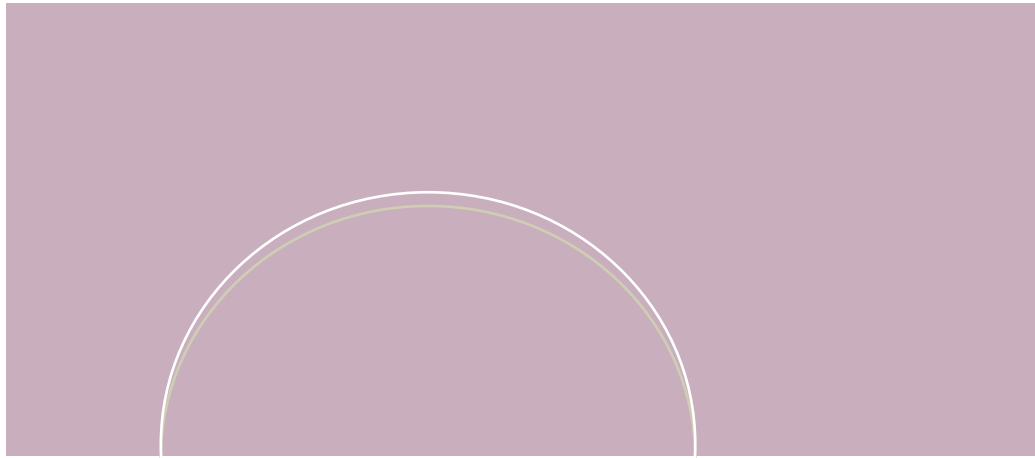
**DEPARTMENT OF PRODUCTION  
AND QUALITY ENGINEERING**

  
Per Schjølberg

Associate Professor/Head of Department

  
Marvin Rausand  
Responsible Professor





**NTNU**

Norwegian University of  
Science and Technology