

Preface

Accidents have probably happened since the first caveman lit the first fire, but for many centuries the consequences of accidents were mostly limited to the people directly doing the work – what we now call the people at the sharp end. The introduction of technology to the work process changed all that. This development may with some justification be linked to the industrial revolution and even more precisely to the year 1769 when James Watt patented the steam engine. The industrial revolution introduced the large-scale use of machines as part of human work beginning with mining and manufacturing, and thereby inevitably changed the very nature of work. Machines did not only make production faster and more efficient but also increased the severity of consequences when something went wrong. The replacement of human muscular power by machines created a need for control, which quickly led to increasingly complex technological systems. Since any piece of technology can fail, it was inevitable that more complex technology meant more failures – and also greater consequences of those failures.

This development is excellently illustrated by the story of the high-pressure steam engine, which came into widespread use in steamboats and industrial production in the beginning of the 19th Century (Leveson, 1994). From the very start the use of high-pressure steam engines was marred by a number of cases where the machine exploded, injuring or killing crew, passengers, and workers. According to Leveson, the U.S. Commissioner of patents estimated that between 1816-1848 there had been 233 steamboat explosions, resulting in 2,562 persons killed and 2,097 injured (a rather remarkable ratio from a contemporary point of view). The steamboat was a new technology, which brought significant advantages, but also – inevitably – significant risks.

As the use of technology became more widespread, the consequences of accidents were no longer confined to the people at the sharp end but could affect both bystanders and people who were completely unrelated to the work process. Beginning slowly, the number of accidents soon started to grow although it was not until the first decades of the 20th Century that accident statistics became

commonplace. We are today inundated with statistics about accidents for practically every field of endeavour, but better knowledge of occurrences does not by itself seem to have any dampening effect.

In the second half of the 20th Century, writing about accidents has increased in part to meet the need of improved safety. Many books have been written about accidents, and it is a safe bet that many more are still to be written. There are two main reasons for that. The first is that accidents always have happened and always will happen, barring some cataclysmic – or providential – event. The second is that the understanding of accidents is still approximate and incomplete, and is likely to remain so for a long time, perhaps indefinitely. Taken together this means that there is an unfulfilled need for a better understanding of the nature of accidents. One way of trying to meet this need is to propose a comprehensive explanation of accidents, which is what this book sets out to do.

What Is this Book About?

Books about accidents can be written in many different ways and in many different styles. Without claiming anything like a comprehensive classification, the accident literature seems to include the following main types.

- Books that look at classes of accidents rather than single events and which try to go beyond the specifics of the accidents and understand the general principles or lessons from them – specifically in relation to the system characteristics that led to them. Many of these propose an overall view or approach to analysing and understanding accidents. The classical work in this group is without a doubt Herbert W. Heinrich's book on Industrial Accident Prevention from 1931, which has been extended and reprinted several times with a fifth edition published in 1980 (Heinrich, Petersen & Roos, 1980). Another important volume is Charles Perrow's book on Normal Accidents (Perrow, 1984, with a second edition in 1999), which put forward the argument that our technological systems now have become so complex that accidents must be seen as the norm rather than exception – commonly referred to as Natural Accident Theory. Other important works are

Amalberti (1996), Leveson (1994), Petroski (1994), Tenner (1997), and Woods et al. (1994).

- Books and papers that provide in-depth accounts of major accidents, often combined with analyses that introduce new ways of thinking or provide new points of view. Two recent examples of that are Dianne Vaughan's treatment of the accident with the space shuttle Challenger in 1986 (Vaughan, 1996) and Scott Snook's account of the 'friendly fire' shoot down of two Black Hawk helicopters over Northern Iraq in 1994 (Snook, 2000). Supplementing these are the detailed technical reports from accidents, which nowadays often are available as documents on the World Wide Web.
- Writings that provide systematic accounts of collections of accidents, often with exemplary analyses of each, but without the intention of proposing a grand theory (e.g., Bignell & Fortune (1984). These are usually focusing on specific domains such as trains, aviation, accidents at sea, etc.
- Books that develop proposals for possible 'mechanisms' of accidents and which describe how specific types of causes can be used to explain how accidents happen. This literature has until recently primarily focused on the legendary 'human error', e.g., (Rasmussen, Duncan & Leplat (1978), Reason (1990), Senders & Moray (1991), Bogner (1994) and many others.
- Books that examine the role of organisations in accidents. These fall into two major subcategories. One puts the focus on accidents on the organisational level, such as Reason (1997) and Vaughan (1996). The other looks more to the way in which organisations can play a role in safety, either in the form of studies of safety culture (Wilpert & Qvale, 1993) or high-reliability organisations (Weick & Sutcliffe, 2001).
- Finally, there are a growing number of books about accident analysis in relation to engineering and construction, such as Harms-Ringdahl, (2001), Kjellen (2000) and Taylor (1993).

Given these many styles of writing about accidents – and probably a few that have been missed – where does this book fit in? Hopefully in the first category, i.e. books that try to go beyond the specifics and formulate some general principle. It can confidently be stated that this

is *not* a book about ‘human error’, or about any specific type of cause or failure. Neither is it a book about accident analysis as such (see, e.g., Hollnagel, 1998, for an example of that). The aim is to offer a framework for understanding accidents so that we are able better to prevent them. This should at the same time provide both a consistent basis for analysing accidents and a method for responding to them in an effective manner – which means something that leads to a reduction in their number and a diminution of their consequences. The framework represents a systemic point of view, according to which accidents are due to complex coincidences rather than distinct, individual causes. The method that goes with the framework is based on the concept of barriers or defences as the effective means against accidents and their consequences. The concept of barriers is obviously not new, as the following chapters will show, but the combination of a systemic view of accidents with barrier functionality is believed to offer an effective solution to accident prevention.

Readership and Outline

This book is intended for practitioners rather than researchers – although both groups hopefully can use it. The reason for this partiality is simple – it is the practitioner who can make changes to practice, not the academic. The intention is that the practically minded reader should be able to read the book without constantly consulting the references and even without caring much about them. On the other hand, the more academically oriented reader should be able to find enough to expand the study of the issues treated in the book. Changes to practice are rather desperately needed if any real reduction in the number of accidents is ever to be achieved. The emphasis is therefore, as the title indicates, on accident prevention and on the role of barriers. The topics treated in the book are organised as follows:

Chapter 1: Accidents and Causes. This chapter provides a broad introduction to accidents, defined as unexpected events that result in unwanted outcomes. It goes on to discuss the range in events and outcomes, i.e., the degree to which events can be predicted and the varying severity of outcomes. Other topics treated are the relation between accidents, incidents and near misses, and the difference between explaining accidents and finding their causes. The chapter ends

by discussing the evolving concept of causes and the concomitant change from an absolute to a relative understanding of what a cause is.

Chapter 2: Thinking about Accidents. In order to understand accidents it is necessary to describe them, and the description inevitably involves the use of an accident model. Most approaches to accident analysis and prevention focus on the methods without addressing the issue of the underlying models. Or rather, they imply a certain type of model and assume that it is universally accepted. It is, however, not only useful but also necessary to be aware of which accident model lies behind, since this determines both the search principles and the goals of the analysis. The chapter presents three characteristic types of accident models: the sequential, the epidemiological, and the systemic. The three types correspond to the gradual realisation that accidents are due to complex coincidences rather than root causes. The systemic type of accident models represents the current understanding, specifically the role of blunt end – sharp end factors, and also provides the basis for the functional resonance accident model developed in Chapter 5.

Chapter 3: Barriers Functions and Barrier Systems. Although the concept of a barrier is used rather freely in the accident literature, there have been relatively few attempts thoroughly to analyse what a barrier is. The chapter presents each of these and goes on to make a distinction between barrier functions and barrier systems. The former describes what barriers do (to prevent, protect, etc.) whereas the latter describes how it is done, for instance whether entry is prevented by a door or a sign. The chapter introduces four different types of barrier systems called physical, functional, symbolic, and incorporeal; each of these may support one or more barrier functions, but in practice a barrier usually combines two or more barrier systems. As each type of barrier system has its strengths and weaknesses the choice of a barrier to solve a concrete problem is always a trade-off, for instance between cost and efficiency. The relative qualities of the four barrier systems are discussed as a starting point for barrier design. Finally, the chapter considers how other types of barriers, e.g., organisational barriers and actions, can be seen as specific instances of the four systems.

Chapter 4: Understanding the Role of Barriers in Accidents. In the commonly used methods for risk analyses, such as fault trees and event trees, barriers can be represented in a straightforward manner as nodes in the trees. Indeed, if a possible scenario is described as a sequence or tree of possible events, the semantics of a barrier is to block or break

the path between two nodes. Where the fault tree achieves this through logical conditions, other approaches represent barriers directly as interruptions of a path. Yet the notion that a barrier is a simple way of hindering something from happening is unfortunately misleading. Barriers often have unwanted side-effects and may even under certain conditions have the opposite of the desired effect. For example, while a cell door may prevent inmates from escaping it may also prevent fire fighters from entering during an emergency. Barriers are furthermore just one of several ways of responding to an accident, and should be seen as a possible tool rather than as a panacea.

Chapter 5: A Systemic Accident Model. In the contemporary view, accidents are seen as emerging phenomena in complex systems, and as the result of an aggregation of conditions rather than the inevitable effect of a chain of courses. In a nominal work situation, people can in principle manage just by follow rules and procedures. In practice, however, they must always balance resources against requirements and constantly make adjustments to what they do in order to achieve their goals. Since this efficiency-thoroughness trade-off is necessary for complex systems to work in the first place, it is generally useful rather than harmful. Yet in addition to its usefulness it is also a source of variability and may as such help us understand why accidents happen. The occurrence of unwanted effects from performance variability can be explained using the concept of resonance, and the chapter ends by describing a systemic accident model based on the principle of functional resonance.

Chapter 6: Accident Prevention. The last chapter proposes how the functional resonance accident model can be used in accident prevention. This is achieved through four steps that are described in detail and illustrated by a practical example. The steps comprise identifying the essential system functions, determining the potential for variability, defining the functional resonance – which is the main source of risks, and finally deciding on appropriate countermeasures. The method underlines the need of creative – or requisite – imagination and of using an accident model that matches the complexity of the systems being considered. Consonant with the systemic accident model, an important countermeasure is to manage the performance variability in the system, as a functional barrier system that complements the more conventional use of barriers.

Acknowledgements

In February 1676, Sir Isaac Newton famously wrote in a letter to Robert Hooke that ‘if I have seen farther than others, it is because I was standing on the shoulders of giants.’ Today few people can rightfully claim the same, both because the views are more bewildered and because there are fewer giants around. Yet it is as true today as it was in 1676 that any work is a product of what has gone before and that it may offer a specific, albeit limited, view of what may happen in the future. The perspective put forward by this book reflects the experience from many years of working in projects related to risk and system safety as well as from numerous discussions with friends and foes alike. To the latter I owe a debt of gratitude because they have forced me to improve arguments and revise lines of reasoning. From the former I rely on varied schedule reinforcement to prevent me from wandering completely off the track. Finally, I would like to thank Sue Bogner, Paulo Victor de Carvalho and Richard Cook for detailed comments to a draft version of this book.

Erik Hollnagel, April 2004.