The role of System Dynamics in the analysis of Human and Organisational Factors for Accident Analysis and Probabilistic Risk Analysis

Magdalena Gajdosz

Submitted for the degree of

Doctor of Philosophy

Department of Management Science
University of Strathclyde
Glasgow, UK

2015

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: Date:

Table of Contents

ABSTRACT

The overall aim of this thesis is to improve the understanding of the role of System Dynamics (SD) in the analysis of Human and Organisational Factors (HOFs) for Accident Analysis (AA) and Probabilistic Risk Analysis (PRA). PRA and AA are important elements of the risk management of complex technological systems. They help duty holders ensure compliance with the health and safety law. Logical and mathematical modelling plays an important role in PRA and is gaining increasing recognition within the AA community. Models help to identify hazards and adverse effects and help to explain how and why accidents occur. They also enable the risk to be expressed quantitatively.

SD is a modelling approach that has been proposed to be used within PRA and AA to support analysis of HOFs. Risks do change over time as a result of changes in HOFs, and SD has significant capabilities for capturing mechanisms that drive human and organisational behaviour over time and influence risks and contribute to accidents. However, the published literature lacks explicit discussion of the role that SD could play in the analysis of HOFs for PRA and AA. The aim of this thesis is to address this gap.

To achieve the thesis aim, the research work was divided into two areas for investigation:

1. Exploration of when SD could be used in the analysis of HOFs for PRA and AA.
2. Application of SD to the analysis of HOFs for PRA and AA to gain an understanding of the issues involved in using SD in these areas.

These investigations led to lessons that contribute to knowledge of the use of SD within PRA and AA. Any modeller considering the use of SD within PRA or AA will benefit from the conclusions of this thesis.

CHAPTER 1: Introduction

1.1 Introduction

In the UK, the Health and Safety at Work Act requires that the risks arising from work activities should be managed to the level “as low as reasonably practicable” (ALARP) by those who create them. Management of these risks is particularly important in complex technological systems such as nuclear power plants, hazardous waste facilities, chemical plants, space systems, offshore oil and gas extraction facilities and transportation systems. Accidents associated with the operation of these systems are rare, but when they do occur, they are usually very severe. The 2010 Polish Air Force TU-154 aircraft crash near Smolensk, Russia is an example of such an accident. The crash resulted in the loss of the aircraft and death of 96 people that were on board during the accident. These included the then President of Poland Lech Kaczynski and his wife, the president of the National Bank of Poland, Polish government officials, members of Polish parliament and Polish military officials.

Probabilistic Risk Analysis (PRA) and Accident Analysis (AA) are important elements of the risk management of complex technological systems. PRA is concerned with identification of hazards, potential adverse effects associated with these hazards and estimation of the likelihood that these adverse effects will realize. AA involves analysis of how and why an accident has occurred and helps to prevent accident reoccurrence. PRA is concerned with identifying and examining potential accidents (prospective analysis) and AA is concerned with examining accidents that have occurred (retrospective analysis). They are complementary activities that help those responsible for risk management of complex technological systems to:

- understand the risks associated with the operation of these systems
- avoid costs associated with the occurrence of accidents such as loss of reputation, drop in staff morale, downtime, need to pay compensation to the affected parties or even bankruptcy
- ensure compliance with the health and safety law.

Logical and mathematical modelling plays an important role in PRA (see, for example, Bedford and Cooke, 2001) and is gaining increasing recognition within the AA community (see, for example, Sklet, 2004; Energy Institute, 2008; Johnson, 2003). A model can be usefully defined as "*an external and explicit representation of part of reality as seen by the people who wish to use that model to understand, to change, to manage and to control that part of reality*" (Pidd, 2009, p.12). Models help to depict complex technological processes, identify hazards and potential adverse effects associated with these hazards. They also enable risks to be expressed quantitatively. When an accident occurs, models can be used within AA to reconstruct the events that led to the accident and understand which risk control measures were ineffective and why.

Development and use of modelling approaches for PRA and AA to inform risk management of complex technological systems is an on-going research topic. For example, the Reliability Engineering and System Safety journal, an international journal well-known in the risk management field, highlights this research area within the statement of its aims and scope. The recently created Elsevier journal, Analytic Approaches in Accident Research, is entirely devoted to the topic of developing new approaches, including modelling approaches, to support the study of transportation and non-transportation-related accidents.

System Dynamics (SD) is a modelling approach well known in Operational Research/Management Science (OR/MS) that has been proposed to be used within PRA and AA (e.g. Mohaghegh et al., 2009, Cooke, 2003). It has been suggested that SD could be used to support the analysis of Human and Organisational Factors (HOFs). The importance of HOFs as contributors to risks and accidents in complex technological systems is undisputed. However, there are a number of open challenges in modelling them adequately. One of these challenges is the dynamic nature of humans and organisations. SD has significant capabilities for capturing mechanisms that drive human and organisational behaviour over time and could be used to capture the dynamic impact of HOFs on risks and accidents within PRA and AA. However, the published literature on the use of SD within PRA and AA lacks explicit consideration of the role of SD within these two areas. Good understanding of the benefits and limitations of using SD in the analysis of HOFs for PRA and AA is essential if SD is to be successfully applied to such analysis. Lack of knowledge of the benefits and limitations of using SD in the analysis of HOFs for PRA will lead to inadequate modelling of HOFs and inadequate insights to inform risk management of complex technological systems. Lack of knowledge of the benefits and limitations of using SD in the analysis of HOFs for AA will lead to poor learning from accidents and design of ineffective accident prevention measures. The aim of this thesis is to address this gap.

1.2 The aim of the thesis

The overall aim of this thesis is to improve the understanding of the role of SD in the analysis of HOFs for PRA and AA. Thus, this thesis brings together and explores four topics: Probabilistic Risk Analysis, Accident Analysis, Human and Organisational Factors Analysis and System Dynamics.

Before SD can be used in the analysis of HOFs, a decision needs to be made on whether SD is a suitable approach to model HOFs within a particular PRA and AA. Therefore, the first aim of this thesis is

- *to explore when SD could be used in the analysis of HOFs for PRA and AA*

This should help those considering using SD in the analysis of HOFs to decide whether SD could be used in any individual PRA or AA. It is hoped that this exploration will help to identify situations in which SD could be used to support the analysis of HOFs for PRA or AA.

The second aim of this thesis is

– *to explore how SD could be used in the analysis of HOFs for PRA and AA and whether there are any issues associated with the use of SD in these areas*

This should help those wishing to use SD in the analysis of HOFs to develop SD models for PRA and AA. Overall, this thesis should provide modellers with better understanding of what can be achieved by using SD in the analysis of HOFs for PRA and AA and the limitations of SD in these areas.

1.3 Methodological approach underpinning the research

The overall aim of the research was to gain insights into when and how SD could be used in HOF analysis for PRA and AA and to improve the understanding of the role of SD in these areas. Thus, the research was exploratory in nature (Saunders et al., 2012). The following research activities were undertaken to support explorations in this thesis:

– *SD, AA and PRA literature was used to explore when SD could be used in HOF analysis for AA and PRA*

Anyone considering using SD in the analysis of HOFs for PRA and AA needs to decide whether SD will be used in any individual PRA or AA. The discussion of the situations in which SD could be used in the analysis of HOFs for AA and PRA is presented in Chapter 3 of this thesis.

– *SD was used within AA and PRA to explore how it could be applied to support HOF analysis for AA and PRA*

Those who decide to use SD to model HOFs for AA or PRA need to have a good understanding of practical aspects of applying SD. The discussion of how SD could be used to support HOF analysis for PRA and AA is presented in Chapter 4 and Chapter 5. Chapter 4 illustrates how SD could be used within AA by presenting application of SD to the analysis of HOFs that contributed to the 2007 Grayrigg train accident. Chapter 5 illustrates how SD could be used within PRA by presenting the application of SD to the analysis of HOFs contributing to the unavailability of an engineered safety system at a process plant.

The research strategy adopted to support explorations in this thesis is multi-methodological in nature and combines elements of well-established research approaches: literature review, case study approach and modelling approach. The philosophy underlying this research strategy is critical realism as formulated largely by Bhaskar (Archer, 1998). To critical realists all research approaches are fallible ways of engaging with the external reality as they focus on certain aspects of the reality, while ignoring others. Thus, when applying a particular research approach to investigate a situation "*we are really like blind men led into an arena and asked to identify an entity (say an elephant) by touching one part of that entity (say a leg). Certainly we might make better guesses if we could pool the information of all the blind men, each of whom has touched a different part of the elephant"* (Smith, 1975, p.273 in Johnson and Duberley, 2000, p.168). Thus, critical realists strongly support methodological pluralism. Moreover, critical realists legitimise the use of both extensive approaches (e.g. statistical data analysis) and intensive approaches (e.g. case studies, literature review) (Archer, 1998). However, there is still little guidance in the critical realist literature on how these different approaches could be combined. The author of this thesis selected a literature review, a case study approach and a modelling approach as she believes they effectively complement and support one another and are best suited for the purpose of exploring when and how SD could be used in HOF analysis for AA and PRA. The SD, AA and PRA literature was judged by the author to be a rich source of data to explore the key features of SD and when it could be used in the analysis of HOFs for AA and PRA. It provided a good background for further research, i.e. applying SD to HOF analysis within AA and PRA. To illustrate how SD could be used within AA and fully explore issues associated with its use in this area, it was essential to apply SD to the analysis of a real and recent accident. To illustrate how SD could be used within PRA and fully explore issues associated with its use in this area, it was essential to apply SD to the analysis of a real problem faced by a company that operates a complex technological system. Thus, it was decided to combine a case study approach and a modelling approach.

Another important philosophical assumption underlying this research is the critical realist belief that all accounts of external reality produced by researchers are incomplete, limited and dependent on different factors, for example, historical context in which these accounts are produced. As a result, any knowledge claims made at any point in time may be wrong and all accounts of external reality are thus revisable. This encapsulates what Archer (1998) calls "epistemological relativism", i.e. a conviction that knowledge is not absolute, but socially constructed. Thus, research is seen as an iterative and on-going activity. A good example of this is the research in the AA area. In the past, the beloved notion of AA researchers, and underlying most approaches supporting HOF analysis for AA, was the notion of a "root cause". A root cause can be defined as "*the most basic cause [of the accident] that can be reasonably identified and that management has control to fix*" (Paradies and Busch, 1988 in Livingston et al., 2001, p.1, words in the brackets added). Nowadays, a number of authors argue that the concept of a "root cause" limits the usefulness of HOF analysis within AA for risk management (e.g. Reason, 1997; Hollnagel, 2004; Leveson 2004; Reason, 2006). One of the key questions is: How do we stop and decide what is "the most basic cause"? To use Reason's words (1997, p.15): "In theory, one could trace the various causal chains back to the Big Bang." This is discussed in more detail in Chapter 2 of this thesis. In summary, it needs to be remembered that the research project encapsulated in this thesis is also a limited and incomplete contribution to knowledge, constrained by available time and resources and dependent on the context in which it was undertaken. The limitations of this research are fully discussed in Chapter 6 of this thesis.

Related to the above is the critical realist claim that not all accounts of the external reality are equal. There is no "judgemental relativism", rather "judgemental rationality". A rational choice can be made between different accounts using criteria such as practical adequacy of the constructed account of the external reality (Archer, 1998). Different accounts of external reality can be accepted or rejected based on how successful they are in supporting human endeavours. The aim of this thesis is to provide those wishing to use SD in HOF analysis for AA and PRA with insights into when and how SD could be used within these areas. The value of these insights, and thus the value of this thesis, can ultimately be assessed based on how successful these insights are in supporting modellers who would like to use SD within AA and PRA. This could not be evaluated as part of this research project, but could be investigated in the future.

1.4 Structure of the thesis

Chapter 2 provides background information on the research presented in this thesis. It introduces the reader to the field of the risk management of complex technological systems and reviews the literature that led to the specification of the overall aim of this thesis. This should enable the reader to fully understand the remaining chapters of the thesis.

Chapter 3 presents the discussion of when SD could be used in the analysis of HOFs for PRA and AA. Chapter 4 demonstrates and discusses how SD could be used in HOF analysis for AA. Chapter 5 demonstrates and discusses how SD could be used in HOF analysis for PRA. Finally, the key findings and limitations of the research, plus recommendations for further research, are presented in Chapter 6. The structure of this thesis is graphically depicted in Figure 1-1 which also highlights the key questions that each chapter is trying to answer. Arrows indicate the logical connection between the chapters. The development of Chapter 4 and Chapter 5 has informed one another. This is explained throughout the thesis and is not depicted in Figure 1-1 for the sake of simplicity.

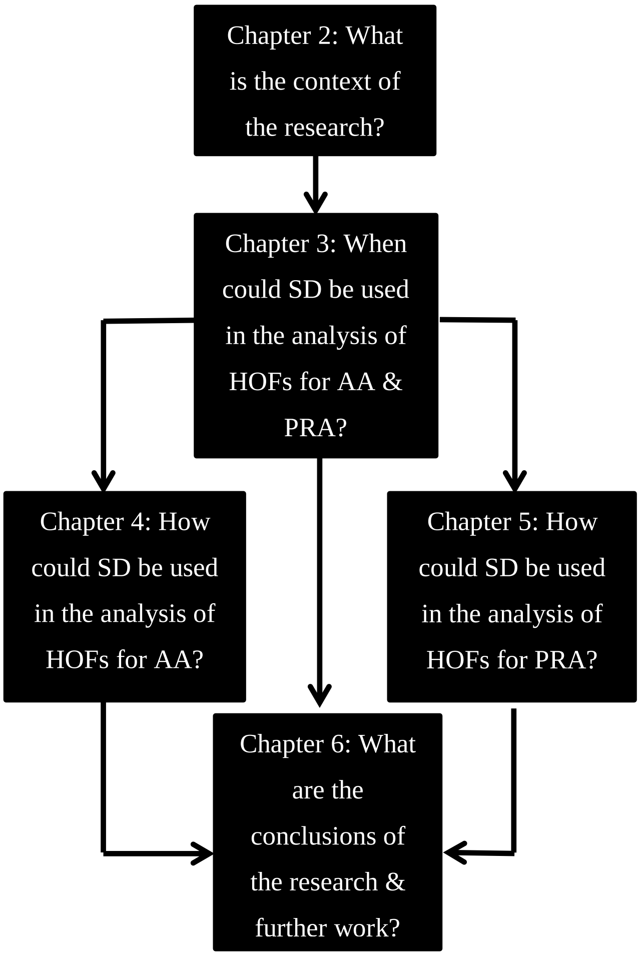

Chapter 2: What is the context of the research?
Chapter 3: When could SD be used in the analysis of HOFs for AA & PRA?
Chapter 4: How could SD be used in the analysis of HOFs for AA?
Chapter 5: How could SD be used in the analysis of HOFs for PRA?
Chapter 6: What are the conclusions of the research & further work?

Figure 1-1: Structure of the thesis

CHAPTER 2: Background information

2.1 Introduction

The overall aim of this thesis is to improve the understanding of the role of SD in the analysis of HOFs for PRA and AA. Thus, this thesis brings together and explores four topics: PRA, AA, HOF analysis and SD.

Four studies had greatly influenced the specification of the overall aim of this thesis. The first one was the 2008 EPSRC funded project "*Rethinking Human Reliability Analysis Methodologies"* that brought together academics from the University of Wales, Manchester Business School, University of Strathclyde, University of Lancaster, University of Nottingham, Cranfield University and University of Kingston. The main findings of this project were published in the Safety Science journal (see French et al., 2011). The key conclusion from the study was that the modelling approaches traditionally used in the analysis of HOFs for PRA need to be extended to include our current understanding of human and organisational behaviour.

The second study that had influenced this thesis was conducted by the group of researchers from the University of Maryland in the USA and published in the Reliability Engineering and System Safety journal (see Mohaghegh et al., 2009). The journal article reviews a number of modelling approaches that could be used to capture HOFs for PRA more adequately. SD is one of the reviewed approaches and the authors discuss how it could be combined with approaches traditionally used within PRA.

The 2009 article of Zahra Mohaghegh and her colleagues points to the 2004 Ph.D. thesis of David Cooke from the University of Calgary in Canada, which discusses the use of SD within HOF analysis for AA. This is the third study that had influenced the research presented in this thesis.

The fourth study was the investigation report into the 2006 British RAF Nimrod XV230 aircraft crash in Afghanistan (Haddon-Cave, 2009). The report was brought to the attention of the author of this thesis by Professor Jerry Williams. Professor Williams has developed the Human Error Assessment and Reduction Technique (HEART) and greatly contributed to the area of HOF analysis for PRA. The investigation report discusses the circumstances that led to the RAF Nimrod XV230 aircraft crash during a mission over Afghanistan on the 2nd September 2006. According to the report, the aircraft suffered a mid-air fire which resulted in the loss of the aircraft and the death of all 14 crew members on board. The aircraft crew neither contributed to the fire nor had any chance of controlling the fire. The key conclusion of the investigation report is that the human and organisational factors that contributed to the crash arose years before the accident and included the following:

- Nimrod aircraft XV230 design flaws introduced at three stages: in 1969, 1979 and 1989
- poor assessment of risks associated with the operation of the Nimrod XV230 aircraft; the assessment was mandated by regulations officially introduced in 2002, was undertaken between 2001 and 2005 and captured in the Nimrod Safety Case; if it had been done properly, it would have identified the aircraft design flaws and would have probably prevented the accident
- major organisational changes in the arrangements for Defence equipment and RAF aircraft between 1998 and 2006 which *"led to a dilution of the airworthiness regime and culture within the Ministry of Defence, and distraction from safety and airworthiness issues as the top priority"* (Haddon-Cave, 2009, p. 12); these organisational changes were underlying the poor preparation of the Nimrod Safety Case
- delays in the Nimrod MRA4 replacement programme which resulted in the Nimrod XV230 still flying in 2006; if there had been no delays, the Nimrod XV230 would have already reached its out-of-service date and would have been replaced by Nimrod MRA4.

It has been long recognized that HOFs play an important role in accidents. The significant role of HOFs in accidents has been highlighted by a number of publications over the years, including Turner (1978), Perrow (1984), Reason (1990, 1997) and Rasmussen (1997). In addition, the importance of HOFs was highlighted during the investigations into the Three Mile Island accident (1979), Bhopal disaster (1984), Chernobyl (1986), Challenger disaster (1986) (Kirwan, 1994) and more recently in the Columbia disaster (2003) or Polish Air Force TU-154 crash in Russia (2010). The Haddon-Cave investigation report confirms that HOFs still significantly contribute to accidents and presents a compelling illustration of how seemingly remote Organisational Factors can contribute to major accidents.

The four studies discussed above motivated the author to explore in detail the literature concerning the topics of PRA, AA, HOF analysis and SD. These explorations led to specification of the aim of this thesis and are captured in this chapter.

Firstly, key terms used in this thesis are defined. Secondly, the nature of factors contributing to accidents in complex technological systems is discussed. The special emphasis is placed on HOFs. Then, the objectives and key stages of AA and PRA are presented and the role of HOF analysis within PRA and AA is explained. Next, the traditional approaches used in the analysis of HOFs for PRA and AA are discussed. Finally, the SD modelling approach is introduced and its use to support risk management of complex technological systems is briefly discussed.

Overall, this chapter introduces the reader to the field of risk management of complex technological systems and presents the critique of the relevant literature that led to the specification of the aim of this thesis. The information provided in this chapter should enable the reader to fully understand the remaining chapters of this thesis.

2.2 Definition of key terms

Previous sections introduced terms such as *hazards, risks, accidents* and *risk management.* Obviously, these terms are very important in the field of the risk management of complex technological systems. However, there is often disagreement on what these terms actually mean. Sometimes, the same terms are defined differently in various studies. This can be confusing. The aim of this section is to provide the reader with definitions of these terms as used within this thesis.

2.2.1 Hazards, risks and accidents

The Health and Safety Executive (HSE) (2013), a national independent organisation that regulates work-related health and safety in the UK, defines *hazard* and *risk* as follows:

> ***Hazard*** - "*is a source of danger. It can be anything, e.g. an object, condition or activity that can cause adverse effects*".
>
> ***Risk** – "is the likelihood that a hazard will cause its adverse effects, together with a measure of the effect. It is a two-part concept and you have to have both parts to make sense of it. Likelihoods can be expressed as probabilities (e.g. one in a thousand), frequencies (e.g. 1000 cases per year) or in a qualitative way (e.g. negligible, significant, etc.). The effect can be described in many different ways. For example:*
>
> - *The annual risk of a worker in Great Britain experiencing a fatal accident [adverse effect] at work [hazard] is less than one in 100,000 [likelihood];*
> - *About 1500 workers each year [likelihood] in Great Britain suffer a non-fatal major injury [adverse effect] from contact with moving machinery [hazard]; or*

- *The lifetime risk of an employee developing asthma [adverse effect] from exposure to substance X [hazard] is significant [likelihood].”*

Apart from harm to people, other adverse effects of concern in the field of the risk management of complex technological systems include harm to the environment and property damage.

A simple example illustrates the difference between hazards and risks. A floor that was just mopped presents a hazard to people who pass through it as they may slip, fall and injure themselves. When a wet floor warning sign is placed on the floor, then the hazard is still present, but the risk is reduced. If somebody slips on the wet floor, falls and injures themselves, we say that the hazard caused its adverse effects and an accident occurred. Leveson (1995) defines an accident as “*an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss”* (p.175). She differentiates an accident from an incident, which she defines as “*an event that involves no loss (or only minor loss), but with the potential for loss under different circumstances”* (p. 176). This thesis is mainly concerned with accidents. However, the discussion applies to both accidents and incidents.

2.2.2 Risk management

The HSE defines risk management as a process that involves assessing risk, putting sensible measures in place to control these risks, and making sure these controls work in practice (HSE, 2014).

The risk management process is depicted in Figure 2-1.

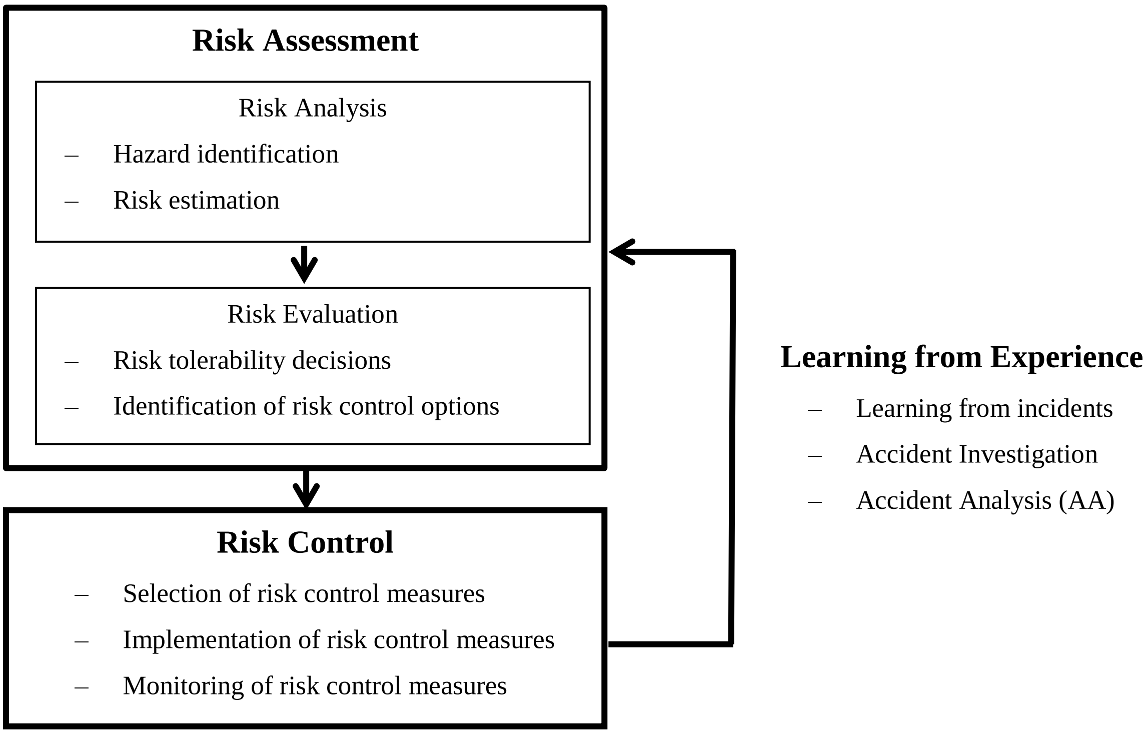

Risk Assessment
Risk Analysis
– Hazard identification
– Risk estimation
Risk Evaluation
– Risk tolerability decisions
– Identification of risk control options
Risk Control
– Selection of risk control measures
– Implementation of risk control measures
– Monitoring of risk control measures
Learning from Experience
– Learning from incidents
– Accident Investigation
– Accident Analysis (AA)

Figure 2-1: Risk management process (adapted from BSI, 1996)

Risk Assessment, Risk Control and Learning from Experience are the key of parts of the risk management process.

Risk Assessment involves Risk Analysis and Risk Evaluation. Risk Analysis is concerned with identification of hazards and potential adverse effects and the estimation of the level of risk. Risk Analysis that expresses risk quantitatively is often referred to as Quantitative Risk Analysis or Probabilistic Risk Analysis. The last term, Probabilistic Risk Analysis (PRA) is usually used in the literature and is used throughout this thesis. Risk Evaluation involves making judgements on whether the level of risk is tolerable or not and identification and analysis of risk control options. The outputs of Risk Assessment include the following:

- information on hazards and potential adverse effects associated with these hazards
- assessment of the level of risk arising from work activities
- information on which work activities contribute to the risk level the most and merit closer examination

- risk tolerability decisions
- information on potential risk control measures and costs and benefits associated with their implementation.

These are important inputs into the decision on whether actions should be taken by the duty holder to ensure that the risks are ALARP and what should be done to bring the risks to the ALARP level.

Risk Control involves selecting, implementing and monitoring risk control measures. The outputs of Risk Control include the following:

- decisions on which risk control measures should be implemented and how they should be implemented
- assurance that risk control measures are continuously applied in practice.

Learning from Experience involves learning from observed incidents and accidents. When an accident occurs, Accident Investigation and Accident Analysis (AA) should be conducted. AA involves a structured analysis of how and why an accident occurred and helps to understand which risk control measures were ineffective and why they were ineffective. AA may be conducted as part of Accident Investigation or later and may involve analysis of an accident report. The outputs of the Learning from Experience process may include the following:

- information on effectiveness of risk control measures
- areas of risk assessment that need to be reviewed
- recommendations for new risk control measures and information on costs and benefits associated with their implementation
- information on new risks that need to be assessed
- recommendations for improving the risk management process.

These are important inputs into the decision on what actions should be taken by the duty holder to keep the risks at the ALARP level or bring them back to the ALARP level.

Risk Assessment, Risk Control and Learning from Experience are complementary activities concerned with ensuring that risks are ALARP and preventing accident occurrence or reoccurrence. There are a number of factors that contribute to risks and accidents and these are discussed in the section that follows.

2.3 Nature of accidents

Rasmussen (1997) and Leveson (2004) list a number of changes that have occurred after World War II and transformed the nature of modern systems and accidents. Firstly, the fast pace of technological change and the scale and complexity of industrial installations have increased. Secondly, rapid development of communication technology and dependence on information systems has led to a high interconnectedness of systems, where a single decision can have huge consequences and can quickly propagate throughout the society. The relatively recent crisis in the world financial system that was triggered by problems in the United States banking system in 2007 can be seen as an example of this mechanism. In addition, an increase in the aggressiveness and competitiveness of the environments in which many duty holders operate has led to a situation where the key focus is on short-term incentives rather than long-term benefits such as welfare and safety. Finally, the pace of technological changes is much faster than the changes in management and regulatory structures that are supposed to control the risks posed by this technology. This all has raised the potential for and severity of accidents associated with the operation of complex technological systems.

It is now recognised that accidents associated with the operation of complex technological systems occur due to a combination of "*multiple factors, where each may be necessary but where they are only jointly sufficient to produce the accident*" (Reason et al., 2006, p. 2). These factors are often labelled in the PRA and AA literature as Technical, Human and Organisational Factors. To put it very simply, Technical Factors are concerned with hardware and software issues. Human Factors concern actions and decisions of people involved in operation and maintenance of equipment. Organisational Factors relate to the wider organisational context in which equipment is operated and maintained and people work, including the arrangement of work processes and interactions between people. There is a tendency in the PRA and AA literature to use the term:

- Human Factors when discussing decisions and actions of people at operational levels of the company, i.e. operators and maintainers involved in daily operation and maintenance of technical systems
- Organisational Factors when discussing decisions and actions of people who are not actively involved in operation and maintenance of technical systems. These people include senior managers, designers of equipment etc. Their decisions and actions may create conditions (for further discussion see the next section) that can influence performance of technical systems and operators and maintainers. In addition, decisions and actions of managers shape organisational structure (i.e. how work processes are arranged) and organisational safety culture (see the next section).

The significant role of Human Factors and Organisational Factors (HOFs) in accidents has been recently emphasized by Enrico Zio. In his article, published in the Reliability Engineering and System Safety journal, he argues that:

> *"(...) the experience accumulated on occurred industrial accidents in the last few decades has clearly shown that the organizational and human factors play a significant role in the risk of system failures and accidents, throughout the life cycle of a system. This is due also to the fact that the reliability of the hardware components utilized in technological systems has significantly improved in recent years, particularly in those systems requiring high safety standards like those employed in the nuclear and aerospace applications. As a consequence, the relative importance of the errors of the organizations managing the systems and of the human operators running them on the risks associated to the operation of these systems has significantly increased (...)"* (2009, p. 131).

The significant role of HOFs in accidents has been highlighted by a number of publications over the years, including Turner (1978), Perrow (1984), Reason (1990,

1997) and Rasmussen (1997). In addition, the importance of HOFs was highlighted during the investigations into the Three Mile Island accident (1979), Bhopal disaster (1984), Chernobyl (1986), Challenger disaster (1986) (Kirwan, 1994) and more recently in the Columbia disaster (2003), Royal Air Force (RAF) Nimrod aircraft accident in Afghanistan (2006) and Polish Air Force TU-154 crash in Russia (2010). They all have indicated that humans and systems "*tend to introduce significant correlations and dependencies*" which can reduce the effectiveness of safety barriers implemented at hazardous facilities to protect against hazards (French et al., 2011, p.754). Our current understanding of how HOFs contribute to risks and accidents is discussed in the next section.

2.4 Human and Organisational contribution to risks and accidents

It is now widely recognised in the PRA and AA literature that:

- Decisions and actions of different people, from operators, maintainers, through designers to managers, can contribute to accidents (Reason, 1997). Some of these decisions and actions are taken years before an accident occurs. Turner (1978) refers to this when he talks about long "incubation periods" of accidents.
- Decisions and actions of people, decisions of managers and designers in particular, may create undesirable conditions such as design flaws, time pressure, understaffing, fatigue, inexperience, and unworkable procedures which are often "latent" (Reason, 1997) - their existence is revealed only when an accident occurs. It is the interaction of these conditions with local events and unsafe acts of frontline staff that usually triggers accidents. Similarly, Rasmussen (1997) describes accidents as the final stage of a system's "migration" to a state of increasing risk and the boundary of acceptable safety performance, where a slight variation in somebody's behaviour can lead to an accident. Had this particular "variation" been avoided, something else, at a different point in time would have led to the accident.

- Decisions and actions of people depend on their level of commitment towards safety, their knowledge and their experience, and these are shaped by organisational safety culture. The notion of safety culture was coined after the Chernobyl disaster (1986) (Cox and Flin, 1998). Safety culture was defined by the International Atomic Energy Agency (IAEA) (1991) as *"that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance"* (p.4*).* Since then it has been used in other industries and a number of new definitions and measures of safety culture have been proposed. Development of most of them was mainly informed by the studies on organisational culture (Cox and Flin, 1998). Later a debate on the relationship between safety culture and safety climate has emerged. The most recent and useful attempt to define these terms is the publication of Mohaghegh and Mosleh (2009a). They explore the concepts of safety culture and safety climate in an attempt to clarify a "*theoretically sound set of principles on which models of organisational influences could be built"* (p. 1139). They found Shein's (1992) definition of organisational culture very useful and used it to define safety culture as "*a pattern of shared basic assumptions that the group learned as it solved its safety problems (external and internal), that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those safety problems*" (p. 1152). They distinguished safety climate from safety culture and defined safety climate as *"a perceptual construct originating at the individual level, called psychological safety climate. Psychological safety climate is the individual's perception of organizational safety structure and practices. If a consensus among the individuals' perceptions exists, their perceptions can be meaningfully aggregated to represent the subunit or organizational safety climate"* (p. 1154).
- In day-to-day decision making, while responding to local pressures and performance and cost goals in the competitive environment, people adjust their behaviour to find easier and faster ways to perform tasks (Rasmussen,

1997). While this process may be sensible at the time and often leads to innovation and improvement of work processes, it may also lead to systematic degeneration of defences and risk controls (e.g. safety procedures and processes) (Rasmussen, 1997; Leveson, 2004; French et al., 2011).

- Human decisions and actions operate within feedback structures. Decisions are based on the available information about the state of the technical systems, which lead to actions that change the state of these systems and then lead to new decisions and actions, forming a feedback loop. This feedback loop often involves delays and non-linear relationships. Time is required to collect information and make decisions based on the collected information. Also, time is required to convert decisions into actions that change the state of technical systems. Apart from this, there may be non-linear relationships between inputs and outputs at various stages of this process that may significantly affect the state of the system over time. Interacting feedback loops, delays and non-linear relationships may lead to unintended consequences of human decisions and actions and affect the effectiveness of the human control of technical systems (Leveson, 2004).
- People make decisions and take actions within their local setting and often do not account for the possible effects of these decisions on other parts of the system. The "Principle of bounded rationality" formulated by Herbert Simon in 1957 refers to these limits of human decision-making. It suggests that complexity of real world processes, time constraints and limitations in human cognitive capabilities make it impossible for humans to behave in an "objectively rational" manner (Simon, 1957; see also Simon, 1982; Cyert and March, 1963; Nelson and Winter, 1982; Hogarth, 1987; Kahneman et al., 1982; Bazerman, 2006). Daily human decision-making processes involve a number of "heuristics and biases". People cannot process all the information that is needed for rational decision-making and take "shortcuts", e.g. they use rules of thumb and simple routines when selecting information to be assessed and making decisions. For example, they use information that is readily available or can be easily recalled. Most of the decisions that are made this way *"are sound using a local judgement criterion and given the time and*

budget pressures and short-term incentives that shape behavior. Experts do their best to meet local conditions and in the busy daily flow of activities are unaware of any potentially dangerous side effects. Each individual decision may appear safe and rational within the context of the individual work environments and local pressures, but may be unsafe when considering the larger socio-technical system as a whole: It is difficult if not impossible for any individual to judge the safety of their decisions when it is dependent on the decisions made by other people in other departments and organizations" (Leveson, 2004, p.246). In addition, people perform poorly when dealing with dynamic systems. When assessing information and making decisions, they often do not account for feedback processes, delays between actions and their results, and non-linear relationships (see e.g. Diehl and Sterman, 1995; Paich and Sterman, 1993, Kampmann and Sterman, 1998, Sterman, 2000).

In summary, it could be argued that analysis of accidents, both potential (the domain of PRA) and those that have already occurred (the domain of AA), is a challenging research area at the interface of engineering and social science. As reliability of equipment has increased over the years, the key areas of concern in the risk management of complex technological systems have moved towards human and organisational aspects of these systems (Leveson, 2004; Zio, 2009; French et al., 2011). Decisions and actions of various people, from operators and maintainers, through designers to managers can contribute to accidents in a number of ways. A number of approaches have been proposed to capture the contribution of HOFs to accidents and risks. The traditional approaches used within AA and PRA to support the analysis of HOFs will be discussed in the sections that follow. Before this, the objectives and key stages of PRA and AA will be described. The sections that follow should provide the reader with a good understanding of the role of HOF analysis within PRA and AA and the benefits and limitations of the approaches currently used to support it.

2.5 Accident Analysis (AA)

The aim of this section is to provide an overview of AA and HOF analysis for AA, including their objectives, key stages and the approaches traditionally used to support them.

2.5.1 Overview

AA is concerned with analysis of accidents that have occurred. The objective of AA is to answer the following questions:

1. What happened?
2. Why did it happen?

The overall approach adopted within traditional AA is referred to as the Root Cause Analysis (RCA) approach (Livingston et al., 2001; Energy Institute, 2008). In this approach, accidents are conceptualised as sequences of discrete events and conditions which lead to adverse effects. An event represents a single, discrete occurrence of very short duration characterised by a change of state. A condition represents a state that exists for some period of time (Kingston et al., 2007). The specification of the sequence of events and conditions answers the first question above: "What happened?" This provides a good basis for the subsequent analysis of root causes of the accident that answers the second question above. As mentioned in the previous chapter, a root cause can be defined as "*the most basic cause [of the accident] that can be reasonably identified and that management has control to fix*" (Paradies and Busch, 1988 in Livingston et al., 2001, p.1, words in the brackets added).

The key stages of AA can be characterised as follows (Livingston et al., 2001):

1. Identification and analysis of the sequence of events and conditions which led to the observed adverse effects.
2. Identification of critical events and conditions in the sequence of events and conditions identified in the previous stage. These critical events and conditions are referred to as direct causes of the accident.

3. Identification and analysis of root causes of the critical events and conditions identified in the previous stage.

There are a number of approaches that are used to support RCA. Livingston et al. (2001) and Johnson (2003) review the frequently used approaches. Popular approaches to identify events and conditions comprising an accident include the Events and Causal Factors Analysis (ECFA) approach and the Events and Conditional Factors Analysis (ECFA+) approach. ECFA+ (Kingston et al., 2007) is based on the ECFA approach that was developed by Buys and Clark (1995). These approaches are often combined with Barrier Analysis and Change Analysis (see Johnson, 2003) or Fault Tree Analysis (Vesely et al., 1981) to facilitate the identification of direct causes of the accident. The aim of Barrier Analysis is to analyse the risk control measures that were in place at the time of the accident and find out why they were inadequate. Change Analysis is used to analyse the differences between what occurred and what was expected to occur (Johnson, 2003). Fault Tree Analysis is a modelling approach usually used to identify faults that have led to the top event of a fault tree, e.g. an equipment failure (Vesely et al., 1981). Livingston et al. (2001) review a number of approaches to support identification of root causes of accidents. The majority of them are checklists presented in a form of a tree or a simple list, e.g. Management and Oversight Risk Tree (MORT) (Johnson, 1973). In addition, all-encompassing approaches exist, often software based and developed for specific industries, which cover all three AA stages defined above, for example Reason Root Cause Analysis developed by Decision System Inc. in 1997 (Livingston et al., 2001). These approaches usually utilise and combine other approaches such as ECFA, Barrier Analysis or Fault Tree Analysis. Overall, it could be argued that most approaches used to support AA offer a structured way of analysing information coming from Accident Investigation and identifying root causes of accidents and are not modelling approaches as defined in the OR/MS literature. Fault Tree Analysis, ECFA and ECFA+ could be considered as exceptions. However, it could be argued that the usefulness of modelling approaches is acknowledged in the AA literature and they are getting increasing recognition in the AA community (see e.g. Sklet, 2004; Energy Institute, 2008; Johnson, 2003).

An overview of HOF analysis and discussion of the limitations of the RCA approach is presented in the next section.

2.5.2 HOF analysis for AA

HOF analysis for AA is concerned with identification, description and analysis of how people contributed to the accident and identification of human and organisational root causes of the accident. The approaches mentioned in the previous section such as ECFA, ECFA+, Barrier Analysis, Change Analysis and even Fault Tree Analysis can be used to analyse all aspects of accidents, including HOFs. However, there are also approaches specifically devoted to the task of HOF analysis. The Energy Institute in its 2008 report (Energy Institute, 2008) reviews both types of approaches and discusses how they could be used to support HOF analysis. Examples of these approaches include Why Because Analysis (WBA) and the Human Factors Analysis and Classification System (HFACS). WBA starts with the description of the accident (e.g. train derailed) and proceeds by using the “why-because” structure e.g. train derailed (why?), because rails were broken. Thus, the logic behind it is the same as in Fault Tree Analysis. The HFACS provides a set of checklists that can help to classify HOFs involved in the accident. It usually complements other methods such as ECFA or ECFA+.

Overall, the key characteristics of the RCA approach underlying traditional AA and HOF analysis for AA are as follows:

– explanation and representation of accidents in terms of discrete events and conditions leading to adverse effects
– search for root causes of accidents.

This approach has a number of limitations, especially when used to analyse HOFs. RCA relies on the representation of accidents in terms of events and conditions. However, as discussed in the previous sections, human decision-making operates within feedback structures. Decisions are based on the available information about the state of the technical systems, lead to actions that change the state of these systems and then lead to new decisions and actions, forming a feedback loop. It is difficult to incorporate these types of structures in sequential, event-based models such as ECFA, ECFA+ or Fault Trees (see e.g. Leveson, 2004).

A number of authors argue that the concept of a "root cause", underlying traditional approaches to AA and HOF analysis, limits the usefulness of HOF analysis within AA for risk management (e.g. Reason, 1997; Hollnagel, 2004; Leveson, 2004; Reason, 2006). As mentioned before, a root cause can be defined as "*the most basic cause [of the accident] that can be reasonably identified and that management has control to fix*" (Paradies and Busch, 1988 in Livingston et al., 2001, p.1; words in the brackets added). However, how do we stop and decide what is "*the most basic cause*"? To use Reason's words (1997, p.15): "*In theory, one could trace the various causal chains back to the Big Bang*."

In addition, the results of RCA may be misleading and lead to the design of ineffective accident prevention measures. To understand the last suggestion let us consider an example, described by Mohaghegh and Mosleh (2009a), of three Systems A, B and C that have "training" and "selection" systems of varying quality. Let us assume the following:

- System A has a "medium" quality training system and a "medium" quality selection system
- System B has a "low" quality training system and a "high" quality selection system
- System C has a "low" quality training system and a "low" quality selection system.

On average, the level of staff competence, the output of the selection and training systems, will be the same in Systems A and B. If an accident happens in System C, the accident investigation may identify an inadequate training system as one of the root causes of the accident, despite the fact that the same quality of the training system in System B did not lead to the accident. A different explanation would be more useful. The accident occurred in System C as a result of the *interaction* between the training and the selection system. Each of these systems was necessary but not sufficient for the accident to occur**,** but they were jointly sufficient to lead to the accident.

2.5.3 Summary

AA is concerned with analysis of accidents that have occurred. It helps those responsible for risk management of complex technological systems understand how and why an accident happened so that its reoccurrence can be prevented.

HOF analysis for AA is concerned with identification, description and analysis of how people contributed to the accident and identification of human and organisational root causes of the accident.

The key characteristics of the RCA approach underlying traditional AA and HOF analysis for AA are as follows:

- explanation and representation of accidents in terms of discrete events and conditions leading to adverse effects
- search for root causes of accidents.

Sequential and event-based approaches such as ECFA, ECFA+ or Fault Tree Analysis are not capable of capturing feedback relationships, characteristic of HOFs. In addition, the search for root causes of accidents can often lead to design of inadequate accident prevention measures.

AA is concerned with analysis of accidents that have occurred. PRA is concerned with analysis of potential accidents. These two types of analysis are conceptually similar: they both involve retreating from a previous understanding of a system and developing a new understanding of a system and risks it is exposed to (Dekker, 2006). In addition, the assumptions underlying root-cause-based AA and PRA are also similar. This is discussed in the next section.

2.6 Probabilistic Risk Analysis (PRA)

The aim of this section is to provide an overview of PRA and HOF analysis for PRA, including their objectives, key stages and the modelling approaches traditionally used to support them.

2.6.1 Overview

PRA is concerned with analysis of potential accidents that have not occurred yet. The objective of PRA is to answer the following questions (Bedford and Cooke, 2001):

1. What can happen?
2. How likely is it to happen?
3. Given that it occurs, what are the consequences?

To answer the first question PRA identifies hazards and the ways in which adverse effects may realize. In PRA, as in AA, the conversion of hazards into their adverse effects (and thus specification of what may happen) is conceptualised by the sequence of discrete events (e.g. emergency power generator fails) and conditions (e.g. low temperature present), called a scenario, and represented graphically using Event and Fault Trees (Bedford and Cooke, 2001).

Event Trees use “forward logic”, i.e. analysis starts with an “initiating event” (anything that causes deviation from the desired system operation) and different ways in which this event may lead to adverse effects are considered. These events are usually ordered temporally. A Fault Tree uses a “backward logic”, i.e. given a particular event (top event), for example, a failure of a system, different combinations of basic events that can lead to the top event are considered. Event Trees are used to show evolution of a system over time. Fault Trees provide a static view of a system (Bedford and Cooke, 2001).

The uncertainty associated with the occurrence of events in each scenario is quantified by probabilities or frequencies. Thus, the second question is answered by specifying the probability or frequency of each scenario occurring. Each scenario leads to an "end state", which defines the consequences of an accident. The specification of "end states" is the answer to the third question. Thus, the output of PRA is the estimate of risk that is defined as a series of triplets (scenario, probability, consequence) (Bedford and Cooke, 2001).

Apart from Event and Fault Trees, other modelling approaches used within PRA include the Bayesian Belief Net (BBN) and Common Cause Failure approaches that are used to capture uncertain dependencies between events and conditions using conditional probabilities (Bedford and Cooke, 2001).

As PRA supports analysis of events and conditions that are highly uncertain and that almost never occur, the validation of models created to support PRA is difficult. The PRA Procedures Guide developed by the U.S. National Regulatory Commission (USNRC) (1983), a guide to PRA that is well-known in nuclear industry, states the following:

> *"Theoretically, a PRA has quality when it represents real life, but this attribute cannot be measured. Therefore, a PRA is said to have quality when the insights or risk profiles it produces reflect the appropriate use of risk-assessment methods as well as information about the plant - and when the resulting documentation clearly and accurately conveys the resulting insights and risk profiles as well as their bases"* (p. 2-13).

Thus, to build confidence in PRA models and their outcomes, and due to the interdisciplinary nature of the topic, a number of people are involved in PRA, e.g. people who have good knowledge of PRA and modelling approaches used to support it, and people who have extensive knowledge of the system such as operators, maintainers, engineers and experts in HOF analysis. In addition, "quality" of the

PRA models and their outputs is enhanced if the following steps are taken (USNRC, 1983):

- clear definition of the objectives and scope of the study
- selection of accepted sources of information – this is particularly important when quantifying accident sequences; the data inputs required for PRA include component failure rates, repair times, common cause probabilities, human error probabilities and uncertainty characterisations; these inputs can be obtained by statistical analysis of raw data, from generic data sources or obtained from experts – in each case the data source and procedure used to obtain these data should be clearly documented
- assumptions underlying PRA models and sources of information should be clearly documented
- if possible, PRA models and their outcomes should be reviewed by a range of people, e.g. the PRA team members, those who have the knowledge of the system, by peers – people who are not involved in the study, but have knowledge and capabilities equivalent of those who have undertaken the particular PRA – and by management to confirm that the PRA met the objectives specified at the beginning of the study.

This concludes the overview of PRA. Now, the focus will move to HOF analysis for PRA, which is discussed in the next section.

2.6.2 HOF analysis for PRA

The approaches to the analysis of HOFs for PRA can be usefully divided into two groups: Human Reliability Assessment (HRA) approaches and Organisational Factors Analysis (OFA) approaches. The focus of HRA is on the identification and analysis of decisions and actions of operators and maintainers that can contribute to the scenarios captured by Fault and Event Trees. The analysis of the wider organisational context, in which operators and maintainers work, is usually very limited. OFA has been suggested in the PRA literature to address this limitation of the HRA approaches. The traditional HRA and OFA approaches are discussed below.

Human Reliability Assessment

One of the well-known and comprehensive publications in the area of HRA for PRA is Kirwan's 1994 book entitled "A guide to practical Human Reliability Assessment". In addition, recently, The Health and Safety Laboratory (HSL) (2009) prepared a review of HRA approaches for the Health and Safety Executive (HSE). The content of this section is largely derived from these two publications.

According to various sources (e.g. Kirwan, 1994; Swain, 1990), HRA dates back to the 1950s/1960s. The first large-scale application of HRA within a PRA study was the WASH-1400 Reactor Safety Study (Rasmussen, 1975) that focused on the analysis of risks associated with the operation of a nuclear power plant (Bedford and Cooke, 2001).

HRA is concerned with identifying what human errors can occur, how likely they are to occur and, if appropriate, designing measures to:

- prevent errors from occurring
- reduce likelihood of errors
- reduce the impact of errors on the analysed system.

The term "human error" can be defined as "*any member of a set of human actions or activities that exceeds some limit of acceptability, i.e. an out of tolerance action (or failure to act) where the limits of performance are defined by the system*" (Swain, 1989 in Kirwan, 1994, p. 1).

To fit into the quantitative and probabilistic PRA framework, HRA is also quantitative and probabilistic in nature and it involves estimation of Human Error Probabilities (HEPs). HEPs are usually defined as the ratio of the number of errors that occurred and the number of opportunities for error (Kirwan, 1994). However, Bedford and Cooke (2001, p. 220) find this definition highly unsatisfactory as it is difficult to categorize opportunities for errors when it comes to humans. Humans learn from mistakes and there are no two individuals who would face the same situation with the same level of experience. Thus, they conclude that HEPs should be based on the subjective definition of probability (According to the subjective interpretation of probability, probability that A will occur P(A) can be defined as a "*degree of belief, of one individual, in the occurrence of A*" [Bedford and Cooke, 2001, p. 24]).

The key steps in traditional HRA are as follows (Kirwan, 1994):

1. **Problem definition** – make a decision on what HRA should focus on. This is related to the scope of the PRA study. The human tasks usually analysed include those performed by operators and maintainers under normal operating conditions and those performed after an "initiating event" has occurred. The former include routine tasks such as maintenance, testing, calibration and restoration tasks. These tasks can introduce latent faults (dormant state of an item characterised by its inability to perform a required function) into the engineered safety systems designed to mitigate the consequences of "initiating events". The latter tasks involve diagnosis and decision-making tasks that are critical to cope with the abnormal situation that arises after an "initiating event" occurs
2. **Task Analysis** – define how selected tasks should be carried out
3. **Human Error Identification** – identify possible errors in performing the tasks. These errors may include: errors of omission (failing to carry out a required task), errors of commission (performing an action that is not required, e.g. selecting wrong control or issuing wrong command) and error-recovery opportunities (actions that can recover previous errors)
4. **Representation** – represent the above information in a form that facilitates quantification of human errors. As PRA usually uses Fault and Event Trees, human errors are often embedded in this framework
5. **Human Error Quantification** – estimate HEPs and assess the impact of contextual factors on human performance. This is usually accomplished by making HEPs functions of selected Performance Shaping Factors (PSFs) i.e.

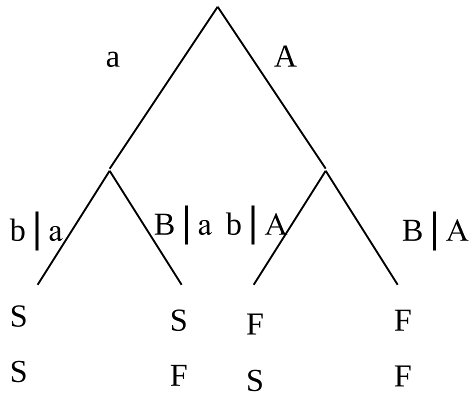
any characteristics of a human or the environment in which he/she is working that influences his/her performance

6. **Impact Assessment** – once human errors have been quantified and represented in Fault and Event Trees and the overall risk has been calculated it can be assessed whether the risk is too high. If yes, it can be determined which factors contribute to the level of risk the most. If human errors significantly contribute to the overall risk, then they can be selected for error reduction
7. **Error Reduction Analysis** – design measures to prevent errors from occurring, to reduce their likelihood or to reduce their impact on the analysed system.

A number of approaches have been developed to support different stages of the HRA process, the Human Error Quantification stage in particular. Recently, the Health and Safety Laboratory (HSL, 2009) prepared a review of HRA approaches for the Health and Safety Executive (HSE). Their report provides in-depth description and discussion of 35 approaches identified in the published and non-published literature on the subject and distinguishes 1st and 2nd generation approaches. The key 1st generation approaches discussed in the report are the following:

- Technique for Human Error Rate Prediction (THERP)
- Human Error Assessment and Reduction Technique (HEART).

THERP (Technique for Human Error Rate Prediction) is the most comprehensive 1st generation HRA approach. It was developed at Sandia National Laboratories (see Swain and Guttmann, 1983) and used in the 1975 WASH-1400 Reactor Safety Study (Rasmussen, 1975). The THERP procedure follows the HRA process described above (i.e. problem definition, task analysis etc.). Essentially, the THERP procedure involves identification of human activities with the potential to affect the analysed system's performance, decomposition of these activities into tasks, assignment of nominal HEPs to each task, assessment of the effects of PSFs on performance of each task, assessment of the effects of dependence between tasks and estimation of the overall HEP associated with performing this sequence of tasks. The sequences of human tasks are modelled using HRA event trees. Each branch of the tree represents a success or failure in accomplishing a particular action. An example HRA event tree is presented in Figure 2-2. Task “A” in Figure 2-2 could be calibration of a sensor by a technician. Assigned to the branches are the probabilities of successfully (a) or unsuccessfully (A) completing task “A”. The following branches represent conditional probabilities of successfully/unsuccessfully completing task “B” given the successful/unsuccessful completion of task “A”. The completely successful path is the first path ending with SS (success, success).



Task “A” = the first task

Task “B” = the second task

a = probability of successful performance of task “A”

A = probability of unsuccessful performance of task “A”

b│a = conditional probability of successful performance of task “B” given a

B│a = conditional probability of unsuccessful performance of task “B” given a

b│A = conditional probability of successful performance of task “B” given A

B│A = conditional probability of unsuccessful performance of task “B” given A

S = success

F = failure

Figure 2-2: An example of a HRA event tree

Different types of HEPs are associated with the use of HRA event trees. Nominal HEPs are probabilities of human errors without considering the effects of site-specific PSFs (e.g. poor lighting, high level of noise). Nominal HEPs along with the modifying values of PSFs are provided for THERP analysts in the THERP handbook

(Swain and Guttmann, 1983). Basic HEPs are the probabilities of human errors without considering the conditional effects of other tasks. Conditional HEPs are modifications of basic HEPs which account for the conditional impact of other tasks. It is very important that the dependence between tasks is correctly reflected via the use of conditional probabilities (Swain and Guttmann, 1983).

THERP is very popular among practitioners and has been widely used in practice. The key advantage of using the THERP approach is the THERP handbook that provides comprehensive guidance and numerical data to support analysts. However, the application of the THERP procedure can be very resource intensive and time consuming.

The HEART (Human Error Assessment and Reduction Technique) approach (Williams, 1986, 1988) was developed by Jerry Williams and designed to be a simple approach to quickly assess probabilities of human errors. HEART describes:

– nine Generic Task Types (GTTs), each with a nominal HEP assigned to it
– a set of Error Producing Conditions (EPCs) to account for site-specific conditions and modify nominal HEPs (EPCs play the same role as PSFs in the THERP approach).

The role of the analyst is (Williams, 1986, 1988):

– to describe the analysed task as one of the nine GTTs
– assign a nominal HEP to the task
– determine whether any EPCs are present in the scenario considered; if yes, then the nominal HEP for this task should be modified by the relevant EPC multiplier.

In the HEART approach, HEP is calculated using the following formula:

$$\boldsymbol{HEP} = HEP_N * \quad {}_{i=1}^{n}[(Maximum_{EPC_i} - 1) * Effect_{EPC_i} + 1]$$

$\boldsymbol{HEP_N}$ – nominal HEP for a particular generic task type (GTT) that represents probability of human error when task is performed in “perfect conditions”

$\boldsymbol{Maximum_{EPC_i}}$ – the maximum strength of the effect that EPC can have on task performance

$\boldsymbol{Effect_{EPC_i}}$ - the strength of the effect that the EPC has on task performance (where the value of 1 is the maximum possible effect).

$\boldsymbol{HEP_N}$ and $\boldsymbol{Maximum_{EPC_i}}$ for a predefined set of EPCs have been provided by the method. Expert judgement is needed to assess the value of $\boldsymbol{Effect_{EPC_i}}$**.**

The key advantage of HEART, as compared to THERP, is that it is a quick and not resource intensive approach of assessing HEPs. However, it provides little guidance of how to select appropriate GTTs, account for the impact of EPCs, assess $\boldsymbol{Effect_{EPC_i}}$ and account for dependencies between tasks. Barry Kirwan and his colleagues (see Kirwan et al., 2004, 2005) used HEART as a basis for the development of another approach called Nuclear Action Reliability Assessment (NARA). Essentially, NARA has the same logic as HEART, but incorporates updated GTTs, EPCs and quantitative data to better fit the needs of PRA and HRA studies for the UK Nuclear Power Plants (Kirwan, 2004).

The HSL’s report summarises the status of the 1st generation approaches as follows: “*First generation approaches (...) are often criticised for failing to consider such things as the impact of context, organisational factors and errors of commission. Despite these criticisms they are useful and many are in regular use for quantitative risk assessments.”* An example of an error of commission (performing an action that is not required) would be when an operator is required to push a button, but pushes a wrong one instead. Errors of commission as such might significantly contribute to the risk level, yet they are very difficult to predict. They might occur at any stage in a task and might not be related to the task’s objectives at all (Kirwan, 1994, p. 177). Also, although some of the 1st generation approaches highlight the importance of the context, they do not provide practical guidance for identifying contextual factors and the likelihood of their occurrence (Cooper et al., 1996, p. A-8).

In response to the criticisms of the 1st generation approaches, the development of the 2nd generation approaches has been taking place since the 1990s. An example of a 2nd generation approach is A Technique for Human Event Analysis (ATHEANA) (Cooper et al., 1996; USNRC, 2000; Forester et al., 2007).

ATHEANA has been developed for the nuclear industry and involves the same steps as the traditional HRA process described above, i.e. problem definition, human error identification, representation, quantification and impact assessment stages. The key points of difference between ATHEANA and the 1st generation approaches such as THERP are summarised below (Cooper et al., 1996, p. 3.2):

- ATHEANA provides more detailed guidance regarding the identification and analysis of errors of commission
- ATHEANA involves more comprehensive consideration of contextual factors affecting human behaviour. The important part of the analysis is the identification, definition and estimation of the likelihood of the existence of Error-Forcing Contexts (EFCs) for each identified human error. EFCs are abnormal situations in which human errors are more likely to occur. EFCs represent the effect of the interaction between performance shaping factors and plant conditions.

NUREG – 1880 describes a structured process for identification of errors of commission and EFCs (see Forester et al., 2007). The recommended sources of data for quantifying human errors within the ATHEANA approach include the following (Cooper et al., 1996, p. 3.6):

- plant-specific or generic failure data (e.g. frequencies of hardware failures)
- plant-specific or generic operating practices (e.g. frequency of preventive maintenance)
- generic human performance data
- expert judgement (e.g. judgement of plant personnel).

Additionally, to support the quantification stage of ATHEANA, an expert elicitation approach was proposed by Forester et al. (2004).

Overall, the key benefit of ATHEANA is that it provides a structured process for developing important qualitative insights on how contextual factors can affect human performance and result in errors. However, the quantitative part of the approach has been criticised and the overall approach has been described as time-consuming and resource-intensive as only a few duty holders will be in a position to conduct such an extensive analysis as envisaged by ATHEANA's developers (HSL, 2009).

As the work on the 2nd generation approaches is still ongoing, the 1st generation HRA approaches are still very popular among practitioners (Chandler et al., 2006). However, as already mentioned, they have a number of limitations of which managers are not always fully aware. These limitations have been recently discussed by French et al. (2011) in their article entitled "*Human Reliability Analysis: A critique and review for managers*". Some of these limitations also apply to the 2nd generation approaches. They include the following:

- A lot of HRA approaches "*tend to focus on easily describable, sequential, generally low-level operational tasks. Yet the human behaviour that is implicated in many system failures may occur in other quite different contexts, maybe in developing higher level strategy or during the response to an unanticipated initiating failure event*" (p.755).
- *"(...) HRA focuses on human errors, whereas many systems failures may arise not just despite, but sometimes because of fully appropriate and rational behaviour on the part of those involved. Thus we need a broader understanding of human behaviour than that relating to human error. We also need to recognise that cultural, organisational, social and other contexts influence behaviour, perhaps correlating behaviour across a system, thus invalidating assumptions of independence commonly made in risk and reliability analyses"* (p.755).

– *"There is a further aspect of context that HRA should consider: decision context. The judgements and decisions needed of humans in a system can vary from those needed to perform mundane repetitive operational tasks through more complex circumstances in which information needs to be sought and evaluated to identify appropriate actions to the ability to react to and deal with unknown and unanticipated. Decision processes will vary accordingly. Design decisions can inadvertently introduce further risks to the system that arise from limitations inherent in human foresight. This means that the appropriate HRA methodology to assess the risks associated with the human decision making behaviour may vary with the details of that context"* (p. 759).

One of the key limitations mentioned above and supported by others (e.g. Leveson, 2004) is that the current HRA approaches rarely recognise or adequately represent the different contexts that influence human behaviour such as the wider organisational context in which operators and maintainers are working and the decision context. As mentioned in previous chapters, the importance of Organisational Factors is acknowledged in the PRA literature and is undisputed. Organisational Factors may act as a common factor affecting dissimilar human and also technical system elements at the same time and thus correlate parameters in the PRA models such as equipment failure rates, human error probabilities and component repair times. Not accounting for Organisational Factors in HOF analysis for PRA may lead to a serious underestimation of the risk level.

Some of the traditional HRA approaches such as THERP or HEART account for the impact of the contextual variables on human behaviour such as time pressure, quality of training or workload by selecting Performance Shaping Factors (PSFs) or Error Producing Conditions (EPCs) and by multiplying nominal HEPs by PSF/EPC multipliers to increase this probability. However, usually only proximate influences are taken into account. These approaches do not go beyond PSFs and do not explicitly represent the wider organisational influences on human and technical system performance.

Additionally, while analysing human behaviour, one should consider the decision context in which this behaviour occurs. As French et al. (2011) point out: "*For repetitive events the key contextual pressures on operators that may modify their behaviour are likely to relate to complacency and organisational issues such as excessive workloads or requirements to work at the same task too long. (...)In responding to events ranging from an indication of departure from normal operations to a full blown crisis, adrenaline, the importance of the matter, as well as cognitive interest are likely to focus the mind. So the operators' performance is more likely to be affected by issues such as cognitive overload, miscommunication between several operations and a range of behaviours that we commonly call panic!"* (p.759).

Organisational Factors Analysis

While we can apply the concept of normative (required and acceptable) behaviour to the technical system and even humans, we cannot use the same approach while analysing Organisational Factors. Bier (1999) points out "*there is no 'correct' management style, corporate culture, organisational structure. Rather, these various elements must be consistent both with the demands of the system's environment and with each other"* (p. 707- 708). Differing configurations of management styles, corporate cultures and organisational structures can still produce the same safe (or unsafe) performance. Davoudian (1994a,b) argues that to account for the impact of Organisational Factors on human and technical system performance the following are required:

- models of the system as a whole
- models that will allow for quantification and incorporation of the impact of organisational factors into PRA.

Investigation reports from large scale accidents combined with the existing literature and theories are good sources of information for the creation of the first types of models, i.e. the models of systems as a whole. For example, Cooke (2003, 2004) developed a holistic System Dynamics model of the Westray mine to support his analysis of the Westray mine disaster. He used the model to show how "*Westray management (...) priority on 'production at all costs' over safety in the mine (...) created a chain of events leading to the disaster"* (p.143). His model was later adapted by Mohaghegh et al. (2009) and used within a PRA in the aviation context.

There have been a number of attempts to quantify the impact of Organisational Factors and to incorporate them into PRA. Mosleh and Mohaghegh (2009a) in their review of the publications in this field list the following approaches: MACHINE (Embrey, 1992), WPAM (Devoudian et al., 1994a,b), SAM (Pate – Cornell and Murphy, 1996), Omega Factor Model (Mosleh and Golfeiz, 1999) and Causal Modelling of Air Safety (Roelen et al., 2004). In terms of the key features of these approaches, Mohaghegh and Mosleh (2009a) point out the following:

- Human Factors, including individual decisions and actions, safety critical tasks or models of work processes serve as the link between Organisational Factors and Technical Factors. In addition, Mosleh and Golfeiz (1999) proposed to link Organisational Factors with Technical Factors by using the Omega Parameter, which is a ratio of component failures due to Organisational Factors to component inherent failures
- Analysts use Bayesian Belief Networks (BBNs) or flow diagrams to connect Organisational Factors with Human and Technical Factors (see e.g. Roelen et al., 2004; Devoudian et al., 1994a,b)
- Most of the above approaches use expert judgement, sometimes combined with other tools such as surveys, behavioural checklists, interviews or some relevant data to measure and estimate different model elements.

Mohaghegh and Mosleh (2009a) conclude that there is lack of a comprehensive theory and modelling principles underlying the developments in the area of OFA. Thus, after reviewing the relevant literature, they propose to improve the theoretical foundations of OFA by offering a set of guidelines that could inform the efforts in the field and by reviewing a number of techniques that could support OFA. For example, they clarify the relationships between safety culture and safety climate and define two aspects of Organisational Factors: social (safety culture and safety climate) and structural (organisational structure and practices). In addition, they argue that analysis of HOFs needs to be closely integrated with the analysis of Technical Factors and will require a “hybrid strategy”, i.e. a combination of various modelling approaches to capture these factors adequately. A number of different candidate modelling approaches are proposed, including:

- formal PRA techniques (e.g. Event Sequence Diagram, Fault Tree Analysis, Event Tree Analysis) to represent accident sequences
- process modelling techniques (e.g. Flow Chart, State Chart Diagram, Event Driven Process Chain, Integrated Definition Methodology, Structured Analysis and Design Technique - SADT)
- regression-based techniques (Path Analysis, Structural Equation Modelling - SEM)
- Bayesian Belief Nets and Influence Diagrams
- deterministic dynamic techniques (e.g. System Dynamics or Agent-Based Modelling).

System Dynamics (SD) and the potential benefits of using it within PRA and AA will be discussed in Section 2.7. Before that, a short summary of the topics discussed so far will be provided.

2.6.3 Summary

PRA and AA are important parts of the risk management of complex technological systems. PRA is concerned with identification of hazards, potential adverse effects associated with these hazards and estimation of the likelihood that these adverse effects will realize. AA involves identification of how and why an accident occurred and helps to prevent accident reoccurrence. PRA is concerned with identifying and examining potential accidents (prospective analysis) and AA is concerned with examining accidents that have occurred (retrospective analysis). Logical and mathematical modelling plays an important role in PRA and is gaining increasing recognition within the AA community. HOF analysis is an important part of both PRA and AA. HOFs concern decisions and actions of people involved in design, operation, maintenance and management of complex technological systems. Human decisions and actions operate within feedback structures that involve time delays and non-linear relationships. This is difficult to incorporate in sequential, event-based approaches supporting traditional HOF analysis for AA and PRA. SD is capable of modelling these structures and has been proposed to support analysis of HOFs for AA and PRA. SD and the potential benefits and limitations of using it within AA and PRA are discussed in the next section.

2.7 System Dynamics (SD)

The aim of this section is to introduce SD and discuss its use in the area of risk management of complex technological systems.

2.7.1 Introduction to SD

The foundations of SD were laid in Industrial Dynamics (1961) by Jay Forrester. He described SD as a simulation modelling approach – an approach which focuses on developing a mathematical model to be studied by the means of computer simulation. The purpose of SD, as explained by Forrester, is "*the investigation of the information-feedback character of industrial systems and the use of models for the design of improved organisational form and guiding policy"* (p.13). Essentially, SD, as envisioned by Forrester, was to assist decision-makers in the analysis of the feedback structure of industrial systems and system design and control. Later the name Industrial Dynamics was changed to System Dynamics to reflect the applicability of SD to the analysis of other types of social systems.

Over the years a number of interpretations of Forrester's initial ideas have arisen. Lane (1999) categorised these interpretations and distinguished different types of SD modelling practice, including the following: "Initial SD", "Broad SD", "Interactive SD", "Policy engineering" and "Austere SD". The "Initial SD" practice reflects the ideas presented in Forrester (1961) and later extensions captured in Forrester (1968a,b, 1969, 1971a,b) (Lane, 1999). Lane argues that other types of SD practice are "*elaborations, extensions and implementations*" of Forrester's (1961) key ideas

(Lane, 1999, p. 503). Thus, while characterising the SD modelling approach in this section, the focus is on the “Initial SD” practice. The discussion has been structured around the following questions:

- What is modelled? (What entities are assumed to exist?)
- How is it modelled? (How are the assumed entities modelled?)
- Why is it modelled? (What is the purpose of modelling? How does this purpose affect the model validation process?)

This form of characterisation of a modelling approach was adapted from Mingers (2003).

What is modelled?

Forrester’s focus on the information-feedback characteristics of social systems reflected his experience as a servomechanisms engineer in Massachusetts Institute of Technology’s (MIT’s) Servomechanisms Laboratory and ideas from engineering control theory (Richardson, 1991). Servomechanisms (or information-feedback systems) are automatic devices that control the performance of a mechanism by sensing errors and sending error-correction signals. For example, while at MIT’s Servomechanisms Laboratory, Forrester worked on servomechanisms for controlling radar antennae and gun mounts (Forrester, 1995). SD is the application of these control theory feedback concepts to the analysis of social systems.

In information-feedback systems, information about the state of the system is used to change the current state of the system. In social information-feedback systems, information about the state of the system is collected and used by people to inform decisions and actions that change the state of the system. This is schematically depicted in Figure 2-3.

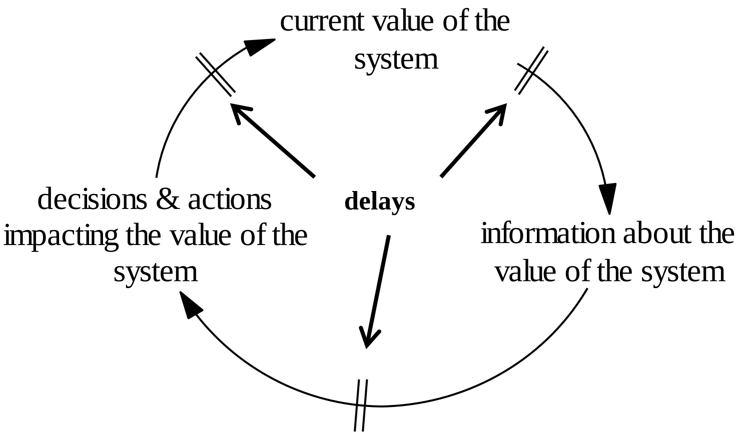

current value of the system
delays
decisions & actions impacting the value of the system
information about the value of the system

Figure 2-3: Information feedback structure of social systems.

The process of collecting and converting information into decisions and actions that affect the state of the system is governed by "*policies*" or "*decision rules*". Forrester's definition of a policy is much broader than "*a formal written organisational policy*". For Forrester policy is simply *"(...) a statement giving the relationship between information sources and resulting decision flows"* (1961, p. 96-97).

The process of collecting and converting information into decisions and actions often involves delays. Time is required to collect information and make decisions based on the collected information. Also, time is required to convert decisions into actions that change the state of the system. In addition, there might be non-linear relationships between inputs and outputs at various stages of this process that may significantly affect the state of the system over time.

A production-distribution system is a classic example given by Forrester of a social information-feedback system. At the end of the production - distribution chain, customer orders deplete retailer's inventory. The information on the customer orders and current stock levels is used by the retailer to order products from distributors or directly from the plant. The products are delivered from the plant or distributor and replenish retailer's inventory so that the retailer can fulfil customer orders. This simple process is complicated by the fact that there are a number of delays involved. Time is needed to collect information about inventory levels, to order products from the plant/distributors and to transport products from the plant/distributors to the retailer. In addition, there are non-linear relationships between inputs and outputs at various stages of this production-distribution process. For example, the fluctuations of the production rate are much higher than the fluctuations of the customer purchase rate (Forrester, 1961). These delays and fluctuations can affect the retailer's ability to fulfil customer orders.

In the SD modelling approach it is assumed that the feedback structure of information feedback systems drives the behaviour of these systems over time. The impact of variables that are outside the system boundary is assumed to be inconsequential. In addition, the information-feedback structure that governs the behaviour of information-feedback systems over time is assumed to be external to the observer, i.e. it is assumed to objectively exist "out there". Also, the assumptions concerning human nature seem to be deterministic. Forrester (1961) argues that "*decisions are not entirely 'free will' but are strongly conditioned by the environment*" (p.17).

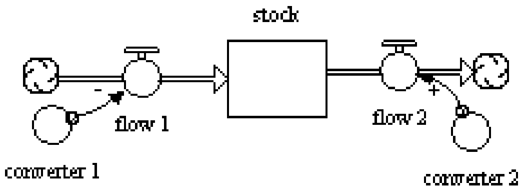
How is it modelled?

The key steps in the SD modelling, as described by Forrester (1961, p.45), are as follows:

1. Definition of the problem (defining the purpose for which the model is built)
2. Description of the system (collection and presentation of the information on the key factors relevant to the problem at hand)
3. Development of a mathematical model of the system (capturing the system feedback-structure using mathematical symbols)
4. Simulation (using the model to simulate the operation of the system over time and to perform experiments)
5. Interpretation of the simulation output (analysis of the results of experiments and comparison to the behaviour of the actual system)

6. System redesign (changing the system structure in order to improve the performance of the system).

The SD modelling approach employs integral and differential equations to represent the key aspects of the information-feedback systems. As the modelled systems are complex and usually no analytical solution for differential equations can be found, these equations are solved numerically. The process is facilitated by the use of computer. To improve the communication of the key assumptions underlying an SD model, diagramming techniques are used that represent the integral and differential equations graphically. These diagramming techniques are typically used before or/and after the mathematical model is built (Lane, 2008). In the former case, the graphical representation is used to facilitate the development of a mathematical model. In the latter case, the graphical representation is used to communicate the key features of an existing mathematical model and to communicate the key conclusions from SD analysis. Two graphical representations are dominant in the SD community nowadays: causal loop diagrams and stock and flow diagrams. Causal loop diagrams are high-level, simplified representations of the feedback structure of the system. Stock and flow diagrams are based on the diagrams used by Forrester in his 1961 book. The key benefit of stock and flow diagrams over causal loop diagrams is that they allow for the places of accumulation (stocks) in the system to be represented (Sterman, 2000; Lane, 2008). These diagrams will be described here and used throughout this thesis. The key elements of these diagrams are shown and explained in Figure 2-4.



Stocks represent **state variables** and describe the condition of a system at any time. Stocks can be physical or non-physical in nature, e.g. they can represent the amount of water in a bathtub (measured in litres), the number of people in a queue, the level of employee competence or commitment (dimensionless, on a scale of 0 to 1) etc.

Flows represent **rate (action) variables** and determine the change per time unit of the state variables. A flow can be used to represent the amount of water flowing into a bathtub per hour, a number of people joining a queue per minute, change in employee competence per day etc. Clouds at the beginning or end of flows indicate the boundary of the model.

Converters represent **constants** or **auxiliary variables** that modify flows.

Arrows represent the **relationships** between the elements of the model and show the direction of influence. An arrowhead indicates the variable that is being influenced.

"+" sign means that an increase (decrease) in **X** results in a value of **Y** that is greater (smaller) than it would have been had **X** not changed

"-" sign means that an increase (decrease) in **X** results in a value **Y** that is smaller (greater) than it would have been had **X** not changed

Figure 2-4: Key elements of a stock and flow diagram

The following assumptions are made when building SD models:

– Variables change continuously with respect to time. Forrester (1961) argues that "*As a starting point, the dynamics of the continuous-flow model are usually easier to understand and should be explored before complications of discontinuities and noise are included"* (p.65). In addition he explains that: **"***Discreteness of events is entirely compatible with the concept of information-feedback systems, but we must be on guard against unnecessarily cluttering our formulation with the detail of discrete events that only obscure the momentum and continuity exhibited by our industrial systems"* (p.67)

– Noise is usually not important and can be omitted from the model. Noise is defined as *"... the part of the decision flow for which we have no satisfactory causal hypothesis"* (Forrester, 1961, p.43). Forrester argues that "*The*

> *preferred practice is to begin with the continuous (nonstochastic) structure of system decisions and later add randomness (...)"* (Forrester, 1961, p.61).

In addition, Forrester (1961) discusses some further points that he considers good practice:

- "*All constants and variables of the model can and should be counterparts of corresponding quantities and concepts of the actual system"* (Forrester, 1961, p.61)
- "*Particular attention must be given to determining what information is actually available and used at each point in the system – much information is not available, much of what is available is not actually used, what is used is not necessarily the most effective of that available"* (Forrester, 1961, p.63).

Various pieces of data are needed to develop the model, for example the data on:

- the structure of the analysed system, i.e. how the parts of the system, relevant to the problem at hand, are related to each other
- policies (decision rules) that guide decision-making within the system, i.e. conversion of information into decisions and actions that affect the state of the system.

The above data can be collected from various sources. The key ones are written organisational records and people. Organisational records include operating procedures, written formal policy, organisational charts, emails, reports, databases etc. In terms of people as sources of the information, the concept of mental models is used within the SD community (Groesser and Schaffernicht, 2012). A mental model is an informal model of how the system operates that people hold in their heads. This includes people's understanding of how information is actually used within the system and how decisions are actually made (as opposed to what is written in procedures). While the organisational records can be accessed directly, mental model data needs to be elicited through, for example, interviews and observation. This internally stored mental data is, according to Forrester (1961), even more important than the externally stored data on tangible objects.

Why is it modelled?

As explained in the previous sections, systems that can be conceptualised as social information-feedback systems are governed by interacting feedback loops that involve delays and non-linear relationships between inputs and outputs. This makes these systems dynamically complex and makes it difficult to anticipate the behaviour of these systems over time. The SD modelling approach supports analysis of these dynamically complex systems and helps people understand and manage them. However, the purpose of SD models, as envisaged by Forrester and succinctly expressed by Lane (1999, p. 503) is "*not just to explain but to aid system re-design and to promote individual and organizational learning in order to impart 'a better intuitive feel [which] improves ...judgement about the factors influencing company success'"* (Forrester, 1961, p.45). To achieve this purpose "precise quantitative predictions of the future" are not required. Rather, the focus is on the identification of "the trends of the key variables" (Roberts et al., 1983, in Howick, 2001, p. 102). This means that the assumptions that underlie most SD models (variables change continuously with respect to time and noise is usually not important and can be omitted from the model) are entirely appropriate for the purpose of SD models.

Forrester (1961, p.56) discusses a number of possible outputs of the SD modelling process that can inform system re-design:

– "*determining the degree to which the (...) system is sensitive to changes in a policy or in system structure*"
– determining "*the relative value of information of differing kind, accuracy, and timeliness*"
– showing "*the extent to which the system amplifies or attenuates disturbances impressed by the outside environment*"
– "*determining vulnerability [of the system] to fluctuation, overexpansion, and collapse*"
– pointing "*the way to policies that yield more favourable performance*".

The model purpose and desired outputs affect the model validation process. Model validation is an important part of the model development process. The purpose of model validation is to ensure that a model is suitable for its purpose and model users can have confidence in model outputs (Williams, 2008; Pidd, 2009). Forrester (1961) argues that an SD model is suitable (valid) for the intended purpose, as described above, if its structure and the behaviour correspond to the structure and behaviour of the actual system. In the former case, each equation, system boundary, variables and links between variables should be examined in relation to the actual system. In the latter case, *"(...) a model should be judged by its ability to reproduce or to predict the behaviour characteristics of the system – stability, oscillation, growth, average periods between peaks, general time relationships between changing variables, and tendency to amplify or attenuate externally imposed disturbances"* (Forrester, 1961, p. 54). "*The ability of a model to predict the state of the real system at some specific future time is not a sound test of model usefulness*" (p. 115). A wide range of information about the actual system, including written, numerical records, available literature and people's mental model data, can be used to compare the elements of the model structure and behaviour to the structure and behaviour of the actual system. However, Forrester (1961, p. 115) argues that the "*ultimate test*" of model suitability for the intended purpose is "*whether or not better systems result from investigations based on model experimentation. (...) The pertinent test is that of utility in improving management practice*." Thus, ultimately, the focus is not on developing models that *accurately* represent the external reality. Rather, according to Forrester, the focus should be on developing models that are useful in serving the purpose of aiding system re-design. "*As a result, the usefulness, and hence validity, of such models would only be appropriately judged in a personal way, 'the evaluation of improved managerial effectiveness will almost certainly rest on a subjective judgement rendered by managers in regard to the help they have received'* [from engaging with a model]" (Forrester, 1961, p.115,) (Lane, 1999, p. 503; words in brackets added). Thus, according to Forrester, validity of a model is, ultimately, a matter of a subjective opinion of those who will be using the model to redesign the system. This view has been shared by other system dynamics practitioners (Barlas, 1996; Barlas and Carpenter, 1990). Barlas (1996) argues that a

SD model validation is “gradual process of confidence building” among model users and it has “informal, subjective and qualitative components” (p.188). However, he stresses that both formal/quantitative and informal/qualitative tests can be used by model users to help them to build confidence in SD models developed. Over years, a number of tests have been discussed to support model users in model validation process (see e.g. Forrester and Senge, 1980; Barlas, 1989, 1996; Barlas and Carpenter, 1990 and Sterman, 2000).

The last decade has seen attempts to apply SD to support risk management of complex technological systems. These are discussed in the next section.

2.7.2 System Dynamics and risk management of complex technological systems

There have been several attempts to apply SD in the area of risk management of complex technological systems. These are briefly discussed below.

Cooke (2003) used SD in his analysis of the factors that contributed to the 1992 Westray mine disaster and showed that “*Westray management placed priority on ’production at all costs’ over safety in the mine, which created a chain of events leading to the disaster”* (p.143). Cooke (2003, p.141) argues that “*the traditional approach to accident investigation follows a linear process of ‘root-cause analysis’, which ignores the effect of feedback and complex interactions between system variables. System dynamics is a tool that can be used to address these concerns”*. However, this work excludes detailed examination of the characteristics of the root-cause analysis approaches and excludes explicit discussion of whether SD should replace the traditional approaches entirely or whether it should be combined with them and how this could be accomplished. Later work of Cooke builds on his SD analysis of Westray mine disaster. Cooke and Rohleder (2006) use SD to explore the benefits of implementing an incident learning system. They use variables *Management Commitment to Safety* and *Personal Commitment to Safety* to represent organisational safety culture and use SD to show how this safety culture can be improved over time by implementing an incident learning system. Their experiments using SD highlight that it may take years to build safety culture and that safety culture can "*wax and wane as productivity pressures come and go"* (p. 231). They use the SD model and simulations to demonstrate the long term, disastrous effects of people not reporting incidents on safety culture and suggest that companies *"should implement a reward system to encourage reporting of incidents and implementation of corrective actions"* (p. 231). This work discusses important archetypical mechanisms that shape safety culture and uses SD to represent these mechanisms and perform experimentation.

The study of Marais et al. (2005) is part of the same line of research. The authors use SD to represent "*archetypes for organisational safety*" that "*model common dynamic organizational behaviours that often lead to accidents"* (p. 565). Among others, using a set of causal loop diagrams, they discuss detrimental effects of complacency, bureaucracy or "*fixing systems rather than root causes*" of accidents. The link between their work and accident analysis and risk analysis is explicit and clear. They argue that: *"As accident analysis and investigation tools, the archetypes can be used to develop dynamic models that describe the systemic and organizational factors contributing to accidents. As risk analysis tools, the archetypes can be used to improve understanding of the ways that risk can arise in complex socio-technical systems"* (p. 565). However, the authors' discussion is generic in nature and there is no demonstration of how SD could be used within PRA or AA.

A similar line of research, but in the SD literature, is the work of Carhart and Yearworth (2010). They highlight the role of archetypes and argue that they could be used to transfer knowledge of HOFs among duty holders and industries. They argue that:

> "*The introduction of system dynamics into the event analysis toolbox, both for internal investigations and the extraction of learning through the exploration of external events could improve the understanding of their underlying causality. This could produce deep learning with a dynamic and contextual appreciation not provided by the current models and tools."* (p. 15)

In addition to the above, Dulac et al. (2005) and Salge and Milling (2006) used SD to model and analyse factors that contributed to the Columbia and Chernobyl disasters, respectively. However, again, there is no detailed discussion in these studies of approaches traditionally used within AA and the role that SD should play in AA.

In terms of using SD for prospective accident analysis, i.e. risk analysis, the group of researchers at MIT was one of the first to propose using SD in this area. For example, Dulac et al. (2005) proposed to combine SD and the STAMP approach and applied this hybrid approach to the analysis of the NASA safety programs. Dulac (2007) developed a set of executable SD models that could be used to analyse time-dependant risks, assist managers in safety related decision-making, create and test mitigation actions and policies and monitor systems for states of increasing risk. The STAMP approach was proposed by Leveson (2004) as an alternative to traditional PRA models and Dulac (2007) does not discuss how SD could be used in the PRA context. Later Dulac et al. (2008) proposed how SD could be used in risk analysis in the healthcare domain. They combined System Dynamics with a Discrete Event Simulation approach to investigate the factors that influence the probability that safety controls (e.g. procedures) will be waived by physicians.

Finally, Mohaghegh et al. (2009) suggested that SD could be used to capture the impact of HOFs on risk within PRA. They showed how SD could be combined with Bayesian Belief Networks, Event Sequence Diagrams (ESDs) and Fault Trees (FTs) within the aviation context. Essentially, they argue that in order to effectively incorporate the impact of HOFs into PRA, one needs to apply a “hybrid” modelling approach. The basic elements and the structure of their hybrid approach (which they use to analyse the impact of airline maintenance operations on the system risk) is summarised in the picture below.

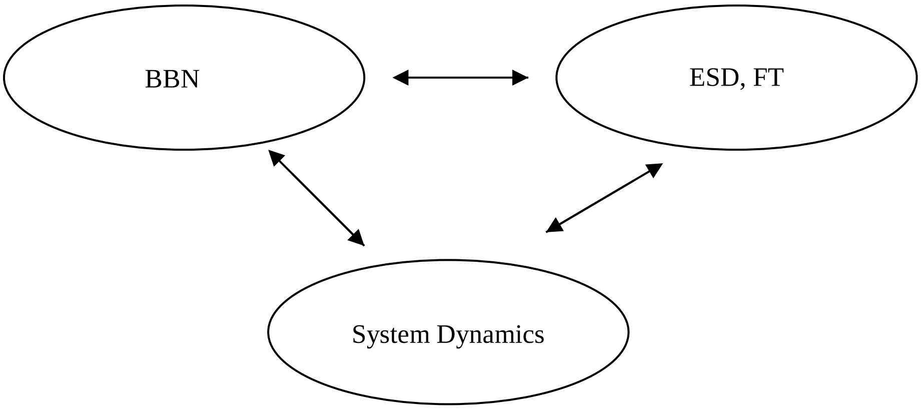


Figure 2-5: Hybrid modelling approach (Mohaghegh et al. 2009b)

The mechanics of the model are the following: the intersection between BBN and ESD-FT parts is supported by the Hybrid Causal Methodology (HCM) and the IRIS software that were developed and described by Mosleh et al. (2005 in Mohaghegh et al., 2009) and Wang (2007 in Mohaghegh et al., 2009). Outputs from both these elements are then fed into the SD module to account for time delays and feedbacks in the system. This connection is, in turn, supported by the SD software Stella and its ability to import and export data. In their example of the application of their hybrid approach, the authors use:

- SD to model safety culture, financial stress, organisational safety practices such as training and hiring and individual-level Performance Shaping Factors
- BBN is used to model maintenance practices and
- FTs and ESDs are used to model technical system risk.

The key contribution of their work was to show how SD could be combined with modelling approaches traditionally used within PRA and to provide a software solution to execute the model. However, they do not explicitly discuss how they developed their hybrid model and whether there are any issues associated with combining SD with modelling approaches traditionally used within PRA.

In summary:

- All of the above studies suggested that it would be beneficial to use SD in the area of risk analysis or accident analysis. Most of them argued that the approaches traditionally used within accident analysis and risk analysis are static and cannot deal with feedback and non-linear relationships, which are present in complex technological systems, and highlighted that System Dynamics is capable of dealing with these problems.
- None of the above studies discussed whether it would be beneficial to combine SD with approaches traditionally used within AA, how it could be achieved and what would be the limitations.
- Apart from Mohaghegh et al. (2009), none of the above studies show how SD could be used within the PRA framework of Fault and Event Trees. However, Mohaghegh and her colleagues only demonstrate that it is feasible to use SD, but they do not discuss in detail the benefits and limitations of using SD in this context.
- As discussed in previous sections, there are a number of well-established modelling approaches used within PRA and AA. The question that arises is whether SD should be combined with them or used as a stand-alone approach. The work of Mohaghegh et al. (2009) suggests that SD can complement modelling approaches traditionally used within PRA. Thus, it can be deduced that SD could probably be combined with approaches traditionally used within AA. Overall, there is little discussion in the PRA and AA literature on how the approaches traditionally used within PRA and AA could be combined with SD and whether there are any issues associated with combining SD with these approaches.

These all are important gaps in the PRA and AA literature and the aim of this thesis is to address them. The summary of the discussion in this chapter and the identified gaps in the literature is provided in the next section.

2.8 Summary of chapter

This chapter provided background and justification for the research undertaken by the author and presented in this thesis. The key conclusions from the review of PRA, AA and SD literature are summarised below:

- Accidents associated with the operation of complex technological systems occur due to a combination of Technical, Human and Organisational Factors. The relative importance of HOFs as contributors to risks and accidents has significantly increased in recent years.
- HOFs represent decisions and actions of different people, from operators, maintainers, through designers to managers, who can contribute or have contributed to accidents. These decisions and actions depend on their level of commitment towards safety, their knowledge and experience, which are shaped by the organisational safety culture and operate within feedback structures. These feedback structures involve time delays and non-linear relationships. In addition, people make decisions and take actions within their local setting and do not account for the possible effects of these decisions on other parts of the system. Also, due to limitations of attention, memory and time, human mental models of complex systems are not capable of processing all the information that is needed for fully rational decision-making. These all often lead to unintended consequences of human decisions and actions and make human and organisational factors very difficult to capture in a model.
- Sequential and event-based approaches traditionally used within PRA and AA are not capable of capturing some of the key characteristics of HOFs such as feedback, non-linear relationships or time delays. SD is capable of modelling these structures and has been proposed to support analysis of HOFs for AA and PRA. However, the extent to which SD can meet the purposes of HOF analysis for PRA and AA and the issues associated with the use of SD within PRA and AA have been scarcely discussed in the PRA and AA literature. If SD is to be used successfully within PRA and AA, modellers wishing to use it need to fully understand what can be achieved when using SD and need to appreciate limitations that exist when SD is used for this type of analysis.

Before SD can be used in the analysis of HOFs, a decision needs to be made whether SD is a suitable approach to model HOFs within a particular PRA and AA. Therefore, the first aim of this thesis was specified as

- *to explore when SD could be used in the analysis of HOFs for PRA and AA*

This should help those considering using SD in the analysis of HOFs to decide whether SD could be used in any individual PRA or AA. Thus, the aim of the next chapter is to discuss situations in which SD could be used to support the analysis of HOFs for PRA or AA.

CHAPTER 3: When can SD be used in the analysis of HOFs for PRA & AA?

3.1 Introduction

There is little literature on the subject of which criteria could be used to assess whether SD can be used to model a situation. The latest discussion in this area is Howick (2001) who has proposed a set of criteria that could be used to assess suitability of SD to model a particular situation. As the development of these criteria was based on an extensive literature review and the criteria provide a useful and simple way of assessing the suitability of SD to model a situation, they will be used to structure the discussion on when SD could be used in the analysis of HOFs for PRA and AA.

3.2 Criteria to assess the suitability of SD to model a situation

Howick (2001) has proposed a set of criteria that could support modellers in their decision of whether SD could be used to model a particular situation. Her criteria are formulated as questions. She proposes that these questions could be asked at the beginning of a study and *"should be used as guidelines to assist the discussion between those who are involved in deciding whether or not SD should be used to model a situation"* (2001, p.143). Of course, each HOF analysis for PRA and AA will be different. However, there are some generic issues involved in the application of SD that will be common to most of these HOF analyses. The aim of this chapter is to discuss these generic issues. Howick's criteria are presented below. They will be explained and discussed in more detail in the sections that follow.

1. *Does the situation contain feedback loops and are they of importance to the purposes of the study?*

2. *Does the situation exhibit changes through time and are they of importance to the purposes of the study?*

3. *Practically, can it be done?*

In particular:

a. *Can the situation be visualised at an early stage in terms of stocks and flows?*

b. *Is there sufficient, reliable information and data available which will enable a model to be populated to such a level that [the model user] is in a stronger position when compared to the [model user] not having the model?*

3.3 Does the situation contain feedback loops and are they of importance to the purposes of the study?

As mentioned in the previous chapter, Forrester (1961) argues that some social systems could be described as information-feedback systems. In information-feedback systems information about the state of the system is collected and used to make decisions and take actions to change the state of these systems. Before applying SD to model any situation, analysts should, first of all, ask themselves whether the situation to be modelled can be described as an information-feedback system, or alternatively, whether the situation to be modelled contains feedback loops. However, before applying SD to model any situation, analysts should also ask themselves whether the situation requires explicit modelling of these feedback loops. Coyle (1973, cited in Howick, 2001, p. 51) summarises this as follows:

> "(…) *it is impossible to think of even the simplest operation, such as opening a door, which is not a feedback process. Whether it is worth explicitly modelling the feedback structure instead of merely treating the dynamic behaviour as a stochastic process as in stock control is quite another matter. The key lies in the purpose of the model (...). If one is interested in a wider view with objectives of controllability and stabilization then a structured control model has to be built."*

Thus, before SD can be used to support the analysis of HOFs for PRA and AA, modellers should ask themselves the following questions:

– Are the HOFs to be modelled within PRA or AA governed by feedback loops?
– Should we model these feedback loops explicitly?

This is discussed in the sections that follow.

3.3.1 Does the situation contain feedback loops?

As mentioned in Chapter 1, Human Factors concern decisions and actions of people involved in operation and maintenance of technical systems. Organisational Factors relate to the wider context in which technical systems are operated and maintained and operators and maintainers perform their tasks. Thus, HOFs concern decisions and actions of people at many organisational levels, from operational to managerial, engaged in the risk management of technical systems.

Forrester (1968, p.4-4) argues that:

> *"Whatever the nature of the decision process, it is always (...) [embedded] within a feedback loop. The decision is based on the available information; the decision controls an action that influences a system (...); and new information arises to modify the decision stream."*

And

> "*A decision process can be part of more than one feedback loop."*

Thus, following Forrester, it could be concluded that HOFs contain feedback loops as they concern decisions and actions of people. In principle, each decision and action is based on some sort of available information, affects the operation of the system to a greater or lesser extent and thus has consequences that can affect future decisions and actions concerning the system. Overall, human decisions and actions that are of concern in the risk management of complex technological systems could be divided into two categories:

- decisions and actions repeated through time that are associated with tasks performed on a regular basis such as maintenance, testing, calibration and restoration tasks; these tasks are important, because they can introduce latent faults into the engineered safety systems designed to mitigate the consequences of "initiating events"; other tasks that are performed on a regular basis include supervision, staffing, staff training etc.
- one-off decisions and actions that introduce discrete and usually significant changes in the operation of complex technological systems, e.g. diagnosis and decision-making tasks that are critical to cope with an abnormal situation that arises after an "initiating event" occurs, decisions to change the organisational structure etc.

It could be argued that feedback mechanisms are of more concern in the case of decisions and actions repeated through time. In the case of one-off decisions:

- there might be no opportunity to collect the feedback, modify decision and affect the state of the system (e.g. during an accident the operator chooses a wrong control which results in an explosion – the state of the system changes so significantly that it can be categorised as a completely new system that requires a significantly different set of decisions)
- a decision and its consequences are far away in time (e.g. a decision to change organisational structure – it will take a lot of time to implement the new organisational structure and assess its performance thus the decision to implement the organisational structure and decision to modify the organisational structure will be made in different sets of circumstances and these two decisions could be treated as independent decisions).

Thus, it can be concluded that feedback mechanisms will be of concern to those modelling HOFs if the following conditions are met:

- human decisions and actions to be modelled repeat over time
- the organisational structure within which these decisions and actions are made does not significantly change over time.

The information-feedback character of human risk management of technical systems is acknowledged in the PRA and AA literature. For example, it was described well by Rasmussen (1997) and is reflected in Figure 3-1.

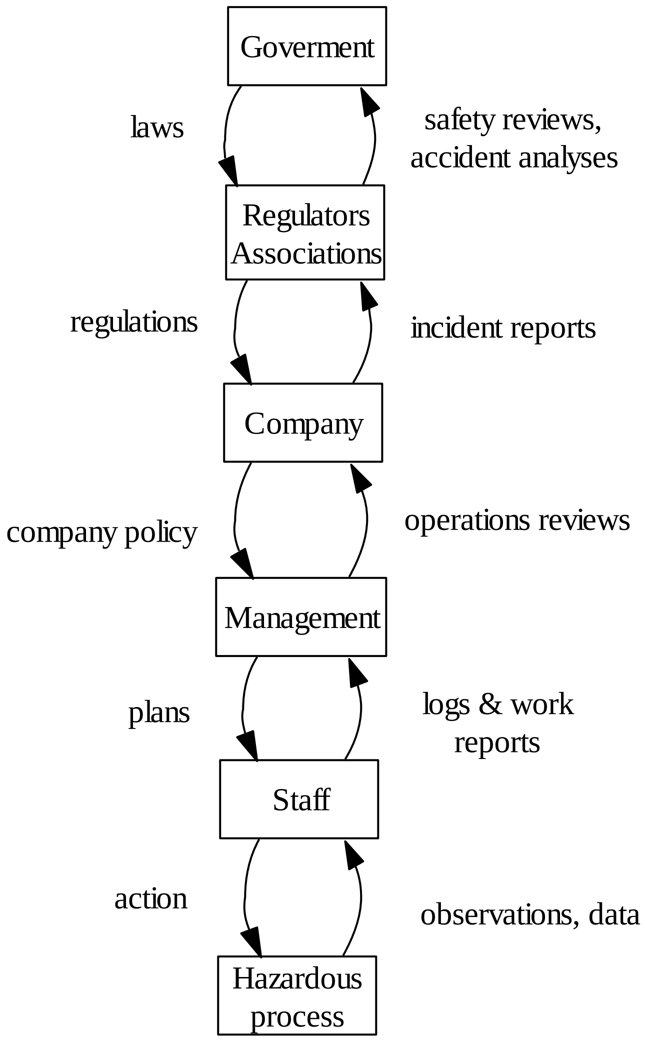


Figure 3-1: Socio-technical system involved in risk management (adapted from Rasmussen, 1997)

Rasmussen highlights the fact that companies do not operate in a vacuum. They function within a regulatory framework represented by regulators, associations and the government shown in Figure 3-1. All entities in Figure 3-1, i.e. staff, management, company, regulators, associations and the government are linked by a set of feedback loops. For example, the data collected by staff during daily work activities that control hazardous processes is used to make decisions and take direct and immediate actions that change the work activities and affect the hazardous processes. The data collected by staff is reflected in various logs and work reports that are used by Management to create long-term plans in relation to the work activities that control the hazardous work processes. The logs and work reports are also used for operations reviews that influence the company policy that should be reflected in all the organisational plans and decisions and actions of frontline staff. Overall, it is clear that feedback loops should be of interest to those who wish to analyse HOFs. However, analysts should also ask themselves whether these loops should be modelled explicitly. And this, as it was discussed above, relates to the purpose of HOF analysis for PRA and the purpose of HOF analysis for AA. These topics will be discussed in the sections that follow.

3.3.2 Are feedback loops of importance to the purpose of HOF analysis for PRA?

HOF analysis for PRA needs to meet the purposes of the PRA study for which it is carried out. As mentioned in Chapter 1, PRA helps duty holders ensure that risks are ALARP and thus ensure compliance with the health and safety law. The objective of PRA is to answer the following questions:

1. What can happen?
2. How likely is it to happen?
3. Given that it occurs, what are the consequences?

The achievement of this objective can serve many purposes. French et al. (2011) divided these purposes into two categories:

– Summative: PRA provides the measure of the risk associated with a particular technical system or a hazardous process and this can be used to obtain a license from the regulator or to evaluate alternative technical system designs

– Formative: Information and models developed during a PRA study can provide insights into the adequacy of technical system design and its operation. This insight can then be used to improve the technical system. In addition, the information and models developed during a PRA study can be

> used to train staff, develop emergency-response plans, and to improve the design of human tasks and processes and the organisational structure and safety culture.

HOF analysis can serve both of these purposes. When HOF analysis is used within a summative PRA study, it helps to estimate the probabilities of a technical system failure. In this type of situation, the focus is on analysing the direct actions and decisions of frontline staff involved in the maintenance and operation of the technical system. The goal of this analysis is to find out what can go wrong, calculate human error probabilities and incorporate these probabilities into Event and Fault trees. This is the typical area of application of the traditional HRA approaches such as THERP or HEART. The explicit models of the wider organisational feedback-driven processes in which the decisions and actions of frontline staff are embedded are usually out of scope of summative analyses. It usually suffices to treat the decisions and actions of frontline staff as an output of a stochastic process rather than explicitly account for feedback loops in which these decisions and actions are embedded.

When, HOF analysis is used formatively, it helps to improve the design of human tasks, processes and the organisational structure. The scope of HOF analysis used for formative PRA analysis is much wider than the scope of HOF analysis used for summative PRA analysis. The focus of formative HOF analysis is on improving organisational structure, culture and processes and thus the control of risk rather than merely on helping to quantify the risk level. This requires a good understanding of the processes involved in the control of risk and explicit models of the wider organisational feedback-driven context of frontline staff decisions and actions are needed. This is precisely the kind of situation to which Coyle (1973, cited in Howick, 2001, p. 51) refers when saying:

> *"If one is interested in a wider view with objectives of controllability and stabilization then a structured control model has to be built."*

Thus, when HOF analysis is used formatively within PRA, it is likely that explicit modelling of feedback loops will be required.

In summary:

- HOF analysis for PRA is concerned with the analysis of decisions and actions of people at different organisational levels, from operational to managerial, involved in risk management of technical systems. Human decisions and actions are embedded within a set of feedback loops. Thus, HOFs affecting the risk levels and considered within PRA can be described as an information-feedback system. Feedback loops will be of interest to HOF analysts when these HOFs concern human decisions and actions that are repeated through time and made within an organisational structure that does not significantly change over time.
- One should consider explicit modelling of feedback loops within HOF analysis and the use of SD when one is interested in improving the control of risks associated with a particular technical system rather than the merely in quantification of this risk.

3.3.3 Are feedback loops of importance to the purpose of HOF analysis for AA?

As mentioned in Chapter 1, AA helps duty holders ensure that risks are ALARP and thus ensure compliance with health and safety law. The key objective of AA is to answer the following questions:

1. What happened?
2. Why did it happen?

The purposes that are served by accomplishing this objective may include the following:

- To prevent accident reoccurrence
- To improve the control of risk.

HOF analysis for AA serves these purposes by determining whether, how and why humans contributed to the accident. Overall, the key goal of HOF analysis for AA is to understand how decisions and actions of humans contributed to the accident and why these decisions were made and actions taken. As mentioned in Chapter 2, accidents in hazardous industries rarely involve random errors of frontline staff. More often, a number of people at different organisational levels, from frontline staff to senior managers, are involved. In addition, their decisions and actions are not simple errors or mistakes. Rather they are influenced by the feedback-driven organisational context in which the frontline staff perform their tasks. If one wants to understand these decisions and actions and prevent the accident reoccurrence or improve risk control, one needs to understand the feedback processes that govern them. In these situations, one should consider explicit modelling of feedback loops in HOF analysis for AA and the use of SD.

In summary:

- HOF analysis for AA is concerned with the analysis of decisions and actions of people at different organisational levels, from operations to managerial, who contributed to the accident. Human decisions and actions are embedded within a set of feedback loops. Thus, HOFs that contributed to the accident and are considered within AA can be described as an information-feedback system. Feedback loops will be of importance to HOF analysts when these HOFs concern human decisions and actions repeated through time.
- If the decisions and actions of people involved in the accident are not a result of a simple error or mistake, but are influenced by the wider feedback-driven organisational context in which these people perform their task, one should consider explicit modelling of the feedback structures and the use of SD.

3.4 Does the situation exhibit changes through time and are they of importance to the purposes of the study?

Of course, humans and systems do change over time. For example, the knowledge and commitment of frontline staff or managers can deteriorate over time. It should be stressed here that not all situations that change over time can be modelled using SD. Howick (2001, p. 66) clarifies the meaning of this criterion by saying that the changes through time exhibited by a particular situation to be modelled should be "*caused endogenously by the system structure. Such endogenous system behaviour can be triggered by an exogenous input. However, the changes through time should not be entirely due to the behaviour of an exogenous trigger."* Thus, the full criterion should be formulated as follows:

> *Does the situation exhibit changes through time that are caused endogenously by the system structure and are these changes of importance to the purposes of the study*?

The "system structure" relates to how different parts of the system are related to one another (Forrester, 1961). As mentioned in the previous sections, HOF analysis is concerned with the analysis of human decisions and actions that can affect risk and contribute to accidents. These decisions and actions operate within feedback loops. Forrester (1968, p. 4.5) argues that:

- *"(...) feedback loop is the basic structural element in systems"* and
- *"dynamic behaviour is generated by feedback".*

Thus, HOFs that are of interest to PRA and AA do exhibit changes through time that are caused endogenously by the feedback structure of the system. In the previous sections it was discussed when the feedback structure of HOFs should be explicitly modelled within HOF analysis. If feedback structure is important to the purpose of HOF analysis for PRA and AA then the changes through time that are generated by this feedback structure are also important to the purposes of HOF analysis for PRA and AA.

3.5 Practically, can it be done?

Before SD can be applied to the analysis of HOFs for PRA and AA, analysts need to ask themselves whether it will be possible to develop an SD model and use it in the analysis of HOFs. The work of Mohaghegh et al. (2009) and Cooke (2003, 2004) suggests that SD could be and has been used in the past in the analysis of HOFs for PRA and AA, respectively. The question is to what extent SD can be applied in the analysis of HOFs for PRA and AA. The two common hurdles that need to be overcome are captured by the following questions proposed by Howick (2001):

- *Can the situation be visualised at an early stage in terms of stocks and flows?*
- *Is there sufficient, reliable information and data available which will enable a model to be populated to such a level that [the model user] is in a stronger position when compared to the [model user] not having the model?*

These two issues will be explored in the sections that follow.

3.5.1 Can the situation be visualised at an early stage in terms of stocks and flows?

As mentioned in the previous chapter, stocks and flows are key building blocks of stock and flow diagrams used in SD to represent the structure of information-feedback systems. Stocks represent state variables and describe the condition of a system at any time. Flows represent rate variables and determine the change in stocks per time unit. Stocks and flows reflect accumulation and depletion processes in the system. They represent how change occurs in the system over time.

In general, it is not difficult to visualise HOFs in terms of stocks and flows. For example, tangible elements of systems such as staff, cash, and resources can be easily represented using stocks. Also, intangible elements of systems such as the commitment, experience and knowledge of employees could also be visualised as stocks. Similarity, changes in these elements of systems such as hiring of employees, decrease or increase in cash or resources, decline in commitment, learning or forgetting of what has been learnt can easily be visualised as flows. Thus, overall, modellers who want to apply SD in the analysis of HOFs should be able to easily visualise HOFs in terms of stocks and flows.

Additionally, the SD literature provides examples of generic stock and flow structures that could be adapted and used to represent HOFs. For example, Cooke (2003) adapted generic SD structures described by Sterman (2000), and used it to model factors that contributed to the Westray mine disaster. These generic stock and flow structures included, for example, those used to represent structures responsible for changes in the number of staff in a company and changes in their experience. Mohaghegh et al. (2009), in turn, adapted the stock and flow structures developed by Cooke (e.g. structures responsible for changes in staff commitment to safety over time). Thus, adapting SD structures developed for the purpose of explaining why an accident happened is another way of creating an initial SD model to be used in the analysis of HOFs for PRA. This is an example of how PRA can learn from AA. AA gives an opportunity to create generic stock and flow structures that can be later adapted to be used within HOF analysis for PRA. However, the generic stock and flow structures found in the SD literature can also be adapted and used within HOF analysis for PRA.

The ability to visualise HOFs as stocks and flows is one of the two key issues that need to be considered before an SD model can be developed. The second issue is concerned with quantifying these stock and flow structures. This will be discussed in the next section.

3.5.2 Is there sufficient information and data available to populate stock and flow structures?

Analysts that consider using SD in the analysis of HOFs for PRA and AA need to ask themselves whether there is sufficient, reliable information and data available to populate stock and flow structures. This assumes that stocks and flows need to be quantified. However, this might not be the case.

There is a debate in the SD literature on the necessity of simulation (see, for example, Wolstenholme, 1999; Coyle, 2000, 2001; Homer and Oliva, 2001; Richardson, 1999, 2000; Lane 2008). The main point against developing quantitative SD models is the need to quantify soft variables (e.g. staff commitment to safety). In principle, soft variables could be captured by dimensionless variables. For example, Cooke (2004) represented management commitment to safety as a dimensionless variable on a scale from 0 to 100. However, Coyle (2000) argues that it is often not clear what is meant be these numbers. He gives an example of quantifying the variable *Ability to implement plans:* "*A scale from 0 to 1 is superficially tempting but what would 0.5 mean? If it means that half the plans can be implemented, which half is it? If it means that all the plans can be half implemented, then what is half a plan? It is into that kind of trap that relentless emphasis on quantification can lead"* (p. 237-238). Thus, he argues that in some cases the sole use of a qualitative SD model is not only useful, but also necessary. Another point of view is provided by Oliva and Homer (2001):

> *"We argue that simulation nearly always adds value, even in the face of significant uncertainties about data and the formulation of soft variables. This value derives from the fact that simulation models are formally testable, making it possible to draw behavioral and policy inferences reliably through simulation in a way that is rarely possible with maps alone. Even in those cases in which the uncertainties are too great to reach firm conclusions from a model, simulation can provide value by indicating which pieces of information would be required in order to make firm conclusions possible. Though qualitative mapping is useful for describing a problem situation and its possible causes and solutions, the added value of simulation modeling suggests that it should be used for dynamic analysis whenever the stakes are significant and time and budget permit"* (p.347).

Overall, development and effective use of qualitative SD models requires a lot of prior training and experience. In addition, Richardson argues that "*In fact, I think most system dynamics practitioners would argue that using qualitative maps well for analysing a dynamic system requires a great deal of experience and expertise in quantitative system dynamics modelling"* (1999, p.441).

It can be argued that the use of a qualitative SD model will be sufficient for the purposes of most AA as they focus on explaining how a particular accident occurred and why. One can consider developing a quantitative SD model and simulation for AA, but only when the benefits of simulation will be considered as greater than the effort put into the quantification process. However, when SD is used within PRA, the qualitative SD analysis should be followed by quantitative SD analysis as modellers are interested in estimating the sensitivity of model output to different model structures. The author of this thesis follows Homer & Oliva (2011) in arguing that quantitative SD analysis can still be useful even if a number of soft variables will be involved. Quantitative SD analysis can assist modellers in identifying areas that may have relatively higher impact on a system's performance than others and focus further analysis and data collection processes. If one wants to perform quantitative SD analysis, numerical data is needed to quantify the model. At the beginning of a HOF analysis, analysts need to consider whether the benefits of simulation will exceed the effort put into the data collection and quantification process and whether the quantitative SD analysis will not exceed the budgetary and time constraints of the study.

The data needs associated with the use of SD in HOF analysis for PRA and AA are discussed in the sections that follow.

3.5.3 Data needs associated with the use of SD in HOF analysis for PRA

The traditional HOF analysis for PRA involves the following stages (Kirwan, 1994):

1. Analysis of PRA scenarios, identification of PRA scenarios to which people are contributing and definition of human tasks performed within these scenarios.

2. Analysis of how the identified tasks should be carried out by people.
3. Analysis of what can go wrong while performing the task.
4. Analysis of dependencies within and between people who perform the tasks in the PRA scenario identified.
5. Quantification of Human Error Probabilities (HEPs).
6. Identification of the context in which the task is performed and estimating its impact on Human Error Probabilities. This is accomplished by making HEPs functions of selected Performance Shaping Factors (PSFs) i.e. any characteristics of a human or the environment in which he/she is working that influences his/her performance.

As mentioned in the previous sections of this chapter, this type of HOF analysis is usually performed within summative PRA studies. When HOF analysis is used formatively, then one needs to consider explicit modelling of the organisational context within which frontline staff perform their tasks. These types of HOF analysis have a wider scope and require much more information and data to be collected than is needed for traditional HOF analyses. As mentioned in the previous sections, the HOF analysis used formatively is the area where SD can contribute the most.

The information and data required for the development of SD models for formative PRA studies will include the following:

- Information on the key variables representing the organisational context that influence the parameters in PRA models. These variables will be represented by stocks in the SD model.
- Information on processes that lead to changes in stocks over time. The changes in stocks will be represented as flows in the SD model.
- Information on policies that govern the flows within the SD model
- Quantitative data to populate stock and flow structures within the SD model.

It is very likely that:

- these types of information and data will not be readily available or even will not exist in the system for which the PRA study is performed

- it might be time consuming and costly to collect some information and data. This refers particularly to the collection of quantitative data to populate stock and flow structures within the SD model.

In these cases, expert judgement might be sought to quantify the key parameters and policies in the SD model (Howick, 2001). Modellers need to decide whether such an SD model will still be of benefit.

3.5.4 Data needs associated with the use of SD in HOF analysis for AA

The traditional HOF analysis for AA involves the following stages:

1. Analysis of the sequences of events and conditions that led to the accident
2. Identification and analysis of events and conditions where people played some role
3. Analysis of why people contributed to the sequence of events

The first two stages focus on what happened, i.e. on the immediate events that comprised the accident. The key part of HOF analysis is to determine why these events occurred. The scope of this part of HOF analysis has been getting very wide in recent years and thus the scope of data that is gathered is also very broad.

The scope of information and data collected for traditional HOF analysis within AA will probably be broad enough for the purposes of SD modelling. However, the nature of the information and data that is needed for SD modelling and traditional Root Cause Analysis is significantly different. The focus of Root Cause Analysis is to identify the events, conditions and root causes that explain why the accident happened. The focus of SD analysis is to identify the feedback structures that generated these events and conditions and led to the accident. The Root Cause Analysis reflects what Sterman (2000, p. 27) calls an "*event-based, open-loop view of causality"* that ignores feedback processes or at least is not focused on explicitly considering feedback processes, time delays between actions and response or in reporting of information.

Thus, in summary, data that needs to be collected to perform SD analysis of HOFs for AA will be relating to the same human and organisational processes as data needed for Root Cause Analysis. However, the emphasis will be shifted from the events themselves to the processes that govern these events. Essentially, it means that different types of questions will be asked while performing SD analysis as compared to Root Cause Analysis. Instead of repeatedly asking:

“Why this occurred?” until we reach a “root cause”

(as it is suggested in one of the Root Cause Analysis techniques called 5 Whys), analysts will ask the following question while performing SD analysis:

> “What is the feedback structure that led to the development of the immediate events leading to the accident?”

3.6 Summary of Chapter

The aim of this chapter was to discuss when SD could be used in the analysis of HOFs for PRA and AA.

The following conclusions have been reached:

- HOF analysis for PRA and AA is concerned with the analysis of decisions and actions of people at different organisational levels, from operational to managerial, involved in risk management of technical systems. Human decisions and actions are embedded within a set of feedback loops. Thus, HOFs considered within PRA and AA can be described as information-feedback systems. Feedback loops will be of interest to HOF analysts when these HOFs concern human decisions and actions that are repeated through time and made within an organisational structure that does not significantly change over time.

- One should consider explicit modelling of feedback loops within HOF analysis for PRA and the use of SD when one is interested in improving the control of risks associated with a particular technical system or hazardous process rather than the merely in quantification of this risk.
- If decisions and actions of people involved in the accident are not a result of a simple error or mistake, but are influenced by the wider feedback-driven organisational context in which these people perform their task, one should consider explicit modelling of the feedback structures and the use of SD.
- If feedback structure is important to the purpose of HOF analysis for PRA and AA then the changes through time that are caused by this feedback structure are also important to the purposes of HOF analysis for PRA and AA.
- In general, it is not difficult to visualise HOFs in terms of stocks and flows. Additionally, the SD literature provides examples of generic stock and flow structures that could be adapted and used to represent HOF for PRA and AA. Adapting SD structures developed for the purpose of explaining why an accident happened is another way of creating an initial SD model to be used in the analysis of HOFs for PRA. This is an example of how PRA can learn from AA.
- It can be argued that the use of a qualitative SD model will be sufficient for the purposes of most AA situations as they focus on explaining how a particular accident occurred and why. One can consider developing a quantitative SD model and simulation for AA, but only when benefits of simulation will be considered as greater than the effort put into the quantification process.
- However, when SD is used within PRA, the qualitative SD analysis should be followed by quantitative SD analysis as modellers are interested in estimating the sensitivity of model output to different model structures. Quantitative SD analysis can assists modellers in identifying areas that may have relatively higher impact on a system’s performance than others and focus further analysis and data collection processes. If one wants to perform quantitative SD analysis, numerical data is needed to quantify the model. At the beginning

of a HOF analysis, analysts need to consider whether benefits of simulation will exceed the effort put into the data collection and quantification process and whether the quantitative SD analysis will not exceed the budgetary and time constraints of the study.

- The information and data required to develop and populate an SD model for HOF analysis within PRA go beyond what is usually required in the traditional HOF analyses. It is very likely that these types of information and data will not be readily available or even will not exist in the system for which the PRA study is performed. Also, it might be time consuming and costly to collect some information and data. This refers particularly to the collection of quantitative data to populate stock and flow structures within the SD model. In these cases, expert judgement might be sought to quantify the key parameters and policies in the SD model. Analysts need to decide whether such an SD model will still be of benefit.
- The data that needs to be collected to perform SD analysis of HOFs within AA will be relating to the same human and organisational processes as data needed for traditional HOF analysis within AA. However, while collecting the data, the emphasis will be shifted from seeking information on the events that contributed to the accident to the feedback processes that govern these events.

3.7 Using SD in the analysis of HOFs for AA & PRA – introduction to Chapter 4 and Chapter 5

As discussed in the previous chapters, AA and PRA are important parts of the risk management of complex technological systems. Chapter 2 described the key features of PRA and AA and HOF analysis for AA and PRA. It also highlighted the limitations of approaches traditionally used within these areas. Chapter 3 built on Chapter 2 and explored when SD could be used in the analysis of HOFs for AA and PRA. The aim of the next two chapters, and at the same time, the second aim of this thesis, is to illustrate how SD could be used in the analysis of HOFs for AA (Chapter 4) and PRA (Chapter 5) and discuss issues involved in the use of SD in these areas.

This should help those wishing to use SD in the analysis of HOFs to develop SD models for PRA and AA.

Chapter 4 illustrates how SD could be used within AA by applying SD to the analysis of HOFs that contributed to the 2007 Grayrigg train accident. Chapter 5 illustrates how SD could be used within PRA by presenting the application of SD to the analysis of HOFs contributing to the unavailability of an engineered safety system at a process plant. The rationale for the selection of these two cases is fully explained in the respective chapters. These two HOF analyses were undertaken in the same order as presented in this thesis. First, SD was used to support analysis of the Grayrigg train accident. Then, SD was applied to the analysis of HOFs contributing to the unavailability of an engineered safety system at a process plant. This particular order was mainly motivated by the access to an external organisation that would provide data for the second case and this access was only given later in the Ph.D. project. However, it was also important that the retrospective SD analysis of the Grayrigg train derailment could provide an opportunity for learning that could be brought into the second case. It was not just one way learning though. The learning from the prospective SD analysis at a process plant was also brought into the retrospective analysis and, as a result, the original analysis of the Grayrigg train derailment was modified. This is discussed in more detail at the end of Chapter 4.

CHAPTER 4: Using SD in the analysis of HOFs for AA

4.1 Introduction

This chapter presents the application of SD to the analysis of HOFs that contributed to the 2007 Grayrigg train derailment. First, basic information about the accident, its consequences, data sources and why it was selected for analysis is provided. Next, the objectives of the analysis and the approach to the analysis are discussed. The analysis of the accident, the models that supported the analysis and the key findings are discussed in the sections that follow. The methodological choices that were made are explained throughout these sections. Finally, the key issues associated with the use of SD in the analysis of HOFs for AA are discussed.

4.2 Background information

4.2.1 Introduction to the accident and data sources

The Virgin Train, the 17:15 service from London Euston to Glasgow, derailed at Lambrigg 2B points located near Grayrigg in Cumbria on 23 February 2007. All nine vehicles of the train derailed. One passenger died and eighty-six passengers and two train crew members were injured as a result of the derailment.

Network Rail (who owns, operates and maintains the railway infrastructure at Grayrigg) and the Rail Accident Investigation Branch (RAIB) (an independent railway accident investigation organisation for the United Kingdom) conducted investigations into the causes of the derailment. Network Rail released its summary report in September 2007 (Network Rail, 2007). Following the report, three Network Rail workers were arrested under suspicion of manslaughter (BBC, 2007). They have all been released without charges due to “insufficient evidence to proceed with the investigation” (BBC, 2009).

In October 2008, the RAIB released the report from its investigation into the Grayrigg train derailment (RAIB, 2011). This report had wider scope than the 2007 report released by Network Rail. It examined Network Rail's train infrastructure inspection and maintenance arrangements in more detail. The last version of this report, released in 2011, was the main source of data for the analysis presented in this chapter.

4.2.2 Why was this accident selected for analysis?

There are several reasons why it was decided to apply SD to the analysis of the 2007 Grayrigg train derailment. They are summarised below:

- Transportation systems belong to the category of complex technological systems described in Chapter 2. The hazards involved in the maintenance and operation of transportation assets and infrastructure in general, and train assets and infrastructure in particular, are numerous and not easy to identify. Adverse effects of accidents are usually very severe, including multiple fatalities. The selected accident displays the complexity and severity characteristic of accidents in other hazardous industries. Whilst the technological systems and processes that are being managed do differ among various hazardous industries, the methodological issues associated with the modelling and analysis of these systems and processes will be common and of interest to all of these industries
- The early assessment of the factors involved in the accident, using the criteria described in Chapter 3, indicated that SD could be used to model the HOFs that contributed to the accident. Firstly, the report released by Network Rail (2007) after the accident and the report produced by the RAIB (2011) indicated extensive human involvement in the accident. In addition, the reports suggested that decisions and actions of people involved in the accident were influenced by the wider feedback-driven organisational context in which these people were performing their assigned tasks. As discussed in Chapter 3, SD can contribute the most to the analysis of the organisational context that influences human decisions and actions. Practically, it was not

difficult to visualise the HOFs involved in the accident in terms of stocks and flows and an initial, simple SD model was easily constructed. The data in the RAIB report was sufficient to construct a stock and flow diagram and perform qualitative SD analysis.

- The RAIB report (RAIB, 2011), which was the main source of data for the analysis, was the result of an independent and comprehensive inquiry and provided credible and rich data for the analysis. Also of importance is that the data in the report was well presented and structured and its quantity manageable, which facilitated the analysis. Very often investigations into major accidents are conducted by large groups of people and this makes it very difficult to prepare a well written, structured and consistent report of a manageable size.

4.3 Objectives & scope of the analysis

As already mentioned, the main objective of the analysis was to examine the HOFs that contributed to the Grayrigg train derailment. Additionally, it was decided to focus on the HOFs that Network Rail had control over and had the power to change in the future.

4.4 Approach to the analysis

As discussed in Chapter 2, the traditional approach to AA involves the following steps (Livingston et al., 2001):

1. Identification and analysis of the sequence of events and conditions which have led to the observed adverse effects.
2. Identification of critical events and conditions in the sequence of events and conditions identified in the previous stage. These critical events and conditions are referred to as direct causes of an accident.
3. Identification and analysis of root causes of the critical events and conditions identified in the previous stage.

HOF analysis for AA is concerned with identification, description and analysis of how people contributed to the identified sequence of events and conditions and identification of human and organisational root causes of the identified critical events and conditions. As discussed in Chapter 3, SD can contribute the most to the analysis of the feedback-driven organisational context that influences human decisions and actions and underlies conditions present at the time of the accident. Overall, a clear picture of the sequence of events and conditions involved in the accident is needed to define the scope for HOF analysis in general and SD analysis in particular. Thus, a hybrid strategy, described below, was adopted and the analysis divided into two stages:

- **Stage 1: Development of an Event and Conditional Factors (ECF) chart**
  The purpose of developing this chart was twofold. Firstly, it was used to capture and present events and conditions necessary and sufficient for the accident to occur. If any of these events and conditions had not occurred, the train would not have derailed at 20:12 on 23 February 2013 at Lambrigg 2B points. Secondly, the ECF chart was used to identify the critical events and conditions which Network Rail had control over and which could have been prevented.

  An ECF chart is the output of Events and Conditional Factors Analysis (ECFA+) (Kingston et al., 2007), discussed in Chapter 2. ECFA+ is a simple approach often used in accident investigations and analyses to graphically depict the key events and conditions that contribute to accidents (Energy Institute, 2008) and to support subsequent root-cause analysis of the accident (Kingston et al., 2007). As this study focuses on explaining why the train derailed, the chart does not include events and conditions that occurred/existed after the train derailment.

- **Stage 2: Development of an SD model**
  The SD model was used to capture the structure of Network Rail's inspection, maintenance and risk management systems designed to keep the

infrastructure fit and safe for train use and control the risk of train derailment. The purpose of the model was to support analysis of the organisational context that influenced the events and conditions identified using the ECF chart.

4.5 Stage 1: Analysis of events and conditions involved in the accident

This section presents the analysis of the events and conditions that were necessary and sufficient for the Grayrigg train derailment to occur. If any of these events had not occurred, the train would not have derailed at 20:12 on 23 February 2013 at Lambrigg 2B points. The events are presented in Figure 4-1 and Figure 4-2 using an ECF chart.

The conventions adopted for creating this type of chart are described below (Kingston et al., 2007):

- Events describe a single, discrete occurrence of very short duration characterised by a change of state. Events are phrased in the active voice as actor + action + object and in the present tense (e.g. “Smith (actor) moves (action) a valve handle (object)”). Events are represented using rectangles.
- Conditions represent a passive state that exists for some period of time (e.g. “Road open to traffic”). “Non-events”, i.e. events that should have occurred according to some procedure or standard, but did not happen are treated as conditions. Conditions are represented using ovals.
- The arrows between conditions and events, between events and between conditions represent causal relationships. For example, an arrow from event A to event B should be read as “A leads to B”.
- If there is more than one arrow arriving at an event or condition, the logical relationship is equivalent to an AND logic, as used in Fault Tree Analysis (FTA). What constitutes an explanation of an event or a condition should be sufficient (i.e. if all events and conditions explaining an event/condition occur, the explained event/condition will always happen) and necessary (i.e.

if any of the events/conditions explaining an event/condition does not occur, the explained event/condition will not occur).

- Events are arranged chronologically – later events are always to the right of earlier events.
- All events, conditions and relationships between them should be supported by appropriate evidence. All events and conditions in the ECF diagram presented in Figure 4-1 and Figure 4-2 are linked to the appropriate page and paragraph in the RAIB report (page/paragraph convention is used). Other supporting evidence, including direct quotes from the RAIB report that support each event, condition and relationship between them, is presented in Appendix J.
- If the evidence to support an event, condition or relationship among chart elements is lacking, but this event, condition or relationship presents a plausible hypothesis, then a dashed line should be used to indicate this.
- If possible, the time of event occurrence is stated.

The analysis of the data in the report that preceded the development of the ECF chart is described in the next section. The key technical terms, important to understand the events and conditions in the ECF chart, are explained in Section 4.5.2 The process of ECF chart verification and validation is described in Section 4.5.3. The key take-away points from the ECF chart are summarised in Section 4.5.4**.**

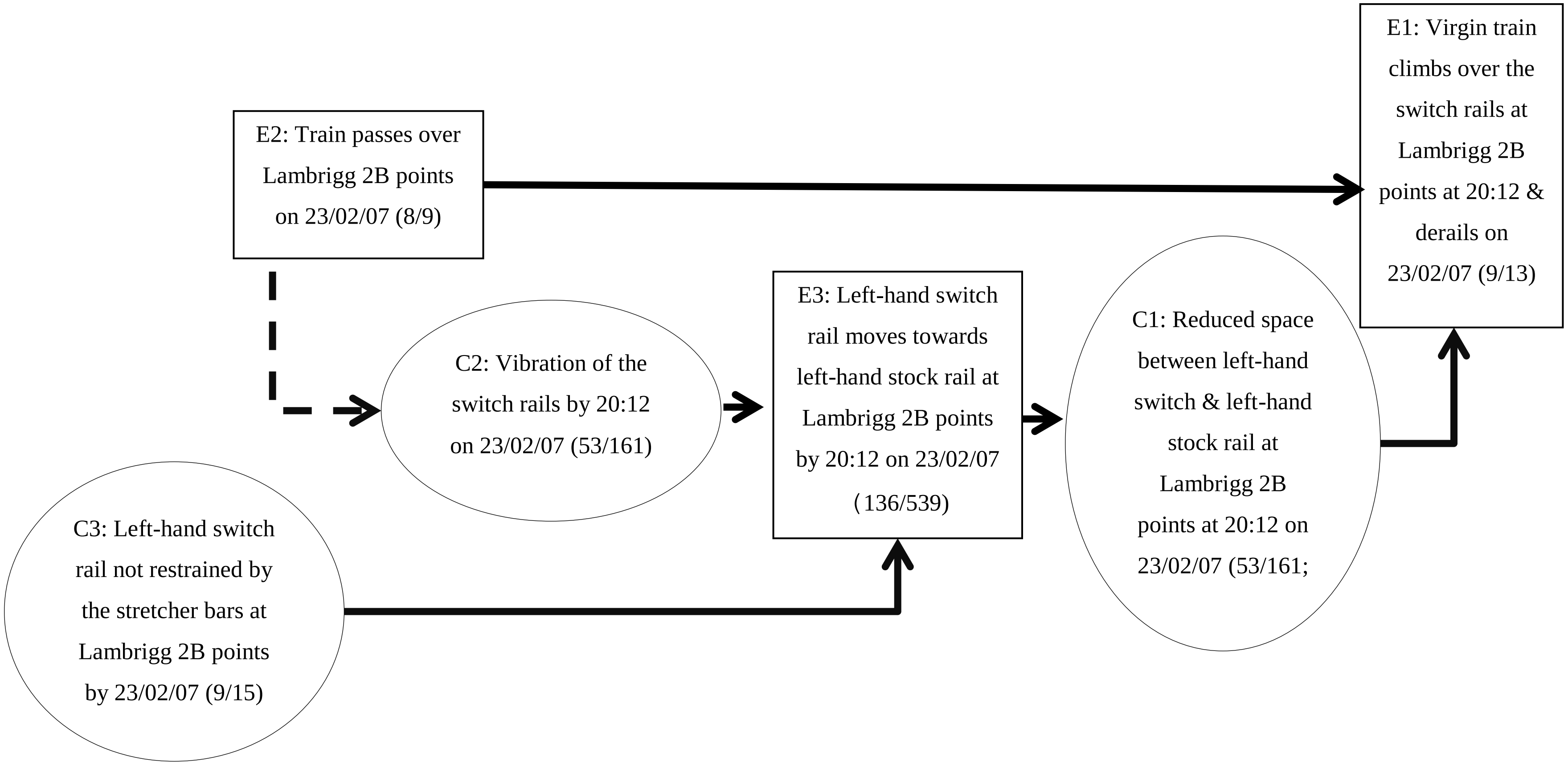

E1: Virgin train climbs over the switch rails at Lambrigg 2B points at 20:12 & derails on 23/02/07 (9/13)
E2: Train passes over Lambrigg 2B points on 23/02/07 (8/9)
C2: Vibration of the switch rails by 20:12 on 23/02/07 (53/161)
E3: Left-hand switch rail moves towards left-hand stock rail at Lambrigg 2B points by 20:12 on 23/02/07 (136/539)
C1: Reduced space between left-hand switch & left-hand stock rail at Lambrigg 2B points at 20:12 on 23/02/07 (53/161;
C3: Left-hand switch rail not restrained by the stretcher bars at Lambrigg 2B points by 23/02/07 (9/15)

Figure 4-1: ECF chart (part 1)

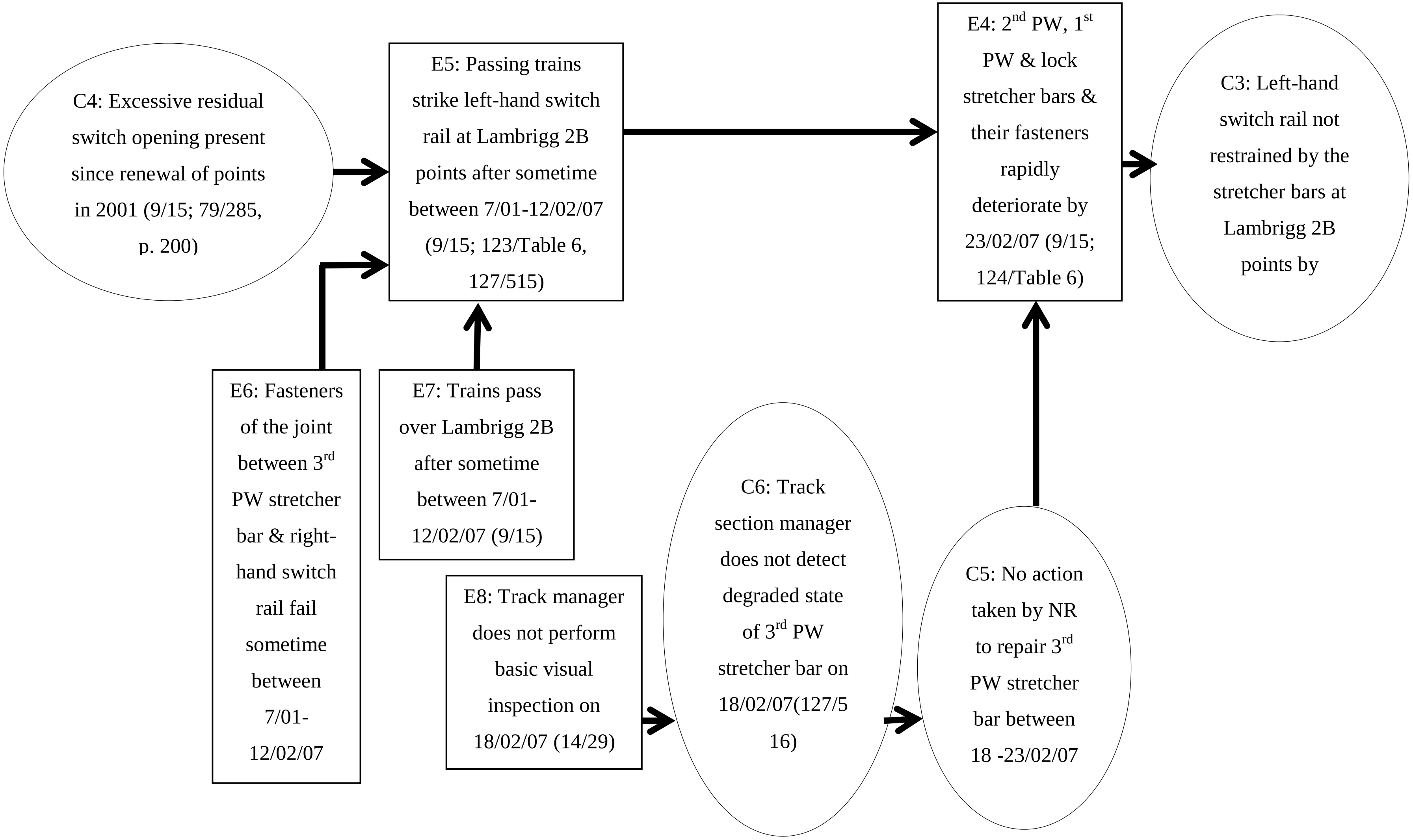

C4: Excessive residual switch opening present since renewal of points in 2001 (9/15; 79/285, p. 200)
E5: Passing trains strike left-hand switch rail at Lambrigg 2B points after sometime between 7/01-12/02/07 (9/15; 123/Table 6, 127/515)
E4: 2nd PW, 1st PW & lock stretcher bars & their fasteners rapidly deteriorate by 23/02/07 (9/15; 124/Table 6)
C3: Left-hand switch rail not restrained by the stretcher bars at Lambrigg 2B points by
E6: Fasteners of the joint between 3rd PW stretcher bar & right-hand switch rail fail sometime between 7/01-12/02/07
E7: Trains pass over Lambrigg 2B after sometime between 7/01-12/02/07 (9/15)
E8: Track manager does not perform basic visual inspection on 18/02/07 (14/29)
C6: Track section manager does not detect degraded state of 3rd PW stretcher bar on 18/02/07(127/516)
C5: No action taken by NR to repair 3rd PW stretcher bar between 18 -23/02/07

Figure 4-2: ECF chart (part 2)

4.5.1 Analysis of the RAIB report

Before the ECF chart was developed, the RAIB report was analysed.

Very often, reports from investigations into large-scale accidents are very sizeable documents, spanning hundreds of pages. Reading the entire document may, in itself, take a long time – not to mention using this document to develop a model. At the same time it is important that the critical pieces of information in the report are identified and reflected in the model. Thus, effective initial analysis of the report, before model development begins, is very important. The approach adopted to analyse the report from the investigation into the Grayrigg train derailment is summarised below.

First, a good understanding of the structure and overall content of the report was sought. The content of the chapter *"Summary of the report into the derailment at Grayrigg on 23 February 2007"* and *"The cause of derailment"* was examined to get a high-level overview of the accident, i.e. what happened and why. The rest of the document was also scanned briefly to get an understanding of the key issues covered in the report.

The next step involved more detailed analysis of two chapters: *"Summary of the report into the derailment at Grayrigg on 23 February 2007"* and *"The cause of derailment"*. These chapters were carefully read and divided into smaller pieces of text each covering one important piece of information. An extract from the report that shows how the analysis was conducted is presented below:

> *"The train derailed as it passed over 2B points* | *which were in an unsafe state.*| *A combination of failures of stretcher bars and their joint to the switch rails allowed the left hand switch rail to move, under its natural flexure, towards the left-hand stock rail.*| *The left-hand wheels of either the first or second bogie on the leading vehicle (it is not clear which) passed the wrong*

> *side of the left-hand switch rail |and were forced into the reducing width between the switch rails.| The wheels then derailed by climbing over the rails.| All the other vehicles of the train derailed as a consequence.|"*(p.9)

The two summary chapters were used to get a high-level understanding of what happened and why and were used to create an initial ECF diagram. The diagram was then elaborated, verified and validated while examining the rest of the report. This simple strategy of "divide and conquer" ensured that the researcher did not get bogged down with the details and was able to focus on the critical pieces of information in the report.

4.5.2 Explanation of key technical terms used in the RAIB report

A set of points, as defined in the RAIB (2011) report, is *"an assembly of two moveable rails (the switch rails) and two fixed rails (the stock rails) and other components used to divert vehicles from one track to another"* (p.203). The key elements of the Lambrigg 2B points are presented in Figure 4-3.

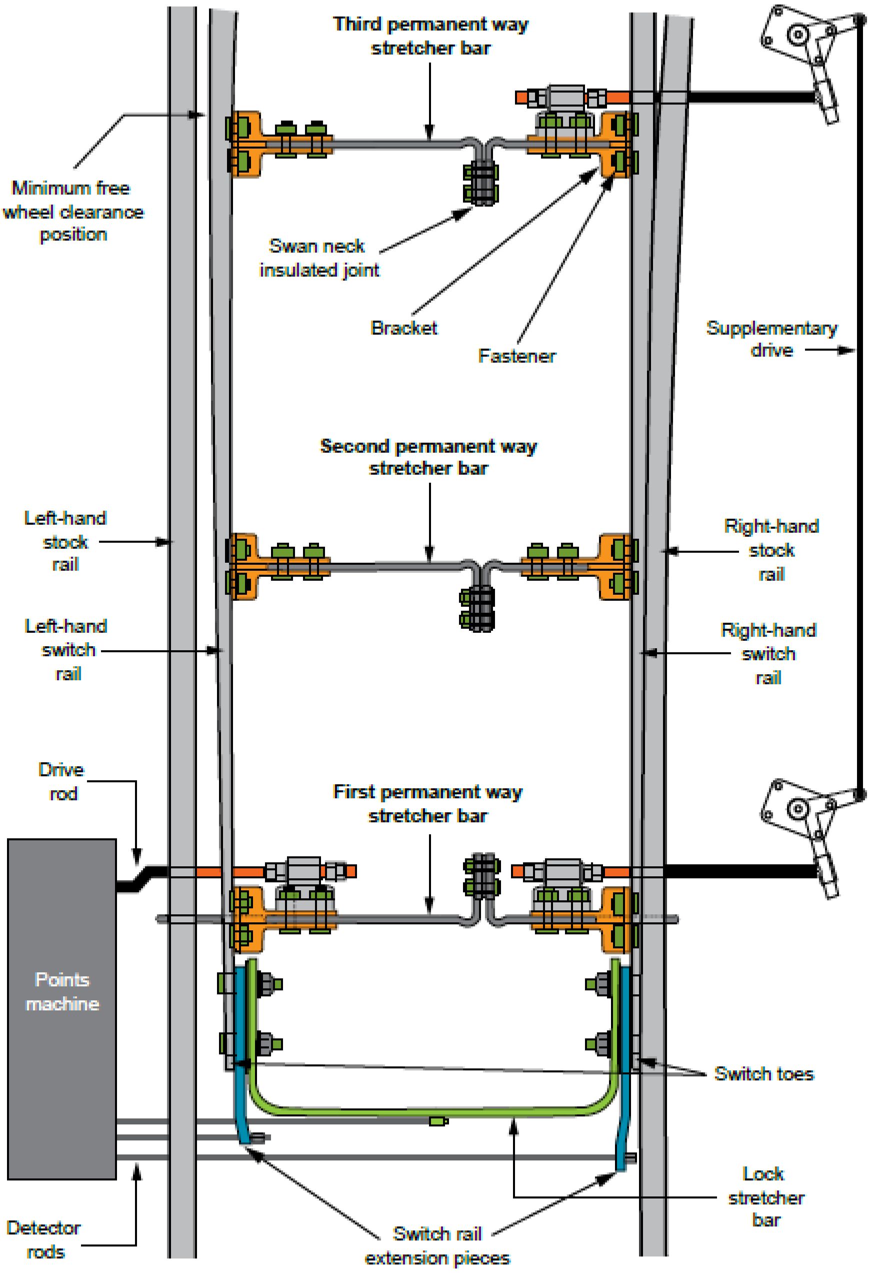

Third permanent way stretcher bar
Minimum free wheel clearance position
Swan neck insulated joint
Bracket
Fastener
Supplementary drive
Second permanent way stretcher bar
Left-hand stock rail
Right-hand stock rail
Left-hand switch rail
Right-hand switch rail
Drive rod
First permanent way stretcher bar
Points machine
Switch toes
Lock stretcher bar
Detector rods
Switch rail extension pieces

Figure 4-3: Layout of points at Lambrigg 2B points (RAIB, 2011)

The key technical terms used in the ECF chart are explained in Figure 4-4.

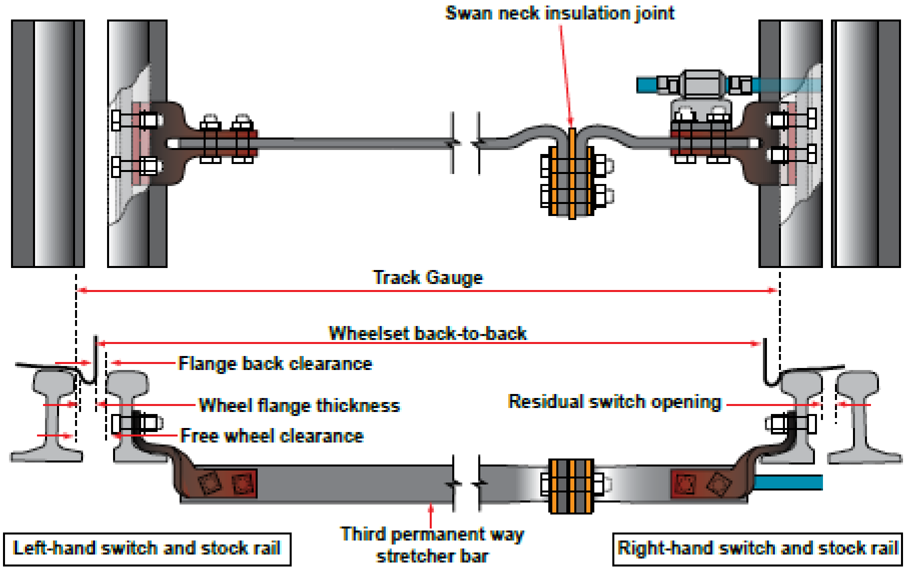

Swan neck insulation joint
Track Gauge
Wheelset back-to-back
Flange back clearance
Wheel flange thickness
Free wheel clearance
Residual switch opening
Left-hand switch and stock rail
Third permanent way stretcher bar
Right-hand switch and stock rail

Figure 4-4: Key technical terms relating to Lambrigg 2B points explained (RAIB, 2011)

The set of points at Lambrigg was subject to an inspection and maintenance regime. The responsibility for this set of points was split between the Carnforth track engineering staff and the Carlisle signal engineering staff (RAIB, 2011, p.60). The Carlisle signal engineering staff were responsible for maintenance of signalling assets in the area, including three-monthly maintenance of the points at Lambrigg. In particular, they were required to check the condition of stretcher bars and tighten any loose fasteners. The Carnforth track engineering staff were responsible for conducting weekly basic visual inspections of track and signalling assets, including Lambrigg 2B points, within their area. In addition, they were responsible for maintenance of track assets. The track section manager based in the Carnforth depot was responsible for planning and staffing weekly basic visual inspections of track and signalling assets and planning and staffing maintenance of track assets. The key responsibilities of Carnforth track engineering staff while carrying out weekly basic visual inspections of track and signalling assets were:

- to identify track and signalling asset defects as defined by appropriate Network Rail procedures
- to repair, if possible, or report defects to be repaired.

The reported defects were then to be investigated either by track or signalling engineering staff and appropriate remedial actions taken.

Network Rail had two key management information systems in place at the time of the accident. The Ellipse system was used to record and manage defects awaiting maintenance. The SINCS system was used to record and store the signalling asset failure data. Network Rail collected data related to a set of defined Key Performance Indicators (KPIs). Data in the Ellipse and SINCS systems, and data on KPIs, were to be regularly analysed to assess performance of the assets and take appropriate actions if a problem was identified.

The terms explained here will be used to summarise the key points to be taken out of the ECF chart. First, however, the process of ECF chart development and validation will be discussed.

4.5.3 ECF validation

As mentioned previously, model validation is an important part of the model development process. The purpose of model validation is to ensure that a model is suitable for its purpose and model users can have confidence in model outputs (Williams, 2008; Pidd, 2009). The purpose of developing an ECF chart for Grayrigg train derailment was to capture events and conditions necessary and sufficient for the accident to occur and facilitate identification of critical events and conditions. Network Rail's or RAIB's personnel involved in the analysis of Grarigg train derailment could be the potential users of the chart. If that was the case, a number of approaches could be taken to build the confidence of chart users in the ECF chart, for example:

- ECF chart could be built during a workshop with Network Rail's or RAIB's personnel (Kingston et al., 2007). This approach would build users' understanding of the chart and would lead to an increased ownership of the chart. However, this approach is not always possible as it may be difficult to bring together in one place all different people.

- ECF chart could be created by the researcher and its key events, conditions and relationships between then could be discussed during one-to-one interviews with Network Rail's or RAIB's personnel.

The main user of the ECF chart developed to support the analysis of Grayrigg train derailment was the researcher and thus, it was important that the researcher had the confidence in the developed chart. This is discussed below.

As mentioned previously, the RAIB report (RAIB, 2011), which was the main source of data for the analysis, was the result of an independent and comprehensive inquiry and thus provided credible and rich data for the analysis. Also of importance is that the data in the report was well presented and structured and its quantity manageable, which facilitated the analysis. Thus, the process of ECF chart development using the data from the RAIB report was straightforward. The report clearly listed all the events and conditions that were necessary and sufficient for the accident to occur (see the section in the report entitled *"The cause of the derailment"*). The events and conditions were described well and the relationships among them clearly explained. This formed a good basis for development of the ECF chart. In addition, each event and condition in the ECF chart and the relationships between them were examined to ensure that they are consistent with the guidelines developed by Kingston et al. (2007) and described earlier in this section. Also, all events and conditions in the ECF chart were supported by the appropriate fragment of text in the report and linked to the corresponding page and paragraph in the RAIB report. Other supporting evidence, including direct quotes from the RAIB report that support each event, condition and relationships between them, is presented in Appendix J.

4.5.4 Analysis of the events and conditions captured by the ECF chart

The key take-away points from the ECF chart presented in Figure 4-1 and Figure 4-2 are summarised below:

- The event that initiated the accident is Event 6: *"Fasteners of the joint between 3rd PW stretcher bar & right-hand switch rail fail sometime between 7/01-12/02/07".* This event, combined with Condition 4 and Event 7 led to the contact between the left-hand switch rail and the wheels of the trains that were operating on the line after the joint failed. This led to the accelerated deterioration of other components of Lambrigg 2B points (Event 4).
- The accelerated degradation of 2B points could have been prevented if the points had been inspected on 18 February 2007. The Network Rail standards require that "*should any cracked or broken bars or brackets be found, the signaller must be informed immediately and a 20 mph emergency speed restriction shall be imposed for up to 36 hours, providing all nuts were secure and tight. If these conditions cannot be met or if it is considered unsafe, block the line*" (RAIB, 2011, p. 226, paragraph 7). Thus, if the inspection had occurred as expected, then the degradation of 3rd PW stretcher bar would have been detected and action taken to repair the points and ensure safety of the line. The train derailment on 23 February 2007 would have been prevented. However, the track section manager, who agreed to inspect 2B points, forgot to do it. Thus, the inspection of Lambrigg 2B points was not carried out on 18 February 2007 (Event 8) and all three stretcher bars and the locker bar at the Lambrigg 2B points were allowed to degrade. As a result the left-hand switch rail moved towards the stock rail (Event 3), the wheels of the Virgin train were forced into the reduced width between switch rails, climbed over the rails and the train derailed on 23 February 2007.

Event 6, Event 8 and Condition 4 were necessary for the accident to occur and Network Rail had control over them. These were the critical events or direct causes of the accident. These critical events were selected for further analysis with the objective of explaining why these events and conditions arose. This was accomplished with the help of an SD model that captured the structure of Network Rail's inspection, maintenance and risk management system whose role was to ensure safety of the railway infrastructure and control the risk of train derailment.

The SD model is presented in Section 4.6. Analysis of why Event 6, Event 8 and Condition 4 arose is presented in Section 4.7.

4.6 Stage 2a: SD model development

As explained in the previous sections, the critical events and conditions identified during the ECFA+ analysis were as follows:

- Event 6: *"Fasteners of the joint between 3rd PW stretcher bar & right hand switch rail fail sometime between 7/01-12/02/07"*
- Event 8: *"Track manager does not perform basic visual inspection on 18/02/07"*
- Condition 4: *"Excessive residual switch opening present since renewal of points in 2001"*

Event 6 and Condition 4 reflect poor condition of the infrastructure assets that contributed to the derailment. Thus, the SD model was used to capture the organisational processes designed to keep the condition of these assets under control. Event 8 reflects an action of the Network Rail staff involved in the inspection of the assets, which is one of the organisational processes designed to keep the condition of these assets under control. Thus, the special focus in the SD model is placed on the structure of the infrastructure inspection process. The model and its key sectors are described in detail below.

4.6.1 Model overview

The model consists of three sectors. The sectors and relationships between them are depicted in Figure 4-5.

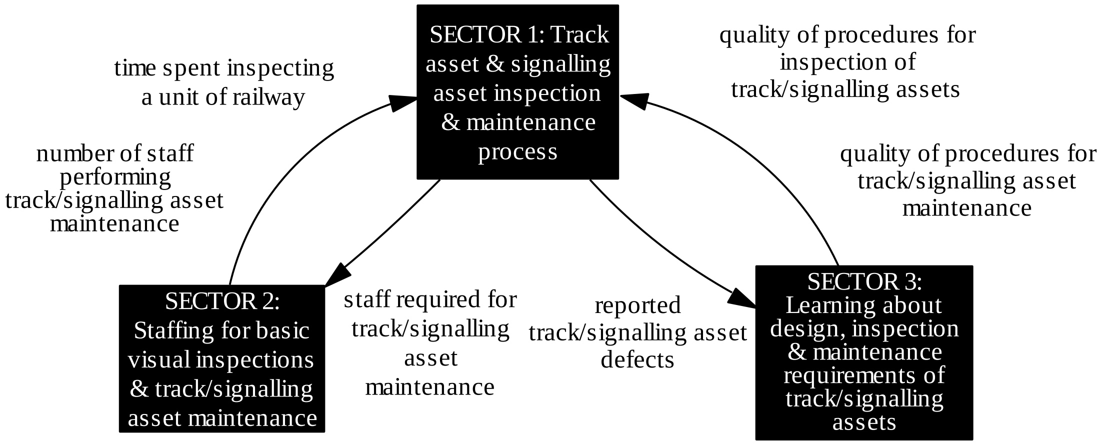

SECTOR 1: Track asset & signalling asset inspection & maintenance process
time spent inspecting a unit of railway
number of staff performing track/signalling asset maintenance
quality of procedures for inspection of track/signalling assets
quality of procedures for track/signalling asset maintenance
SECTOR 2: Staffing for basic visual inspections & track/signalling asset maintenance
staff required for track/signalling asset maintenance
reported track/signalling asset defects
SECTOR 3: Learning about design, inspection & maintenance requirements of track/signalling assets

Figure 4-5: Overview of the SD model

The arrows in Figure 4-5 show the direction of influence. The pieces of text next to the arrows represent outputs of the respective model sectors. These variables feed into the sectors to which the arrows are pointing. The sectors and the relationships between these sectors are explained in detail in the subsequent sections of the report. A short summary description of the model structure is provided below.

As explained in Section 4.5.2, track and signalling assets were inspected by Carnforth track engineering staff during weekly basic visual inspections. Any defects identified were either repaired or reported so that the appropriate remedial action could be taken. The process of track and signalling asset inspection and maintenance is captured in Sector 1 of the model.

Any *Reported track/signalling asset defects*, which are an output of Sector 1 and feed into Sector 3, were investigated if judged appropriate by those repairing these defects. These detected defects were the key inputs into the process of learning about design, inspection and maintenance requirements of track and signalling assets that is represented by Sector 3.

As already mentioned, inspections of track and signalling assets and maintenance of track assets were carried out by Carnforth track engineering staff. Carlisle signal engineering staff were responsible for maintenance of signalling assets in the

Lambrigg area. The number of track engineering staff that would carry out the inspection and the number of track engineering staff that would perform track maintenance activities was planned before the inspection and maintenance activities took place. The number of staff required for track asset maintenance, and also the number of staff required for signalling asset maintenance, depended on the number of detected track defects. Sector 2 represents the process of staffing basic visual inspections and track/signalling asset maintenance activities. There are two key outputs of this process:

- *Time spent inspecting a unit of track* which is influenced by the number of staff assigned to inspect a particular section of the railway
- *Number of staff performing track/signalling asset maintenance*

These outputs of Sector 2 feed into Sector 1. *Time spent inspecting a unit of track* affects the quality of basic visual inspection. *Number of staff performing track/signalling asset maintenance* affects the rate at which track defects are removed.

These sectors and the relationships between them are described in more detail in the sections that follow. The model was created using the information captured in the 2011 RAIB report. The references to specific parts of the RAIB report that support the key structures of the SD model are given throughout the chapter.

The scope of the SD model was influenced by the ECFA+ analysis as explained earlier in this chapter. Only the factors that have contributed to critical events and conditions identified in the ECF diagram (Event 8, Event 6 and Condition 4) were captured in the SD model. Table 4-1 lists the sectors of the model, the key elements included in each sector of the final SD model and justification for inclusion. The sectors and their elements and how the researcher went about developing the model are fully described later in this chapter.

Table 4-1: Key elements included in final SD model

Sector	Key element of the model	Justification for inclusion
Sector 1: Track asset & signalling asset inspection & maintenance process	Track asset & signalling asset deterioration process	This affected the number of defects to be investigated during weekly basic visual inspections and the number of defects to be reported and maintained and thus, it affected the number of staff needed for their maintenance.
	Quality of basic visual inspections	This determined the number of signalling and track defects identified per week and it was affected by the *Time spent inspecting a unit of track.* This in turn was affected by the number of staff inspecting track and the time available to inspect the truck.
	Quality of asset maintenance	This affected the condition of assets.
Sector 2: Staffing for basic visual inspections & track/signalling asset maintenance	Number of staff required and available for basic visual inspections and maintenance of track/signalling assets	Affected the quality of inspections and rate at which track/signalling defects were removed
Sector 3: Learning about design, inspection and maintenance requirements of track/signalling assets	Quality of track/signalling asset design	Affected the track/signalling asset deterioration process
	Willingness to investigate track/signalling asset defects & quality of investigation	Affected the learning about track/signalling asset design, inspection and maintenance requirements and thus the asset condition.

4.6.2 Sector 1

The key elements of Sector 1 are depicted in Figure 4-6. The structure of the inspection and maintenance regime for track assets and the inspection and maintenance regime for signalling assets is similar. They both involve processes of asset deterioration, defect identification and corrective maintenance of defects. The SD structure used to capture this process of detecting and correcting flaws in systems is well known in the SD literature (see e.g. Lyneis & Ford, 2007) and was also used within the area of accident analysis and risk management (see e.g. Hoffman and Wilkinson, 2011). Hoffman and Wilkinson used this SD structure to depict how the oil and gas industry manages the hazards they face.

In the model, *Track asset deterioration* and *Signalling asset deterioration* are both affected by *Poor weather conditions* (RAIB, 2011, p. 71/paragraph 244) and *Quality of track/signalling asset design* (RAIB, 2011, p.14/paragraph 30). Defect identification in both cases is affected by the *Quality of basic visual inspection, Time between inspections* and whether there are *Independent inspections of track/signalling defects* conducted.

Quality of basic visual inspection performed by track engineering staff is affected by four factors (RAIB, 2011 p. 69/233-236):

- *Time spent inspecting a unit of railway*
- *Track engineering staff competence*
- *Quality of procedures for inspection of signalling & track assets*

Corrective maintenance of (track/signalling) assets (number of defects removed per week) is affected by *Quality of (track/signalling) asset maintenance* and *Number of staff performing (track/signalling) asset maintenance.* The quality of asset maintenance is influenced by the competence of staff performing maintenance and the existence of adequate procedures for the maintenance of assets.

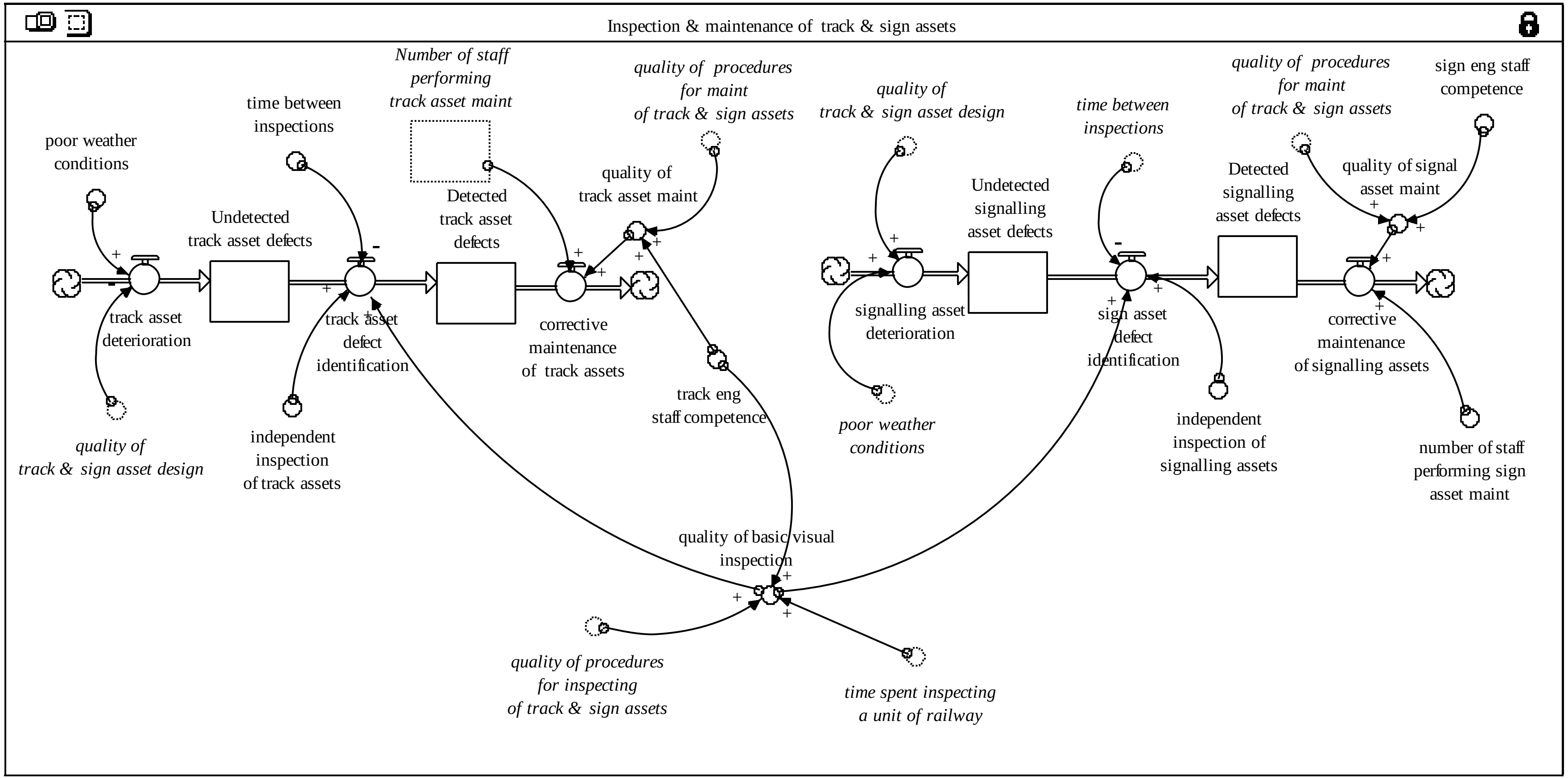

Inspection & maintenance of track & sign assets
Number of staff performing track asset maint
quality of procedures for maint of track & sign assets
quality of track & sign asset design
time between inspections
quality of procedures for maint of track & sign assets
sign eng staff competence
time between inspections
poor weather conditions
Undetected track asset defects
Detected track asset defects
quality of track asset maint
Undetected signalling asset defects
Detected signalling asset defects
quality of signal asset maint
track asset deterioration
track asset defect identification
corrective maintenance of track assets
signalling asset deterioration
sign asset defect identification
corrective maintenance of signalling assets
track eng staff competence
quality of track & sign asset design
independent inspection of track assets
poor weather conditions
independent inspection of signalling assets
number of staff performing sign asset maint
quality of basic visual inspection
quality of procedures for inspecting of track & sign assets
time spent inspecting a unit of railway
+
-

Figure 4-6: Sector 1 of the model

4.6.3 Sector 2

The key elements of Sector 2 are depicted in Figure 4-7. Carnforth track engineering staff at Network Rail were responsible for carrying out basic visual inspections of the railway and corrective maintenance of detected track asset defects. A responsibility of the track section manager was to ensure that enough staff were assigned for basic visual inspection every week so that it could be completed in the time available (*Time available to inspect railway*). Basic visual inspections had priority over maintenance (RAIB, 2011, p.224, paragraph 12). Network Rail used some standard timings (*Time needed to inspect railway)* for planning the *Number of track engineering staff required for inspection* (RAIB, 2011, p. 69/236). If there was a gap between track engineering staff readily available for inspection and staff required (*Gap between track engineering staff required & readily available*) then the track section manager had to take actions to reduce the gap. One of the options available to him was to reduce *Number of track engineering staff available for track asset maintenance* and assign these staff to inspect the track (RAIB, 2011, p.224, paragraph 12). Other *Actions to reduce the gap between staff required & available for inspection* included asking staff to work overtime (RAIB, 2011, p.224, 12). The *Number of staff inspecting the railway* and *Time available to inspect railway* affected the *Time spent inspecting a unit of railway* and, thus, the *Quality of basic visual inspection.*

The *Number of staff required for track asset maintenance* depends on the number of *Detected track asset defects*. If there is a gap between staff required and staff available for track asset maintenance, the track section manager can, for example, procure the services of agency staff (*Actions to reduce gap between staff required & available for track maintenance*), assuming he has *Senior management support* (RAIB, 2011, p. 71/244). As mentioned in the previous section, the resulting *Number of staff performing track asset maintenance* affects the *Corrective maintenance of track assets* (number of track defects removed per week).

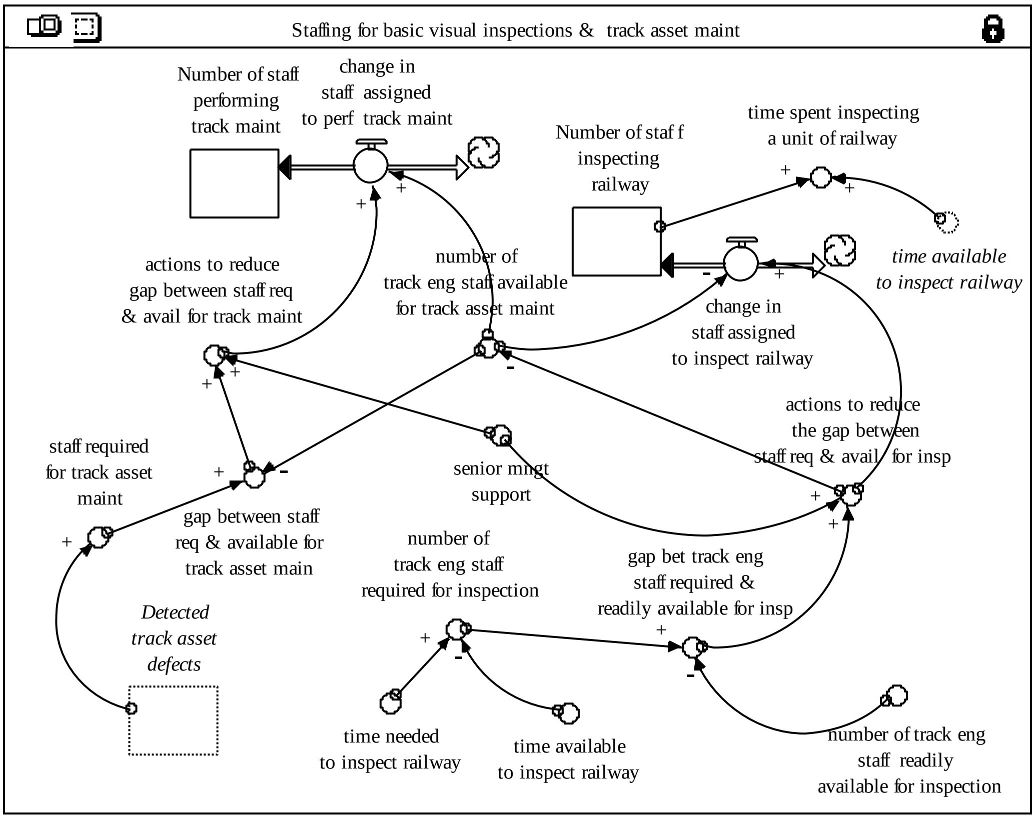

Staffing for basic visual inspections & track asset maint
Number of staff performing track maint
change in staff assigned to perf track maint
Number of staf f inspecting railway
time spent inspecting a unit of railway
time available to inspect railway
actions to reduce gap between staff req & avail for track maint
number of track eng staff available for track asset maint
change in staff assigned to inspect railway
actions to reduce the gap between staff req & avail for insp
staff required for track asset maint
gap between staff req & available for track asset main
senior mngt support
number of track eng staff required for inspection
gap bet track eng staff required & readily available for insp
Detected track asset defects
time needed to inspect railway
time available to inspect railway
number of track eng staff readily available for inspection

Figure 4-7: Sector 2

4.6.4 Sector 3

The key elements of Sector 3 are depicted in Figure 4-8. *Detected track/signalling asset defects* increase the number of *Reported track/signalling asset defects* and, subsequently, *Investigations into track/signalling asset failures* and the number of *Lessons learnt on design, inspection & maintenance requirements of track/signalling assets.* Other ways of increasing lessons learnt include performing trend analysis of track/signalling asset failure data and performing analysis of existing track/signalling assets using tools such as Failure Modes and Effects Analysis. The number of lessons learnt can lead to actions to improve *Quality of track/signalling asset design* and *Quality of procedures for inspection of track/signalling assets* and *Quality of procedures for maintenance of track/signalling assets*. Increase in *Quality of track/signalling asset design*, slows down *Track/Signalling asset deterioration* (Sector 1). *Quality of procedures for inspection of track/signalling assets* and *Quality of procedures for maintenance of track/signalling assets* increase the *Quality of basic visual inspection* and *Quality of track/signalling asset maintenance,* respectively.

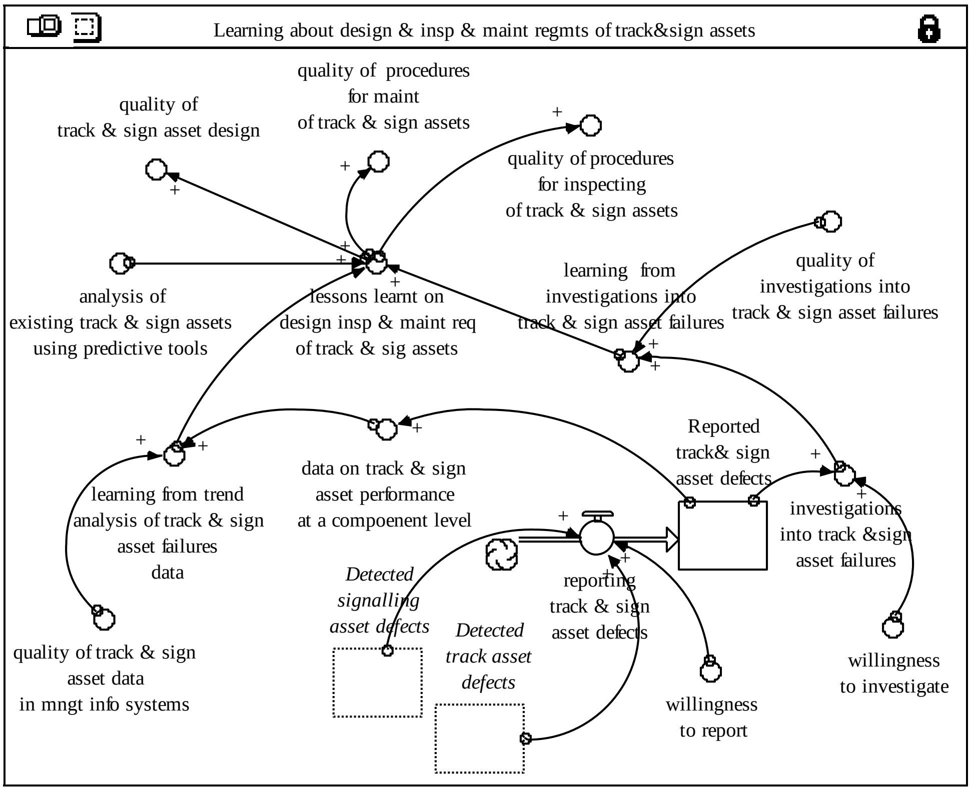

Learning about design & insp & maint regmts of track&sign assets
quality of track & sign asset design
quality of procedures for maint of track & sign assets
quality of procedures for inspecting of track & sign assets
quality of investigations into track & sign asset failures
analysis of existing track & sign assets using predictive tools
lessons learnt on design insp & maint req of track & sig assets
learning from investigations into track & sign asset failures
Reported track& sign asset defects
learning from trend analysis of track & sign asset failures data
data on track & sign asset performance at a compoenent level
investigations into track &sign asset failures
Detected signalling asset defects
Detected track asset defects
reporting track & sign asset defects
willingness to report
willingness to investigate
quality of track & sign asset data in mngt info systems

Figure 4-8: Sector 3

4.6.5 SD model validation

The SD model was used to capture the structure of Network Rail's inspection, maintenance and risk management systems designed to keep the infrastructure fit and safe for train use and control the risk of train derailment. The purpose of the model was to support analysis of the organisational context that influenced the events and conditions identified using the ECF chart. Again, if the SD model was developed as part of an accident investigation, then the structure of the model could be validated by the Network Rail's or RAIB's staff who would be the main users of the model. Different approaches could be adopted. For example, the model could be created from scratch during a workshop with the Network Rail's/RAIB's staff. Alternatively, the model could be created by an analyst using the available data and the staff would be asked to comment upon it during individual interview sessions or during a workshop or series of workshops.

The main user of the SD model developed to support the analysis of Grayrigg train derailment was the researcher and thus, it was important that the researcher had the confidence in the developed model. This is discussed below.

Overall, the ECF chart clearly indicated that the key organisational process relevant to the Grayrigg train derailment was the infrastructure inspection and maintenance process. Thus, the SD model development started with identifying the key stocks associated with Network Rail's infrastructure inspection and maintenance regime designed to keep the risk of train derailment under control. The key stocks that were identified and are in the final SD model are:

- *Undetected track/signalling asset defects*
- *Detected track/signalling asset defects*

Identification of these stocks was preceded by the examination of the archetypal SD structures relevant to the problem at hand. Inspection and maintenance is a process of detecting and correcting flaws in the systems. This process is well-known in the SD literature and referred to as a "rework cycle" (Lyneis and Ford, 2007). This "rework cycle" structure was also used within the area of accident analysis and risk management (see e.g. Hoffman and Wilkinson, 2011). Hoffman and Wilkinson used this SD structure to depict how the oil and gas industry manages the hazards they face. The archetypal "rework cycle" SD structure was adapted, i.e. the stocks *Undetected track/signalling asset defects and Detected track/signalling asset defects* were used. The subsequent modelling activity focused on identifying the key flows responsible for changes in these two stocks and then on identifying the key factors impacting these flows. Thus, the approach to the SD model development was one of progressive elaboration using the information in the RAIB report and generic SD structures found in the SD literature.

Development of the stock and flow diagram, using the data captured in the RAIB report, was not an easy task. The RAIB report was a source of secondary data and was not prepared with the development of an SD model in mind. Thus, the pieces of data required to develop the SD model [e.g. data on the structure of the analysed system, data on flows between different parts of the system and data on policies (decision rules) that guide decision-making within the system] were often not explicitly discussed in the report. The researcher's approach to build confidence in the model was to ensure that all key structures of the SD model, described in the previous sections, were substantiated by the appropriate, supporting fragment of text in the RAIB report and linked to the corresponding page and paragraph in the RAIB report. If the relationship between the SD model structure and the report was not obvious, the researcher was explicit about the assumptions underlying the creation of this particular structure.

4.7 Stage 2b: Analysis of HOFs that contributed to the events and conditions identified in the ECF chart

This section presents analysis of why Event 6, Event 8 and Condition 4, identified using the ECFA+ analysis, arose.

4.7.1 Event 8

The simplified part of the SD model relevant to Event 8, *Track manager does not perform basic visual inspection on 18/02/07,* is presented in Figure 4-9. The circumstances that increased the *Probability that track manager decides to perform basic visual inspection himself* are described below.

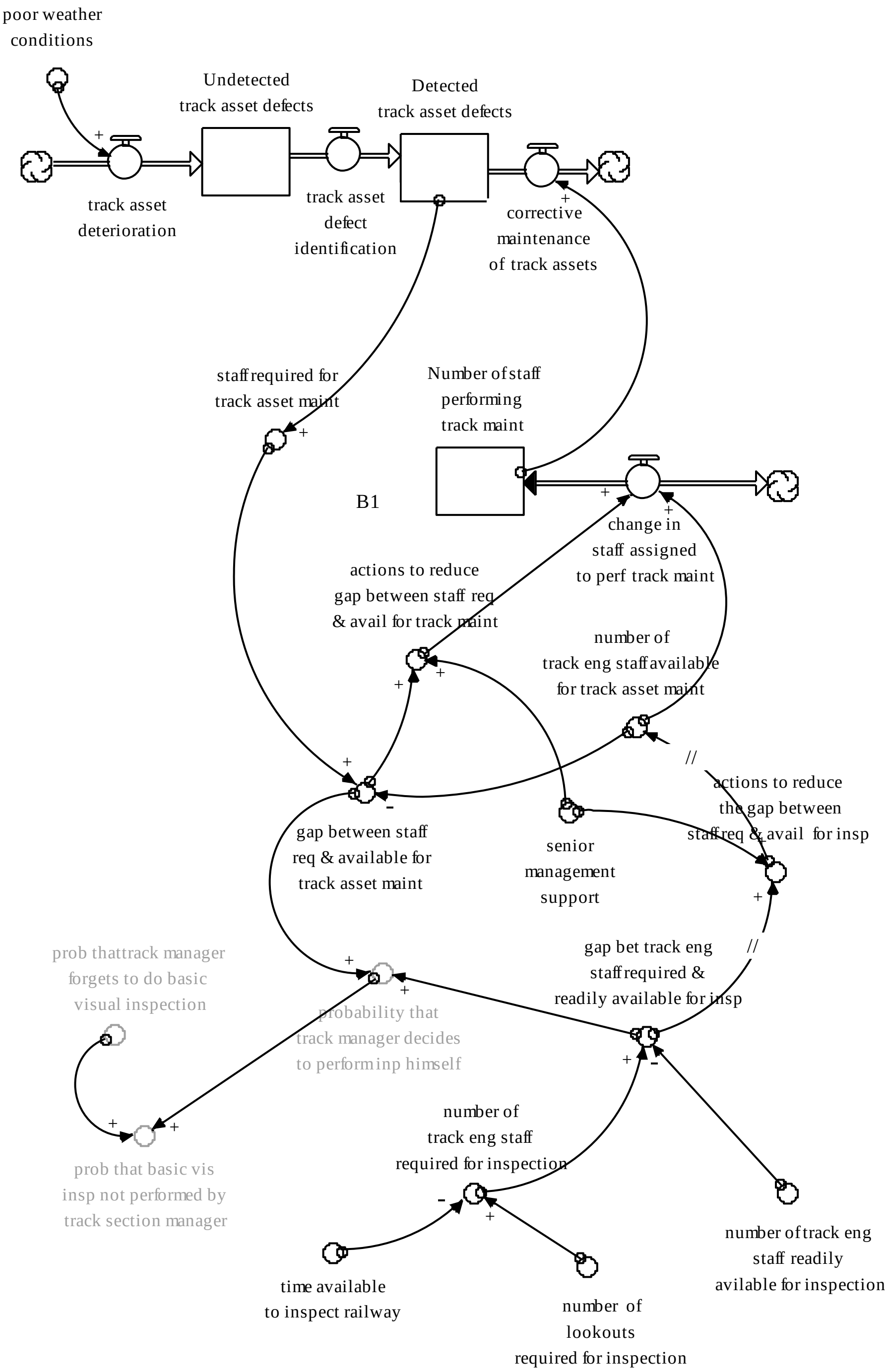

poor weather conditions
Undetected track asset defects
Detected track asset defects
track asset deterioration
track asset defect identification
corrective maintenance of track assets
staff required for track asset maint
Number of staff performing track maint
B1
change in staff assigned to perf track maint
actions to reduce gap between staff req & avail for track maint
number of track eng staff available for track asset maint
//
actions to reduce the gap between staff req & avail for insp
gap between staff req & available for track asset maint
senior management support
gap bet track eng staff required & readily available for insp
//
prob that track manager forgets to do basic visual inspection
probability that track manager decides to perform inp himself
prob that basic vis insp not performed by track section manager
number of track eng staff required for inspection
time available to inspect railway
number of lookouts required for inspection
number of track eng staff readily avilable for inspection
+
-

Figure 4-9: Factors contributing to Event 8 in the ECF chart

Towards the end of 2005 Network Rail authorised tilting trains to run at enhanced permissible speed (EPS) in the Lambrigg area. As a result, inspection and maintenance of the railway in this area could only be done within a possession, i.e. "*a period of time during which one or more tracks are blocked to normal service trains to permit work to be safely carried out on or near the line"* (RAIB, 2011, p. 199). This essentially meant that basic visual inspections of track and signalling assets could only be carried out during weekends (RAIB, 2011, p. 224/13). Thus, *Time available to inspect railway* had been significantly reduced since 2005 until the occurrence of the accident and there were no changes to the technology that would allow the completion of inspection and maintenance in the time available. In order to ensure the same level of quality of inspection, more staff were needed to conduct the inspections.

In addition, in April 2006, the duration of the possession was reduced from 29 hours at the weekend to approximately 11 hours on Saturday night and Sunday morning (RAIB, 2011, p. 224/13). This meant that the Carnforth section of the railway could only be inspected between dawn and around 10:30 on Sunday mornings. This was related to the fact that basic visual inspections could only be done in the daylight (RAIB, 2011, p.225/paragraph 15).

The reduction in the *Time available to inspect railway* at the end of 2005 and later in April 2006 resulted in the increase in the *Number of track engineering staff required for inspection.* No extra resources were provided to conduct the mandatory basic visual inspections (RAIB, 2011, p. 224/paragraph 12). The Carnforth track section manager had to devise options for reducing the *Gap between track engineering staff required & readily available for inspections* so that inspections could be completed in the time available. If an inspection was not completed on Sunday morning, then the railway would have to be closed to normal traffic during the week and train service would be disrupted. This was highly undesirable (RAIB, 2011, p.225/paragraph16).

In order to reduce the *Gap between track engineering staff required & readily available for inspections* the track section manager tried different options. One of the options was to ask staff to work overtime (*Actions to reduce the gap between staff required & available for inspection*). However, there were constraints set by senior management on how much overtime could be booked (*Senior management support*). Other options included bringing in agency staff to perform track maintenance, so that Network Rail staff could focus on basic visual inspections. This is not explicitly mentioned in the report, but there were probably delays between identifying gaps, taking action to correct these gaps and observing results of these actions as there was always lack of required resources (delays are indicated in Figure 4-9 by two lines crossing an arrow). Another option to reduce the *Gap between track engineering staff required & readily available for inspections* was to make track engineering staff inspect the track rather than perform corrective maintenance of track defects. This option increased the number of staff that could be assigned to basic visual inspections, but had significant side effects. Essentially, it reduced the *Number of track engineering staff available for track asset maintenance*, increased the *Gap between track engineering staff required & readily available for track maintenance* and decreased the *Number of staff performing track maintenance.* This resulted in the decrease in the rate of *Corrective maintenance of track defects* and led to an increase in the backlog of track asset maintenance. Thus, this option affected the workings of balancing loop B1. The effect on the maintenance backlog between April 2006 and the beginning of 2007 is described in the RAIB report as follows:

> *"Although there was an adverse impact on the maintenance backlog, witnesses stated that during the summer of 2006 the effect was limited by drier weather, which stabilised the ballast and helped to slow the deterioration in track condition. At the end of August 2006, authority was given by local management for the procurement of the services of an eight-member agency gang to undertake maintenance activity that would otherwise have been undertaken on Sunday mornings by staff who were now required for patrolling or lookout duties. Despite this, the backlog worsened during the autumn of 2006 due to the wetter weather, and by the end of that year the critical maintenance backlog was reaching levels that management at local and territorial level deemed unacceptable. A major effort was made at the beginning of 2007 to reduce the backlog, and more resources were introduced in the form of contract staff to manage possessions, thereby releasing supervisors and other staff to spend more time on basic duties, and providing management focus on the critical backlog items in the 'plan-do-review' meetings. As a result a downward trend was seen through the first two months of the year"* (p. 71/paragraph 244).

Delays between recognising the *Gap between staff required & readily available for track asset maintenance* and taking *Actions to reduce the gap between staff required & available for track maintenance* and between taking the actions and seeing their effects, reduced the effectiveness of the feedback loop controlling the process of corrective maintenance of track defects. This was worsened by an increase in *Poor weather conditions* that increased *Track asset deterioration* and consequently the number of *Detected track asset defects*.

The increased *Gap between track engineering staff required & readily available for inspections* and *Gap between staff required & readily available for track asset maintenance* throughout 2006 and in 2007 increased the *Probability that track manager decides to perform basic visual inspection himself*. Performing basic visual inspections by track managers was one of the options available to the track section manager to deal with staffing difficulties and was allowed by the Network Rail standards (RAIB, 2011, p.59/paragraph 192). On 12 February 2007 the track section manager agreed to perform a basic visual inspection on 18 February 2007. He did that to release two members of his staff to perform maintenance of another section of the railway (RAIB, 2011, p. 67/257). In the week between 12 and 18 February he forgot that he agreed to carry out the inspection and he did not do it (Event 8).

The SD diagram clearly depicts the following:

- the exogenous factor was the reduction in *Time available for inspection* which disrupted the operation of Network Rail's inspection and maintenance regime
- Network Rail was not prepared to deal with this disruption and ensure adequate *Number of staff performing track maintenance* and adequate *Number of staff inspecting railway*
- the track manager's local efforts to comply with the company standards and ensure that basic visual inspections are completed every week imbalanced the stock *Number of staff performing track maintenance.* This resulted in unintended consequences in the form of increased backlog of track asset maintenance and affected the safety of the train infrastructure (thus it affected the workings of the balancing loop B1 designed to keep the number of track asset defects under control)
- delays in Network Rail's efforts to provide the adequate number of staff for inspection and maintenance prolonged the imbalance of the stock *Number of staff performing track maintenance*
- track manager efforts to ensure adequate level of the stocks *Number of staff inspecting railway* and *Number of staff performing track maintenance* finally led him to perform railway inspection himself (which was allowed by company standards) and this was the final stage of a system's "migration" to a state of increasing risk and the boundary of acceptable safety performance, where subsequent slight variation in track manager's behaviour (he forgot to inspect part of the track) led to the derailment.

4.7.2 Event 6 and Condition 4

The part of the SD model relevant to Event 6 and Condition 4 is presented in Figure 4-10**.** According to the RAIB report there was a lack of recognition throughout Network Rail of the importance of the residual switch opening and its correct value which resulted in an excessive residual switch opening (Condition 4). Also, according to the RAIB report, the initiating failure of the fasteners of the joint between the 3rd stretcher bar and the right-hand switch rail (Event 6) was either because the traffic conditions between 7/01-12/02/07 at Lambrigg 2B points were beyond joint design capability or because the joint fasteners were not properly tightened during maintenance on 7/01/07. Thus, the circumstances responsible for Condition 4 and Event 6 were related to the quality of track/signalling asset design and the quality of procedures for maintenance of assets. This in turn related to the ineffective process of learning from experience by Network Rail – see balancing loops B2, B3 and B4.

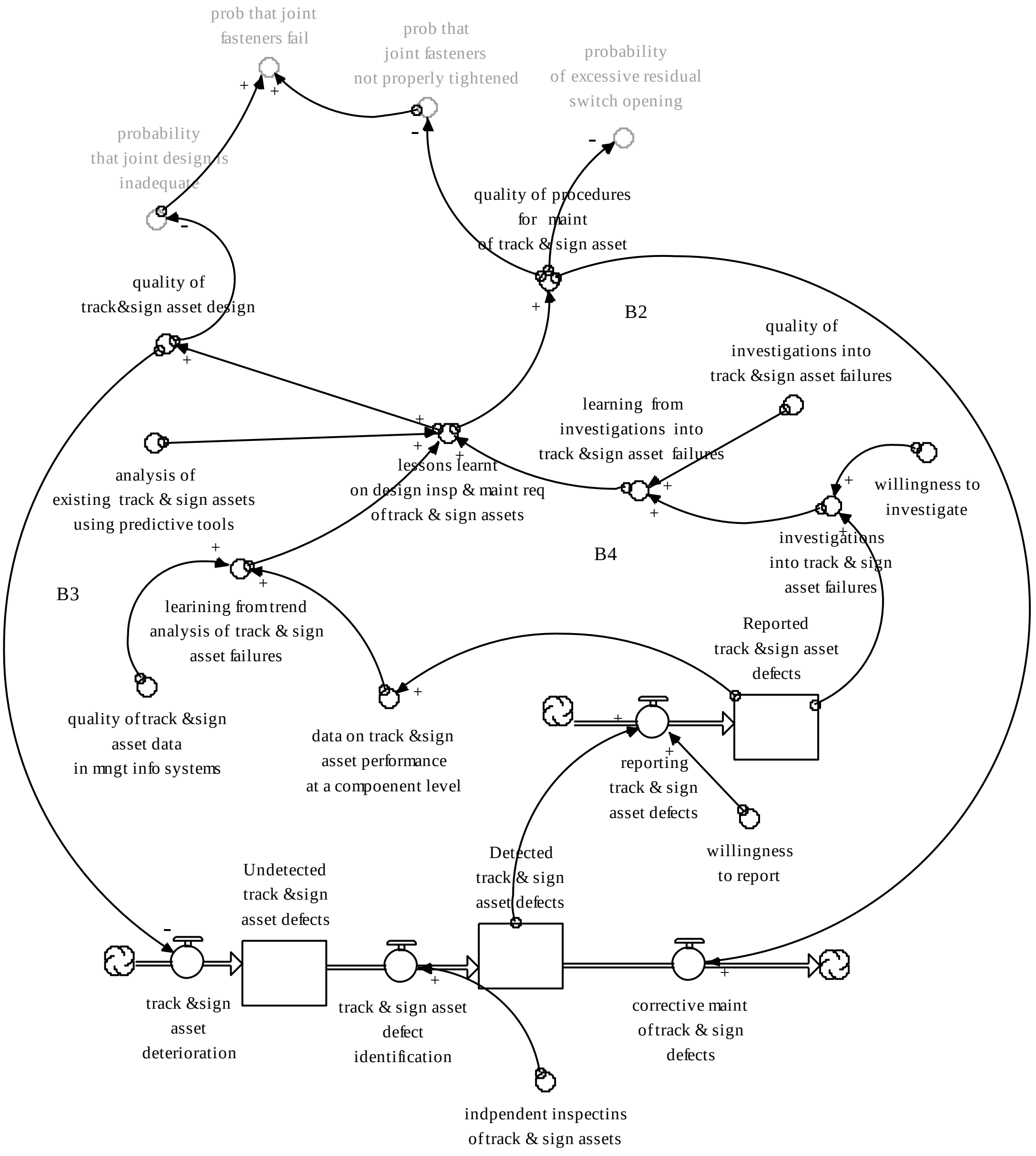

prob that joint fasteners fail
prob that joint fasteners not properly tightened
probability of excessive residual switch opening
probability that joint design is inadequate
quality of procedures for maint of track & sign asset
quality of track&sign asset design
B2
quality of investigations into track &sign asset failures
learning from investigations into track &sign asset failures
willingness to investigate
analysis of existing track & sign assets using predictive tools
lessons learnt on design insp & maint req oftrack & sign assets
investigations into track & sign asset failures
B4
B3
learining fromtrend analysis of track & sign asset failures
Reported track &sign asset defects
quality oftrack &sign asset data in mngt info systems
data on track &sign asset performance at a compoenent level
reporting track & sign asset defects
willingness to report
Undetected track &sign asset defects
Detected track & sign asset defects
track &sign asset deterioration
track & sign asset defect identification
corrective maint oftrack & sign defects
indpendent inspectins oftrack & sign assets

Figure 4-10: Factors contributing to Event 6 and Condition 4 in the ECF chart

Factors that weakened the process of learning from experience and increased *Probability that joint design is inadequate*, *Probability that joint fasteners are not properly tightened* and *Probability of excessive residual switch opening* at Lambrigg 2B points are summarised below:

- lack of *Independent inspections of track/signalling assets* limited the data on points defects that could be analysed for trends or lead to investigations into the causes of failures (RAIB, 2011, p. 86/313)
- *Investigations into track/signalling asset defects* were decreased by the reduced *Willingness to investigate* expressed by the view of Network Rail's engineering staff that *"it would take a repeated failure to trigger some form of investigation"* (RAIB, 2011, p.77/278)
- *Analysis of existing track/signalling assets using predictive tools* (e.g. Failure Modes and Effects analysis, Hazard and Operability Study) at Network Rail was limited which further affected the lessons that could have been learnt about track/signalling asset design, inspection and maintenance requirements (RAIB, 2011, p.103/paragraph 405)
- *Quality of track/signalling asset data in management information systems* was poor which limited the learning that could be gained from trend analysis of points component failure data; in particular, "*there was no explicit requirement to enter details of stretcher bar failures into SINCS until April 2006. Even after this date it is unclear whether the definition of failure in SINCS included loose or missing fasteners"* (RAIB, 2011, p. 102/401)
- *"Network Rail's key performance indicators did not include any specific reference to the condition of stretcher bars, brackets, fasteners or flangeway clearance"* (RAIB, p. 102/401) which limited *Data on track/signalling asset performance at a component level*.

4.8 Summary of the findings

The Grayrigg derailment analysis presented above and supported by the use of ECF and SD models led to the following findings:

- The ECFA+ analysis led to the identification of events and conditions that were sufficient and necessary for the accident to occur, Network Rail had control over them and they could have been prevented. The critical events and conditions that were identified using the ECF chart were as follows:
    - **Condition 4: "***Excessive residual switch opening present since renewal of points in 2001"*
    - **Event 6: "***Fasteners of the joint between 3rd PW stretcher bar & right-hand switch rail fail sometime between 7/01-12/02/07"*
    - **Event 8:** *"Track manager does not perform basic visual inspection on 18/02/07"*

- The ECF chart was used to identify critical events and provided the scope for further analysis using SD. The SD model was used to analyse how the critical events and conditions arose.
- Existence of **Condition 4** and occurrence of **Event 6** were associated with Network Rail's poor knowledge of the design, performance, inspection and maintenance requirements of their points assets. This was related to the ineffective learning from experience feedback loop.
- Occurrence of **Event 8** was related to the track access problems and requirement to complete weekly basic visual inspections during weekends only. Due to staff shortages, the track section manager was in a way "forced" to perform the weekly inspection himself to release two resources to work elsewhere, but subsequently forgot to do it.
- The SD model provided a good depiction of the undesirable consequences for track maintenance of the track manager's actions to ensure that basic visual inspections were completed every week. It clearly showed how these undesirable consequences were related to:
  - the division of responsibilities among track engineering staff, who were responsible for both weekly basic visual inspections of track and signalling assets and the maintenance of the track assets, and
  - track manager's best efforts to comply with the company standards
- The stocks in the SD model clearly indicated the variables in the system which change over time contributed to the accident such as *Undetected track/signalling asset defects*, *Detected track/signalling asset defects, Number of staff inspecting railway*, *Number of staff performing track maintenance*. The flows in the model clearly indicated the processes responsible for accumulation/drainage of the key stocks, e.g. *track/signalling asset deterioration, track/signalling asset defect identification, corrective maintenance of track/signalling assets, change in staff assigned to perform track maintenance, change in staff assigned to inspect railway.* Finally, the stock and flow diagram clearly depicts the balancing (or control) loops designed to keep the risk of train derailment under control, as well as the factors that weakened these loops and contributed to the train derailment. This facilitated the analysis and identification of the key changes over time at Network Rail that have contributed to the accident, in particular the changes in the inspection and maintenance area that have affected the behaviour of the track section manager and also contributed to inadequate track and signalling asset design and maintenance procedures.

4.9 Discussion

The key issues associated with the use of SD within HOF analysis for AA are summarised below:

- The SD was used to complement Event and Conditional Factors Analysis that is traditionally used to support accident investigation and analysis. ECFA + was used to identify the events and conditions that were necessary and sufficient for the accident to occur, Network Rail had control over them and they could have been prevented. This helped to focus the SD analysis on the key factors that contributed to the accident and defined the scope for the SD model. SD was used to model the structure of the inspection, maintenance and risk management system at Network Rail that was relevant to the accident. Then the SD model was used to explain which aspects of Network Rail's inspection, maintenance and risk management system contributed to the events and conditions identified using the ECFA+ approach. Thus, SD was directly linked to the particular events and conditions that were necessary and sufficient for the accident to occur.
- The ECFA+ focused on the events close in time to the accident. The SD modelling focused on capturing the structure of processes that were in operation at Network Rail more than one year before the accident and which contributed to the generation of events and conditions that led to the accident. The ECFA+ provided a static picture of discrete, immediate events and existing conditions involved in the accident. SD provided a picture of the feedback structure of the organisational processes that were in place at Network Rail and generated the events identified using the ECFA+ analysis. In particular, the SD model clearly depicted the key balancing loops designed to keep the risk of train derailment under control and the factors that weakened the effectiveness of these loops and contributed to the accident.
- The proximate events and conditions that have occurred are just one set of all events and conditions that could have occurred. If this particular set had not occurred, probably another set of events at a different point in time would have led to the derailment. Thus, looking at just the proximate events and conditions is not sufficient. To prevent an accident, one should examine the organisational processes which control and generate sequences of events (Leveson, 2004). Also, the analysis of organisational processes will lead to a higher level of learning that could be used for design of control measures for protection against a wider set of accidents rather than just one particular accident. SD can be used to capture the structure of these organisational processes and provide analysts with much higher level learning than the ECFA+ approach. Moreover, analysis using the

ECFA+ approach provides a “context-specific” description of the accident. If one wants to obtain a generic learning to be shared within the industry, one should move to “concept-based” description of the accident (Dekker, 2002). A universal stock and flow structure of SD models could serve as effective means for capturing and sharing key lessons from accidents between duty-holders within the same industry.

- It would have been difficult to develop the SD model without prior construction of the ECF diagram. The ECF diagram provided the focus for the SD model so that key organisational factors involved in the accident were considered. Overall, it is much easier to develop an ECF diagram than to develop a stock and flow diagram. In the former case, the development of the model is much more structured and no extensive training or experience is required. One starts with the key event (e.g. train derailment) and works systematically backwards to identify and analyse events and conditions that have contributed to the final event. Development of an SD model requires a lot of prior training and experience. However, the prior development of an ECF diagram can facilitate, and is a good starting point, for the development of an SD model.

The findings of the ECFA+ and SD analysis of the Grayrigg train derailment, as presented in this chapter, do not differ much from the key findings presented in the RAIB report. However, there are some clear benefits of applying these two modelling approaches:

- The use of an ECF chart and stock and flow diagram can provide analysts with a concise summary of the key factors that contribute accidents and can facilitate discussion of how and why these accidents have happened.
- The key output of the RAIB report is a list of factors involved in the accident, grouped into causal, contributory and underlying factors. The description and explanation of the causal factors, representing technical and human factors, the relationships between them and how they contributed to the accident was detailed, comprehensive and well structured. These factors were captured by the ECF chart and, as mentioned earlier, the ECFA+ analysis of the accident was a relatively straightforward task. However, the RAIB’s description and explanation of the contributory and underlying factors, representing human and organisational contributors to the accident, the relationships between them and how they contributed to the accident was not so detailed, comprehensive and well structured. The RAIB report focused on listing the key weaknesses in the Network Rail’s inspection, maintenance and risk management regime without clearly describing and explaining how these weaknesses arose and the mechanisms that generated them. The benefit of combining an ECF chart with an SD

model is that they together present the interactions between technical, human and organisational elements in one concise picture. For example, they clearly showed how the track access problems influenced the track manager's decision to perform basic visual inspection himself and how this contributed to the final train derailment. In addition, the SD model provided a good depiction of the undesirable consequences for track maintenance of the track manager's actions to ensure that basic visual inspections were completed every week. It clearly showed how these undesirable consequences were related to:

  - the division of responsibilities among track engineering staff, who were responsible for both weekly basic visual inspections of track and signalling assets and the maintenance of the track assets, and
  - track manager's best efforts to comply with the company standards

  Also, the ECF chart and the SD model clearly depicted how Network Rail's poor learning from experience might have contributed to excessive residual switch opening (Condition 4) and the failure of the fasteners of the joint between the 3rd PW stretcher bar & right-hand switch rail fail (Event 6).

- Assuming that the model is validated by the investigation team or Network Rail staff who have a good knowledge of topics covered by the model, the ECF and SD models could facilitate development of measures to prevent accident reoccurrence. The models built using the data from the investigation report could serve as a starting and reference point for the discussion between people from various areas, e.g. maintainers, designers, human factors specialists and management, on how this type of accident and similar ones could be prevented in the future.
- It often happens during the accident investigation that there are differing opinions on some aspects of an accident or that there is a lot of uncertainty associated with how and why an accident occurred. There is usually a lot of uncertainty associated with the impact of human and broader organisational factors. By using models such as an ECF chart and an SD model in particular, all the alternative views can be presented and assumptions can be made explicit and transparent, which can support further analysis of the accident and development of accident preventive measures.
- SD provides an alternative to the traditional event-based sequential models view of accidents. Using the words of Wolstenholme (1999), qualitative SD "*enhances linear and 'laundry list' thinking by introducing circular causality and providing a medium by which people can externalise mental models and assumptions and enrich these by sharing them"* (p. 424). SD focuses on the dynamic nature of human and organisational

factors and the identification of feedback structures responsible for this behaviour over time. It also stresses the importance of delays. As mentioned before delays were not explicitly discussed in the RAIB report. The use of the SD model pointed to the situations where these delays could have played key roles. For example, delays in bringing in resources to support basic visual inspections and asset maintenance led to the situation in which the track manager had to perform the basic visual inspection himself so that two staff members could perform asset maintenance elsewhere.

- The ECF diagram that was created to facilitate analysis of the Grayrigg derailment could be compared to the existing Fault and Event Trees created as part of previous PRA for Network Rail and could help to identify events that have not been recognised in previous PRAs for Network Rail. In addition, existing Event Trees could be compared to the ECF diagram from the analysis of the Grayrigg train derailment in an attempt to generalise the ECF diagram to represent a wider set of accidents against which Network Rail should be protected. This generalised ECF diagram could be then used to see whether feedback loops captured by the SD model could lead to other accidents than the one that actually happened. This could lead to identification of events in the existing Fault and Event trees that could potentially be affected by these feedback loops captured in the SD model. The learning from this analysis could be brought into a future PRA study. For example, the SD structures identified in the retrospective analysis, and representing the organisational context affecting a range of events, could be used to quantify the impact of this context on events in Fault and Event Trees.

4.10 Using SD in the analysis of HOFs for AA & PRA – summary of Chapter 4 and introduction to Chapter 5

This chapter illustrated how SD could support the analysis of HOFs for AA. It presented the application of SD to the analysis of HOFs that contributed to the 2007 Grayrigg train derailment. The key benefits of using SD and issues associated with its application within AA were discussed. The next chapter explores the application of SD to the analysis of HOFs for PRA. However, before moving to the next chapter, another important topic will be discussed.

As already mentioned in the previous chapter, the retrospective and prospective HOF analyses described in this thesis were undertaken in the same order as presented in this thesis. First, SD was used to support analysis of the Grayrigg train accident. Then, SD was applied to the analysis of HOFs for PRA. The retrospective SD analysis of the Grayrigg train derailment provided an opportunity for learning that was brought into the second case. In addition, the learning from the prospective SD analysis for PRA was also brought into the retrospective analysis and, as a result, the original analysis of the Grayrigg train derailment was modified. This two-way learning is briefly discussed below:

– As mentioned before, development and effective use of qualitative SD models requires a lot of prior training and experience. In addition, Richardson argues that "*(...) that using qualitative maps well for analysing a dynamic system requires a great deal of experience and expertise in quantitative system dynamics modelling"* (1999, p.441). The researcher fully agrees with this quote. Using SD prospectively to model HOFs, as in Chapter 5, helped the researcher to clarify the process of applying SD to the retrospective analysis of Grayrigg train derailment. In particular, using SD prospectively helped the researcher to clarify the link between the ECF diagram and the SD model of the factors that contributed to the Grayrigg train derailment. As a result, the researcher introduced three variables in the SD model that served as a connection between the ECF diagram and the SD model:
    - *"Probability that joint fasteners fail"* (links to "*Event 6: Fasteners of the joint between 3rd PW stretcher bar & right-hand switch rail fail sometime between 7/01-12/02/07"* in the ECF diagram)
    - *"Probability of excessive residual switch opening"* (links to "*Condition 4: Excessive residual switch opening present since renewal of points in 2001*" in the ECF diagram)
    - *"Probability that basic visual inspection is not performed by track section manager"* (links to "*Event 8: Track manager does not perform basic visual inspection on 18/02/07"* in the ECF diagram)

– In the previous chapter it was concluded that modelling approaches such as ECFA+, traditionally used in HOF analysis for AA, provide a static picture of the events and conditions that were necessary and sufficient for the accident to occur. In addition, they usually focus only on the proximate technical and human events and conditions and have limited capabilities to account for wider organisational factors. These proximate events and conditions are just one set of all the events and conditions that could have occurred. If one particular set had not occurred, probably another set of events at a different point in time would have arisen. Thus, looking at just the proximate events and conditions is not sufficient. To prevent an accident, one needs to examine the organisational processes that *"control a sequence of events and describe system and human behaviour over time* *rather than [consider] events and human actions individually"* (Leveson, 2004, p.247). SD is capable of describing "system and human behaviour over time" and was used in this chapter to complement ECFA+ analysis for AA. The analysis presented in this chapter indicated that the sole use of SD, without prior use of ECFA+, would have been difficult. The ECF chart defined the scope and boundary for the subsequent SD analysis. Illustrating how ECFA+ and SD could be combined and discussing benefits and limitations of mixing these two approaches is an important contribution of this thesis. It also suggests that it might be feasible and beneficial to combine SD with modelling approaches traditionally used in HOF analysis for PRA, which has already been recognised in the PRA literature (e.g. Mohaghegh et al., 2009). This realization has informed the development of the SD model presented in the next chapter and led to the consideration of whether it would be beneficial to combine SD with modelling approaches traditionally used to support PRA. In addition, the application of SD to HOF analysis for AA, presented in this chapter, indicated that the development of an SD model can be facilitated by adapting archetypal SD structures described in the SD literature. For example, the SD model that supported the analysis of the Grayrigg train derailment was based on the "rework cycle" SD structure well-known among SD modellers working in the area of project management (Lyneis and Ford, 2007). Thus, the creation of the SD model presented in the next chapter was preceded by the examination of the archetypal SD structures relevant to the problem at hand. Finally, Chapter 2 indicated that traditional PRA is quantitative in nature. Thus, it needs to be considered whether and how SD can fit into this type of framework. The use of SD within AA, presented in this chapter, highlighted that quantifying SD models in this area might be difficult due to the existence of a number of soft variables such as "willingness to investigate" or "quality of investigation". This issue will be explored later in the next chapter.

CHAPTER 5: Using SD in the analysis of HOFs for PRA

5.1 Introduction

The previous chapter illustrated how SD could be used in HOF analysis for AA.

AA is an important part of the risk management of complex technological systems. It is a retrospective analysis concerned with examining accidents that have already occurred. It complements PRA which is concerned with identification of hazards and potential adverse effects and estimation of the likelihood that these adverse effects will realize. Both AA and PRA help those responsible for risk management of complex technological systems to avoid costs associated with the occurrence of accidents, understand the risks associated with the operation of these systems and ensure compliance with health and safety law.

As explained previously, logical and mathematical modelling plays an important role in PRA and gains increasing recognition in the AA community. SD is a modelling approach that can support HOF analysis for both PRA and AA. The previous chapter illustrated how SD could be used in HOF analysis for AA and discussed issues and benefits associated with using SD in this area. This chapter illustrates how SD could be used in HOF analysis for PRA. SD is applied to the analysis of HOFs contributing to the unavailability of a standby power system at a process plant. The standby power system (SPS) is part of the electric power system supporting the plant. Its role is to provide alternating current power to the plant in the event that all off-plant power sources are lost. This event could be captured as an “initiating event” in a PRA for the plant and the SPS as the system designed to mitigate the consequences of this event.

Background information on the electric power system supporting the plant, including a description of the SPS and discussion on why this area was selected for PRA, are presented in the next section. Next, the objectives of the analysis and the approach to the analysis are discussed. The analysis of the HOFs contributing to the unavailability of the SPS at the plant, the models that supported the analysis and the key findings are discussed in the sections that follow. Also, the issues involved in using SD in the analysis of HOFs for PRA are discussed. 0lists the key abbreviations and Appendix B provides definitions of the key technical terms used throughout this chapter.

5.2 Background information

The aim of this section is to introduce the reader to the SPS at the plant. The selection of this particular system for PRA and HOF analysis is discussed first. The sections that follow describe the SPS in more detail. This should provide the reader with information sufficient to understand the remaining sections of this chapter.

5.2.1 Why was an SPS at a process plant selected for PRA and HOF analysis?

The aim of this chapter is to illustrate how SD could be used to support HOF analysis for PRA and discuss whether there are any issues associated with using SD in this area. There are several reasons why it was decided to apply SD to the analysis of HOFs contributing to the unavailability of a SPS at a process plant. They are summarised below:

- Process plants belong to the category of complex technological systems described in Chapter 2. The hazards involved in the maintenance and operation of the systems used within process plants are numerous and not easy to identify. Adverse effects of accidents may be very severe.
- As discussed in Chapter 2, the human tasks that are usually analysed as part of HOF analysis for PRA include those performed by operators and maintainers under normal operating conditions and those performed after an “initiating event” occurs. The former can introduce latent faults into the engineered safety systems designed to mitigate the consequences of “initiating events”. The latter tasks are critical to cope with an abnormal situation that arises after an “initiating event” occurs. This chapter illustrates how SD could be used to support analysis of the first type of tasks, i.e. tasks performed under normal operating conditions which can introduce latent faults into the engineered safety systems designed to mitigate the consequences of “initiating events”. The uncertainty associated with modelling these types of tasks is smaller compared to the tasks performed in abnormal situations. The tasks performed under normal operating conditions involve tasks such as maintenance, testing, calibration and restoration tasks. What is to be done as part of these tasks is highly standardised and prescribed by the organisational policy and relevant written procedures. There is relatively little diagnosis and decision-making which are more characteristic of the tasks performed in abnormal conditions. Thus, the potential human errors and equipment failures are relatively easier to identify in tasks performed under normal operating conditions. Also, we have more knowledge on the

factors that shape human performance and equipment operation in normal operating conditions and how errors and failures occur.

– The early assessment of the factors affecting availability of the SPS at the plant indicated that SD could be used to model the situation. Firstly, the sponsor of the project indicated extensive human involvement in the maintenance process of this system and suggested that this area may largely contribute to the unavailability of the SPS. Overall, decisions and actions of people involved in the maintenance of safety critical systems are influenced by the wider feedback-driven organisational context in which these people are performing their assigned tasks. As the purpose of conducting PRA and HOF analysis was to improve the control of risks and safety, explicit modelling of the organisational feedback structure and the use of SD was seen to be beneficial. Practically, it was not difficult to visualise the HOFs involved in potential accidents in terms of stocks and flows and an initial, simple SD model was easily constructed.

An overview of the analysed system and problem area is provided in the next section.

5.2.2 Electric power system supporting the plant

Figure 5-1 shows a simplified representation of the electric power system.

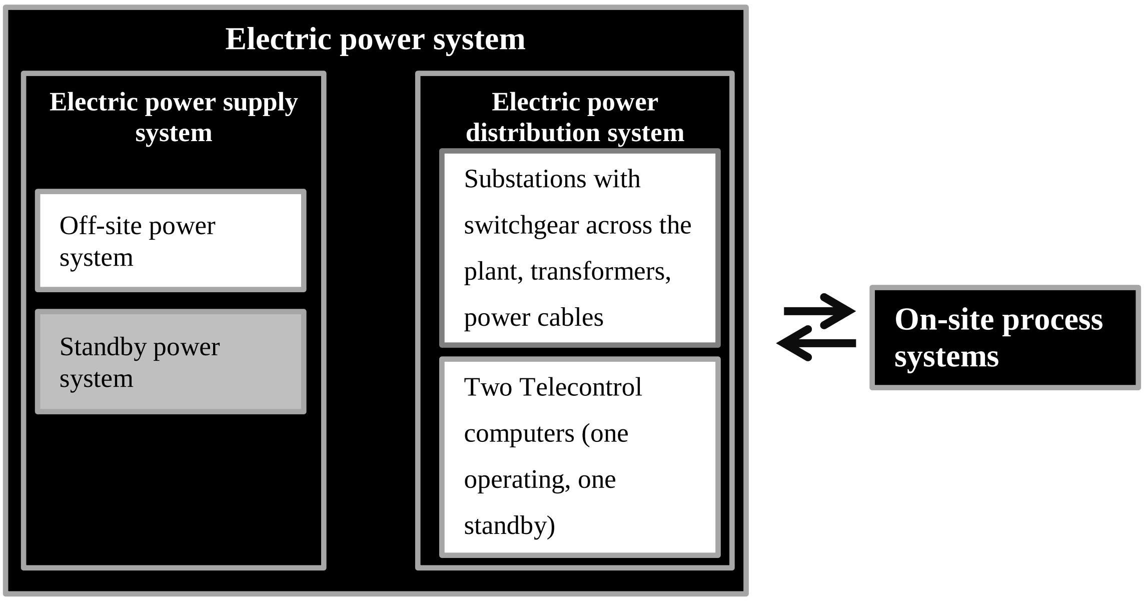

Electric power system
Electric power supply system
Off-site power system
Standby power system
Electric power distribution system
Substations with switchgear across the plant, transformers, power cables
Two Telecontrol computers (one operating, one standby)
On-site process systems

Figure 5-1: Key components of the electric power system supporting the plant

The primary means of supplying alternating current (AC) power to the plant is the national grid (off-site power system). In addition, the plant is equipped with diverse backups:

- four 2 Megawatts (MW) diesel alternator (DA) sets
- one 3.5MW gas turbine (GT1) set
- one 5MW gas turbine (GT2) set

These items constitute the standby power system. If the off-site power system fails, the standby power system can be used to supply power to the on-site process systems. The power is distributed via the distribution system that consists of a number of substations with switchgear, transformers and power cables across the plant and is controlled via the Telecontrol computer.

Standby power system

Figure 5-2 below shows the key components of the standby power system. The DA/GT sets can be controlled either via the local control panels or the load management system. Manual operation of sets via local control panels is difficult and thus the PRISMIC system was developed. It monitors the parameters of the DA/GT sets and sends commands to the local panels, replicating the operator input. There are two systems, A and B, one of which can be selected to control the DA/GT sets.

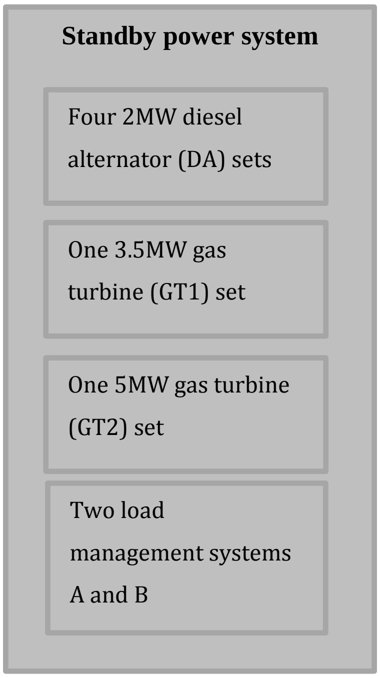

Standby power system
Four 2MW diesel alternator (DA) sets
One 3.5MW gas turbine (GT1) set
One 5MW gas turbine (GT2) set
Two load management systems A and B

Figure 5-2: Key components of the standby power system

DA/GT set failure modes

The required function of the DA/GT sets is to start, load and run for a required time. Thus, the DA/GT set failure modes can be divided into (USNRC, 2007):

- Failure to start
- Failure to load and run for a required time after a successful start

DA/GT set maintenance

In order to ensure that the DA/GT sets will start, load and run when required and to eliminate problems related to underutilisation, they are tested and preventively maintained regularly.

The procedures require that each DA/GT set should be tested fortnightly. DA1 and DA3 should be tested one week with DA2 and DA4 tested the next week.

Preventive maintenance of DA/GT sets can be divided into scheduled maintenance and condition based maintenance that is carried out according to the needs indicated by condition monitoring. There are different types of scheduled maintenance. Plant personnel distinguished 6-monthly, 12-monthly, 24-monthly and 96-monthly maintenance activities of DA sets and 4-monthly and 12-monthly maintenance of GT sets. In addition, when DA/GT sets fail, they are taken for corrective maintenance (CM). Appendix C provides more details on the DA/GT set maintenance process. It presents process flow diagrams with the key actions, decision situations and delays that are part of the maintenance process. These diagrams were used to facilitate the discussions with the plant personnel and informed the development of the model.

DA/GT set states

When DA/GT sets fail, are repaired or taken down for preventive maintenance, they move from one state to another. At any time, a DA/GT set can be in either a standby state or a down state.

A *DA/GT set is in the standby state* when it is able to start, load and run for a required time.

A *DA/GT set is in the down state* when it has a latent or known fault that would prevent it from starting and running when required by the operator or it is disabled for preventive maintenance. Thus, the following types of down states have been defined:

- *Down state due to latent fault*
- *Down state due to corrective maintenance*
- *Down state due to scheduled maintenance*
- *Down state due to condition based maintenance*

Engineers at the plant are in the course of introducing the DA/GT set condition monitoring process. At the moment, some data related to the performance of DA/GT sets is being collected by the staff on a daily basis and preventive actions are carried out if needed. Basically, the technicians are supposed to monitor some of the DA/GT set parameters (e.g. the level of oil) and if they observe any changes (e.g. the oil level is low), they should take an appropriate action (e.g. increase the oil level). Thus, the condition monitoring and condition based maintenance do not affect the availability of DA/GT sets significantly and will not be analysed. In the rest of this chapter the term preventive maintenance (PM) will be used to refer to scheduled maintenance and just three types of down states will be distinguished:

- *Down state due to latent fault*
- *Down state due to corrective maintenance*
- *Down state due to preventive maintenance*

Standby power system capacity

Standby power system capacity is the maximum electric output that can be produced by the standby power system. A precise definition is provided below:

Standby power system capacity = capacity of the DA and GT sets in the standby state = maximum standby power system capacity (16.5MW) - capacity of the DA and GT sets in the down state

Required level of the standby power system capacity

The requirements related to the AC power supply for the plant are stated in the Safety Case for the plant. The Safety Case identifies the load that needs to be supplied within 2 hours from the off-site power system failure. It is currently equal to 7.2 Megawatts (MW). The load can be successfully supplied if the following combinations of alternators are available for service:

- four DA sets (8MW), or
- two DA sets and one GT set (7.5MW or 9MW), or
- one DA set and two GT sets (10.5MW) as both GT sets need power from a DA set to start, or
- two GT sets (8.5MW) started by a mobile diesel alternator.

However, in the future more equipment might be classed as “essential” and the requirement for the standby power system capacity may need to be increased. A new requirement of 11MW has been suggested by the engineers at the plant. If the new requirement of 11MW is introduced, the following combinations of alternators should be available for service to successfully supply the new load:

- four DA sets and one GT set (11.5MW or 13MW)
- two DA sets and two GT sets (12.5MW)

This requires much higher availability of DA/GT sets. Overall, achieving high DA/GT set availability and high standby power system capacity is important for the plant. This requires effective control policies for the standby power system based on a good understanding of the technical, human and organisational aspects of this system.

5.3 Objectives & scope of the analysis

The objective of the analysis is to identify and analyse HOFs that contribute to the unavailability of DA/GT sets for service and reduce the capacity of the SPS. The following aspects are within the scope of the analysis:

- DA/GT set failure and maintenance processes
- actions of technicians involved in the DA/GT set maintenance activities and
- actions of management (supervisors and engineers) who oversee the DA/GT set maintenance activities

The situation when the SPS is actually used to mitigate the consequences of the off-site power system loss is out of the scope of analysis. Thus, the load management computers, their failure and maintenance processes are not included in this analysis. In addition, the analysis does not consider how the operators would behave in the emergency situation of the off-site power system failure and whether and how their behaviour could limit the ability to supply the "essential" load. However, this analysis could be extended in the future to include this.

5.4 Approach to the analysis

As discussed in Chapter 2, the objective of PRA is to answer the following questions:

1. What can happen?
2. How likely is it to happen?
3. Given that it occurs, what are the consequences?

To answer the first question, PRA identifies a sequence of discrete events and conditions, called a scenario, and PRA analysts usually use Event and Fault Trees to represent it. Event Trees use “forward logic”, i.e. analysis starts with an “initiating event” and different ways in which this event can lead to adverse effects are considered. A Fault Tree uses a “backward logic”, i.e. given a particular event (top event), for example, a failure of a system, different combinations of basic events that can lead to the top event are considered. The uncertainty associated with the occurrence of events and each scenario is quantified by probabilities or frequencies. Thus, the second question is answered by specifying the probability or frequency of each scenario occurring. Each scenario leads to an “end state”, which defines the consequences of an accident.

HOF analysis is concerned with identification and analysis of human tasks and organisational factors that contribute to different scenarios. As discussed in previous sections, the human tasks that are usually analysed as part of HOF analysis for PRA include those performed by operators and maintainers under normal operating conditions and those performed after an “initiating event” occurs. Due to reasons explained earlier in the thesis, it was decided to apply SD to the analysis of the former tasks – those which can introduce latent faults into the engineered safety systems designed to mitigate the consequences of “initiating events”. One of the important “initiating events” at the plant, considered in the former PRA for the plant, is the failure of the off-site power system. If the off-site power system fails then the SPS can be used to supply power to the on-site process systems. Thus, achieving high SPS availability and capacity over time is important to the plant.

Early discussion with the plant personnel revealed that the SPS, including its technical, human and organisational aspects, is a dynamic system that involves feedback loops, delays, discrete events and randomness. This is explained below:

- The SPS is a dynamic system that involves feedback loops. As DA/GT sets fail and are taken for corrective and preventive maintenance, the SPS capacity changes over time. The states that DA/GT sets are in (e.g. standby state or down state) and overall SPS capacity at any point in time affect the actions and decisions of technicians and management involved in the DA/GT set maintenance and oversight. In addition, the behaviour of technicians is affected by the behaviour of management and vice versa. As the aim of the analysis is to explore how the control of risk associated with the SPS could be improved, explicit modelling of feedback loops and the use of SD was required.
- The key technical part of the SPS is the set of four DAs and two GTs. When they fail, they discretely and randomly change their state from the standby state to the down state

due to latent fault. The observation of this particular change in state of DA/GT sets by technicians and managers and taking appropriate actions in response is critical to ensure the adequate level of the SPS capacity over time. Thus, it was decided that explicit modelling and simulation of these discrete changes of state was required.

- There are a number of factors affecting the DA/GT set failure and maintenance processes whose impact on the DA/GT set availability is uncertain. For example, a technician error during maintenance may lead to the DA/GT set failure. To capture the impact of these factors, conditional probabilities were employed and used to calculate the unconditional probabilities of DA/GT set failures. These unconditional probabilities were then used to simulate DA/GT set failures over time and identify the factors that significantly contribute to DA/GT set unavailability over time.

SD software packages are capable of representing continuous and discrete systems and randomness (Coyle, 1985). Thus, the entire model was described using the SD notation and implemented in the specialist SD software Stella.

5.5 Data collection

Data for the study was collected via semi-structured interviews with the plant personnel during visits to the plant, analysis of documents provided by the plant and data found in SD and PRA the literature.

Before the plant was visited, the author was provided with documents describing the SPS system, its key physical components and their maintenance requirements and how the SPS fits into the wider electric power system supporting the plant. This provided the author with the background information necessary to prepare for interviews with the plant personnel. This background information was presented in Section 5.2 of this chapter.

Overall there were four Site visits and the process of data collection to develop and quantify the model was iterative. A summary report was written after each visit and sent to the plant personnel to confirm the key information collected during the visit.

The purpose of the first Site visit was to:

- meet members of the Risk group at the plant who were the key customers of the study

- get introduced to two system engineers who had good knowledge of the electric power system supporting the Site and were selected by the project sponsor to support the researcher in on-site data collection
- familiarise with the parts of facility and equipment to be potentially analysed, e.g. gas turbines, diesel alternators, substations, Telecontrol computers etc.
- to define the scope of the analysis and agree on the next steps

The key part of the first Site visit was a meeting and discussion with the two system engineers and agreeing on the scope of the analysis (as finally defined in Section 5.3). It was agreed that a simple strategy of "divide and conquer" should be adopted and the initial analysis should focus at this stage only on one part of the electric power system over which the Site had direct control and power to influence its performance in the future. It was agreed that the study should focus on DA/GT sets and their availability for service and that the load management computers could be excluded from the analysis at this stage. It was decided that the focus of the next Site visits should be for the researcher and the system engineers to review in detail the following topics:

- the role of the SPS in general, and the role of DA/GT sets in particular and how DA/GT sets interact with other pieces of equipment
- the maintenance requirements of DA/GT sets , i.e. what maintenance tasks are performed, how often and their impact on the SPS availability for service
- other technical, human and organisational factors that may affect availability of the SPS for service

After the first visit, flow charts were created to represent the DA/GT set testing and maintenance processes and key personnel activities performed in relation to the equipment (see Appendix C). These flow charts were used during the subsequent two plant visits to support semi-structured interviews with the system engineers selected by the project sponsor to support the study. One of the engineers had been working more than 10 years at the plant. The second system engineer was less experienced and worked at the plant for less than 10 years. Both had been involved in availability management of DA/GT sets and had a good understanding of the role of DA/GT sets and their testing and maintenance requirements. The interviews were done separately with each of the engineer. Flow charts describing the DA/GT set testing and maintenance processes were presented to each of the engineers and systematically discussed to provide the researcher with a good understanding of the following topics:

- key stages of DA/GT set testing and maintenance processes & where humans are involved

- key actions and decisions of the personnel involved in testing and maintenance of DA/GT sets
- key pieces of information needed at various stages of the testing and maintenance process
- key delays involved in testing and maintenance of DA/GT sets

There were approximately four interviews with each of the engineers during the two Site visits until the researcher was clear on how testing and maintenance is performed. If there were any discrepancies between the system engineers they were discussed in the next round of interviews and clarified. Thus, the approach to the interviews was one of progressive elaboration in which flow charts were the key focus of each interview and their elements and links between them were discussed until there was an agreement between the system engineers and the researchers that the testing and maintenance of DA/GT sets are appropriately represented by the flow charts. The final flow charts were then used to structure the initial model.

The impact of technicians and wider organisational factors on DA/GT set failure and maintenance processes was also discussed during the first plant visit. However, the input provided by system engineers on these aspects was limited. Thus, the researcher and project sponsor decided that the PRA literature should be investigated to identify the generic and common human and organisational factors affecting equipment performance and availability of equipment for service. This involved literature review covering both scientific papers (from PRA and SD areas) and published HSE reports. The objective was to identify the SD structures that could be adapted and used to model factors affecting availability of the SPS. The review of the literature indicated that the studies of Mohaghegh et al. (2009), Dulac et al. (2008) and Cooke (2003, 2004) were relevant to the problem at hand and the SD structures used in these studies could be adapted for the analysis of the availability of the SPS at the process plant.

In addition, the first plant visit indicated that there was no readily available quantitative data on DA/GT set historical failures and maintenance activities and that the data would need to be collected. In principle, such data could be obtained from statistical analysis of information in the plant information systems. However, due to constraints on resources and plant access, and concerns about the applicability of the data it was decided not to take this path. Thus, it was decided by the researcher and the project sponsor to use readily available generic quantitative data on alternator failure times to quantify the model and run simulations. In addition, it was agreed that expert judgement could be used to estimate some of the parameters in the model such as maintenance times (this is explained later in this chapter).

5.6 Model development

5.6.1 Overview of the model

The model consists of three sectors presented in Figure 5-3. The arrows in Figure 5-3 show the direction of influence. The pieces of text next to the arrows represent variables that are outputs of the respective model sectors. These variables feed into the sectors to which the arrows are pointing. Sector 1 was developed based on the interviews with the plant personnel and using the flow charts (see Appendix C) validated during these interviews. Development of Sector 2 and Sector 3 of the model was informed by the PRA literature. Particularly useful was the work of Mohagdegh et al. (2009), introduced in Chapter 2. Mohagdegh and her colleagues discussed how Organisational Factors and Technical System Factors can be linked via Human Factors in a model and how SD could complement modelling approaches traditionally used in PRA. The sectors and the relationships between these sectors are explained in detail in the subsequent sections of this chapter. A short summary description of the model structure is provided below.

When DA/GT sets fail, are repaired or taken down for preventive maintenance, they move from one state to another (Sector 1). The time spent in the *down states due to preventive* and *corrective maintenance* depends on active maintenance times and logistic delays. In the period between preventive maintenance (PM) tasks and testing a fault might develop in a DA/GT set and this condition will be latent until this DA/GT set is taken down for PM or testing. The transition between the *standby state* and the *down state due to latent fault* is determined by the DA/GT set standby failure rate. This rate is influenced by the maintenance quality (Sector 2). More specifically, the rate of DA/GT set failures is a function of the *Probability of substandard maintenance* (an output of Sector 2). In addition, as DA1 and DA3 (and also DA2 and DA4) are tested simultaneously, there is the conditional probability represented by the *Beta factor* that a cause of a failure of one of the sets from the pair will be shared by the second set, given that the first one has failed.

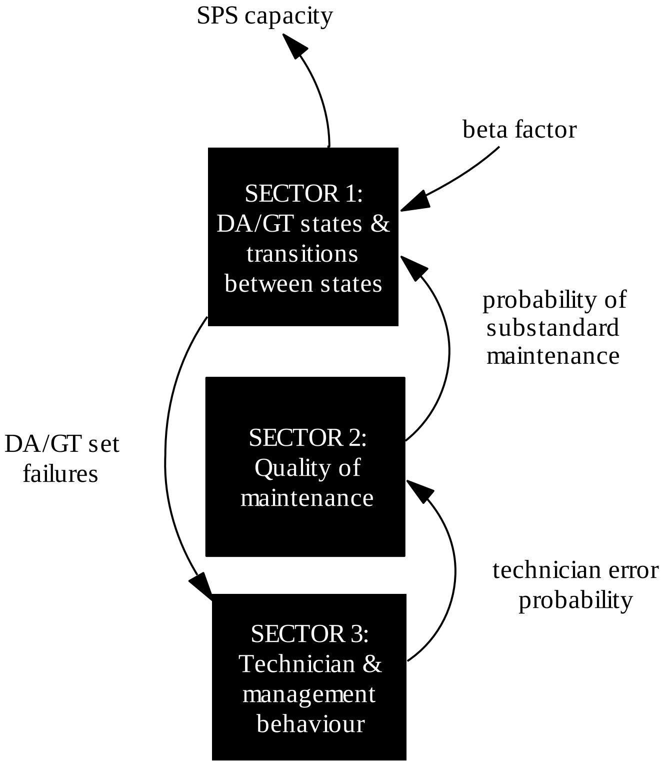

SPS capacity
beta factor
SECTOR 1: DA/GT states & transitions between states
probability of substandard maintenance
DA/GT set failures
SECTOR 2: Quality of maintenance
technician error probability
SECTOR 3: Technician & management behaviour

Figure 5-3: Model sectors

The detection of a DA/GT set failed state (output of Sector 1) acts as a control mechanism for technicians and management (supervisors and engineers) and influences their behaviour (Sector 3). This behaviour, which is characterised in the model by variables *Management commitment to safety & quality*, *Technician commitment to safety & quality* and *Technician competence*, influences the variable *Technician error probability* (an output of Sector 3). *Technician error probability* affects the *Probability of substandard maintenance* (an output of Sector 2) and the DA/GT set standby failure rate.

5.6.2 Model scope

Table 5-1 lists the key elements included (I) and excluded (E) from the final model.

Table 5-1: Key elements included & excluded from the final model

Sector of the model	Key elements of the model	I/E	Justification for inclusion/exclusion
Sector 1: DA/GT states & transitions between states	DA set 6-monthly (6M), 12M, 24M and 96M preventive maintenance (PM)	I	Affects DA set availability for service
	GT set 4M and 12M PM	I	Affects GT set availability for service
	DA/GT set failures	I	Affects DA/GT set availability for service
	DA/GT set load testing	I	Load testing is done to detect whether any of the DA/GT sets are in the down state due to latent fault
	DA/GT set load testing time	E	It takes two hours to test DA/GT sets thus there is no significant impact on the DA/GT set availability for service
	Contracting CM of DA/GT sets out to a third party	I	Increases CM time
	Availability of spare parts for PM & CM	I	Lack of parts increases CM & PM time & decreases DA/GT set availability for service
Sector 2: Quality of maintenance	Quality of PM	I	PM of poor quality can contribute to the increase in DA/GT set failures and decrease the DA/GT set availability for service
	Quality of CM	E	Much more DA/GT set PMs than CMs are carried out. Thus, quality of CM could be ignored in this study
Sector 3: Technician & management behaviour	Technician competence & commitment to safety & quality	I	Influences quality of PM
	Management commitment to safety & quality	I	Influences technician competence & commitment to safety & quality

Appendix F lists all the assumptions that were made during the model building process. Appendix G list and describes the key parameters used in the model.

5.6.3 Sector 1: DA/GT set states & transitions between states

The overview of Sector 1 of the model is presented in Figure 5-4. A high-level description of this sector is provided below.

When DA/GT sets fail, are repaired or taken down for preventive maintenance, they move from one state to another. Generally, as explained in previous sections, a DA/GT set can be in only one of four states: a *standby state*, a *down state due to preventive maintenance*, a *down state due to latent fault* and a *down state due to corrective maintenance*.

The model represents all six DA/GT sets. The DA/GT sets in various states are aggregated in corresponding stocks. The stocks are shown in Figure 5-4**.** For example, the DA/GT sets that are in the *down state due to latent fault* are aggregated in the stock *Gensets with latent faults*. This stock is measured in Megawatts (MW) and reflects the combined capacity (in MWs) of the DA/GT sets that are in the *down state due to latent fault*. Similarly, the stocks *Gensets with latent fault taken down for PM* and *Gensets with no latent fault taken down for PM* aggregate the DA/GT sets in the *down state due to preventive maintenance* (there are two types of these sets distinguished: the ones with a latent fault and the ones without a latent fault).

The stocks *Gensets with recognised faults*, *Gensets ready for CM*, *Gensets that undergo active CM*, and *Gensets waiting for parts* aggregate the DA/GT sets in the *down state due to corrective maintenance*. These four stocks reflect different stages of the corrective maintenance process.

The stock *Gensets in standby state* aggregates the DA/GT sets in the standby state. The standby power system capacity at any time is equal to the level of the stock *Gensets in standby state*, i.e. it is the sum of capacities of the sets in the standby state.

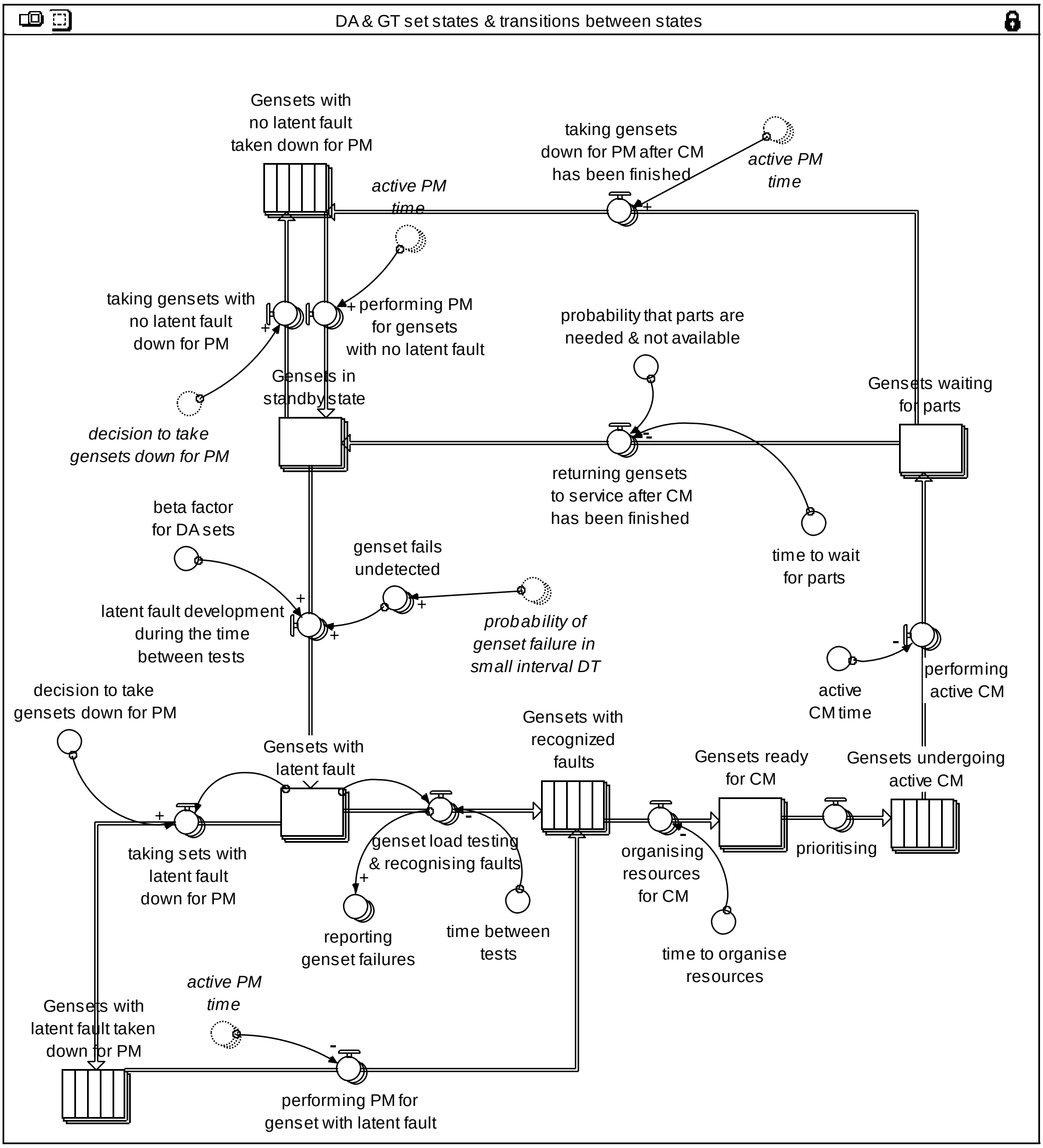

DA & GT set states & transitions between states
Gensets with no latent fault taken down for PM
active PM time
taking gensets down for PM after CM has been finished
active PM time
taking gensets with no latent fault down for PM
performing PM for gensets with no latent fault
probability that parts are needed & not available
Gensets in standby state
Gensets waiting for parts
decision to take gensets down for PM
returning gensets to service after CM has been finished
beta factor for DA sets
time to wait for parts
genset fails undetected
latent fault development during the time between tests
probability of genset failure in small interval DT
performing active CM
active CM time
decision to take gensets down for PM
Gensets with recognized faults
Gensets with latent fault
Gensets ready for CM
Gensets undergoing active CM
taking sets with latent fault down for PM
genset load testing & recognising faults
organising resources for CM
prioritising
reporting genset failures
time between tests
time to organise resources
active PM time
Gensets with latent fault taken down for PM
performing PM for genset with latent fault
+
-

Figure 5-4: Sector 1: DA/GT set states & transitions between states

Transitions (rate variables) between stocks represent DA/GT set failure processes or actions of people involved in the DA/GT set maintenance activities. For example, the *Latent fault development during the time between tests* process is modelled in the following way:

- Every small interval of time between calculations (called delta time and represented by ΔT or DT in the model) a number is sampled from a uniform distribution. If this number is smaller than the *Probability of genset failure in small interval DT*, then the set fails and has a latent fault.

– In addition, every time DA1 (DA2) fails, a number is sampled from a uniform distribution. If this number is smaller than the *Beta factor for DA sets* then DA3 (DA4) fails as well and vice versa. The beta factor accounts for common cause failures during testing for sets that are tested simultaneously (DA1 and DA3 are tested simultaneously one week and DA2 and DA4 are tested simultaneously the next week).

The failed state of DA/GT sets is detected during the next DA/GT testing or preventive maintenance. If the failed state is detected during preventive maintenance, then once preventive maintenance work is finished the set undergoes corrective maintenance.

The segments of Figure 5-4 are described in detail below.

Latent fault development process

During the time between load testing and PM activities, a latent fault can develop in a DA/GT set. When this happens, the DA/GT set "transforms" to the failed state. This failed state will not be detected until the next test or PM. The transition from the *standby state* to the latent failed state is represented in the model by the rate variable *Latent fault development during the time between tests*. It is assumed that the transition occurs at a random time with a *Probability that latent fault develops in an interval DT* that is equal to $\boldsymbol{1 - e^{-\lambda * DT}}$**.** Here an exponential time to failure reliability model is assumed. It assumes that failures occur independently of each other and at a constant rate. According to the PRA procedures guide (1983), exponential distribution is most commonly used to model time to failure in PRA studies (USNRC, 1983). "*It is used basically for two reasons: (1) many reliability studies have found the exponential justifiable on empirical grounds and (2) both the theory and the required calculations are simple. It is important to note that, even though the time to failure is not exponential over the entire life of the component, the in-use portion may be exponential. This assumes replacement by a component that is also in its exponential-behavior time period* " (USNRC, 1983, p. 5-4). There was no evidence found at the plant to contradict the use of the exponential time to failure model and thus the researcher decided to use this distribution to model the time to failure for DA/GT sets.

The factors that influence *Probability that latent fault develops in an interval DT* are shown in Figure 5-5 which is part of Sector 1 of the model.

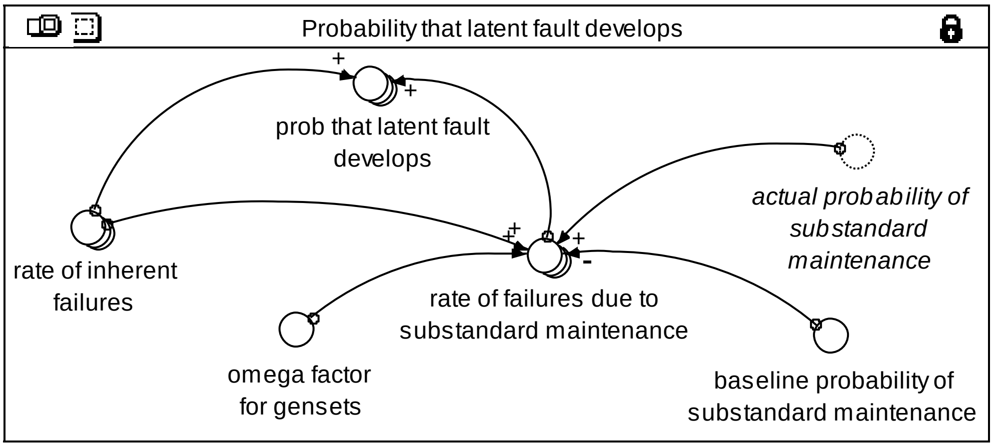

Probability that latent fault develops
prob that latent fault develops
rate of inherent failures
actual probability of substandard maintenance
rate of failures due to substandard maintenance
omega factor for gensets
baseline probability of substandard maintenance
+
+
+
+
-

Figure 5-5: Factors influencing probability that latent fault develops in a DA/GT set

If there are no undesired organisational influences then the rate λ is equal to the rate of inherent failures λ_I which is equivalent to the failure behaviour expected by the manufacturer and represents failure mechanisms that cannot be controlled by the plant. If there are some undesired organisational influences on the failure rate, then the rate λ will be bigger than λ_I. This new bigger rate can be shown to be a function of λ_I and the omega parameter (Mosleh et al., 1997). The omega factor is defined as follows:

$\omega = \frac{\lambda_{SM}}{\lambda_I}$, where λ_{SM} − rate of failures due to substandard maintenance

The rate $\lambda = \lambda_I + \lambda_{SM}$ which is equivalent to $\lambda = \lambda_I + \omega\lambda_I$

In particular, it can be shown that (Mohagdegh et al., 2009):

$$\lambda = \lambda_I + P_{ASM\_DA\_GT\_set}\ \ t\ \ * \frac{\omega_{DA\_GT\_set}}{P_{BSM\_DA\_GT\_set}} * \lambda_I$$

where:

t − time

$\omega_{DA\_GT\_set}$ – the omega factor for DA/GT sets; it can be estimated from failure databases using the following equation $\omega_{DA/GT\ set} = N_{SM}/N_I$, where N_I is the number of inherent failures for DA/GT sets and N_{SM} is the number of failures due to substandard maintenance for DA/GT sets

$P_{BSM\_DA\_GT\_set}$ − baseline probability of substandard maintenance for DA/GT sets

$P_{ASM\_DA\_GT\_set}$ − actual probability of substandard maintenance for DA/GT sets

Appendix D provides more details on how the above equation was derived. The rate of inherent failures λ_I for DA/GT sets was derived from the data provided in NUREG/CR 6928 (USNRC, 2007) report (see Appendix E).

There is a lot of uncertainty associated with the omega parameter for DA/GT sets $(\omega_{DA\_GT\ set})$. The study of maintenance databases from three British nuclear power stations (Morris et al., 1998) indicates that the ratio of failures due to substandard maintenance to inherent failures (N_{SM}/N_I) for various pieces of equipment including diesel generators could be as big as 7:1. In this study of the standby power system supporting the plant, the omega parameter for DA/GT sets is assumed to be equal to 2 $(\omega_{DA\_GT\ set} = 2)$. However, the results of sensitivity analysis using a range of values for this parameter are also provided in Section 5.8.3 of this chapter.

Sector 2 and Sector 3 of the model are used to calculate the value of the actual probability of substandard maintenance for DA/GT sets $(P_{ASM\_DA\_GT\_set})$. The baseline probability of substandard maintenance for DA/GT sets $(P_{BSM\_DA\_GT\_set})$ is assumed to be equal to the initial value of $P_{ASM\_DA\_GT\_set}$.

Corrective maintenance process

Every two weeks each DA/GT set is run to check whether it will function according to the requirements (e.g. some parameters of diesel engine performance are being recorded and analysed). In the model, the DA/GT sets that are in the stock *Gensets with latent fault* fail to start or to load and run for a required time after a successful start. When this happens, the fault is diagnosed and necessary resources need to be organised. A lognormal distribution (see Appendix G for its parameters) was established for the time to organise resources based on the interviews with the plant personnel as there was no quantitative data readily available.

If there are more than two DA/GT sets waiting for active corrective maintenance, then the DA/GT set with the highest capacity is dealt with first. This is reflected in the rate variable *Prioritising* that mimics the decision-making process. Also, it is assumed that active corrective maintenance can be carried out on only one DA/GT set at a time. If one DA/GT set is waiting for parts to be fitted then active corrective maintenance can be carried out on another DA/GT set. *Active CM time* is the time needed to carry out corrective maintenance work once the fault is diagnosed and necessary human resources and parts are available. A lognormal distribution was established for the *Active CM time* based on the interviews with the plant personnel as there was no quantitative data readily available.

If the faulty DA/GT set sub-items need to be replaced and spare parts are not in the plant, they need to be ordered. As explained by the plant personnel, the logistic delays related to the unavailability of spare parts are extremely important as a lot of DA/GT set control systems are old, i.e. if any of these pieces of equipment fail, it might take some time to find the supplier of the parts and replace them. In the model, the situation where parts are needed and not available has the probability that is equal to the variable *Probability that parts are needed & not available*. In the model, every time a latent fault develops in a DA/GT set, a number is sampled from a uniform distribution. If this number is smaller than the *Probability that parts are needed & not available*, the set needs to wait for the parts to arrive before it is returned to service. A lognormal distribution was established for the *Time to wait for parts* based on the interviews with the plant personnel.

Preventive maintenance process

In the model, DA/GT sets that are in the *standby state* or *down state due to latent fault* are taken down for preventive maintenance at the times specified by the maintenance schedule (see Appendix G). As they are being maintained, they reside in the stock *Gensets with no latent fault taken down for PM* and *Gensets with latent fault taken down for PM*, respectively. The residence time depends on the *Active PM time*. A point estimate was established for the active PM time based on the interviews with the plant personnel. This time depends on the type of PM. Appendix G details the parameters used.

In addition to the above, a DA/GT set can only be taken down for PM if it does not undergo corrective maintenance. If it does, then the active corrective maintenance needs to be finished first. Then, the DA/GT set can be taken down for PM. This decision-making process is accounted for in the model by the variable *Decision to take genset down for PM* in Figure 5-4.

5.6.4 Sector 2: Quality of maintenance

The overview of Sector 2 of the model is presented in Figure 5-6 below. This sector accounts for the factors that influence the variable *Actual probability of substandard maintenance* that was introduced in Sector 1 of the model. A description of this sector is provided below.

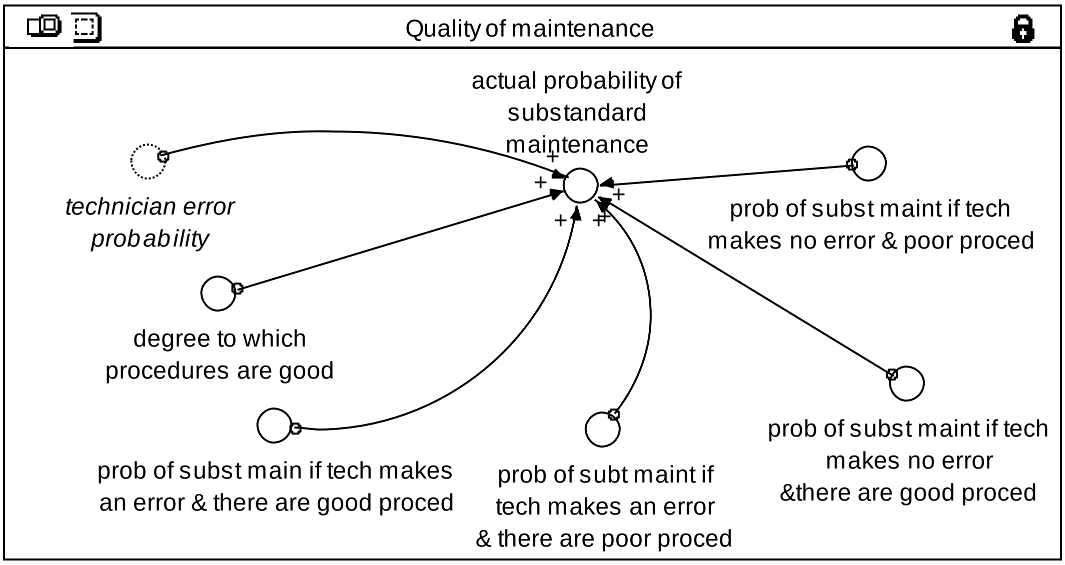

Quality of maintenance
actual probability of substandard maintenance
technician error probability
degree to which procedures are good
prob of subst main if tech makes an error & there are good proced
prob of subt maint if tech makes an error & there are poor proced
prob of subst maint if tech makes no error &there are good proced
prob of subst maint if tech makes no error & poor proced
+
+
+
+
+
+

Figure 5-6: Sector 2: Quality of maintenance

As there are many more preventive maintenance tasks done for DA/GT set than corrective maintenance tasks, the potential undesired impact of preventive maintenance is considered in the model. The preventive maintenance tasks are either of good or poor quality. The probability that preventive maintenance is of poor quality is represented by the variable *Actual probability of substandard maintenance.*

Overall, quality of maintenance can be influenced by the following factors (HSE, 2000):

– technician actions during maintenance (e.g. incorrect alignment of couplings on pipes causing overheating, bolts torqued inadequately or missing, pipelines incorrectly connected, lack of maintenance)

– quality of maintenance procedures (e.g. poor or missing procedures)

– quality of tools/equipment (e.g. tools out of specifications)

– quality of parts/materials (e.g. materials out of specifications)

Based on the analysis of the maintenance procedures, interviews with the plant personnel and literature review, technician actions and quality of procedures were selected as the main factors that influence the *Actual probability of substandard maintenance*. These factors are uncertain and were quantified in the model using probability. Each of these factors has a set of binary states, “technician error[1]”/“no technician error” and “good”/”poor”, respectively, assigned to it. A probability distribution over each of these sets represents the degree of belief as to which of

[1] The term “error” is defined as a deviation from a procedure and/or incorrect use of resources and tools. This definition does not cover errors due to missing/poor procedures. This is covered by the factor “*quality of procedures*”.

these two states is the true state of the factor. The probability distributions are presented in Table 5-2, Table 5-3 and Table 5-4.

Table 5-2: Probability distribution over the set of states associated with technician actions

The probability of	
Technician error	**No technician error**
P_{TE}	**P_{NTE} =1- P_{TE}**

Table 5-3: Probability distribution over the set of states associated with quality of procedures.

The probability that **quality of procedures** is	
Good	**Poor**
P_{PG}	**P_{PP} = 1- P_{PG}**

Table 5-4: Probability distribution over the set of states associated with maintenance quality.

If **technician** made	If **quality of procedures is**	Then the conditional probability of	
		Substandard maintenance is	**Good maintenance is**
Error	**Good**	**P_{TE_PG}**	**1- P_{TE_PG}**
Error	**Poor**	**P_{TE_PP}**	**1- P_{TE_PP}**
No error	**Good**	**P_{NTE_PG}**	**1- P_{NTE_PP}**
No error	**Poor**	**P_{NTE_PP}**	**1- P_{NTE_PP}**

Thus, the unconditional *Actual probability of substandard maintenance* is calculated as follows:

$$\begin{gathered} P_{ASM\_DA\_GT\_set} = P_{TE} * P_{PG} * P_{TE\_PG} \\ + P_{TE} * (1 - P_{PG}) * P_{TE\_PP} \\ + (1 - P_{TE}) * P_{PG} * P_{NTE\_PG} \\ +(1 - P_{TE}) * (1 - P_{G}) * P_{NTE\_PP} \end{gathered}$$

5.6.5 Sector 3: Technician & management behaviour over time

The overview of Sector 3 of the model is presented in Figure 5-7. This section of the model accounts for the factors that influence the variable *Technician error probability* that was introduced in the previous section of this chapter. This sector is divided into four modules which are described below.

Probability of technician error

The variables that affect the *Technician error probability* were developed based on the generic AMO (ability, motivation, opportunity) model (Boxall and Purcell, 2003) of factors influencing human performance found in the literature (Mohaghegh et al., 2009). These variables are presented in Figure 5-7 and are described below:

Technician competence (ability) is a capacity to carry out DA/GT set maintenance activities adequately and is a combination of knowledge of procedures, skills and experience.

Time pressure (opportunity) relates to the available time to carry out the DA/GT set maintenance tasks; high time pressure means that there is less time to perform DA/GT set preventive maintenance tasks, e.g. because other urgent tasks need to be completed.

Technician commitment to safety & quality (motivation) is a willingness to perform the preventive maintenance tasks according to the standards specified in the relevant procedures.

The approach taken to model these factors is based on the model developed by Mohaghegh et al. (2009). Mohaghegh and her colleagues developed their model using the SD structures developed by Cooke (2003, 2004) who used SD to analyse the factors that contributed to the Westray mine disaster. He based his model on the generic SD structures presented by Sterman (2000). These structures present the generic feedback mechanisms that drive the behaviour of groups of people observed in a wide range of systems.

Following Mohaghegh et al. (2009) the effect of *Technician competence*, *Time pressure* and *Technician commitment to safety & quality* on the *Technician error probability* was incorporated into the model using the NARA approach (Kirwan et al., 2004, 2005). This approach is often used by HRA practitioners to account for the impact of various performance shaping factors on human error probability. The NARA approach was introduced in Chapter 2.

The word “relative” used in Figure 5-7 means that technician competence and technician commitment to safety & quality variables are normalised to their reference values. These reference values represent the desired values required by safety or other standards.

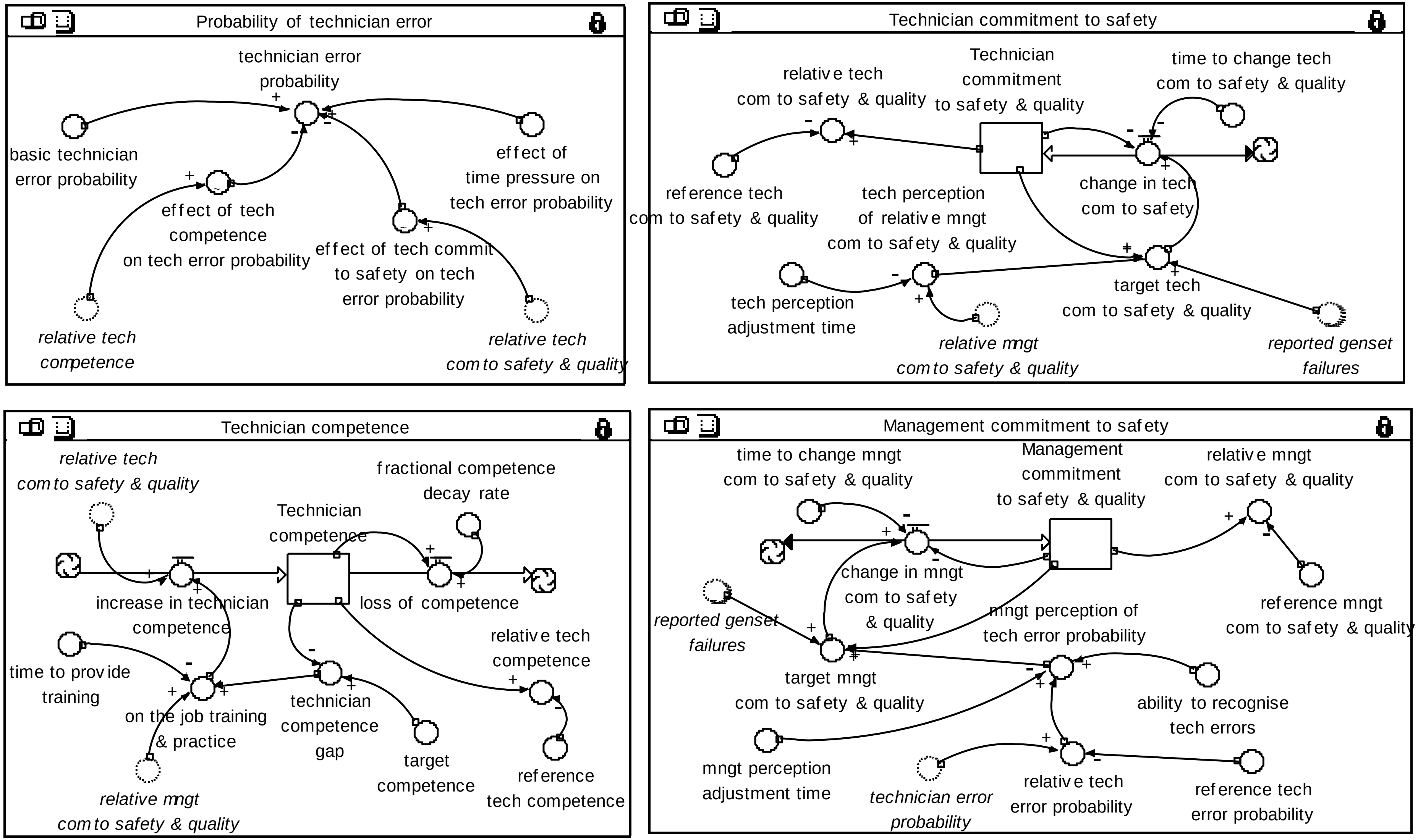

Probability of technician error
technician error probability
basic technician error probability
effect of time pressure on tech error probability
effect of tech competence on tech error probability
effect of tech commit to safety on tech error probability
relative tech competence
relative tech com to safety & quality
Technician commitment to safety
relative tech com to safety & quality
Technician commitment to safety & quality
time to change tech com to safety & quality
reference tech com to safety & quality
tech perception of relative mngt com to safety & quality
change in tech com to safety
tech perception adjustment time
target tech com to safety & quality
relative mngt com to safety & quality
reported genset failures
Technician competence
relative tech com to safety & quality
fractional competence decay rate
Technician competence
increase in technician competence
loss of competence
relative tech competence
time to provide training
on the job training & practice
technician competence gap
target competence
reference tech competence
relative mngt com to safety & quality
Management commitment to safety
time to change mngt com to safety & quality
Management commitment to safety & quality
relative mngt com to safety & quality
change in mngt com to safety & quality
reported genset failures
mngt perception of tech error probability
reference mngt com to safety & quality
target mngt com to safety & quality
ability to recognise tech errors
mngt perception adjustment time
technician error probability
relative tech error probability
reference tech error probability

Figure 5-7: Sector 3: Drivers of change in technician behaviour

For simplification, it is assumed that the effect of *Time pressure* on *Technician error probability* is constant and reduced to its minimum value. In other words, it is assumed that technicians have the sufficient amount of time to perform DA/GT set preventive maintenance tasks. The factors that drive *Technician commitment to safety & quality* and *Technician competence* are described in the sections that follow.

Technician & management commitment to safety & quality

Technician commitment to safety & quality (willingness to perform the preventive maintenance tasks according to the standards specified in the relevant procedures) is a dimensionless variable. It is represented by the stock in Figure 5-7 and measured on a scale of 0 to 1. *Technician commitment to safety & quality* gradually adjusts to the *Target technician commitment to safety & quality* and the *Time to change technician commitment to safety & quality* determines the speed of this process. *Target technician commitment to safety & quality* is the commitment to safety perceived by technicians as adequate at a particular point in time. It is a function of *Technician perception of relative management commitment to safety & quality* and *Reported genset failures.* These variables are described below.

The variable *Management commitment to safety & quality* represents the attitude of managers towards safety and quality that is visible through promoting and engaging in safety enhancing initiatives, e.g. safety briefings, safety tours, staff training (Human Engineering, 2005) and ensuring that maintenance is performed to the highest standard.

As technicians observe and engage in these safety initiatives they gradually update their beliefs about the required or adequate level of commitment to safety and quality at any time (*Target technician commitment to safety & quality*) and adjust their current level of commitment to safety. This is reflected in the degree to which the preventive maintenance tasks are performed according to the standards specified in the relevant procedures.

With regards to the *Reported genset failures*, it is assumed (optimistically) that experiencing a DA/GT set failure works as a control mechanism for *Technician commitment to safety & quality*. Every time a DA/GT set failure is experienced by technicians and is reported to management, the *Technician commitment to safety & quality* increases rapidly to its reference value level as technicians attempt to minimise the risk of future DA/GT set failures due to substandard maintenance. It is also assumed that the *Reported DA/GT set failures* work as a control mechanism for management by forcing them to investigate the cause of the failure and take an active interest in the issues related to DA/GT set operation and maintenance in an attempt to prevent future DA/GT set failures. This influence is shown in the module *Management commitment to safety & quality* in Figure 5-7.

Management commitment to safety & quality is also influenced by the *Technician error probability as perceived by Management,* which depends on management's ability to recognise that technicians do not perform DA/GT set preventive maintenance according to the standards expressed in the relevant procedures. This could be recognised by closely monitoring the state of technician competence or by assessing technician attitudes towards safety and quality. If this is not possible or difficult, other indicators can be used as well, e.g. frequency of maintenance revisits due to maintenance errors (including those identified during post maintenance testing), frequency of "wrong parts used", frequency of the use of incorrect tools etc. (HSE, 2000).

The effect of *Technician error probability as perceived by Management* on *Target management commitment to safety* is modelled using the learning curve model. Learning curve theory provides models that link aspects such productivity, quality and cost with experience with a particular process (see, for example, Wright, 1936; Yelle, 1979; Teplitz, 1991). Here, following Cooke (2003, 2004), it will be assumed that the target commitment to safety will change by a given percentage with each doubling of the *Technician error probability as perceived by Management.*

Technician competence

As mentioned earlier, technician competence is a combination of technician knowledge of procedures, skills and experience and is approximated in the model by the number of days of relevant on-the-job training and practice. When technician competence is below the *Target competence* level, technicians receive additional training and an opportunity to consolidate their knowledge and skills through practice. The training is delivered with a delay that is related to finding the appropriate time and resources to deliver the training and increase the competence level.

The amount of training provided will be affected by the *Management commitment to safety & quality* and whether the management will be willing to support training activities at a cost of technicians not performing some other important activities. Also, if *Technician commitment to safety & quality* is low, the effective competence gained during training will be lower. In addition, it is assumed that technician competence decays exponentially at a constant fractional decay rate as technicians require refresher training.

It is assumed that the initial value of technician competence is 10 weeks that is 70 days, the same as the *Reference technician competence*. Also, it is assumed that the objective of management is to train technicians to the *Target competence* level that is equal to the *Reference technician competence*.[2]

5.6.6 Model validation

The key issues related to the development of the SD model within the PRA framework are summarised below:

– As opposed to the models developed to support HOF analysis for AA, presented in the previous chapter, the model developed to support HOF analysis for PRA was quantitative. This required quantification of soft variables such as commitment to safety or level of experience. These soft variables were handled by using dimensionless variables and these variables and the relationships between them were based on the generic models already existing in the literature. However, it needs to be remembered that the SD structures proposed in the literature are usually used to support strategic use of SD, in which SD is used to examine trends in key variables rather than to provide precise predictions for the future. That is why the model presented in this chapter was used in an experimentation mode rather than to provide estimates of the risk. This was related to large uncertainty associated with the impact of HOFs. Thus, the model was used as a vehicle to investigate the relative importance of various structures and identification of areas to which the model output was sensitive. This enabled identification of a potentially important parameter (i.e. the omega parameter, see next sections) on which more data needs to be collected and which needs to be carefully estimated.

– Various types of data can be used to develop SD models. In the study presented in this chapter, plant specific and generic data were used to create and quantify the SD model. Data was elicited from the documents provided by the company, from plant personnel and PRA and SD literature. The model created in this way was still of use as it pointed to

[2] Assuming that there are five maintenance teams, each team works around 1/5 of the year, i.e. around 10 weeks per year. To simplify, it was assumed (following Sterman, 2000), that each team and technician in each team receives 1 week of training and practice per week worked. Thus, each technician receives 10 weeks of training and practice each year. This value was used to represent the *reference technician competence* and it was assumed that management wants to provide technicians with this level of training and practice every year.

structures that can have significant impact on the SPS capacity and indicated areas of the plant on which future data collection effort could focus.

There were different users of the model:

- the Risk group at the plant who sponsored the project
- two system engineers who actively supported the development of the model
- researcher

To ensure users' confidence in the model a number of steps were taken. This is discussed below. To ensure researcher's confidence in the model, a number of tests were performed. The testing process is described below using the framework developed by Sargent's (2013) that is useful when one develops simulation models. It comes from the Discrete Event Simulation literature, but it applies to any simulation models, including SD models (Pidd, 2009). The framework is depicted in Figure 5-8.

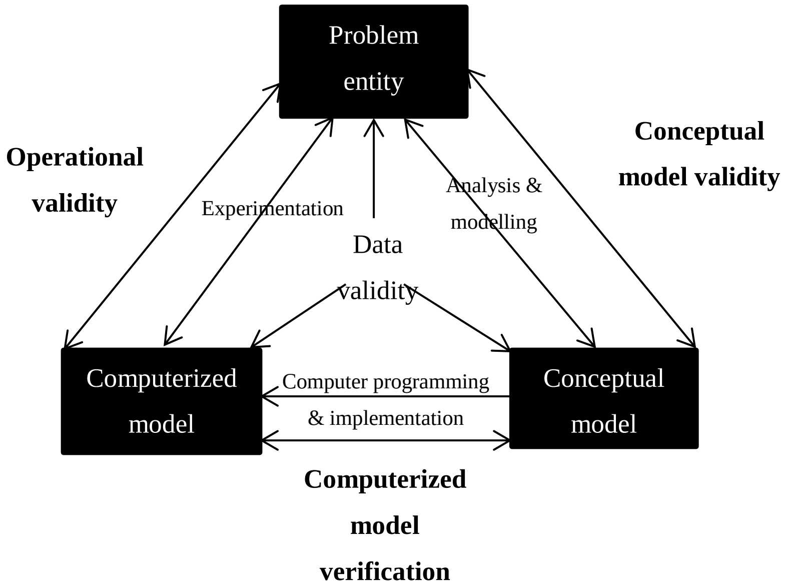


Figure 5-8: Model verification and validation process

Conceptual model validity

The model was created based on semi-structured interviews with the plant personnel, analysis of documents provided by the plant and information found in the PRA and SD literature. The key model structures and assumptions were discussed and validated by the plant personnel to ensure that they adequately represent the system analysed. There were approximately four interviews with each of the engineers during the two Site visits until the researcher was clear on how testing and maintenance is performed. If there were any discrepancies between the system engineers they were discussed in the next round of interviews and clarified. Thus, the approach to the interviews was one of progressive elaboration in which flow charts were the key focus of each interview and their elements and links between them were discussed until there was an agreement between the system engineers and the researcher that the testing and maintenance of DA/GT sets are appropriately represented by the flow charts. The final flow charts were then used to structure the initial model.

Data validity

The values of some of the model parameters were elicited from the plant personnel. However, a lot of the model variables were quantified using the generic data found in the literature as discussed earlier in this chapter. The parameters used within the model and the data sources used to estimate their values are presented in Table 5-5.

Table 5-5: Parameters in the model and data sources used to estimate them

Data source	Parameter
Values found in the documents provided by the plant	– *DA/GT set capacity* – *Time between tests* – *PM schedule*
Values estimated using generic data found in the PRA literature	– *Rate of inherent failures* (USNRC, 2007) – *Omega factor* (Morris et al., 1998) – *Beta factor* (USNRC, 2010)
Values estimated using generic data found in the SD literature (Cooke, 2003; 2004; Mohaghegh et al., 2009)	– *Reference technician commitment to safety & quality* – *Initial/Maximum/Minimum technician commitment to safety & quality* – *Time to change technician commitment to safety & quality* – *Technician perception adjustment time* – *Reference technician competence* – *Target technician competence* – *Fractional competence decay rate* – *Time to provide training* – *Reference management commitment to safety & quality* – *Management learning exponent* – *Time to change management commitment to safety & quality* – *Initial/Maximum/Minimum management commitment to safety* – *Basic technician error probability* – *Maximum effect of technician lack of competence on technician error probability* – *Maximum effect of low technician commitment to safety on technician*

Data source	Parameter
	error probability – *Maximum effect of time pressure on technician error probability* – *Reference technician error probability* – *Effect of time pressure on technician error probability* – *Effect of relative technician commitment to safety & quality on technician error probability* – *Effect of technician competence on technician error probability* – *Technician error probability*
Values elicited from plant personnel	– *Active PM time* – *Active CM time* – *Time to organise resources* – *Time to wait for parts* – *Probability that parts are not available* – *Ability to recognise technician errors* – *Testing dates* – *Probability of substandard maintenance if technician makes an error and quality of procedures is "good"* – *Probability of substandard maintenance if technician makes an error and quality of procedures is "poor"* – *Probability of substandard maintenance if technician doesn't make an error and quality of procedures is "good"* – *Probability of substandard maintenance if technician doesn't make an error and quality of procedures is "poor* – *Degree to which quality of procedures can be described as "good"*

While eliciting the expert judgement an informal process was used. The experts were recruited from the engineers involved in the operation and maintenance of the standby power system. They were asked the following questions:

- What is the most likely value of this parameter?
- What value of this parameter would surprise you? What value of this parameter would you consider to be highly unlikely?

The answers to the first question were used in the initial model. The answers to the second questions were used for sensitivity analysis where applicable. The experts were inquired separately and when there were any differences in views, simply the more pessimistic view was taken into account. The key purpose of this data elicitation was to gain data to populate the initial model and then perform sensitivity analysis to identify the variables with the highest impact on the model output to be investigated in more detail in the future.

In the future, plant specific data could be collected and used to quantify the model to better represent the conditions at the plant. The focus should be on quantifying those model parameters to which the model output is sensitive. Examples of these parameters are discussed in Section 5.8.3.

Computerised model verification

The following key tests were executed to ensure that the model was correctly implemented in Stella (Sterman, 2000):

- Each model equation was inspected individually to ensure that it is adequately formulated, that the units of measure are specified for each variable and to check for consistency.
- An extreme condition test was performed to verify whether the model is robust in extreme conditions (e.g. the situation when all sets transform into the failed state at the same time was investigated and the model behaved as expected) to ensure that the equations were properly formulated.

Operational validity

The following tests were executed to verify whether the model is suitable for the purpose at hand (Sterman, 2000):

- The fixed value tests that involve checking model results against easily calculated values were performed to verify whether the model output is reasonable.
- A sensitivity analysis was conducted because a number of assumptions were made about the model structure and the parameter values.

To ensure system engineers' and the Risk group's confidence in the model, the following was done:

- The purpose and scope of the model was discussed and aligned with the project sponsor. Also, it was agreed that two system engineers will be involved in the study to support the researcher in the development of the model. Finally, it was aligned that if quantitative data is not available, expert judgement or generic data can be used to quantify the model.
- The researcher created flow chart to represent the testing and maintenance process and validated these charts with the engineers. The flow charts were the key focus of interviews with engineers and their elements and links between them were discussed until there was an agreement between the system engineers and the researcher that the

testing and maintenance of DA/GT sets are appropriately represented by the flow charts. The final flow charts were then used to structure the initial model.

– After each Site visit, a report summarising the researcher’s understanding of the key conclusions from the visit was sent to the Risk group and two system engineers and they were actively encouraged to comment upon it. Their comments were then discussed during the next Site visit.

5.6.7 Model limitations

A number of assumptions related to DA/GT set maintenance processes were made during the model building process. These assumptions should be taken into account while interpreting the model results. These assumptions could be relaxed if necessary and the model modified accordingly. Overall, the quantitative results of the simulation runs should be interpreted with caution and not treated as a true representation of the actual unavailability of the SPS. The key assumptions and limitations of the model are listed below:

– For simplification, it was assumed that technicians always have enough time, i.e. as specified in the relevant procedures, to perform preventive maintenance tasks.

– The variable *Management commitment to safety & quality* influences only the variables *Technician commitment to safety & quality* and *Technician competence.* However, it is believed that this variable affects many more aspects of the system, e.g. probability that parts are not available when needed. This issue could be investigated further, the model boundary extended accordingly and sensitivity of the model output to this new structure investigated. If this variable proves to be an important factor, it can be considered while designing the effective control policies for the SPS.

– The values of some of the model parameters were elicited from the plant personnel. However, most of the model variables were quantified using the generic data found in the literature. In the future, the plant specific data could be collected and used to quantify the model to better represent the conditions at the plant.

5.7 Qualitative analysis

The variables mentioned in the previous section of this chapter are embedded in a structure of interacting balancing and reinforcing feedback loops. Analysis of these loops can in itself improve the understanding of the operation of the SPS over time. The simplified model with the key feedback loops highlighted is presented in Figure 5-9.

The key take-away points from Figure 5-9 are summarised below:

- The variable *Technician commitment to safety & quality* and the variable *Technician competence* affect the variable *Technician error probability*. The variable *Technician error probability as perceived by management* affects *Management commitment to safety & quality* which, in turn, affects *Technician competence* and therefore *Technician error probability* (loop *B1*). *Management commitment to safety & quality* also affects *Technician commitment to safety & quality* which affects *Technician error probability* directly (loop *B2*) and via *Technician competence* (loop *B3*). These loops control the level of *Technician error probability* that affects the quality of DA/GT set maintenance and *Latent fault development during the time between tests*. The strength of the impact of *Technician error probability* on the SPS capacity over time can be tested by running simulations. This will be discussed in the next section. Overall, the loops *B1, B2* and *B3* represent one mechanism by which the plant can control availability of DA/GT sets for service. Improved technician competence or technician commitment to safety and quality means improved maintenance quality, a smaller number of DA/GT set failures due to substandard maintenance, increased DA/GT set availability for service and improved SPS capacity. The plant management may consider how to assess and measure the current levels of technician competence and technician commitment to safety and quality. Also, the plant may consider the introduction of indicators that could inform management of high levels of technician errors during maintenance. For example, the frequency of maintenance revisits due to maintenance errors (including those identified during post maintenance testing), frequency of "wrong parts used", frequency of the use of incorrect tools etc. (HSE, 2000) could be measured and monitored. High levels of these indicators would warn the plant management of poor maintenance practices existing at the plant.
- The level of *Technician competence* is controlled within the loop *B4*. When *Technician competence* is below the *Target competence* level, technicians receive additional training and opportunities to consolidate their knowledge and skills through practice. The training is delivered with a delay that is related to finding the appropriate time and resources to deliver the training and embedded within the variable *Time to provide training*. The longer the *Time to provide training*, the slower the rate at which *Technician competence* will increase and the longer the time needed to bring *Technician competence* to the target level. The plant management may consider how to reduce *Time to provide training* and increase the rate at which *Technician competence* increases over time.

- *Management commitment to safety & quality* is influenced by *Technician error probability as perceived by management*. This perception is related to the management’s ability to recognise that technicians do not perform DA/GT maintenance according to the standards expressed in the relevant procedures. The variable *Ability to recognise technician errors* is the common part of the three control loops mentioned above: *B1*, *B2* and *B3*. It might be important, because its value can potentially determine the strength of all three loops controlling the performance of technicians represented by the variable *Technician error probability*. In addition, the delays such as those embedded within variables *Time to provide training, Management (Technician) perception adjustment time, Time to change management (technician) commitment to safety & quality* can affect the effectiveness of these control loops.
- Two reinforcing loops: *R1* and *R2* are responsible for the change in *Management commitment to safety & quality* and *Technician commitment to safety & quality* over time, respectively. These loops can act as “virtuous circles” leading to the increase in *Management commitment to safety & quality* and *Technician commitment to safety & quality* over time or “vicious circles” leading to the decline in the values of these variables over time. If the latter is the case, strategies need to be developed to break the “vicious” loops or change them into “virtuous” loops. For example, safety campaigns could be carried out to regularly remind technicians and engineers of the importance of good work practices.
- Loops *B5* and *B6* represent the controlling effect of reported DA/GT set failures. It is assumed (optimistically) that an increase in *Reported genset failures* leads to a discrete jump in the value of *Target technician commitment to safety & quality* and *Target management commitment to safety & quality.* An increase in *Target technician commitment to safety & quality* leads to a decrease in the value of *Technician error probability* and *Probability of genset failure in small interval DT* (loop B5). Similarly, an increase in *Target management commitment to safety & quality* decreases *Probability of genset failure in small interval DT* both through increasing *Technician commitment to safety & quality* (loop B6) and increasing *Technician competence*. The variable *Reported genset failures* is the common part of the three control loops mentioned above: *B4*, *B5* and *B6*. It is important, because its value could potentially determine the strength of all three loops controlling the performance of technicians represented by the variable *Technician error probability*. One of the possible implications is that the plant personnel might want to ensure that all genset failures are appropriately reported. When they are reported, they can be investigated and learning will occur. If the failures are not reported,

this may lead to complacency of the staff directly involved in the DA/GT set maintenance, a decrease in commitment to safety, an increase in the *Technician error probability* and finally an increase in DA/GT set failures.

Overall, qualitative analysis, like the one presented above, can provide important insights about the system. However, as Oliva and Homer (2001) point out, *"simulation models are formally testable, making it possible to draw behavioral and policy inferences reliably through simulation in a way that is rarely possible with maps alone. Even in those cases in which the uncertainties are too great to reach firm conclusions from a model, simulation can provide value by indicating which pieces of information would be required in order to make firm conclusions possible. Though qualitative mapping is useful for describing a problem situation and its possible causes and solutions, the added value of simulation modeling suggests that it should be used for dynamic analysis whenever the stakes are significant and time and budget permit"* (p.347). Thus, it was decided to quantify the model and perform quantitative analysis which is discussed in the next section. The sensitivity analysis was performed to indicate the model parameters and structures to which the model output is very sensitive. The insights gained could be used to focus the efforts to collect the plant specific data in the future.

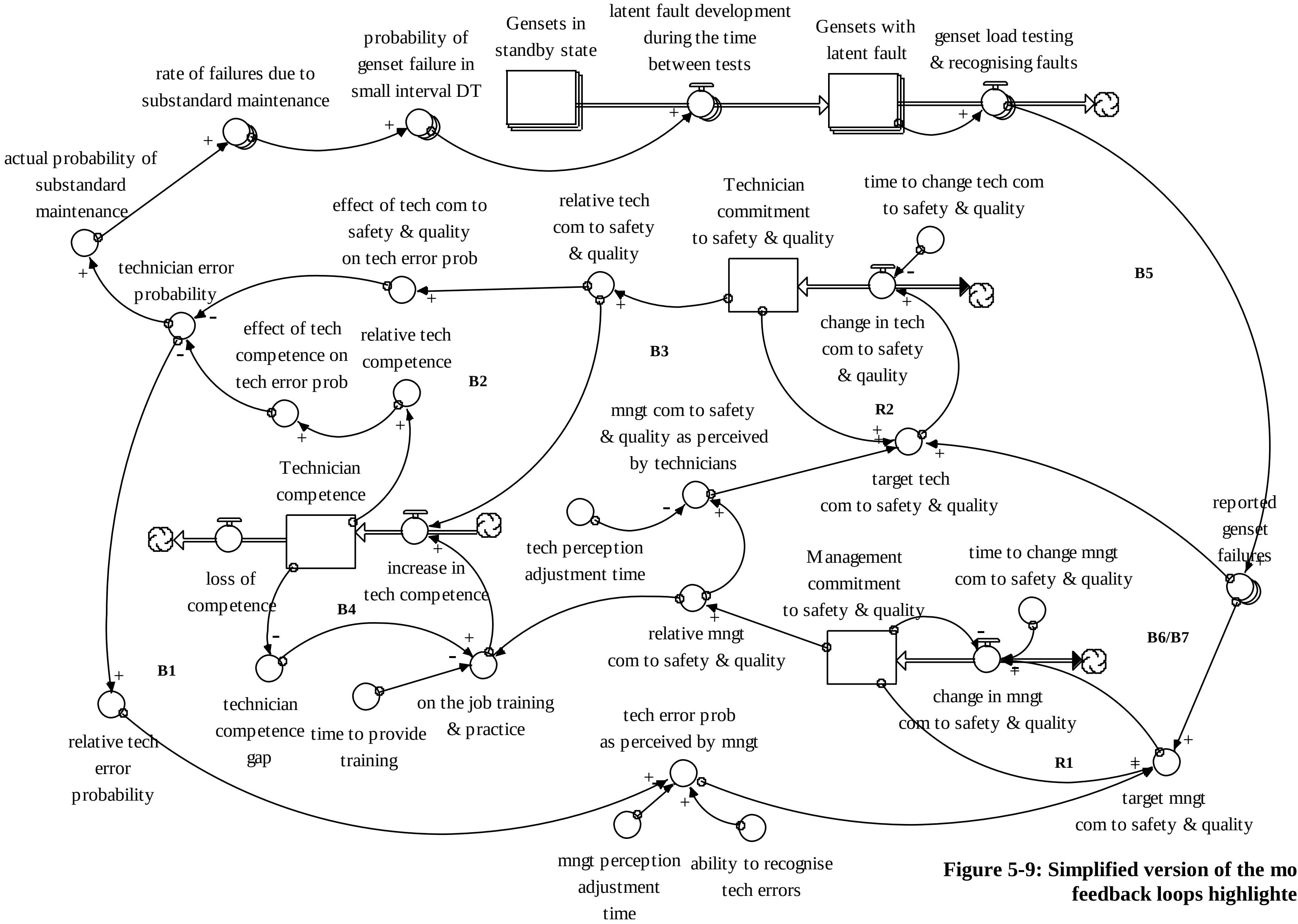

rate of failures due to substandard maintenance
probability of genset failure in small interval DT
Gensets in standby state
latent fault development during the time between tests
Gensets with latent fault
genset load testing & recognising faults
actual probability of substandard maintenance
effect of tech com to safety & quality on tech error prob
relative tech com to safety & quality
Technician commitment to safety & quality
time to change tech com to safety & quality
technician error probability
effect of tech competence on tech error prob
relative tech competence
change in tech com to safety & qaulity
B5
B3
B2
R2
mngt com to safety & quality as perceived by technicians
target tech com to safety & quality
Technician competence
reported genset failures
tech perception adjustment time
loss of competence
increase in tech competence
Management commitment to safety & quality
time to change mngt com to safety & quality
B4
relative mngt com to safety & quality
B6/B7
B1
technician competence gap
time to provide training
on the job training & practice
change in mngt com to safety & quality
tech error prob as perceived by mngt
R1
relative tech error probability
target mngt com to safety & quality
mngt perception adjustment time
ability to recognise tech errors

Figure 5-9: Simplified version of the model with the key feedback loops highlighted

5.8 Quantitative analysis

The model described in the previous sections was implemented in the specialist software (Stella) and used to simulate the SPS capacity over time.

Overall, there are two key areas that can affect the SPS capacity: 1) the frequency of DA/GT set failures and 2) the time it takes to recognise the failed state of a DA/GT set and bring it back to the *standby state*.

As described in the previous sections, the frequency of DA/GT set failures is affected by the quality of DA/GT maintenance. Quality of procedures and technician errors during maintenance are the key factors that may affect the quality of DA/GT set maintenance. In a short period of time, equipment and thus procedures used to maintain it do not change significantly and their quality remains at a constant level. Technician errors are a more volatile variable, which is affected by a number of feedback mechanisms. These mechanisms were discussed in the previous section, where the qualitative analysis was performed. It was explained how *Technician error probability* can change as a result of changes in *Technician competence,* and *Technician* and *Management commitment to safety & quality*.

The second area that may affect the SPS capacity is related to the time it takes to recognise the failed state of a DA/GT set and bring it back to the *standby state*. This time is affected by the frequency of DA/GT set testing, *CM time, PM time, Time to organise resources for CM* and *Time to wait for parts to arrive*. According to the plant personnel, the frequency of DA/GT set testing, *CM time* and *PM time* cannot be easily changed or controlled. However, some control can be exerted over the last two variables: *Time to organise resources for CM* and *Time to wait for parts to arrive.* For example, it has been a standard practice at the plant to call out a contractor to the plant every time an uncommon DA/GT set failure occurred. This practice may increase the time to bring a DA/GT set back to the *standby state* significantly. Also, it increases the maintenance costs. Thus, now the plant is considering whether to reduce the occurrence of this practice and involve only the plant personnel when a DA/GT set failure occurs. The delays related to the unavailability of spare parts are also believed by the plant personnel to be very important. Overall, if there are no parts at the plant, a long time may be spent on ordering and waiting for the parts to arrive. In addition, a lot of DA/GT set control systems are old. If any of these pieces of equipment fail, it might take some time to find the supplier of the parts and replace them. The plant may reduce *Time to wait for parts to arrive* by keeping critical parts on-site.

Thus, it was decided by the project sponsor and the researcher to investigate the extent of the impact of maintenance related failures and logistic delays, i.e. *Time to organise resources for CM* and *Time to wait for parts to arrive* on the *SPS capacity.* Three experiments were run:

- Experiment 1 - base case simulation, where "base case" represents the current standby power system set-up (as described in Section 5.6)
- Experiment 2 - impact of maintenance related failures was removed from the base case simulation model and simulation was rerun
- Experiment 3 - impact of logistic delays was removed from the base case simulation model and simulation was rerun

As the output of the simulation is stochastic, each experiment involved 1000 simulation runs[3], each simulating 728 consecutive days during which DA/GT sets are in the standby mode. This was judged by the sponsor of the project to be long enough to capture the effects of preventive and corrective maintenance strategies on the standby power system capacity. The experiments and the results of the statistical analysis of outputs from these three different simulation models are presented in Section 5.8.1 and Section 5.8.2.

As there is a lot of uncertainty associated with some of the parameters of the model, sensitivity analysis was conducted to investigate the impact of extreme values of these parameters on the conclusions reached in Section 5.8.1 and Section 5.8.2. The results of sensitivity analysis are presented in Section 5.8.3.

5.8.1 Experiment 1: Base case simulation

In order to be able to report on the impact of various factors on the SPS capacity over time, a base case simulation run is required. This base case represents the current SPS set-up as described in Section 5.6 of the report. The model was run 1000 times and each run simulated 728 consecutive days (2 years) during which DA/GT sets are in a standby mode. The summary results of the stochastic model output are presented in Table 5-6 below.

[3] Appendix H explains why it was decided to run the model 1000 times.

Table 5-6: Experiment 1 - results for the base case (overall confidence= 85%[4])

	Mean proportion of time during which SPS capacity is below the level of 7.2MW	**Mean proportion of time during which SPS capacity is below the level of 8MW**	**Mean proportion of time during which SPS capacity is below the level of 9MW**
Experiment 1 (base case)	0.011 % ± 0.004%	0.057% ± 0.010%	0.142 % ± 0.016%

The results in each column represent 95% confidence intervals for the mean proportion of time during which capacity is below the level of 7.2MW (key model output measure), 8MW and 9MW, respectively. For example, the mean proportion of time during which the SPS capacity is below the level of 7.2MW is in the interval (0.007%, 0.015%), with 95% confidence. However, the probability that all three confidence intervals contain the respective proportions is only 85%.

5.8.2 Experiments 2 & 3: Impact of logistic delays and maintenance related failures

Two experiments were conducted to investigate the impact of maintenance related failures and logistic delays on the SPS capacity. Each experiment involved running the model 1000 times and each run simulated 728 consecutive days during which DA/GT sets are in a standby mode. These two experiments are described below:

- Experiment 2 - impact of maintenance related failures was removed from the base case simulation model and simulation was rerun
- Experiment 3 - impact of logistic delays was removed from the base case simulation model and simulation was rerun

The key output of each experiment was the data on the proportion of time during which SPS capacity is below 7.2MW. The data from Experiments 2 and 3 was compared to the data from Experiment 1 (base case) using an independent samples t-test (see Appendix I Section A for

[4] Using Boneferroni adjustment or inequality: Suppose that I_s is a 100(1-α_S)percent confidence interval for the measure of performance M_s (where s = 1,2, …, k). Then the probability that all k confidence intervals simultaneously contain their respective true measures satisfies:
$P(M_s \in I_s$ for all s = 1,2, …, k) $\geq 1 - {}_{s=1}^{k} \alpha_S$ whether or not the I_s's are independent (Law & Kelton, 2000, p.542).

more details). The 95% confidence intervals for the differences between the mean proportions of time during which the SPS capacity is below 7.2MW for the experiments are presented in Table 5-7 below.

Table 5-7: Comparing Experiments 2 & 3 to Experiment 1 (overall confidence = 90%)

	95% confidence interval for the difference in mean proportion of time during which standby power system capacity is below 7.2 MW		
Comparison	**Lower**	**Upper**	**Conclusion**
Experiment 1 to 2	0.007%	0.015%	Exp.1 > Exp. 2
Experiment 1 to 3	0.001%	0.010%	Exp.1 > Exp. 3

As it can be seen in Table 5-7, removal of maintenance related failures (Experiment 2) resulted in a statistically significant decrease in the mean proportion of time during which capacity is below 7.2MW. In addition, removal of logistic delays (Experiment 3) also resulted in a statistically significant decrease in the mean proportion of time during which capacity is below 7.2MW. This means that both maintenance related failures and logistic delays statistically significantly affect the level of the SPS capacity. The extent of this impact is represented by the confidence intervals in Table 5-7, with 90% confidence.

This means that strategies could be developed in the future to, for example, decrease the occurrence of maintenance related failures. The model could be used to identify the variables or structures that have the highest impact on the occurrence of technician errors during DA/GT set maintenance. For example, the qualitative analysis presented in Section 5.7 suggested that *Ability to recognise technician errors* is important, because its value can determine the strength of three loops controlling the variable *Technician error probability*. The sensitivity of the model output measures to the changes in the value of *Ability to recognise technician errors* could be investigated. First, however, the model should be quantified with the plant specific data to better represent the conditions at the plant.

5.8.3 Sensitivity analysis

As there is a lot of uncertainty associated with some of the parameters of the model, sensitivity analysis was conducted to investigate the impact of extreme values of these parameters on the conclusions reached in Section 5.8.1 and Section 5.8.2. The results of sensitivity analysis are presented in two parts, **A** and **B**, and reported below.

Part A:

There is a lot of uncertainty associated with the omega parameter for DA/GT sets ($\boldsymbol{\omega_{DA/GT\ set}}$). It represents the ratio of the maintenance related DA/GT set failure rate to the inherent failure rate. It is believed that this single parameter has a large impact on the model output. When there is a lot of preventive maintenance and testing activities carried out, as is the case here, this parameter would be expected to be high. The study of maintenance record databases from three British nuclear power stations (Morris et al., 1998) indicates that the ratio of failures due to substandard maintenance to inherent failures (N_{SM}/N_I) for various pieces of equipment, including diesel generators, could be as big as 7:1. The base case model (used in Section 5.8.1 for Experiment 1) assumed that this ratio is equal to 2. Here, the impact of extreme values of the omega factor (7 and 0.7) is investigated. The results are presented in Table 5-8.

Table 5-8: Sensitivity of the model output to the omega factor for DA/GT sets (sensitivity analysis A)

Experiment	**Mean proportion of time during which SPS capacity is below the level of 7.2MW**	**Mean proportion of time during which SPS capacity is below the level of 8MW**	**Mean proportion of time during which SPS capacity is below the level of 9MW**
Experiment 1 (omega factor = 0.7; overall confidence = 85%)	0.004 ± 0.002%	0.028% ± 0.008%	0.066% ± 0.011%
Experiment 1 (omega factor = 2; overall confidence = 85%))	0.011 % ± 0.004%	0.057% ± 0.010%	0.142% ± 0.016%
Experiment 1 (omega factor = 7; overall confidence = 85%)	0.081% ± 0.012%	0.250% ±0.024%	0.626% ± 0.039%

There is a significant difference between the results of Experiment 1 with different values of the omega factor. Thus, it can be concluded that the value of the omega factor for DA/GT sets should be carefully estimated as the model output is very sensitive to this parameter. As explained previously, the value of this parameter could be estimated from failure databases using the following equation $\omega_{DA/GT\ set} = N_{SM}/N_I$, where N_I is the number of inherent failures for DA/GT sets and $\boldsymbol{N_{SM}}$ is the number of failures due to substandard maintenance for DA/GT sets.

Part B:

The conclusion reached in Section 5.8.2 of the report was as follows:

"(…) *both maintenance related failures and logistic delays significantly affect the level of the standby power system capacity*."

Here, it will be investigated whether this conclusion changes if we change the value of the model parameter characterising maintenance related failures, i.e. the omega parameter for DA/GT sets ($\omega_{DA/GT\ set}$) to the extreme value of 0.7.

The data from the modified Experiments 2 & 3 was compared to the data from the modified Experiment 1 (base case) using an independent samples t-test (see Appendix I Section B for more details). The 95% confidence intervals for the differences between the mean proportions of time during which the standby power system capacity is below 7.2MW for the experiments are presented in Table 5-9 below.

Table 5-9: Comparing modified Experiments 2 & 3 to modified Experiment 1 (overall confidence = 90%, sensitivity analysis B)

	95% confidence interval for the difference in mean proportion of time during which standby power system capacity is below 7.2 MW		
Comparison	**Lower**	**Upper**	**Conclusion**
Experiment 1 to 2 (omega factor =0.7)	0.0004%	0.005%	Exp.1 > Exp. 2
Experiment 1 to 3 (omega factor =0.7)	-0.002%	0.004%	No difference

As it can be seen in Table 5-9 removal of maintenance related failures (Experiment 2) resulted in a statistically significant decrease in the mean proportion of time during which capacity is below 7.2MW. On the other hand, removal of logistic delays did not result in a significant decrease in the mean proportion of time during which capacity is below 7.2MW. Thus it can be concluded that, if the omega factor is as low as 0.7, the maintenance related failures still significantly affect the SPS capacity, but there is no significant contribution from logistic delays.

5.8.4 Summary of the quantitative analysis results

The key experimental and sensitivity analysis results are summarised below:

- In the current SPS set-up the mean proportion of time during which the SPS capacity is below the level of
    - 7.2MW (key model output measure) is contained in the following interval (0.007%, 0.015%)
    - 8MW is contained in the following interval (0.047%, 0.067%)
    - 9MW is contained in the following intervals: (0.126%, 0.158%)

  There is 85% probability that these three intervals simultaneously contain the respective proportions, i.e. hold “true” proportions at the same time. As mostly generic data was used to quantify the model (see Section 5.6.6 on model limitations), the plant specific data could be collected in the future and used to quantify the model to better represent the situation at the plant.
- The SPS capacity can occasionally drop below the level of 7.2MW and stay at this level for a short period of time. This situation will not be reflected in the data recorded in the shift log sheets by the personnel due to the way the data is recorded. For example, the availability is recorded on daily basis, which means that shorter periods of unavailability will not be indicated in the log sheets. Also, if the maintenance work carried out for a DA/GT set is finished by the end of the day, then the practice is to mark this set as available for service for that day in the shift logs. Finally, for obvious reasons, the data does not account for the DA/GT sets in the latent failed state. This was possible using the model. Overall, the data in the shift log sheets, if used to assess the key indicators for the SPS performance could give an overoptimistic impression of system performance.
- The model output is very sensitive to the value of the omega factor. The omega factor represents the ratio of the maintenance related DA/GT set failure rate to the inherent failure rate. The study of maintenance databases from three British nuclear power

stations (Morris et al., 1998) indicates that the ratio of failures due to substandard maintenance to inherent failures (N_{SM}/N_I) for various pieces of equipment including diesel generators could be as big as 7:1. This parameter should be carefully estimated using the plant specific data in order to adequately assess the impact of various factors on the SPS capacity over time.

- Removal of both maintenance related failures (Experiment 2) and logistic delays (Experiment 3) resulted in a statistically significant decrease in the mean proportion of time during which the SPS capacity is below 7.2MW. This means that both maintenance related failures and logistic delays statistically significantly affect the level of the SPS capacity. Sensitivity analysis indicates that even if the omega factor is very low (i.e. equal to 0.7) maintenance related failures still significantly affect the SPS capacity. However, the impact of logistic delays is not statistically significant in this case.
- Strategies could be developed in the future to, for example, decrease the occurrence of maintenance related failures. The model could be used to identify the variables or structures that have the highest impact on the occurrence of technician errors during DA/GT set maintenance. For example, the qualitative analysis presented in Section 5.7 suggested that *Ability to recognise technician errors* could be important, because its value can potentially determine the strength of three loops controlling the variable *Technician error probability*. The sensitivity of the model output measures to the changes in the value of *Ability to recognise technician errors* could be investigated. First, however, the model should be quantified with the plant specific data to better represent the conditions at the plant.

5.9 Discussion

There are a number of benefits associated with the use of SD:

- The model captures the SPS as a whole, including its technical, human and organisational aspects. It enables investigation of the interactions among these aspects and analysis of their relative importance and contribution to the DA/GT set unavailability and low SPS capacity over time.
- The model captures the system engineers' "mental model" of the SPS and it could serve as a reference point in future communication between the Risk Management team and the personnel involved in maintenance of the SPS at the plant. The model should provide the Risk Management team with a better understating of the key factors that contribute to the DA/GT set unavailability and reduced SPS capacity.

- The model could be modified in the future and it could be used to perform what-if analysis. For example, if appropriate, it could be used to evaluate the impact of changing the time between DA/GT set tests from 2 weeks to 1 month on the SPS capacity
- While there was a lot of uncertainty associated with various elements of the model, human and organisational in particular, it was worthwhile to quantify these aspects so that sensitivity analysis could be performed. In this particular example, sensitivity analysis pointed to the relative importance of the omega factor and the need for careful estimation of this factor. Thus, the model pointed to an important area that should be investigated in more detail and could lead to a more focused data collection effort.
- SD structures made it possible to capture feedback-driven behaviour of technicians and managers. Also, the feedback-driven relationship between the technical system and behaviour of technicians and managers was captured. In addition, SD analysis facilitated the identification of key delays in the SPS that may affect the effectiveness of policies designed to control it. Examples of such delays include time to provide training, time to change commitment to safety, time to wait for spare parts to arrive, time to organise resources etc.

5.10 Summary of the chapter

This chapter illustrated how SD could support the analysis of HOFs for PRA. It presented the application of SD to the analysis of HOFs contributing to the unavailability of the SPS at the plant. A model of the SPS, representing changes in SPS capacity over time, was developed to facilitate the analysis. The model was used to simulate the typical system behaviour over a period of 2 years which is long enough to capture the effects of preventive and corrective maintenance strategies on the SPS capacity. Overall, the data collection and model building process contributed to an improved understanding of the physical, human and organisational aspects of the SPS. The key benefits of using SD and issues associated with its application within PRA were discussed. The next chapter concludes the explorations in this thesis.

CHAPTER 6: Conclusions and further work

6.1 Introduction

The overall aim of this thesis was to improve the understanding of the role of SD in the analysis of HOFs for AA and PRA.

In the UK, the Health and Safety at Work Act requires that the risks arising from work activities should be managed by those who create them to the level “as low as reasonably practicable” (ALARP). The management of health and safety risks to the ALARP level is particularly challenging in complex technological systems, e.g. nuclear power plants, hazardous waste facilities, chemical plants, space systems, offshore oil and gas extraction facilities and transportation systems.

PRA and AA are important parts of the risk management of these systems. They help duty holders manage the risks to the ALARP level and ensure compliance with the health and safety law. In addition, PRA and AA help duty holders avoid costs associated with the occurrence of accidents. These costs involve loss of reputation, drop in staff morale, downtime or a need to pay compensation to the affected parties.

Logical and mathematical modelling plays an important role in PRA (see, for example, Bedford and Cooke, 2001) and is gaining increasing recognition within the AA community (see, for example, Sklet, 2004; Energy Institute, 2008; Johnson, 2003). Models help to identify hazards and adverse effects and help to explain how and why accidents occur. They also enable the risk to be expressed quantitatively. SD is a modelling approach that has been proposed to be used within PRA and AA (e.g. Mohaghegh et al., 2009; Cooke, 2003, 2004). The role of SD in these studies was to support the analysis of HOFs. Risks do change over time as a result of changes in HOFs. SD has significant capabilities for capturing mechanisms that drive human and organisational behaviour over time and influence risks and contribute to accidents.

However, the published literature lacks explicit discussion of the role that SD could play in the analysis of HOFs for PRA and AA. A good understanding of the benefits and limitations of using SD in the analysis of HOFs for PRA and AA is essential if SD is to be successfully applied in these areas. Lack of knowledge of the benefits and limitations of SD in the analysis of HOFs for PRA will lead to inadequate modelling of HOFs and inadequate insights into how risks should be managed over the medium and long term time horizon. Lack of knowledge of the benefits and limitations of using SD in the analysis of HOFs for AA will lead to poor learning from accidents and the design of ineffective accident prevention measures. The aim of this thesis is to improve the understanding of the role of SD in the analysis of HOFs for PRA and AA and address the gap identified in the published literature on the topic.

To achieve the thesis aim, the research work was divided into two areas for investigation:

1) Exploration of when SD could be used in the analysis of HOFs for PRA and AA.
2) Application of SD to the analysis of HOFs for PRA and AA to gain an understanding of the issues involved in using SD in these areas.

These investigations led to the lessons that contribute to knowledge of the use of SD within PRA and AA. Any modeller considering the use of SD within PRA or AA will benefit from the conclusions of this thesis.

6.2 Conclusions from the exploration of when SD could be used in the analysis of HOFs for PRA and AA

At the beginning of a PRA or AA study, a decision needs to be made whether SD will be used in the analysis of HOFs. There is little literature on the subject of when SD could be used to model HOFs for PRA or AA. In addition, there is little literature on the criteria that could be used to assess whether SD could be used to model a particular situation. The latest discussion in this area is Howick (2001) who proposed a set of criteria that could be used to assess suitability of SD to model a situation. As the development of these criteria was based on an extensive literature review and the criteria provide a useful and simple way of assessing the suitability of SD to model a situation, they were used to explore when SD could be used in the analysis of HOFs for PRA and AA. The conclusions from these explorations are summarised below:

- HOF analysis for PRA and AA is concerned with the identification and analysis of decisions and actions of people involved in operation, maintenance and risk management of technical systems. Human decisions and actions operate within feedback loops. Humans use information about the state of technical systems to change the state of these systems and control them. The information on the new state of technical systems is then used to generate new decisions and actions that change the state of these systems again and so on. Thus, the human and organisational aspects of complex technological systems considered in PRA and AA can be conceptualised as information-feedback systems. This is the domain of SD and, in principle, SD could be used to model HOFs for PRA and AA. However, it has been argued that SD analysis will be of use mainly for the analysis of HOFs that concern human decisions and actions repeated through time, associated with regular tasks such as maintenance, testing, calibration, restoration tasks, supervision, staffing, staff training etc.

- One should consider explicit modelling of feedback loops within HOF analysis for PRA and the use of SD when one is interested in improving the control of risks associated with operation of complex technological systems rather than merely in quantification of this risk. Thus, SD is likely to be used within PRA, when PRA and HOF analysis are used formatively, e.g. to improve the design of human tasks, organisational structure or to improve safety culture, rather than in a summative way, i.e. to provide a measure of the risk associated with a particular technical system in order to, for example, obtain a license from the regulator or to evaluate alternative technical system designs. SD can help to improve the control of risks by helping to:
    - identify the key balancing and reinforcing feedback loops that drive organisational behaviour over time. An example of a balancing feedback loop would be mechanisms controlling employees' competence levels over time. An example of a reinforcing loop would be mechanisms that drive employees' commitment over time.
    - identify factors that may weaken some of the balancing feedback loops designed to keep human error and equipment failure rates under organisational control. For example, mechanisms controlling employees' competence over time may be weakened by delays in organising training due to continuous lack of time or free resources to deliver the training
    - identify the virtuous and vicious feedback loops that can improve or degrade, respectively, human and technical system performance. For example, human vigilance and commitment to safety has a tendency to gradually decrease over time when there are no accidents or other disturbances. In the long run this can affect the quality of monotonous and repetitive, but important, processes such as preventive maintenance of critical pieces of equipment. In this case, the management may consider implementing different options to break the vicious circle. In the case of maintenance, the management may consider implementing early indicators of decreasing quality of maintenance such as frequency of maintenance revisits due to maintenance, frequency of "wrong parts used", frequency of the use of incorrect tools etc. Overall, SD could be used to identify

    variables that could serve as useful risk indicators and on which data could be collected by duty holders. There have already been studies that started to explore this capability of SD (see e.g. Dulac et al., 2005; Dulac, 2007).
  - identify major delays involved in feedback loops that may affect the effectiveness of the control feedback loops, e.g. delays that can slow learning about technical systems (delays in reporting & investigation of incidents), delays that can affect availability of engineered safety systems (delays in sourcing spare parts when legacy systems are being used, delays in finding resources to perform corrective maintenance).

– If decisions and actions of people involved in the accident that occurred are not a result of a simple error or mistake, but are influenced by the wider feedback-driven organisational context in which these people performed their tasks, one should consider explicit modelling of the feedback structures and the use of SD within AA.

– The feedback structure of information feedback systems generates the behaviour of these systems over time. Thus, if the feedback structure of HOFs is important to the purpose of HOF analysis for PRA and AA then the changes through time that are caused by this feedback structure are also important to the purposes of HOF analysis for PRA and AA.

– In general, it is not difficult to visualise HOFs in terms of stocks and flows that are used within SD. Additionally, the SD literature provides examples of generic stock and flow structures that could be adapted and used to represent HOFs for PRA and AA. Adapting SD structures developed for the purpose of explaining why an accident happened is another way of creating an initial SD model to be used in the analysis of HOFs for PRA. The data collected during Accident Investigation and used within AA provides a rich picture of how humans behave and how organisational processes work in practice. It can provide PRA with important areas on which PRA should focus and data to create an SD model that could be used within PRA. This is an example of how PRA can learn from AA. Also, a universal stock and flow structure of SD models could serve as an effective means for capturing and sharing key lessons from accidents within the industry and could support development of SD models for both AA and PRA. SD could provide a means of moving from a “context-specific set” of accident data to a “concept-based” description of the accident (Dekker, 2002) that could support efforts for further discussion, interpretation and falsification in the industry.

– Data needs associated with the application of SD depend on the type of SD model to be developed. If one wishes to perform qualitative SD analysis, then data on the feedback structure of the human and organisational context (represented as stocks and flows in SD models) and policies that guide human decision making will be required. If one wishes to perform quantitative SD analysis and run simulations, then additional data will be needed to populate stock and flow structures. There is a debate in the SD literature on the benefits and limitations of qualitative and quantitative SD models. Overall, it is less time and resource consuming to develop a qualitative SD model. However, quantitative models and simulation provide a better basis for making inferences about the behaviour of systems over time. Though, one needs be aware of the issues associated with quantification, in particular quantification of soft variables which are numerous in HOF analysis. Analysts need to ensure that the variables reflect the real life concept and can be meaningfully measured. The use of a qualitative SD model will be sufficient for the purpose of HOF analysis for AA, which is to explain the role that human and organisational factors played in the accident. However, when SD is used within PRA, the qualitative SD analysis should be followed by the quantitative one as modellers are usually interested in estimating the sensitivity of model output to different model structures. In this case, data is needed to quantify the model. The SD model created within AA will be more rich and detailed than the SD model created for PRA. Any attempt to quantify SD models within AA will be difficult in principle and would not add significant value to the analysis. AA is concerned with analysing one particular accident and in PRA usually classes of accidents are modelled. Thus, models used within PRA are more generic in nature and provide a higher-level description of human actions and organisational processes than AA models. In principle, PRA models should be much easier to quantify.

– The data required to develop a quantitative SD model for HOF analysis within PRA will go beyond what is usually required for traditional HOF analysis for PRA. It is very likely that these types of data will not be readily available or even will not exist. Also, it might be time consuming and costly to collect some data. This refers particularly to the collection of quantitative data to populate stock and flow structures within the SD model. In these cases, expert judgement or generic data might be sought to quantify the key parameters in the SD model. Analysts need to decide whether such an SD model will still be of benefit.

– The data that needs to be collected to perform SD analysis of HOFs for AA will be relating to the same human and organisational processes as data needed for traditional HOF analysis for AA. However, while collecting the data, the emphasis will be shifted from seeking information on the events that contributed to the accident to the feedback processes that have governed these events.

6.3 Conclusions from the application of SD to the analysis of HOFs for PRA and AA

PRA and AA analysts need to know how SD could be used to analyse HOFs for PRA and AA, and need to be aware of the issues associated with applying SD within these areas. SD was applied to the analysis of HOFs for AA and PRA to explore and understand these issues. The results of these explorations are summarised in the sections that follow.

6.3.1 Application of SD to the analysis of HOFs for AA

SD was applied to the analysis of HOFs that contributed to the 2007 Grayrigg train derailment. The iterative process that has been followed when analysing the accident and could be used in future to support the application of SD within AA is presented in Figure 6-1.

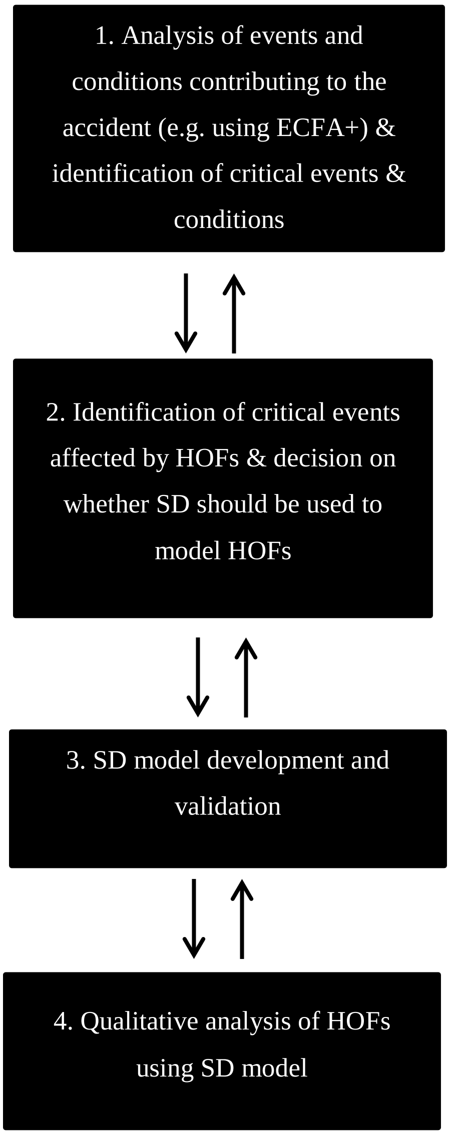

1. Analysis of events and conditions contributing to the accident (e.g. using ECFA+) & identification of critical events & conditions
2. Identification of critical events affected by HOFs & decision on whether SD should be used to model HOFs
3. SD model development and validation
4. Qualitative analysis of HOFs using SD model

Figure 6-1: Process used for the analysis of Grayrigg train derailment

The four steps of the modelling process captured in Figure 6-1are described in more detail below:

1. Analysis of events and conditions contributing to the accident (e.g. using ECFA+) & identification of critical events & conditions

   Overall, a clear picture of the sequence of events and conditions involved in the accident is needed to define the scope for HOF analysis in general and SD analysis in particular. ECFA+ (Kingston et al., 2007) is a simple approach often used in accident investigations and analyses to graphically depict the key events and conditions that contribute to accidents (Energy Institute, 2008). Kingston et al. (2007) list and describe the key conventions involved in carrying out ECFA+ analysis and creating ECF charts (see Section 4.5 for details). The process of creating ECF chart is similar to the creation of a fault tree. An analyst starts with a "top event" (the accident in question, e.g. "train derailed") and breaks it down into contributing events and conditions until "basic events" (critical events and conditions in the context of ECFA+) are reached. The definition of a root cause provided Paradies and Busch (1988 in Livingston et al., 2001) could be used to define the stopping criteria for ECFA+; i.e. events and conditions should be broken down until events and conditions that management has control to fix are reached.

2. Identification of critical events affected by HOFs & decision on whether SD should be used to model HOFs

   Here, firstly, the critical events and conditions identified in the previous step are examined to identify whether humans were involved. Then, criteria described in Chapter 3 can be used to discuss and decide whether SD should be used to model the impact of feedback-driven context on decisions and actions of humans involved in the accident.

3. 3. SD model development & validation

   General procedures for creating SD models have been described by Forrester (1961), Randers (1980), Richardson and Pugh (1981) and Sterman (2000). All these publications stress the importance of defining the problem at hand and the purpose of the SD model. Here, the definition of the problem and the purpose of the SD model are facilitated by the use of ECF chart. An SD modeler should focus the analysis on the events and conditions identified in the previous stage. The development of an SD model should be driven by the question: What organizational changes increased the probability of a particular event occurring or a particular condition existing at the time of the accident?

Once the appropriate organizational area, influencing a critical event or condition in an ECF chart, has been identified (e.g. process of railway inspection), then key stocks describing the state of this area (e.g. undetected track asset defects, staff inspecting railway, staff performing track maintenance) should be identified (Randers, 1980). Subsequently, an analyst should add flows that govern the identified stocks and then key variables within the boundary of the system that impact the behaviour of the flows. Thus, the process of SD model building is one of progressive elaboration in which key stocks are identified first and flows and other variables governing these stocks are gradually added. This process can be aided by the use of generic or archetypal structures already existing in the SD literature. For example, in the case of Grayrigg derailment, inspection and maintenance regime for track and signalling assets involved processes of asset deterioration, defect identification and corrective maintenance of defects. The SD structure used to capture this process of detecting and correcting flaws in systems is well known in the SD literature (see e.g. Lyneis & Ford, 2007) and was also used within the area of accident analysis and risk management (see e.g. Hoffman and Wilkinson, 2011). Hoffman and Wilkinson used this SD structure to depict how the oil and gas industry manages the hazards they face. The stocks and flows structures used by Hoffman and Wilkinson (2011) were adapted and used in the SD model to support Grayrigg train derailment analysis.

There are a number of publications on the SD model verification and validation (Forrester and Senge, 1980; Barlas, 1989, 1996; Barlas and Carpenter, 1990 and Sterman, 2000). See also discussion throughout this thesis and how SD model supporting analysis of Grayrigg train derailment has been validated.

4. Qualitative analysis of HOFs using SD model

   This step involves a systematic examination of identified stock and flow structures and feedback loops and analysis and discussion of how they have increased the probability of a particular critical event or condition occurring. The first step should involve identification of balancing and reinforcing feedback loops. The analysts may examine whether there were any factors that may have weakened some of the balancing feedback loops designed to keep human error and equipment failure rates under organisational control. In particular, analysts should investigate whether there were any major delays that may have affected the effectiveness of the control feedback loops. Then, it can be investigated whether any of the reinforcing feedback loops acted as “vicious circles” that may have gradually degraded system performance over time. If this is the case, then strategies need to be developed to break the “vicious” loops or change them into “virtuous” loops. For example, safety campaigns could be carried out to regularly remind technicians and engineers of the importance of good work practices.

The key conclusions from the application of SD to the analysis of HOFs within the Grayrigg train accident analysis are summarised below:

- SD can complement modelling approaches traditionally used in AA. Those wishing to use SD in the analysis of HOFs for AA may consider combining it with the ECFA+ approach. ECFA+ can be used to identify the events and conditions that were necessary and sufficient for an accident to occur. This can help to identify the critical events and conditions and define the scope for SD analysis. SD could then be used to capture human and organisational processes that generated the critical events and conditions captured by ECFA+.
- Approaches such as ECFA+ are very useful when one tries to analyse physical mechanisms involved in the accident. The analysis using an ECFA+ approach focuses on the events and conditions close in time to the accident. However, the proximate events and conditions that have occurred are just one set of all the events and conditions that could have occurred. If this particular set had not occurred, probably another set of events at a different point in time would have led to the accident. Thus, looking at just the proximate events and conditions is not sufficient to prevent accident reoccurrence. One should examine the organisational processes which control and generate sequences of events (Leveson, 2004). Also, the analysis of organisational processes will lead to a higher level of learning that could be used for the design of control measures for protection against a wider set of accidents rather than just one particular accident. SD can be used to capture the structure of these organisational processes and provide analysts with much a higher level of learning than the ECFA+ approach
- In general, it is much easier to develop an ECF diagram than to develop a stock and flow diagram. In the former case, the development of the model is much more structured and no extensive training or experience is required. One starts with the key event (e.g. train derailment) and works systematically backwards to identify and analyse events and conditions that have contributed to the final event. Development of an SD model requires prior training and experience. However, the prior development of an ECF diagram can facilitate, and is a good starting point for, the development of an SD model.

- ECF charts and stock and flow diagrams can usefully summarise hundreds of pages of investigation reports. They can provide a concise summary of Technical, Human and Organisational Factors that have contributed to an accident, from triggering events and conditions to the final results. They can be used as a reference point and facilitate discussion among experts on the key factors that have contributed to an accident and discussion on accident prevention measures.
- SD provides an alternative to event-based, sequential models traditionally used within AA. As Wolstenholme (1999) puts it, SD "*enhances linear and 'laundry list' thinking by introducing circular causality and providing a medium by which people can externalise mental models and assumptions and enrich these by sharing them"* (p. 424). SD analysis focuses on the dynamic nature of Human and Organisational Factors and enables identification of feedback structures responsible for this behaviour over time. In addition, SD analysis enables identification of delays in the system that might have affected the effectiveness of risk control policies and contributed to the accident.
- During an accident investigation, it often happens that there are differing opinions on some aspects of an accident or that there is a lot of uncertainty associated with how and why an accident occurred. There is usually a lot of uncertainty associated with the impact of Human and broader Organisational Factors. By using models such as an ECF chart and an SD model in particular, all the alternative views can be presented and assumptions can be made explicit and transparent, which can support further analysis of the accident and development of accident prevention measures.
- While there are a number of benefits of using qualitative SD models, they also have a number of limitations. Effective development and effective use of these models requires prior training and experience. In addition, Richardson points out that "*(...) most system dynamics practitioners would argue that using qualitative maps well for analysing a dynamic system requires a great deal of experience and expertise in quantitative system dynamics modelling"* (1999, p.441). Finally, quantitative SD models and simulation usually provide a better basis for making inferences about the behaviour of the analysed system over time than qualitative SD models. Though, one needs be aware of the issues associated with quantification, in particular quantification of soft variables which are numerous in HOF analysis. Analysts need to ensure that the variables reflect the real life concept and can be meaningfully measured.

6.3.2 Application of SD to the analysis of HOFs for PRA

SD was applied to the analysis of HOFs believed to contribute to the unavailability of an SPS at a process plant. The iterative process that has been followed during the analysis and could be used in future to support the application of SD within PRA is presented in Figure 6-2.

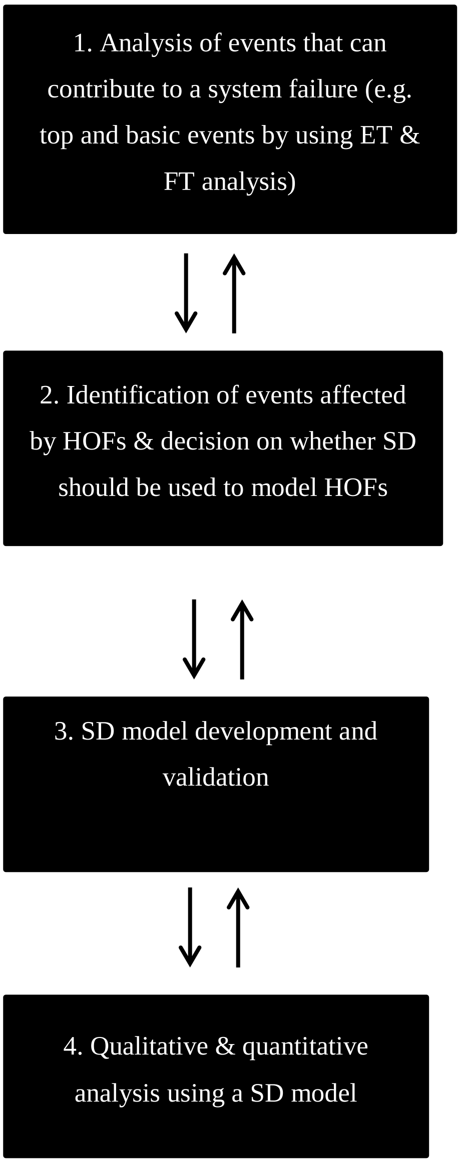

1. Analysis of events that can contribute to a system failure (e.g. top and basic events by using ET & FT analysis)
2. Identification of events affected by HOFs & decision on whether SD should be used to model HOFs
3. SD model development and validation
4. Qualitative & quantitative analysis using a SD model

Figure 6-2: Process used for the analysis of HOFs affecting availability of the SPS at a process plant

The four steps of the modelling process captured in **Error! Reference source not found.** are escribed in more detail below:

1. Analysis of events that can contribute to a system failure (e.g. top and basic events by using ET & FT analysis)

   As discussed in Chapter 2, ET and FT are usually used to depict and quantify scenarios for PRA (see USNRC, 1983; Bedford and Cooke, 2001). ET/FT can be developed by analysts from scratch or ET/ FT developed as part of a previous PRA can be used.

2. Identification of events affected by HOFs & decision on whether SD should be used to model HOFs

   Here, firstly, the events identified in the previous step are examined to identify whether humans are involved. If human involvement is acknowledged, then criteria described in Chapter 3 can be used to discuss and decide whether SD should be used to model the impact of feedback-driven context on decisions and actions of humans involved in the events influencing the analyzed PRA scenario.

3. SD model development and validation

   The purpose of an SD model should be agreed in the previous stage when analyzing ET and FT. An analyst should focus the SD analysis around the events identified in the previous stage (e.g. standby power system not available in case of off-site power system loss). The development of a SD model should be driven by the question: What organizational processes may affect the probability of a particular event occurring? (e.g. What organizational processes may affect the availability of the standby power system at a plant?). Once the appropriate organizational process, influencing an event in ET or FT, has been identified (e.g. maintenance of diesel alternators and gas turbines), then key stocks describing the state of this process should be identified (Randers, 1980) (e.g. alternators in standby state, alternators undergoing active corrective/preventive maintenance). Subsequently, an analyst should add flows that govern the identified stocks and then key variables within the boundary of the system that impact the behaviour of the flows. Thus, as when using SD in PRA the process of SD model building is one of progressive elaboration in which key stocks are identified first and flows and other variables governing these stocks are gradually added. This process can also be aided by the use of generic or archetypal structures already existing in the SD literature.

   A number of data sources can be used to develop and quantify a SD model, for example:

   – interviews with site personnel
   – organisational documents and procedures

- generic data in SD and PRA literature
- observation
- expert judgement elicitation

After the initial data has been gathered, an analyst can create an initial model or a set of simplified diagrams or flow charts, which can be used to facilitate a few rounds of interviews with Site personnel. Another possibility is to share the initial model with a group of personnel in a workshop and use it to elicit and confront different mental models of the system and modify the model.

4. Qualitative & quantitative analysis using the SD model

   The qualitative analysis is similar to the qualitative SD analysis for AA as described in previous section. It involves a systematic examination of balancing and reinforcing feedback loops and delays. The quantitative analysis should focus around investigating the sensitivity of the model output to different model structures. This can be accomplished by modifying the model structures or parameters, re-running the model and comparing its output to the base case simulation run that represent the current system setup. In this way, the structures of the model that have the biggest impact on the model output and overall risk can be identified.

The key conclusions from the application of SD to the analysis of HOFs for PRA are summarised below:

- The human tasks that are usually analysed as part of HOF analysis for PRA include those performed by operators and maintainers under normal operating conditions and those performed after an “initiating event” has occurred. The former may introduce latent faults into the engineered safety systems designed to mitigate the consequences of “initiating events”. The latter tasks are critical to cope with an abnormal situation that arises after an “initiating event” occurs. It is believed that SD is better suited to support the analysis of the first type of tasks, i.e. tasks performed under normal operating conditions which can introduce latent faults into the engineered safety systems designed to mitigate the consequences of “initiating events”. The uncertainty associated with modelling these types of tasks is smaller compared to the tasks performed in abnormal situations. The tasks performed under normal operating conditions involve tasks such as maintenance, testing, calibration and restoration tasks. What is to be done as part of these tasks is highly standardised and prescribed by the organisational policy and relevant written procedures. There is little diagnosis and decision-making, which are characteristic of the tasks performed in abnormal conditions after an “initiating event” occurs. Thus, the potential human errors and equipment failures are easier to identify. Also, we have more knowledge on the factors that shape human performance and equipment operation in normal operating conditions and how these errors and failures occur.

- The data to be used for the application of SD within PRA can be gathered from different sources. For example, data can be elicited via interviews with site personnel, investigation of historical records, analysis of generic data in the PRA and SD literature including archetypal SD structures that can be adapted for the purpose of a PRA study, and expert judgement elicitation.
- PRA is quantitative in nature and usually quantification of SD models to be used within PRA will be required. Quantification of SD models will usually involve quantification of soft variables such as “commitment to safety” or “competence level”. Analysts need to ensure that the variable is clearly defined and reflects the real life concept and can be meaningfully measured (see for example Mohaghegh & Mosleh, 2009b). Also, analysts need to remember that the SD structures proposed in the literature are usually used to support strategic use of SD, in which SD is used to examine trends in key variables rather than to provide precise predictions for the future (Roberts et al., 1983, in Howick, 2001, p. 102). The model should be used as a vehicle to investigate the relative importance of various structures and identification of areas to which the model output is sensitive to. Overall, the use of an SD model can point to important parameters and may lead to more focused data collection efforts.

6.3.3 Application of SD to the analysis of HOFs for AA and PRA

Overall, as highlighted throughout this thesis, the key characteristics of the RCA approach underlying traditional AA and HOF analysis for AA are as follows:

- explanation and representation of accidents in terms of discrete events and conditions leading to adverse effects
- search for root causes of accidents.

However, human decision-making operates within feedback structures. Decisions are based on the available information about the state of the technical systems, which lead to actions that change the state of these systems and then lead to new decisions and actions, forming a feedback loop. It is difficult to incorporate these types of structures in sequential, event-based models such as ECFA, ECFA+ or Fault Trees (see e.g. Leveson, 2004) and usually these feedback relationships are omitted in traditional AA. Usually, after creating an ECF diagram, analysts proceed with the identification of root causes of an accident using a number of checklists and end up with a list of discrete organisational conditions (e.g. constraints on access to the track, lack of resources) that contributed the accident without explicitly and clearly indicating interactions between these organisational conditions and the feedback structures that governed them. For example, the analysis of the Grayrigg train derailment indicated that:

- the exogenous factor (reduction in *Time available for inspection*) disrupted the operation of Network Rail's inspection and maintenance regime
- Network Rail was not prepared to deal with this disruption and ensure adequate *Number of staff performing track maintenance* and adequate *Number of staff inspecting railway.*

The question that could be asked is what could be done in the future to reduce gaps in staff required and available for infrastructure inspection and maintenance processes in case of time or other constraints on the inspection process. One of the potential solutions would be to improve the escalation process from lower level Network Rail managers to the top management and thus reduce delays in procuring additional staff or use the option of existing staff working overtime. This sort of exploration/discussion becomes obvious once one can see a simple SD model, but could easily be omitted when using just an ECF diagram and a "laundry list" of "root causes" of the accident. Overall, models are used not to replace, but to facilitate thinking. It is possible that one can get to the same conclusion by not using an SD model. However, the chances of focusing the analysis on the important issues increase with the use of adequate models of the problem and conclusions of the analysis might be much different depending on the model used.

The same event based, sequential logic underlies ET and FT models used in PRA and thus feedback structures are usually omitted in traditional PRA. Thus, important areas that can potentially contribute to future accidents can be omitted from the analysis. For example, the analysis of HOFs contributing to the availability of the SPS at a process plant that was presented in Chapter 5 could not be easily facilitated using standard FT and ET models used in traditional PRA. One of the focuses of this analysis were virtuous and vicious feedback loops that can improve or degrade, respectively, human and technical system performance. For example, human vigilance and commitment to safety has tendency to gradually decrease over time when there are no accidents or other disturbances. In the long run this can affect the quality of monotonous and repetitive, but important, processes such as preventive maintenance of critical pieces of equipment. It is not difficult to imagine errors of maintenance staff as basic events in a Fault Tree created within traditional PRA. However, Fault Trees do not show and do not have capability to show the feedback-driven mechanisms that can lead to these errors. SD is not only capable of representing these mechanisms, but also allows (when a quantitative SD analysis is done) testing of the strength of the impact of these mechanisms on the probability of the occurrence of these basic events.

Overall, AA and PRA are complementary analyses that could and should learn from one another. There are different ways that this could be achieved, for example:

- the ECF diagram that was created to facilitate analysis of the Grayrigg derailment could be compared to the existing Fault and Event Trees created as part of PRA for Network Rail and could help to identify events that have not been recognised in previous PRAs for Network Rail
- existing Fault and Event Trees could be compared to the ECF diagram from the analysis of Grayrigg train derailment in an attempt to generalise the ECF diagram to represent a wider set of accidents against which Network Rail should be protected; this generalised ECF diagram could be then used to see whether feedback loops captured by the SD model could lead to other accidents than the one that actually happened. This could lead to identification of events in the existing Fault and Event trees that could be potentially affected by the feedback loops captured by the SD model. The learning from this analysis could be brought into a future PRA study. For example, the SD structures identified in the retrospective analysis, and representing the organisational context affecting a range of events, could be used to quantify the impact of this context on events in Fault and Event Trees.

6.4 Contribution of this thesis

The key contributions of this thesis to the body of knowledge are summarised in the sections that follow.

6.4.1 Discussion of when SD could be used within AA and PRA

The SD literature on when SD could be used to model a situation was used to discuss when SD could be used within AA and PRA. This should help those considering using SD in the analysis of HOFs to decide whether SD could be used in any individual PRA or AA.

In particular, it has been suggested that SD could be of use in PRA when one is interested in analysing tasks that are performed by operators and maintainers under normal operating conditions. These tasks may introduce latent faults into the engineered safety systems designed to mitigate the consequences of "initiating events". The uncertainty associated with modelling these types of tasks is smaller compared to the tasks performed in abnormal situations. The tasks performed under normal operating conditions involve tasks such as maintenance, testing, calibration and restoration tasks. What is to be done as part of these tasks is highly standardised and prescribed by the organisational policy and relevant written procedures. There is little diagnosis and decision-making, which are characteristic of the tasks performed in abnormal conditions. Thus, the potential human errors and equipment failures are relatively easier to identify. Also, we have more knowledge on the factors that shape human performance and equipment operation in normal operating conditions and how errors and failures occur.

6.4.2 Discussion and illustration of how SD could be used within AA and PRA

SD has been applied to the analysis of HOFs within AA and PRA. The development of the SD models and key benefits and limitations associated with their use within AA and PRA were explicitly discussed. This could help those wishing to use SD in the analysis of HOFs to develop SD models for PRA and AA.

In particular, it has been illustrated how SD could be combined with the ECFA+ approach that is traditionally used within AA to analyse accidents. The two approaches can effectively complement each other and provide a more comprehensive picture of factors that contribute to accidents. ECFA+ analysis can be used to capture the key events and conditions that were necessary and sufficient for an accident to occur and can focus the SD effort by providing events and conditions to be analysed using SD. SD analysis can depict the structure of the dynamic processes that have brought these events and conditions into existence. Thus, the use of SD within AA will provide analysts with a much higher level of learning than the use of the ECFA+ approach alone and the use of SD can lead to the design of control measures for protection against a wider set of accidents. Moreover, analysis using the ECFA+ approach provides a “context-specific” description of the accident. If one wants to obtain a generic learning to be shared within the industry, one should move to a “concept-based” description of the accident (Dekker, 2002). A universal stock and flow structure of SD models could serve as an effective means for capturing and sharing key lessons from accidents within the industry.

In addition, it has been illustrated how SD could be used within PRA to analyse the impact of HOFs on the availability of engineered safety systems designed to mitigate the consequences of “initiating events”. It was highlighted that SD can improve the understanding of the dynamic impact of HOFs on technical and human system performance by:

- identification of the key balancing and reinforcing feedback loops that drive organisational behaviour over time
- identification of factors that may weaken some of the balancing feedback loops designed to keep human error and equipment failure rates under organisational control
- identification of virtuous and vicious feedback loops that can improve or degrade, respectively, human and technical system performance
- identification of major delays involved in feedback loops that may affect the effectiveness of the control feedback loops.

Also, it has been discussed how AA and PRA could potentially learn from one another and:

- how ECF diagrams and SD models used within AA could be used to inform PRA models
- how PRA models could be used to generalise models created within AA and thus lead to broadening of the lessons learnt from one particular accident that has occurred.

The exploration of how models created within AA and PRA can inform one another is an interesting and important research avenue that could be pursued in the future.

6.4.3 Case study specific contributions

SD was applied to the analysis of HOFs that contributed to the Grayrigg train derailment and HOFs affecting the SPS capacity at a process plant. These analyses led to insights that could inform future risk management of these complex technological systems. The ECFA+ and SD models developed for the Grayrigg analysis provided a transparent picture of the key events, conditions and processes that contributed to the accident. These models could facilitate and serve as a reference point for future discussions among experts on the factors that led to the accident. The SD model developed for the process plant highlighted the importance of maintenance related failures and pointed to the area on which future data collection analysis effort could focus.

6.5 Limitations of the Research

The main limitation of the research summarised in this thesis is that the conclusions, summarised in the previous section, are based on applying SD within only one PRA and one AA case. The limited number of AA and PRA cases explored in this thesis restricts the generalizability of the conclusions reached in this thesis. The issue of generalizability of the case study research is long recognised in the literature on the topic (see e.g. Bryman and Bell, 2007; Yin, 2003). The question is how and whether the findings from the analysis of a single case can be extended to a wider range of cases. In general, case study researchers focus on the rich data and uniqueness of the situation and do not try to generate statements that apply regardless of time and place (Bryman and Bell, 2007). However, this project is different in that it does not focus on the specific features of the analysed organisations, but on how these features can be modelled and analysed using SD and how SD can be used in HOF analysis for PRA and AA. The resulting SD models created to support AA will be different for different organisations, but the modelling principles used to develop these models will be common. The same applies to the SD models created within PRA. Still, only two cases (one to investigate the role of SD in HOF analysis for PRA and one to investigate the role of SD in HOF analysis for AA) were analysed. Therefore SD should be applied to a wider range of cases to provide further confidence in the findings presented in this thesis. For example, to build more confidence in the findings on the role of SD in HOF analysis for AA presented in this thesis, an ECFA+ analysis and SD analysis could be performed for another accident in the transportation industry. Similarly, to build more confidence in the findings on the role of SD in HOF analysis for PRA presented in this thesis, another complex technological system in the process or other industry could be analysed with the use of SD.

6.6 Further work

There are a number of open challenges in the field of HOF analysis for PRA and AA and a number of research avenues that could be pursued in the future. They are briefly summarised below:

- One of the key issues in the area of risk management of complex technological systems is the lack of connectivity between AA and PRA. This relates to the different objectives of these analyses, different sets of approaches that support them and different sets of outputs that are produced by these analyses. For example, while modelling is widely used within PRA, it is much less popular within the AA community. However, as discussed throughout this thesis, these are complementary analyses that could and should learn from one another. Thus, one potential research avenue would be to investigate the barriers to learning between PRA and AA community and how this learning could be improved. In particular, it could be investigated how tools such as SD could facilitate the learning from AA and using it within PRA. For example, the model developed for the analysis of Grayrigg train derailment could be modified and used within a PRA study for Network Rail. This could be done under the assumption that the organisational processes at Network Rail have not significantly changed over the years since the accident which might be a bold assumption. Nevertheless, the research could be carried out to investigate in detail how PRA could learn from AA, in particular in terms of the use of SD models created as part of AA. The critical issue is how analysts should move from detailed SD models reflecting conditions regarding a specific accident to more generic SD models for PRA, which could be used to design control measures for protection against a wider set of accidents. Earlier sections indicate how this work could be started.
- An important on-going issue in the area of HOF analysis for PRA is the identification, quantification and incorporation of HOFs in PRA models. The key question is how to create useful, but not overly simplistic models of HOFs that could be incorporated into current PRA models. Research is required on which HOFs should be included in models of HOFs, in particular SD models, and how they should be operationally conceptualised, measured and meaningfully incorporated into HOF analysis for PRA.

REFERENCES

Archer M. ed., 1998. *Critical realism: essential readings*. London: Routledge.

Barlas, Y., 1989. Multiple tests for validation of system dynamics type of simulation models. European Journal of Operational Research 42 (1), 59–87.

Barlas, Y., 1996. Formal aspects of model validity and validation in system dynamics. System Dynamics Review 12 (3), 183–210.

Barlas, Y. and Carpenter, S., 1990. Philosophical roots of model validation: Two paradigms. System Dynamics Review 6 (2), 148–166.

BBC, 2007. Two men arrested over train crash [Online] (Updated 15 November 2007). Available at: http://news.bbc.co.uk/1/hi/england/7097284.stm
[Retrieved 15 August 2011]

BBC, 2009. No charges over fatal rail crash [Online] (Updated 9 February 2009). Available at: http://news.bbc.co.uk/1/hi/england/cumbria/7879827.stm
[Retrieved 15 August 2011]

Bazerman, M., H., 2006. *Judgement in managerial decision making*. 6th ed. New York: Wiley.

Bedford, T. & Cooke, R., 2001. *Probabilistic Risk Analysis: foundations and methods.* Cambridge: Cambridge University Press.

Bier, V. M., 1999. Challenges to the Acceptance of Probabilistic Risk Analysis. *Risk Analysis*, 19 (4), pp. 703-710.

Bley, D., Kaplan, S. & Johnson, D., 1992. The strengths and limitations of PSA: where we stand. *Reliability Engineering & System Safety*, 38 (1–2), pp. 3-26.

British Standard Institution (BSI), 1991. BS 4778-3.1:1991 *Quality vocabulary - Part 3: availability, reliability and maintainability terms – Section 3.1-3.2: Guide to concepts and related definitions.* London: BSI.

British Standard Institution (BSI), 1996. BS 8444-3: 1996 *Risk management - Part 3: Guide to risk analysis of technological systems.* London: BSI.

Boxall, P. & Purcell, J., 2003. *Strategy and Human Resource Management*. London: Palgrave Macmillan.

Bryman, A. & Bell, E., 2007. *Business research methods*. 2nd ed. Oxford: Oxford University Press.

Buys, J.R. & Clark, J.L., 1995. Events & Causal Factors Analysis. SCIE-DOE-01-TRAC-14-95. Idaho Falls: Technical Research and Analysis Center.

Carhart, N. & Yearworth, M., 2010. The Use of System Dynamics Group Model Building for Analysing Event Causality within the Nuclear Industry. In: Moon, T. H. ed., Proceedings of the 28th International Conference of the System Dynamics Society. Seoul, Korea 25-29 July, 2010. New York, NY: System Dynamics Society.

Chandler, F. T. et al., 2006. Human Reliability Analysis methods: selection guidance for NASA. NASA/OSMA Technical Report: July 2006. National Aeronautics and Space Administration.

Cooke, D. L., 2003. A System Dynamics analysis of the Westray mine disaster. *System Dynamics Review,* 19 (2), pp.139-166.

Cooke, D. L., 2004. The Dynamics and Control of Operational Risk. Ph.D. University of Calgary.

Cooper, S. E., Ramey-Smith, A. M., Wreathall, J., Parry, G.W., Bley, D. C., 1996. A Technique for Human Error Analysis (ATHEANA): technical basis and methodology description. NUREG/CR-6350. Prepared for US Nuclear Regulatory Commission. Upton, NY: Brookhaven National Laboratory.

Coyle, R. G., 1973. On the scope and purpose of Industrial Dynamics. *International Journal of Systems Science,* 4 (3), pp. 397-406.

Coyle, R. G., 1977. *Management System Dynamics*. Chichester: Wiley.

Coyle, R. G., 1985. Representing discrete events in System Dynamics models: a theoretical application to modelling coal production. *Journal of the Operational Research Society*, 36 (4), pp. 307-318.

Coyle, R. G., 2000. Qualitative and quantitative modelling in system dynamics: some research questions. *System Dynamics Review,* 16 (3), pp. 225-244.

Coyle, R. G., 2001. Rejoinder to Homer and Oliva. *System Dynamics Review*, 17 (4), pp. 357–363.

Cox, S. & Flin, R., 1998. Safety culture: Philosopher's stone or man of straw? *Work & Stress: An International Journal of Work, Health & Organisations*, 12 (3), pp. 189-201.

Cyert, R. & March, J., 1963/1992. *A behavioural theory of the firm*. Englewood Cliffs, NJ: Prentice Hall, 2nd ed. Cambridge, MA: Blackweel.

Davoudian, K., Wu, J. S. & Apostolakis, G., 1994a. Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering and System Safety*, 45 (1994), pp. 85-105.

Davoudian, K., Wu, J. S. & Apostolakis, G., 1994b. The work process analysis model (WPAM). *Reliability Engineering and System Safety.* 45 (1-2), pp. 107-125.

Dekker, S., 2002. Reconstructing human contributions to accidents: the new view on error and performance. *Journal of Safety Research*, 33 (3), pp. 371-385.

Dekker, S., 2006. Resilience Engineering: Chronicling the Emergence of Confused Consensus. In Hollnagel, E., Woods, D. D. & Leveson, N., eds. *Resilience Engineering: Concepts and Precepts.* Farnham: Ashgate Publishing.

Diehl, E. & Sterman, J. D., 1995. Effects of Feedback Complexity on Dynamic Decision Making. *Organizational Behavior and Human Decision Processes,* 62 (2)**,** pp. 198-215.

Dulac, N., Leveson, N., Zipkin, D., Friedenthal, S., Cutcher-Gershenfeld, J., Carroll, J. & Barrett, B., 2005. Using System Dynamics for safety and risk management in complex engineering systems. In: Kuhl, M. E., Steiger, N. M., Armstrong, F. B. & Joines, J. A. eds., Proceedings of the 2005 Winter Simulation Conference. Orlando, FL, USA December 4 – 7, 2005. Orlando, FL: IEEE.

Dulac, N., 2007. A framework for dynamic safety and risk management modelling in complex engineering systems. Ph.D. Cambridge, MA: Massachusetts Institute of Technology.

Dulac, N., Leveson, N. & Dierks, M., 2008. System Dynamics Approach to Model Risk in Complex Healthcare Settings: Time Constraints, Production Pressures and Compliance with Safety Controls. In: Dangerfield, Brian C. ed., Proceedings of the 26th International Conference of the System Dynamics Society. Athens, Greece 20-24 July. New York, NY: System Dynamics Society.

Embrey, D. E., 1992. Incorporating management and organisational factors into probabilistic safety assessment. *Reliability Engineering and System Safety*, 38 (1-2), pp. 199-208.

Energy Institute, 2008. Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents. Energy Institute: London. Available at:

https://www.energyinst.org/technical/human-and-organisational-factors/human-and-organisational-factors-incident-accident--invest-analy

[Retrieved 15 June 2010]

Forester, J., Bley, D., Cooper, S., Lois, E., Siu, N., Kolaczkowski, A. & Wreathall, J., 2004. Expert elicitation approach for performing ATHEANA quantification. *Reliability Engineering and System Safety*, 83 (2), pp. 207-220.

Forester, J., Kolaczkowski, A., Cooper, S., Bley, D. & Lois, E., 2007. ATHEANA user's guide. NUREG -1880. Washington, DC: US Nuclear Regulatory Commission.

Forrester, J. W., 1961. *Industrial Dynamics*. Cambridge, MA: The MIT Press.

Forrester, J.W., 1968a. Industrial dynamics - A response to Ansoff and Slevin. *Management Science*, 14 (9), pp. 601-618.

Forrester, J.W., 1968b. *Principles of Systems*. Cambridge, MA: MIT Press.

Forrester, J.W., 1969. *Urban Dynamics*. Cambridge, MA: MIT Press.

Forrester, J.W., 1971a. *World Dynamics*. Cambridge, MA: Wright-Allen Press.

Forrester, J.W., 1971b. The model versus a modelling process. *System Dynamics Review*, 1 (2), pp. 133-134.

Forrester, J. W., 1995. The beginning of System Dynamics. *The McKinsey Quarterly*, 1995 (4), pp. 4-17.

Forrester, J. W. and Senge P. M., 1980. Tests for building confidence in system dynamics models. In: Legasto AA Jr., Forrester JW and Lyneis JM (eds). TIMS Studies in the Management Sciences,14.

French, S., Bedford T., Pollard, S.J.T. & Soane, E., 2011. Human reliability analysis: a critique and review for managers. *Safety Science* 49 (2011), pp. 753-763.

Groesser, S. N. & Schaffernicht, M., 2012. Mental models of dynamic systems: taking stock and looking ahead. System Dynamics Review 28 (1), pp. 46–68. London: The Stationary Office. Available at:

https://www.gov.uk/government/publications/the-nimrod-review

[Retrieved 12 May 2010]

Haddon-Cave, C., 2009. The Nimrod review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006.

Hoffman, I. & Wilkinson, P., 2011. The barrier-based system for major accident prevention: a system dynamics analysis. In: Lyneis, J. M. & Richardson, J. P., eds, Proceedings of the 29th International Conference of the System Dynamics Society. Washington DC, USA 25-29 July, 2011. New York, NY: System Dynamics Society.

Hogarth, R., 1987. *Judgement and choice*, 2nd ed., Chichester: Wiley.

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

Howick, S., 2001. An exploration of the role of system dynamics in the analysis of disruption and delay for litigation. Ph.D. Glasgow: University of Strathclyde.

HSE (Health and Safety Executive), 2000. Improving maintenance: a guide to reducing error. [e-book] HSE Books. Available at:

http://www.hseni.gov.uk/improving_maintenance_-_a_guide_to_reducing_human_error.pdf

[Retrieved 23 November 2012]

HSE (Health and Safety Executive), 2013. ALARP “at a glance” [Online]. Available at:

http://www.hse.gov.uk/risk/theory/alarpglance.htm;

[Retrieved 2 April 2013]

HSE, 2014. How to manage health and safety [Online]. Available at:

http://www.hse.gov.uk/toolbox/managing/index.htm

[Retrieved 3 April 2014]

Health and Safety Laboratory, 2009. Review of human reliability assessment methods. [e-book] Research Report RR679. Available at: http://www.hse.gov.uk/research/rrpdf/rr679.pdf [Retrieved 19 May 2011]

Homer, J. & Oliva, R., 2001. Maps and models in system dynamics: a response to Coyle. System Dynamics Review, 17 (4), pp. 347-355.

Human Engineering, 2005. A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit. Research Report 367. [e-book] Health and Safety Executive. Available at: www.hse.gov.uk/research/rrpdf/rr367.pdf [Retrieved 23 November 2012]

International Atomic Energy Agency, 2007. IAEA Safety Glossary. 2007 edition. Vienna: IAEA. Available at: http://www-pub.iaea.org/books/IAEABooks/7648/IAEA-Safety-Glossary-Terminology-Used-in-Nuclear-Safety-and-Radiation-Protection-2007-Edition [Retrieved 13 May 2010]

Johnson, C. W., 2003. *Failure in safety-critical systems: a handbook of incident and accident reporting*. Glasgow: Glasgow University Press. Available at http://www.dcs.gla.ac.uk/~johnson/book [Retrieved 3 April 2014]

Johnson, W. G., 1973. The Management Oversight and Risk Tree – MORT. SAN 821-2. U.S. Atomic Energy Commission.

Johnson, P. & Duberley, J., 2000. *Understanding management research: an introduction to epistemology.* London: SAGE publications.

Kahneman, D., Slovic P. & Tversky A., 1982. *Judgement under uncertainty: heuristics and biases*. Cambridge: Cambridge University Press.

Kampmann, C. & Sterman, J. D., 1998. Feedback complexity, bounded rationality, and market dynamics. MIT Sloan School of Management. Available at: http://jsterman.scripts.mit.edu/On-Line_Publications.html#1998Feedback [Retrieved 3 April 2013]

Kingston et al., 2007. ECFA+: Events and Conditional Factors Analysis Manual. NRI-4. Delft: The Noordwijk Risk Initiative Foundation.

Kirwan, B., 1994. *Practical guide to human reliability assessment*. London: Taylor and Francis.

Kirwan, B., 2004. Nuclear Action Reliability Assessment (NARA): a data-based HRA tool. In: the 7th international conference on Probabilistic Safety Assessment and Management. Berlin, Germany 14-18 June, 2004: London: Springer.

Kirwan, B., Gibson H., Kennedy, R., Edmunds, J., Cooksley G. & Umbers, I., 2005. Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool. *Safety & Reliability*, 25 (2), pp. 38-45.

Law, A. M. and Kelton, W. D., 2000. Simulation Modeling and Analysis. 3rd edition. New York, NY : McGraw-Hill.

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

Lane, D.C., 1999. Social theory and system dynamics practice. *European Journal of Operational Research,* 113, pp. 501-527.

Lane, D.C., 2008. The emergence and use of diagramming in System Dynamics: a critical account. Systems Research and Behavioral Science, 25, pp. 3-23.

Livingston, A.D., Jackson, G. & Priestley, K., 2001. Root cause analysis: literature review. Contract Research report 325/200. [e-book] Health and Safety Executive. Available at: www.hse.gov.uk/research/crr_pdf/2001/crr01325.pdf
[Retrieved 22 May 2013]

Lyneis J.M. & Ford D. N., 2007. System Dynamics applied to project management: a survey, assessment, and directions for future research. *System Dynamics Review*, 23 (2-3), pp. 157-189.

Mingers, J., 2003. A classification of the philosophical assumptions of management science methods. *Journal of Operational Research Society*, 54, pp. 559-570.

Mohaghegh, Z., Kazemi, R. & Mosleh, A., 2009. Incorporating organisational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: a hybrid technique formalization. *Reliability Engineering and System Safety,* 94 (5), pp. 1000-1018.

Mohaghegh, Z. & Mosleh, A., 2009a. Incorporating organisational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: principles and theoretical foundations. *Safety Science,* 47 (8), pp. 1039-1058.

Mohaghegh, Z. & Mosleh, A., 2009b. Measurement techniques for organizational safety causal models: characterization and suggestions for enhancements. *Safety Science,* 47 (10), pp. 1398-1409.

Morris, I.E., Walker, T. G., Findlay, C.S. & Cochrane, E. A., 1998. Control of maintenance errors. In: Lydersen S., Hansen G.K. and Sandtorv H. eds., Safety and Reliability (ESREL 1998). Rotterdam: Balkema.

Mosleh, A., Goldfeiz, E. & Shen S., 1997. The ω-factor approach for modeling the influence of organizational factors in probabilistic safety assessment. In: Gertman, D., Schurman, D. L. & Blackman, H.S., Global Perspectives of Human Factors in Power Generation, IEEE Sixth

Conference on Human Factors and Power Plants. Orlando, FL, USA 8-13 June 1997. New York, NY: IEEE.

Mosleh, A., Wang, C., Groth K. & Mohaghegh Z., 2005. Integrated methodology for identification, classification and assessment of aviation system risk. Prepared for Federal Aviation Administration (FAA). Center for Risk and Reliability, 2005.

Nelson, R. & Winter, S., 1982. *An evolutionary theory of economic change*. Cambridge, MA: Belknap Press of Harvard University Press.

Network Rail, 2007. Summary report of the investigation into the train derailment of 1S83, the 17.15hrs Virgin Pendolino train from London Euston to Glasgow. Available at: http://www.railwaysarchive.co.uk/docsummary.php?docID=1226 [Retrieved 5 August 2011]

Paich, M. & Sterman, J.D., 1993. Boom, bust, and failures to learn in experimental markets. *Management Science*, 39 (12), pp. 1439-1458.

Paradies, M. & Busch D., (1988). *Root Cause Analysis at Savannah River Plant*. In: Institute of Electrical and Electronics Engineers, IEEE Fourth Conference on Human Factors and Power Plants. Monterey, CA, USA 5-9 June 1988. New York, NY: IEEE.

Pate-Cornell, M. E. & Murphy, D. M., 1996. Human and management factors in Probabilistic Risk Analysis: the SAM approach and observations from recent applications. *Reliability Engineering and System Safety*, 53 (2), pp. 115-126.

Perrow, C., 1984. *Normal Accidents: Living with High-Risk Technologies.* New York, NY: Basic Books.

Pidd, M., 2009. *Tools for thinking: modelling in management science.*3rd edition. Chichester: Wiley.

RAIB (Rail Accident Investigation Branch), 2011. Derailment at Grayrigg. Report 20/2008. Department of Transport. Available at: http://www.raib.gov.uk/publications/investigation_reports/reports_2008/report202008.cfm [Retrieved 5 August 2011]

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Safety Science*, 27 (2/3), pp. 183-213.

Rasmussen, N., 1975. Reactor safety study: An assessment of accident risks in U.S. commercial nuclear power plants. WASH-1400.U.S. Nuclear Regulatory Commission.

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

Reason, J., 1997. *Managing the risks of organisational accidents.* Aldershot: Ashgate.

Reason J., Hollnagel, E. & Paries, J., 2006. Revisiting the Swiss Cheese Model of accidents.

EC Technical/Scientific Report No. 2006-017 (EEC Note 2006/13). Project Saftbuild. Eurocontrol Experimental Centre. Available at: http://www.eurocontrol.int/eec/public/standard_page/DOC_Report_2006_017.html [Retrieved 3 April 2010]

Richardson, G. P., 1991. *Feedback thought in social science and systems theory*. Pegasus Waltham, MA: Communications, Inc.

Richardson, G. P., 1999). Reflections for the future of system dynamics. *Journal of the Operational Research Society*, 50 (4), pp. 440-449.

Roberts N., Andersen D., Deal R., Garet, M. & Shaffer W., 1983. *Introduction to Computer Simulation: A System Dynamics Modeling Approach*. Portland, OR: Productivity Press,

Roelen, A. L. C., Wever R., Hale A. R., Goossens, L. H. J., Cooke R.M., Lopuhaa, R., Simons, M. & Valk, P. J. L., 2004. Causal modeling using Bayesian Belief Nets for integrated safety at airports. *Risk, Decision and Policy,* 9 (3), pp. 207 - 222.

Robinson S., 2004. *Simulation: the practice of model development and use*. Chichester: Wiley.

Salge, M. & Milling P. M., 2006. Who is to blame, the operator or the designer? Two stages of human failure in the Chernobyl accident. System Dynamics Review, 22 (2), pp.
89-112.

Sargent, R. G., 2013. Verification and validation of simulation models. *Journal of Simulation,* 7 (2013), pp. 12-24.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research methods for business students*. 6th ed. Harlow: Pearson.

Simon, H., 1957. *Administrative behaviour: a study of decision-making processes in administrative organizations*, 2nd ed. New York: Macmillan.

Simon, H., 1982. *Models of bounded rationality*. Cambridge, MA: MIT Press.

Sklet, S., 2004. Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials,* 111 (1-3), pp. 29–37.

Smith, H.W., 1975. *Strategies of social research: The methodological imagination*. London: Prentice-Hall, London.

Swain, A.D., 1989. *Comparative evaluation of methods for Human Reliability Analysis*. Koln: Gesellschaft fur Reaktorsicherheit.

Swain, A.D., 1990. Human Reliability Analysis: Need, Status, Trends and Limitations. *Reliability Engineering and System Safety,* 29 (3), pp. 301-313.

Swain A.D. & Guttmann H.E. 1983. Handbook of Human Reliability Analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. U.S. Nuclear Regulatory Commission.

Sterman, J. D., 2000. *Business dynamics: system thinking and modelling for a complex World*. Irwin/McGraw-Hill: Chicago.

Teplitz, C., 1991. *The learning curve deskbook: a reference guide to theory, calculations, and applications*. New York: Quorum Books.

Turner, B. A. & Pidgeon, N. F., 1997. *Man-made disasters.* 2nd ed. Oxford: Butterworth-Heinemann.

U.S. Energy Information Administration, 2012a. What is the difference between electricity generation capacity and electricity generation? Available at: http://www.eia.gov/tools/faqs/faq.cfm?id=101&t=3 [Retrieved 22 October 22]

U.S. Energy Information Administration, 2012b. Glossary. Available at: http://www.eia.gov/tools/glossary/index.cfm?id=H [Retrieved 22 October 22]

U.S. Nuclear Regulatory Commission, 1983. PRA procedures guide. NUREG/CR 2300. Washington, DC: USNRC.

U.S. Nuclear Regulatory Commission, 2000. Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624. Washington, DC: USNRC.

U.S. Nuclear Regulatory Commission, 2007. Industry-average performance for components and initiating events at U.S. commercial nuclear power plants. NUREG/CR 6928. Washington, DC: USNRC.

U.S. Nuclear Regulatory Commission, 2010. CCF Parameter Estimations 2010. Washington, DC: USNRC.

Vesely, W. E., Goldberg, F.F., Roberts, N. H. & Haasl, D. F., 1981. Fault Tree Handbook. NUREG-0492. Washington, DC: US Nuclear Regulatory Commission.

Wang, C., 2007. Hybrid causal methodology for risk assessment. Ph.D. thesis. University of Maryland, Center for Risk and Reliability.

Williams, J. C., 1986. HEART: A proposed method for assessing and reducing human error. In: Proceedings of the 9th Advances in Reliability Technology Symposium. University of Bradford 2-4 April, 1986. Bradford: University of Bradford.

Williams, J. C., 1988. A data-based method for assessing and reducing human error to improve operational performance. In: Institute of Electrical and Electronics Engineers, IEEE Fourth Conference on Human Factors and Power Plants. Monterey, CA, USA 5-9 June 1988. New York, NY: IEEE.

Williams, T., 2008, *Management science in practice.* Chichester: Wiley.

Wolstenholme, E. F., 1999). Qualitative *vs* quantitative modelling: the evolving balance. *Journal of the Operational Research Society* 50 (4), pp. 422-428.

Wright, T. P., 1936. Factors affecting the cost of airplanes. *Journal of Aeronautical Sciences*, 3 (4), pp. 122–128.

Yelle, L. E., 1979. The learning curve: historical review and comprehensive survey. *Decision Sciences*, 10, pp. 302–328.

Yin, R.K., 2003. *Case study research: design and methods*. 4th edition. Thousand Oaks, CA: Sage publications

Zio E., 2009. Reliability engineering: old problems and new challenges. *Reliability Engineering and System Safety*, 94 (2), pp. 125–141.

APPENDICES

Appendix A **Glossary of abbreviations**

CM – corrective maintenance

DA – diesel alternator also referred to as DA set, generating set or genset

GT – gas turbine also referred to as GT set, generating set or genset

PM – preventive maintenance

SPS – standby power system

Appendix B **Glossary of terms used in Chapter 5**

Capacity – the maximum electric output a generating set or combination of generating sets can produce under specific conditions (U.S. Energy Information Administration, 2012a).

Megawatt (MW) – One million watts (U.S. Energy Information Administration, 2012b).

Watt – the electrical unit of power; the rate of energy transfer equivalent to 1 ampere flowing under a pressure of 1 volt at unity power factor (U.S. Energy Information Administration, 2012b).

Load (Electric) – The amount of electric power delivered or required at any specific point or points on a system (U.S. Energy Information Administration, 2012b). The requirement originates at the energy-consuming equipment of the consumers.

AVAILABILITY

Availability – the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided (BSI, 1991)

Non-operating state – the state when an item is not performing a required function (BSI, 1991)

Operating state – the state when an item is performing a required function (BSI, 1991)

Down state – a state of an item characterised either by a fault, or by a possible inability to perform a required function during preventive maintenance (BSI, 1991)

Up state – a state of an item characterised by the fact that it can perform a required function, assuming that the external resources, if required, are provided (BSI, 1991)

Standby state – a non-operating up state during the required time (BSI, 1991)

Required time – the time interval during which the user requires the item to be in a condition to perform a required function (BSI, 1991)

Standby time – the time interval during which an item is in the standby state (BSI, 1991)

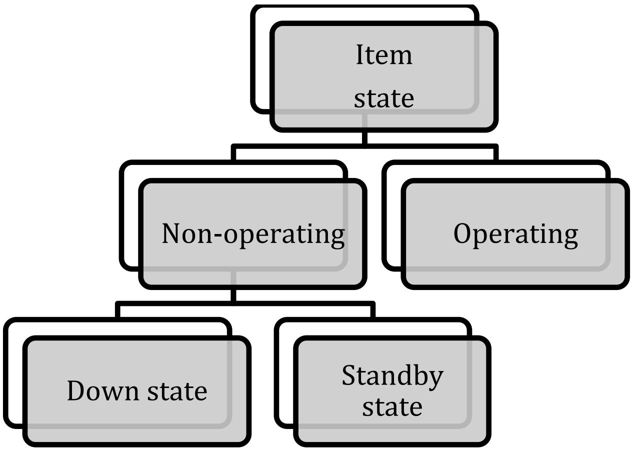


Figure B-1: Item state types [adapted from (BSI, 1991)]

FAILURES & FAULTS

Failure – the termination of the ability of an item to perform a required function (BSI, 1991)

Failure mode – the manner by which a failure is observed by technicians (BSI, 1991)

Fault – the state of an item characterised by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources; failure is an event and fault is a state; a fault is often the result of a failure of the item, but may exist without prior failure (BSI, 1991)

Latent fault – an existing fault that has not yet been recognised and would lead to the failure of an item when it is operated

Fault recognition – the event of a fault being recognised (BSI, 1991)

Fault localisation – actions taken to identify the faulty sub-item or sub-items at the appropriate indenture level (BSI, 1991)

Fault diagnosis – actions taken for fault recognition, fault localisation and cause identification (BSI, 1991)

INSPECTION & MAINTENANCE

Condition monitoring – the continuous or periodic measurement and interpretation of data to indicate the degraded condition of an item and the need for maintenance (BSI, 1991)

Preventive maintenance – the maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item (BSI, 1991)

Condition based maintenance – the maintenance that is carried out according to the need indicated by condition monitoring (BSI, 1991)

Scheduled maintenance – the preventive maintenance carried out in accordance with an established time schedule (BSI, 1991)

Corrective maintenance – the maintenance carried out after fault recognition and intended to put an item into a state in which it can perform a required function (BSI, 1991)

Maintenance time – the time interval during which a maintenance action is performed on an item either manually or automatically, including logistic delays; maintenance might be carried out while the item is performing a required function (BSI, 1991)

Active maintenance time – the part of maintenance time during which a maintenance action is performed on an item, either automatically or manually, excluding logistic delays (BSI, 1991)

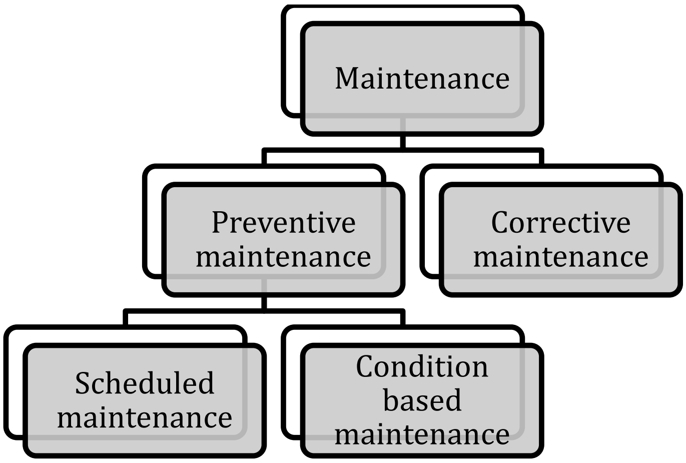


Figure B-2: Types of maintenance [adapted from (BSI, 1991)]

Preventive maintenance time – the part of the maintenance time during which preventive maintenance is performed on an item, including logistic delays inherent in preventive maintenance (BSI, 1991)

Corrective maintenance time – the part of maintenance time during which corrective maintenance is performed on an item, including logistic delays inherent in corrective maintenance (BSI, 1991)

Fault diagnosis time – the time during which fault diagnosis is performed (BSI, 1991)

Logistic delay - the accumulated time during which a maintenance action cannot be performed due to the necessity to acquire maintenance resources; logistic delays can be due to, for example, pending arrival of spare parts, specialist test equipment, information (BSI, 1991)

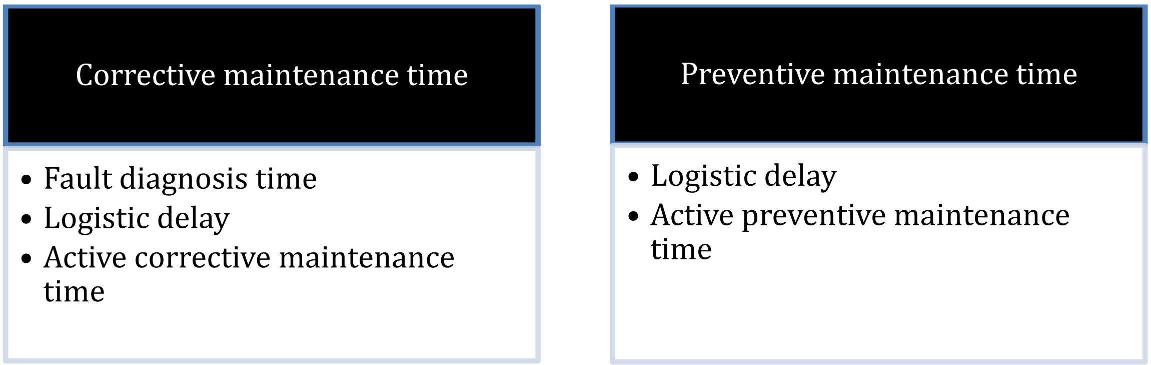

Corrective maintenance time
Fault diagnosis time
Logistic delay
Active corrective maintenance time
Preventive maintenance time
Logistic delay
Active preventive maintenance time

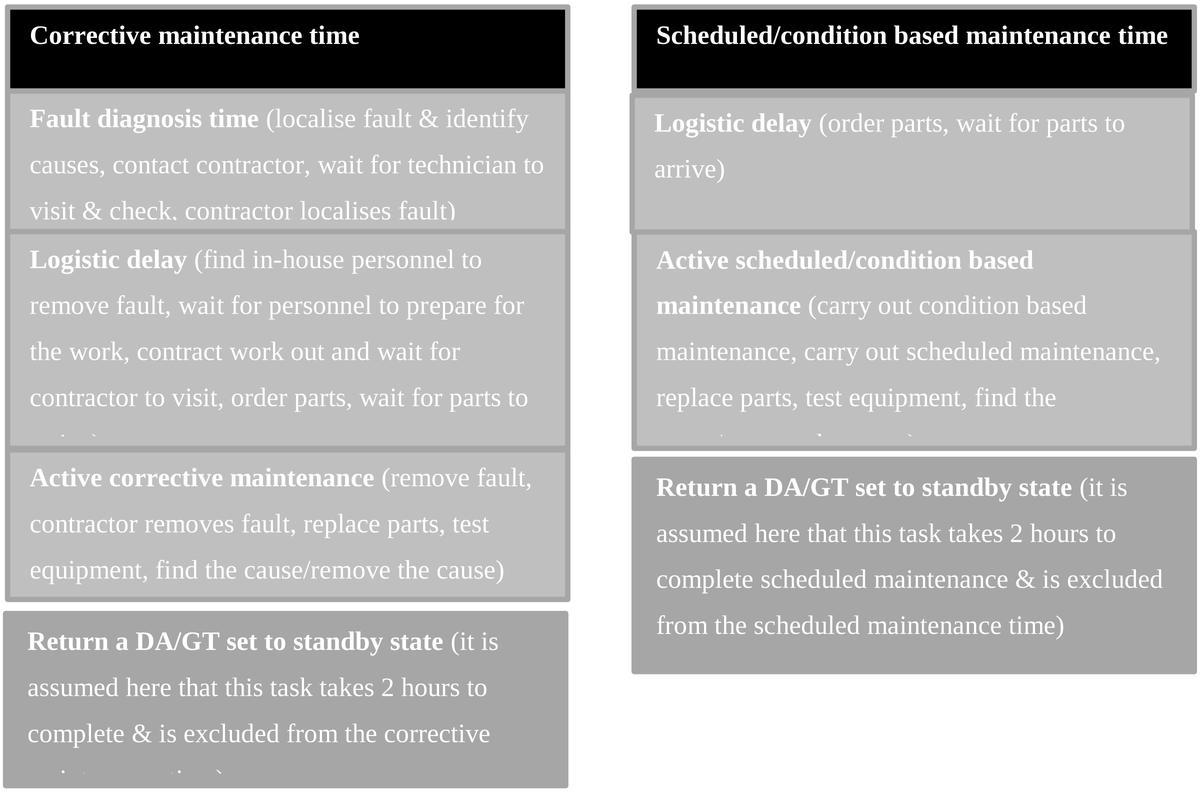
Figure B-3: Definition of corrective & preventive maintenance times ([adapted from (BSI, 1991)]

Appendix C **DA/GT set maintenance**

In order to ensure that the DA/GT sets will start and run when required, they are regularly tested and maintained. Also, if they fail, they are taken for corrective maintenance. Table C-1 below provides a brief description of these processes. Figure C-2 and Figure C-3 show how the tasks within these processes relate to each other. Figure C-1 defines maintenance times by referring to Figure C-2 and Figure C-3.

Table C-1: DA/GT set testing & maintenance strategy

Process	Description
Condition monitoring	Daily measurement and interpretation of data to indicate the degraded condition of an DA/GT set and the need for maintenance
Load testing	DA and GT sets are load tested regularly to eliminate problems related to underutilisation and to ensure that they will start and run when required. The procedures require that each DA set should be tested fortnightly for 2 hours. DA1 and DA2 should be tested one week with DA2 and DA4 tested the next week. GT sets are to be loaded tested fortnightly.
Scheduled maintenance: other (simplified)	It is carried out in accordance with a maintenance time schedule in order to reduce the probability of DA/GT set failure to start or run when the off-site power system is lost. The maintenance schedule depends on the manufacturer maintenance schedule and the Safety Case requirements. Scheduled maintenance tasks for DAs are carried out every: – 6 months (e.g. diesel engines, starting air compressor) – 12 months (e.g. diesel engines, alternator, alternator exciter) – 24 months (e.g. diesel engines, fuel oil supply system, cooling systems, starting air compressor) – 96 months (diesel engines) - carried out by the contractor The contractor carries out the scheduled maintenance for GT sets every 4 and 12 months.
Condition based maintenance	The maintenance that is carried out according to the need indicated by condition monitoring.
Corrective maintenance	It is carried out to remove faults identified during DA/GT set load testing.



Corrective maintenance time

Fault diagnosis time (localise fault & identify causes, contact contractor, wait for technician to visit & check, contractor localises fault)

Logistic delay (find in-house personnel to remove fault, wait for personnel to prepare for the work, contract work out and wait for contractor to visit, order parts, wait for parts to

Active corrective maintenance (remove fault, contractor removes fault, replace parts, test equipment, find the cause/remove the cause)

Return a DA/GT set to standby state (it is assumed here that this task takes 2 hours to complete & is excluded from the corrective

Scheduled/condition based maintenance time

Logistic delay (order parts, wait for parts to arrive)

Active scheduled/condition based maintenance (carry out condition based maintenance, carry out scheduled maintenance, replace parts, test equipment, find the

Return a DA/GT set to standby state (it is assumed here that this task takes 2 hours to complete scheduled maintenance & is excluded from the scheduled maintenance time)

Figure C-1: Maintenance times

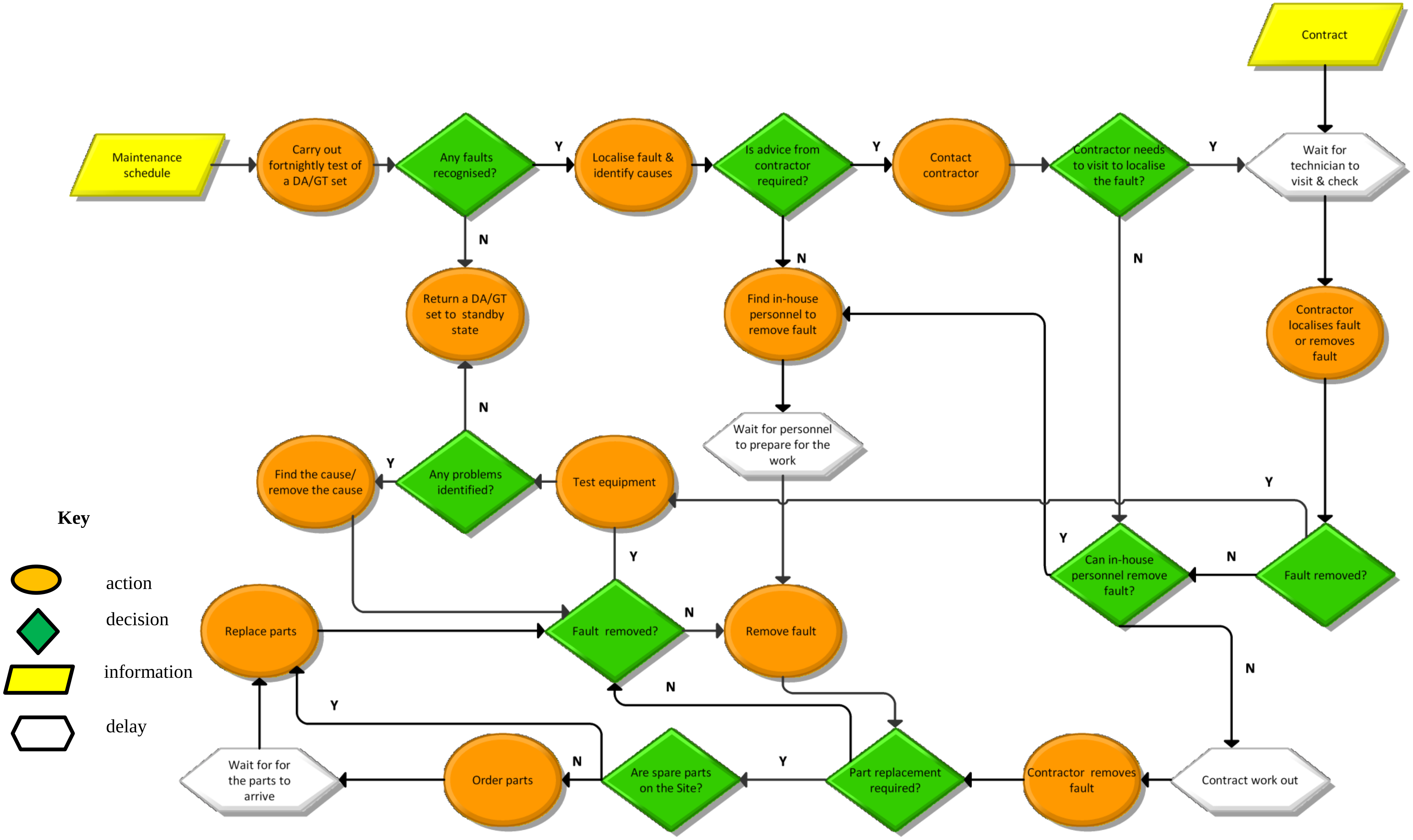

Contract
Maintenance schedule
Carry out fortnightly test of a DA/GT set
Any faults recognised?
Y
Localise fault & identify causes
Is advice from contractor required?
Y
Contact contractor
Contractor needs to visit to localise the fault?
Y
Wait for technician to visit & check
N
N
N
Return a DA/GT set to standby state
Find in-house personnel to remove fault
Contractor localises fault or removes fault
N
Wait for personnel to prepare for the work
Find the cause/ remove the cause
Y
Any problems identified?
Test equipment
Y
Y
Can in-house personnel remove fault?
N
Fault removed?
Key
action
decision
information
delay
Y
N
Replace parts
Fault removed?
Remove fault
N
N
Y
Y
N
Wait for for the parts to arrive
Order parts
Are spare parts on the Site?
Part replacement required?
Contractor removes fault
Contract work out

Figure C-2: DA/GT set load testing and corrective maintenance process

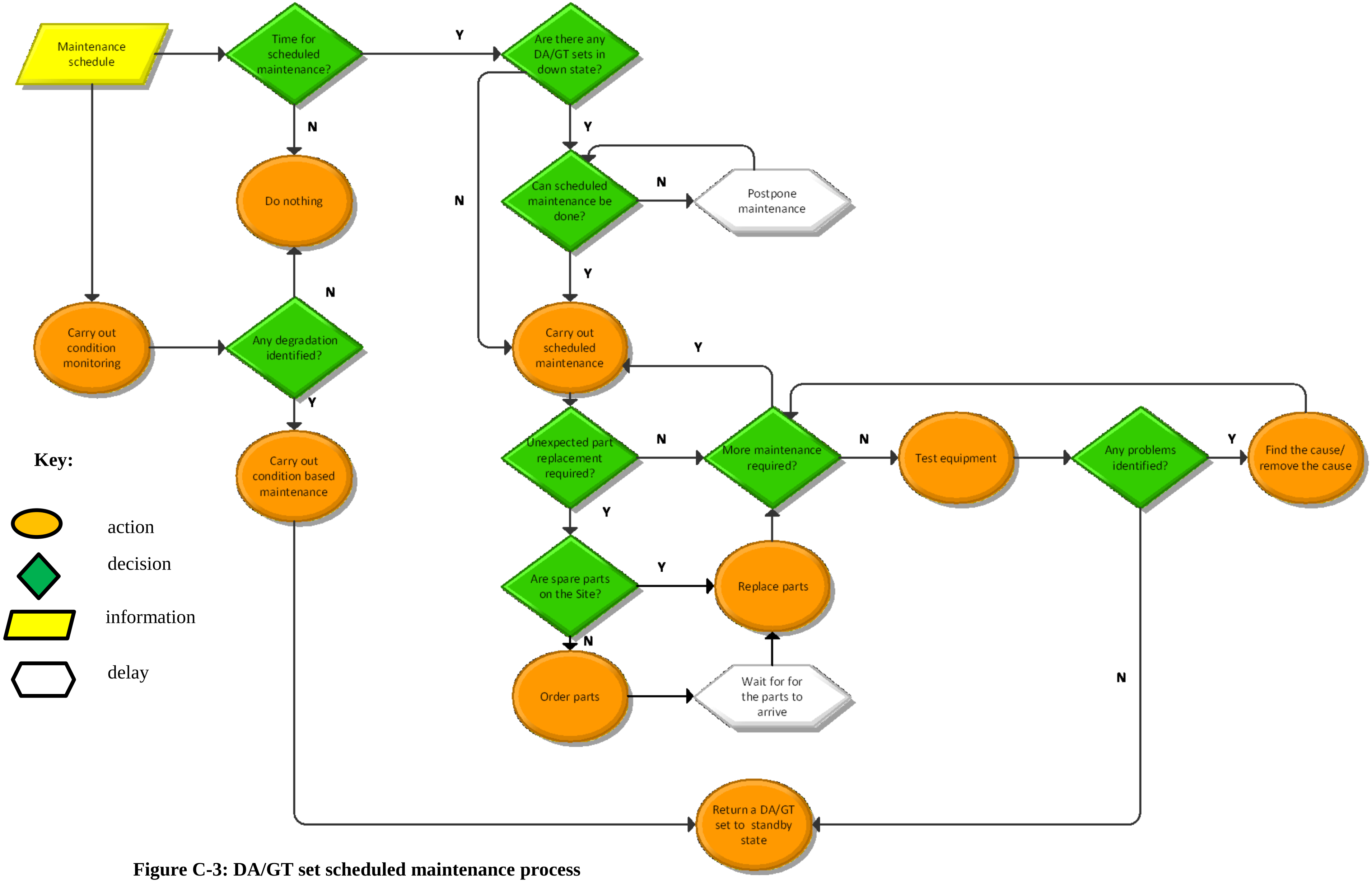

Maintenance schedule
Time for scheduled maintenance?
Y
Are there any DA/GT sets in down state?
N
Do nothing
N
Y
Can scheduled maintenance be done?
N
Postpone maintenance
Y
N
Carry out condition monitoring
Any degradation identified?
Y
Carry out scheduled maintenance
Y
Carry out condition based maintenance
Unexpected part replacement required?
N
More maintenance required?
N
Test equipment
Any problems identified?
Y
Find the cause/ remove the cause
Y
Are spare parts on the Site?
Y
Replace parts
N
Order parts
Wait for for the parts to arrive
N
Return a DA/GT set to standby state
Key:
action
decision
information
delay

Figure C-3: DA/GT set scheduled maintenance process

Appendix D **Omega factor approach**

The transition from the standby state to the latent failed state is represented in the model by the rate variable *latent fault development during the time between tests*. It is assumed that the transition occurs at a random time with a *probability of genset failure in small interval DT* that is equal to $\mathbf{1 - e^{-\lambda * DT}}$ (an exponential time to failure reliability model is assumed). The factors that influence this probability are shown in Figure 5-5 which is part of Sector 1 of the model.
If there are no undesired organisational influences then the rate λ is equal to the rate of inherent failures λ_I which is equivalent to the failure behaviour expected by the manufacturer and represents failure mechanisms that cannot be controlled by the plant. If there are some undesired organisational influences on the failure rate, then the rate λ will be bigger than λ_I. This new bigger rate can be shown to be a function of λ_I and the omega parameter (Mosleh et al., 1997).

The omega factor is defined as follows:

$\omega = \frac{\lambda_{SM}}{\lambda_I}$, where $\lambda_{SM} -$ rate of failures due to substandard maintenance

$$\text{thus } \lambda = \lambda_I + \omega\lambda_I$$

The omega factor can be represented as (Mohagdegh et al., 2009):

$\omega = \frac{N_{SM}}{N_I} = P * K = P_{SM} * P_B * K$

$$P = \frac{N_{SM}}{N_{Maint}} = P_{SM} * P_B$$

$$K = \frac{N_{Maint}}{N_I}$$

$where$

$N_{SM} - number\ of\ maintenance\ related\ failures$

$N_I - number\ of\ inherent\ failures$

$P -\ can\ be\ interepreted\ as\ probability\ that\ maintenance\ activities\ result\ in$
$a\ DA/GT\ set\ failure$

$N_{Maint} -\ number\ of\ maintenance\ activities\ performed\ on\ a\ DA/GT\ set$

$P_{SM} - can\ be\ interpreted\ as\ probability\ of\ substandard\ maintenance\ and\ estimated$

$$as\ \frac{N_{SubMain}}{N_{Maint}}$$

and $N_{SubMain}\ is\ the\ number\ of\ substandard\ maintenance\ activities$

$P_B - can\ be\ interpreted\ as\ probability\ that\ substandard\ maintenance\ will\ result\ in$
$a\ DA/GTsetfailure\ and\ estimated\ as\ \frac{N_{SM}}{N_{SubMain}}$

In addition, it can be shown that

$$\omega = \ P_{ASM\_DA\_GT\_set} * K'$$

$$K' = K * P_B = \ \frac{\omega_{DA\_GT\_set}}{P_{BSM\_DA\_GT\_set}}$$

$where$

$\omega_{DA\_GT\ set} = \frac{\lambda_{SM\_DA\_GT\_set}}{\lambda_{I\_DA\_GT\_set}} = \frac{N_{SM\_DA\_GT\_Set}}{N_{I\_DA\_GT\_set}}$ & $is\ the\ value\ of\ an\ omega\ factor\ for\ DA/GT\ sets$

$P_{ASM\_DA\_GT\_set} -$ is the actual probability of substandard maintenance for DA/GT sets estimated from the model of factors influencing quality of maintenance

$$P_{BSM\_DA\_GT\_sets} = \frac{N_{SubMainDA\_GT\_sets}}{N_{Maint\_DA\_GT\_sets}}$$

& $is\ the\ baseline\ probability\ of\ substandard\ maintenance\ for\ DA/GTsets$

K' is a constant factor and P_{ASM} can change over time as a result of changes in organisational factors over time.

To summarise, the failure rate λ is calculated as:

$$\lambda = \lambda_I + \lambda_{SM}$$

$$\lambda = \lambda_I + \omega\lambda_I$$

$$\lambda = \lambda_I + P_{ASM\_DA\ \_GT\_set}\ \ t\ \ * \frac{\omega_{DA\_GT\_set}}{P_{BSM\_DA\_GT\_set}} * \lambda_I, t - time$$

Appendix E **Rate of inherent DA/GT set failures**

Data related to the inherent DA/GT set failure rates was collected from (USNRC, 2007). Data related to Emergency Diesel Generators (EDGs) and Combustion Turbine Generators (CTGs) in the above mentioned report was obtained from the Equipment Performance and Information Exchange (EPIX) database, covering 1998 – 2002 and included 225 EDGs from 95 plants and 2 CTGs from one plant. The demands for EDGs to start per year ranged from approximately 12 – 50. The average for the data set was equal to 21.5 demands / year, which is equal to approximately 1 demand per 17 days. CTGs were demanded to start once per month.

The estimated mean value for EDG probability of failure to start on demand = 0.005
The estimated value for EDG probability of failure to load and run 1 hour = 0.003
The estimated mean value for CTG probability of failure to start on demand = 0.025
The estimated value for CTG probability of failure to load and run 1 hour = 0.002

P_{DA} (DA failure to start or load & run for 1 h during testing)
= 0.005 + (1-0.005)* 0.003 = **0.008**
Time between tests (DA) = 17 days

P_{GT} (failure to start or load & run for 1 h during testing)
= 0.025+ (1-0.025)* 0.002= **0.027**
Time between tests (GT) = 30 days

As the exponential time-to-failure model is used, the above probabilities were used to calculate the constant DA/GT set rate of inherent failures using the following formula:

$1 – e^{(-\lambda\text{*time between tests})} = P$

$\lambda = - (1/\text{time between tests})*\ln(1-P)$

The inherent failure rates for DA and GT sets are as follows:

$\lambda_{I\_DA} = 0.0005\ \text{day}^{-1}$

$\lambda_{I\_GT} = 0.001\ \text{day}^{-1}$

Appendix F **Key assumptions on the approach**

Key assumptions on the approach adopted in the SD analysis presented in Chapter 5 are summarized below:

- If there are two or more DA/GT sets waiting for PM, the one that has waited the longest is taken down for PM first.
- The general rule of thumb used by the plant personnel is to have no more than one DA/GT set not available for service.
- The set can be taken down for PM if:
    - It is the first in line (according to the PM schedule) to be taken down for PM. In other words, there are no other DA/GT sets that have been waiting longer to be taken down for PM.
    - It does not undergo corrective maintenance. If it does, then the active corrective maintenance needs to be finished first. Then, the DA/GT set can be taken down for PM if all other conditions are satisfied.
- Parts are always available for PM. If a failed state of a DA/GT set is detected during PM than the PM is finished first and then the set undergoes CM.
- Technicians always have enough time, i.e. as specified in the relevant procedures, to perform preventive maintenance tasks.
- If there is more than one DA/GT set waiting to undergo CM, the set with the highest capacity is dealt with first.
- Only one DA/GT set can undergo active CM at any time. If one DA/GT set is waiting for parts to be fitted then active corrective maintenance can be carried out on another DA/GT set.
- It is assumed that the transition from the standby state to the latent failed state occurs at a random time with a probability that latent fault develops in an interval DT that is equal to $\boldsymbol{1 - e^{-\lambda * DT}}$. If DA/GT set maintenance is of good quality then the rate $\boldsymbol{\lambda}$ is equal to constant rate of inherent failures $\boldsymbol{\lambda_I}$ (an exponential constant failure rate reliability model is assumed) which is equivalent to the rate expected by the manufacturer and represents failure mechanisms that cannot be controlled by the plant. If the maintenance activities are substandard, then the failure rate will be bigger than $\boldsymbol{\lambda_I}$. This new bigger rate can be shown to be a function of $\boldsymbol{\lambda_I}$ and the omega parameter (Mosleh et al., 1997). The omega factor is defined as follows:

$\omega = \frac{\lambda_{MF}}{\lambda_I}$, where $\lambda_{MF} -$ rate of failures due to substandard maintenance

$$\text{thus } \lambda = \lambda_I + \omega\lambda_I$$

In particular, it can be shown that: $\lambda = \lambda_I + P_{ASM\_DA\_GT\_set} \;\; t \;\; * \frac{\omega_{DA\_GT\_set}}{P_{BSM\_DA\_GT\_set}} * \lambda_I$

$\boldsymbol{t} -$ time

$\boldsymbol{\omega_{DA\_GT\ set}}$ – the omega factor for DA/GT sets

$\boldsymbol{P_{BSM\_DA\_GT\_set}} -$ baseline probability of substandard maintenance for DA/GT sets

$\boldsymbol{P_{ASM\_DA\_GT\_set}} -$ actual probability of substandard maintenance for DA/GT sets

Appendix D provides more details on how the above equation was derived. The rate of inherent failures λ_I for DA/GT sets was derived from the data provided in the NUREG/CR 6928 (USNRC, 2007) report (see Appendix E for more details). There is a lot of uncertainty associated with the omega parameter for DA/GT sets $(\omega_{DA\_GT\ set})$. The study of maintenance record databases from three British nuclear power stations (Morris et al., 1998) indicates that the ratio of failures due to substandard maintenance to inherent failures (N_{SM}/N_I) for various pieces of equipment including diesel generators could be as big as 7:1. In this initial study of the standby power system supporting the plant, the omega parameter for DA/GT sets is assumed to be equal to 2 $(\omega_{DA\_GT\ set} = 2)$.

Appendix G **Parameters used in the model**

The tables below present and describe model parameters (grouped according to the model sectors) and their values.

Table 0-1: Sector 1- model parameters explained

Sector 1: DA/GT set states & transition between states			
Parameter	**Dimension**	**Value**	**Description**
GT1 set capacity	MW	3.5	Capacity of GT1
GT1 set capacity	MW	5	Capacity of GT2
DA set capacity	MW	2	Capacity of DA

Table 0-2: Sector 2 - model parameters explained

Sector 2: Quality of maintenance			
Parameter	**Dimension**	**Value**	**Description**
λ_I	1/day	DA - 0.0005 GT - 0.001	Rate of inherent failures
$\omega_{DA/GT\ set}$	dimensionless	2	It is a ratio of failures due to substandard maintenance to inherent failures of DA/GT sets
P_{PG}	dimensionless	0.9	Degree to which quality of procedures can be described as "good".
P_{TE_PG}	dimensionless	0.9	Probability of substandard maintenance if technician makes an error and quality of procedures is "good".
P_{TE_PP}	dimensionless	0.99	Probability of substandard maintenance if technician makes an error and quality of procedures is "poor".
P_{NTE_PG}	dimensionless	0.001	Probability of substandard maintenance if technician doesn't make an error and quality of procedures is "good".
P_{NTE_PP}	dimensionless	0.9	Probability of substandard maintenance if technician doesn't make an error and quality of procedures is "poor".
Beta factor	dimensionless	0.1	Probability that the cause of a DA failure will be shared by additional DA, given that a specific DA has failed. This applies to DAs that are tested together, i.e. DA1 & DA3 and DA2 & DA4.
Time between tests	day	14	Time between load testing activities.
Active PM time	Day	1 (DA: 6M, 12M, 24M PM)	Average time to carry out active scheduled maintenance. The variability is very small and was ignored. DA sets undergo 6-monthly (6M), 12-monthly (12M), 24-

Sector 2: Quality of maintenance			
Parameter	**Dimension**	**Value**	**Description**
		1 (GT 4M & 12M PM) 10 (DA3: 96M PM)	monthly (24M) and 96-monthly (96M) PM. Different tasks are done during each type of maintenance. GT sets undergo 4-monthly (4M) and 12-monthly (12M) PM. Different tasks are done during each type of maintenance.

Active CM time	day	Lognormal distribution:
		Mean= 0.25
		St. dev. = 0.25
		Min = 0.125
			Time to carry out active corrective maintenance for DA/GT sets

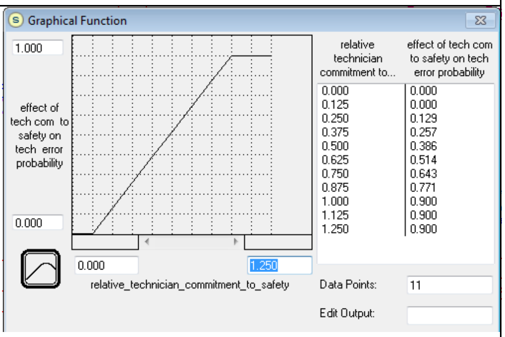
Time to organise resources	day	Lognormal distribution:
		Mean= 0.5
		St. dev. = 0.5
		Min = 0.125
			Time to diagnose fault and find staff in-house to carry out DA/GT set corrective maintenance or contract CM out.

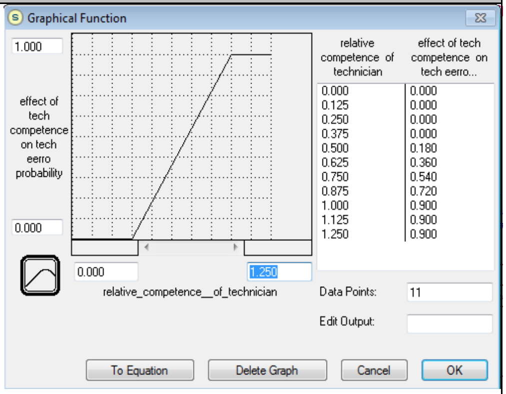
Time to wait for parts	day	Lognormal distribution:
		Mean = 1
		St. dev. = 0.75
		Min = 1
			Time to order and wait for the parts to arrive.

Probability that parts are not available	dimensionless	0.1	Probability that spare parts are not available when needed.
Testing dates	day	DA1 & DA3 - Starts at day 3 & then every 14 days DA2 & DA4 – starts at 10 and then every 14 days GT1 starts at 4 & then every 14 days GT2 starts at 11 & then every 14 days	Times when DA/GT load testing is carried out.

Sector 2: Quality of maintenance			
Parameter	**Dimension**	**Value**	**Description**
PM schedule	day	See Figure G-1 below	DA sets undergo 6-monthly (6M), 12-monthly (12M), 24-monthly (24M) and 96-monthly (96M) PM. Different tasks are done during each type of maintenance. GT sets undergo 4-monthly (4M) and 12-monthy (12M) PM. Different tasks are done during each type of maintenance.

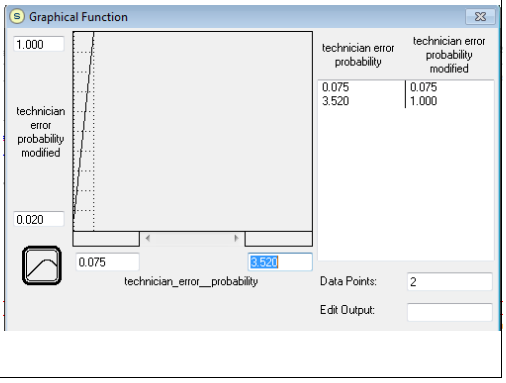
Table 0-3: Sector 3 - model parameters explained

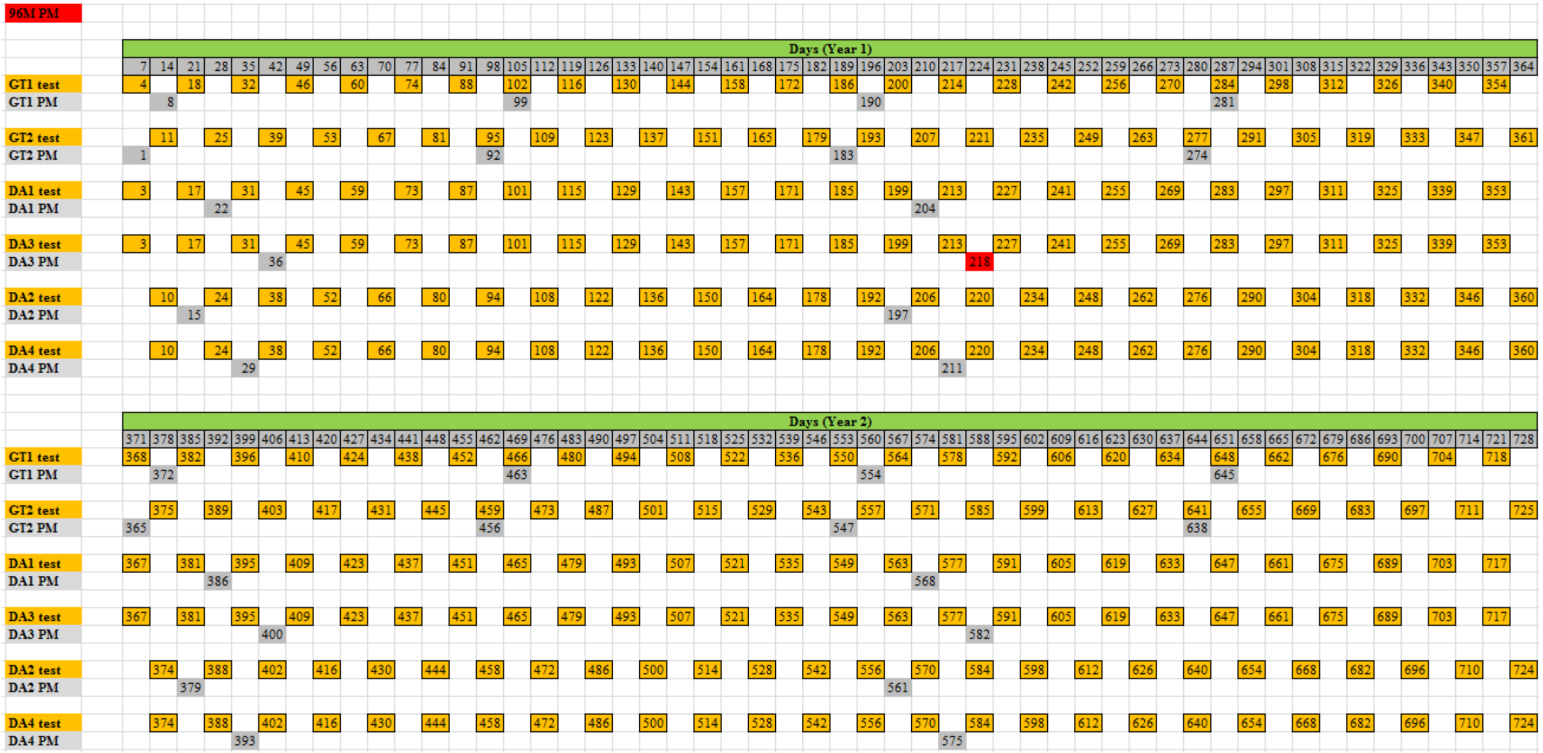
Sector 3: Technician & management behaviour over time			
Parameter	**Dimension**	**Value**	**Description**
Basic technician error probability	dimensionless	0.02	The probability of technician error during preventive maintenance.
Maximum effect of technician lack of competence on technician error probability	dimensionless	8	Maximum amount by which the probability of technician error is to be multiplied if the level of technician competence is low.
Maximum effect of low technician commitment to safety on technician error probability	dimensionless	2	Maximum amount by which the probability of technician error is to be multiplied if the level of technician commitment to safety & quality is low
Maximum effect of time pressure on technician error probability	dimensionless	11	Maximum amount by which the probability of technician error is to be multiplied if there is time pressure
Effect of time pressure on technician error probability	dimensionless	0.1	It is assumed that effect of time pressure is minimal.
Effect of relative technician commitment to safety & quality on technician error probability	dimensionless	graphical function	 Graphical Function 1.000 effect of tech com to safety on tech error probability 0.000 0.000 1.250 relative_technician_commitment_to_safety relative technician commitment to... / effect of tech com to safety on tech error probability 0.000 / 0.000 0.125 / 0.000 0.250 / 0.129 0.375 / 0.257 0.500 / 0.386 0.625 / 0.514 0.750 / 0.643 0.875 / 0.771 1.000 / 0.900 1.125 / 0.900 1.250 / 0.900 Data Points: 11 Edit Output:
Effect of technician competence on technician error probability	dimensionless	graphical function	

Sector 3: Technician & management behaviour over time			
Parameter	**Dimension**	**Value**	**Description**
			 Graphical Function 1.000 effect of tech competence on tech eerro probability 0.000 0.000 1.250 relative_competence__of_technician To Equation Delete Graph Cancel OK relative competence of technician / effect of tech competence on tech eerro... 0.000 / 0.000 0.125 / 0.000 0.250 / 0.000 0.375 / 0.000 0.500 / 0.180 0.625 / 0.360 0.750 / 0.540 0.875 / 0.720 1.000 / 0.900 1.125 / 0.900 1.250 / 0.900 Data Points: 11 Edit Output:
Reference technician commitment to safety & quality	dimensionless	0.8	Technician commitment to safety that is considered normal or it is desired.
Initial/Maximum/Minimum technician commitment to safety & quality	dimensionless	0.8/1/0.1	Maximum/minimum/initial technician commitment to safety & quality
Time to change technician commitment to safety & quality	day	91	Average time needed for technician commitment to safety & quality to change
Technician perception adjustment time	day	91	Average time needed for technicians to change their perception of relative management commitment to safety & quality
Reference technician competence	day	70	Level of competence that is considered normal. Here it is equal to the target competence level.
Target technician competence	day	70	Required level of technician competence
Fractional competence decay rate	1/day	0.0003	Rate at which technicians forget what they have learnt about DA/GT set & associated procedures
Time to provide training	day	91	Average time required to organise & deliver training
Reference management commitment to safety & quality	dimensionless	0.8	Management commitment to safety & quality that is considered normal or is desired
Initial/Maximum/ Minimum management commitment to safety	dimensionless	0.8/1/0.1	Maximum/minimum/initial management commitment to safety & quality
Time to change management commitment to safety & quality	day	91	Average time needed for management commitment to safety & quality to change
Management learning exponent	dimensionless	0.4	Part of the learning curve model that was

Sector 3: Technician & management behaviour over time

Parameter	**Dimension**	**Value**	**Description**
			used to model the impact of management perception of technician error probability on target management commitment to safety. The value of exponent equal to 0.4 is equivalent to around 30% change in management commitment to safety per doubling of management perception of technician error probability.
Ability to recognise technician errors	dimensionless	0.6	Management's ability to recognise that technicians do not carry out DA/GT set preventive maintenance according to the standards expressed in the relevant procedures.
Reference technician error probability	dimensionless	Equal to initial technician error probability	Initial technician error probability
Technician error probability indicator	dimensionless	function	Output of the NARA approach that estimates the impact of time pressure, technician commitment to safety & quality and technician competence on the basic technician error probability.

Technician error probability	dimensionless	graphical function
		min = 0.02
		max = 1
			Transformed technician error probability indicator
			
			Graphical Function
			technician error probability modified: 1.000 – 0.020
			technician_error__probability: 0.075 – 3.520
			technician error probability / technician error probability modified
			0.075 / 0.075
			3.520 / 1.000
			Data Points: 2
			Edit Output:



96M PM

	Days (Year 1)																									
	7	14	21	28	35	42	49	56	63	70	77	84	91	98	105	112	119	126	133	140	147	154	161	168	175	182
GT1 test	4		18		32		46		60		74		88		102		116		130		144		158		172	
GT1 PM		8													99											
GT2 test		11		25		39		53		67		81		95		109		123		137		151		165		179
GT2 PM	1													92												
DA1 test	3		17		31		45		59		73		87		101		115		129		143		157		171	
DA1 PM				22																						
DA3 test	3		17		31		45		59		73		87		101		115		129		143		157		171	
DA3 PM						36																				
DA2 test		10		24		38		52		66		80		94		108		122		136		150		164		178
DA2 PM			15																							
DA4 test		10		24		38		52		66		80		94		108		122		136		150		164		178
DA4 PM					29																					

	Days (Year 1)																									
	189	196	203	210	217	224	231	238	245	252	259	266	273	280	287	294	301	308	315	322	329	336	343	350	357	364
GT1 test	186		200		214		228		242		256		270		284		298		312		326		340		354	
GT1 PM		190													281											
GT2 test		193		207		221		235		249		263		277		291		305		319		333		347		361
GT2 PM	183													274												
DA1 test	185		199		213		227		241		255		269		283		297		311		325		339		353	
DA1 PM				204																						
DA3 test	185		199		213		227		241		255		269		283		297		311		325		339		353	
DA3 PM						218																				
DA2 test		192		206		220		234		248		262		276		290		304		318		332		346		360
DA2 PM			197																							
DA4 test		192		206		220		234		248		262		276		290		304		318		332		346		360
DA4 PM					211																					

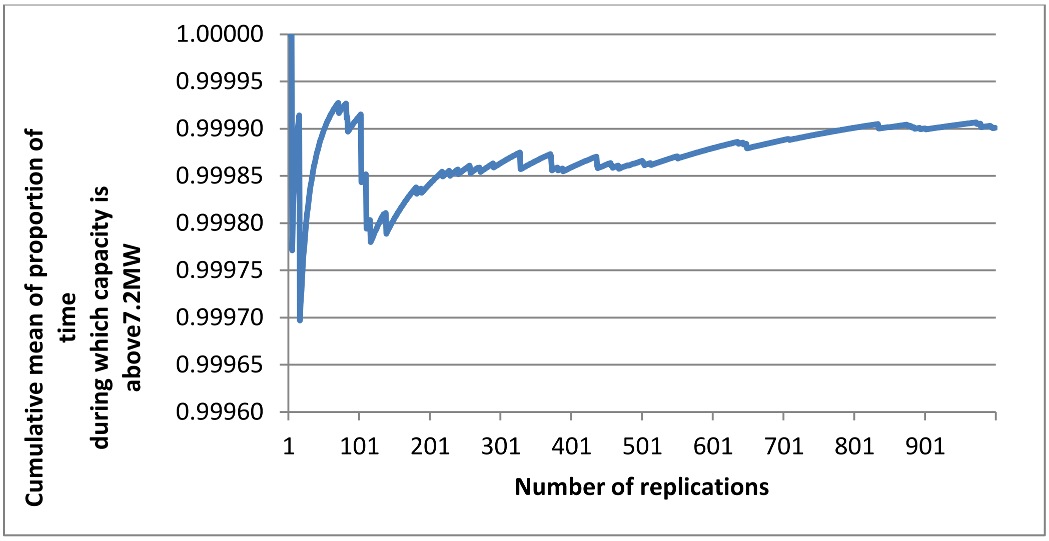
	Days (Year 2)																									
	371	378	385	392	399	406	413	420	427	434	441	448	455	462	469	476	483	490	497	504	511	518	525	532	539	546
GT1 test	368		382		396		410		424		438		452		466		480		494		508		522		536	
GT1 PM		372													463											
GT2 test		375		389		403		417		431		445		459		473		487		501		515		529		543
GT2 PM	365													456												
DA1 test	367		381		395		409		423		437		451		465		479		493		507		521		535	
DA1 PM				386																						
DA3 test	367		381		395		409		423		437		451		465		479		493		507		521		535	
DA3 PM						400																				
DA2 test		374		388		402		416		430		444		458		472		486		500		514		528		542
DA2 PM			379																							
DA4 test		374		388		402		416		430		444		458		472		486		500		514		528		542
DA4 PM					393																					

	Days (Year 2)																									
	553	560	567	574	581	588	595	602	609	616	623	630	637	644	651	658	665	672	679	686	693	700	707	714	721	728
GT1 test	550		564		578		592		606		620		634		648		662		676		690		704		718	
GT1 PM		554													645											
GT2 test		557		571		585		599		613		627		641		655		669		683		697		711		725
GT2 PM	547													638												
DA1 test	549		563		577		591		605		619		633		647		661		675		689		703		717	
DA1 PM				568																						
DA3 test	549		563		577		591		605		619		633		647		661		675		689		703		717	
DA3 PM						582																				
DA2 test		556		570		584		598		612		626		640		654		668		682		696		710		724
DA2 PM			561																							
DA4 test		556		570		584		598		612		626		640		654		668		682		696		710		724
DA4 PM					575																					

Figure G-1: PM schedule

Appendix H **Number of simulation runs**

A graphical approach was used to determine the minimum number of replications needed to obtain a better estimate of the system mean performance (Robinson, 2004). The graphical approach involves plotting the cumulative mean of the model output data for a series of replications. The minimum number of replications required is defined by the point at which the line becomes flat. Performing more replications will give a marginal improvement in the estimate of the mean value. The figure below shows the cumulative mean data for the model output (fraction of time during which the standby power system capacity is below 7.2MW).



The line becomes flat around 800 replications, which is the minimum number recommended. However, because there is some variation in the line beyond 800 replications, a conservative estimate of 1000 replications was made.

Appendix I **Statistical analysis of simulation data**

Section A

These experiments (Experiments 2 & 3) were conducted to investigate the impact of maintenance related failures and logistic delays on the standby power system capacity. Each experiment involved running the model 1000 times and each run simulated 728 consecutive days during which DA/GT sets are in a standby mode. These two experiments are described below:

- Experiment 2 - impact of maintenance related failures was removed from the base case simulation model & simulation was rerun
- Experiment 3 - impact of logistic delays was removed from the base case simulation model & simulation was rerun

The distributions of the fractions of time during which the standby power system capacity is below 7.2MW obtained from the comparative runs were investigated using histograms. The results were not normally distributed. However, the sample sizes were big (i.e. 1000) and the violation of this assumption should not cause any major problems.

To investigate the statistical significance of the differences in proportion between Experiments 2 & 3 and Experiment 1, an independent samples t-test was used. The results of comparing Experiment 1 and Experiment 2 are presented below and followed by the results of comparing Experiment 1 and Experiment 3.

Experiment 1 and **Experiment 2**

Group Statistics

	Experiment	N	Mean	Std. Deviation	Std. Error Mean
Capacity_7_MW	1	1000	.00011	.00065	.00002
	2	1000	.00001	.00013	.00000

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	T
Capacity_7_MW	Equal variances assumed	103.720	.000	5.104
	Equal variances not assumed			5.104

Independent Samples Test

		t-test for Equality of Means		
		df	Sig. (2-tailed)	Mean Differenc e
Capacity_7_MW	Equal variances assumed	1998	.0000004	.0001071
	Equal variances not assumed	1077.201	.0000004	.0001071

Independent Samples Test

		t-test for Equality of Means		
		Std. Error Difference	95% Confidence Interval of the Difference	
			Lower	Upper
Capacity_7_MW	Equal variances assumed	.0000210	.0000660	.0001483
	Equal variances not assumed	.0000210	.0000660	.0001483

Levene's test for equality of variance is significant ($p < 0.05$), so equal variances in two data sets were not assumed. Test for equality of means is significant ($p < 0.05$). Thus, there is a significant difference in the mean proportion of time during which the standby power system capacity is below the level of 7.2MW between the comparative runs.

Experiment 1 and **Experiment 3**

Group Statistics

	Experiment	N	Mean	Std. Deviation	Std. Error Mean
Capacity_7_MW	1	1000	.000115	.000651	.000021
	3	1000	.000061	.000403	.000013

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	T
Capacity_7_MW	Equal variances assumed	18.825	.000	2.219
	Equal variances not assumed			2.219

Independent Samples Test

		t-test for Equality of Means		
		df	Sig. (2-tailed)	Mean Difference
Capacity_7_MW	Equal variances assumed	1998	.027	.0000537
	Equal variances not assumed	1667.106	.027	.0000537

Independent Samples Test

		t-test for Equality of Means		
		Std. Error Difference	95% Confidence Interval of the Difference	
			Lower	Upper
Capacity_7_MW	Equal variances assumed	.0000242	.0000062	.0001012
	Equal variances not assumed	.0000242	.0000062	.0001012

Levene's test for equality of variance is significant ($p < 0.05$), so equal variances in two data sets were not assumed. The test for equality of means is significant ($p < 0.05$). Thus, there is a statistically significant difference in the mean proportion of time during which the standby power system capacity is below the level of 7.2MW between the comparative runs.

Section B

Sensitivity analysis – part B

The distributions of the fractions of time during which the standby power system capacity is below 7.2MW obtained from the comparative runs were investigated using histograms. The results were not normally distributed. However, the sample sizes were big (i.e. 1000) and the violation of this assumption should not cause any major problems.

To investigate the statistical significance of the differences in proportion between Experiments 2 & 3 and Experiment 1, an independent samples t-test was used. The results of comparing Experiment 1 and Experiment 2 are presented below and followed by the results of comparing Experiment 1 and Experiment 3.

Experiment 1 and Experiment 2

Group Statistics

	Experiment	N	Mean	Std. Deviation	Std. Error Mean
Capacity_7_MW	1	1000	.000035	.000368	.000012
	2	1000	.000007	.000129	.000004

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	T
Capacity_7_MW	Equal variances assumed	20.113	.000	2.254
	Equal variances not assumed			2.254

Independent Samples Test

		t-test for Equality of Means		
		df	Sig. (2-tailed)	Mean Difference
Capacity_7_MW	Equal variances assumed	1998	.024	.0000278
	Equal variances not assumed	1240.044	.024	.0000278

Independent Samples Test

		t-test for Equality of Means		
		Std. Error Difference	95% Confidence Interval of the Difference	
			Lower	Upper
Capacity_7_MW	Equal variances assumed	.0000123	.0000036	.0000520
	Equal variances not assumed	.0000123	.0000036	.0000520

Levene's test for equality of variance is significant ($p < 0.05$), so equal variances in two data sets were not assumed. Test for equality of means is significant ($p <0.05$).

Thus, there is statistically significant difference in means between the comparative runs.

Experiment 1 and **Experiment 3**

Group Statistics

	Experiment	N	Mean	Std. Deviation	Std. Error Mean
Capacity_7_MW	1	1000	.0000352	.0003684	.0000117
	3	1000	.0000225	.0002701	.0000085

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	T
Capacity_7_MW	Equal variances assumed	3.051	.081	.880
	Equal variances not assumed			.880

Independent Samples Test

		t-test for Equality of Means		
		df	Sig. (2-tailed)	Mean Difference
Capacity_7_MW	Equal variances assumed	1998	.379	.000013
	Equal variances not assumed	1832.186	.379	.000013

Independent Samples Test

	t-test for Equality of Means	
	Std. Error Difference	95% Confidence Interval of the Difference

			Lower	Upper
Capacity_7_MW	Equal variances assumed	.000014	-.000016	.000041
	Equal variances not assumed	.000014	-.000016	.000041

Levene's test for equality of variance is not significant (p > 0.05), so equal variances in two data sets were assumed. Test for equality of means is not significant (p > 0.05). Thus, there is statistically no significant difference in means between the comparative runs.

Appendix J **ECFA+ analysis**

Table 0-4: ECFA+ analysis – evidence supporting events, conditions & relationships in the chart

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
E1: Train climbs over switch rails at Lambrigg 2B points at 20:12 & derails on 23/02/07	"The left-hand wheels of either the first or second bogie on the leading vehicle (it is not clear which) passed the wrong side of the left-hand switch rail and were forced into the reducing width between the switch rails. The wheels then derailed by climbing over the rails. All the other vehicles of the train derailed as a consequence" (9/13) See also: 23/80 53/161 126/512 136/538-539
E2: Train passes over Lambrigg 2B points at 20:12 on 23/02/07	"On 23 February 2007 at 20:12 hrs, an express passenger train derailed at facing points, known as Lambrigg 2B points, located near Grayrigg in Cumbria." See also 9/13 126/512
Arrow between E2 & E1	"The train derailed as it passed over 2B points which were in an unsafe state." (9/13)
C1: Reduced space between left-hand switch & lefts-hand stock rail at Lambrigg 2B points at 20:12 on 23/02/07	"Vibration from the wheelsets of either train 1S83 or the preceding train, the loss of restraint from the stretcher bars, its natural flexure, and the effect of gravity on the canted track, allowed the left-hand switch rail to close to within 22 mm of its adjacent stock rail" (53/161) "The left-hand wheels of either the first or second bogie on the leading vehicle (it is not clear which) passed the wrong side of the left-hand switch rail and were forced into the reducing width between the switch rails. The wheels then derailed by climbing over the rails. All the other vehicles of the train derailed as a consequence" (9/13)
Arrow between C1 & E1	"(…) the switch rail closed sufficiently to allow more than one of the train's wheelsets to run into the narrowing track gauge between the two switch rails, as evidenced by the bruise on the toe of the left-hand switch rail (paragraph 113). These wheels then derailed by flange climb over the heads of the switch rails (…).

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
	(53/161)
E3: Left-hand switch rail moves towards left-hand stock rail at Lambrigg 2B by 20:12 on 23/02/07	"The movement of the left-hand switch, which initiated the gauge narrowing, occurred either under the preceding train or under the leading bogie of the train without derailment." (136/539)
Arrow between E3 & C1	"The movement of the left-hand switch, which initiated the gauge narrowing, occurred either under the preceding train or under the leading bogie of the train without derailment." (136/539)
C2: Vibration of the switch rails by 20:12 on 23/02/07	Vibration from the wheelsets of either train 1S83 or the preceding train, the loss of restraint from the stretcher bars, its natural flexure, and the effect of gravity on the canted track, allowed the left-hand switch rail to close to within 22 mm of its adjacent stock rail" (53/161)
Arrow between E2 & C2	Vibration from the wheelsets of **either train 1S83** **or the preceding train,** the loss of restraint from the stretcher bars, its natural flexure, and the effect of gravity on the canted track, allowed the left-hand switch rail to close to within 22 mm of its adjacent stock rail" (53/161)
C3: Left-hand switch rail not restrained by the stretcher bars at Lambrigg 2B points by 23/02/07	"The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, the left-hand switch rail was struck by the inner faces of passing train wheels, giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. **This led to the left-hand switch rail becoming totally unrestrained." (9/15)**
Arrow between C3 & E3	Vibration from the wheelsets of either train 1S83 or the preceding train, **the loss of restraint from the stretcher bars**, its natural flexure, and the effect of gravity on the canted track, allowed the left-hand switch rail to close to within 22 mm of its adjacent stock rail" (53/161)
E4: 2nd PW, 1ST PW & lock stretcher barrs & their fasteners rapidly deteriorate by 23/02/07	"The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, the left-hand switch rail was struck by the inner faces of passing train

Event/condition/arrow	Evidence (Page/paragraph in the 2011 RAIB report)
	wheels, giving rise to large cyclic forces. As a consequence, **rapid deterioration of the condition of the remaining stretcher bars** **and** **their fasteners occurred.** This led to the left-hand switch rail becoming totally unrestrained.**”** (9/15) “2nd Permanent Way stretcher bar joints had failed and was missing by 21 February 2007” (124/Table 6) “Failure of 1st Permanent Way stretcher bar and lock stretcher bar between 21 February 2007 and 23 February 2007” (124/Table 6) See also: 13/28 52/160 56/174 57/180 127/513, 515
Arrow between E4 & C3	“The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, the left-hand switch rail was struck by the inner faces of passing train wheels, giving rise to large cyclic forces. As a consequence, **rapid deterioration of the condition of the remaining stretcher bars** **and** **their fasteners occurred.** **This led to the left-hand switch rail becoming totally unrestrained.” (9/15)**
E5: Passing trains strike left-hand switch rail at Lambrigg 2B points after sometime between 7-12/02/07	“flange-back contact” “The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, **the left-hand switch rail was struck by the inner faces of passing train wheels,** giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars

Event/condition/arrow	Evidence (Page/paragraph in the 2011 RAIB report)
	and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15) “The setting of the escapement joint to give a residual switch opening of between 7 and 10 mm (this was greater than the nominally specified value of 1.5 mm), **allowed the flange-back contact by most wheelsets on the left-hand switch rail to occur** **once the third permanent way stretcher bar right-hand bracket to switch rail joint had failed**, increasing the forces seen by the remaining stretcher bars and causing the subsequent collapse of the points system. The excessive residual switch opening was a causal factor of the accident.” (127/515) “3rd Permanent Way stretcher bar right-hand bracket joint failed after 7 January 2007 and on or before 12 February 2007” (123/Table 6) See also: 13/27 45/139 51/154 51/156 52/160 57/180 79/284
Arrow between E5&E4	“The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, **the left-hand switch rail was struck by the inner faces of passing train wheels,** **giving rise to large cyclic forces.** **As a consequence,** **rapid deterioration of the condition of the remaining stretcher bars** **and** **their fasteners occurred.**

Event/condition/arrow	Evidence (Page/paragraph in the 2011 RAIB report)
	This led to the left-hand switch rail becoming totally unrestrained." (9/15)
E6: Fasteners of the joint between 3rd PW stretcher bar & right-hand switch rail fail between 7/01-12/02/07	"**The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose**, and subsequently completely undone. As a result of this, and the excessive residual switch opening, the left-hand switch rail was struck by the inner faces of passing train wheels, giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained." (9/15) "Fasteners - Collective name for the bolts, washers and lock nuts used to secure the stretcher bar components." (page 195) "3rd Permanent Way stretcher bar right-hand bracket joint failed after 7 January 2007 and on or before 12 February 2007" (123/Table 6) See also: 9/14 13/25 45/136-137 45/139 51/155 56/175 57/182 67/226 70/237 78/280 127/514

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
Arrow between E6 & E5	“**The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose**, and subsequently completely undone. **As a result of this**, and the excessive residual switch opening, **the left-hand switch rail was struck by the inner faces of passing train wheels,** **giving rise to large cyclic forces.** As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15)
C4: Excessive residual switch opening present since renewal of points in 2001 (?)	“The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and **the excessive residual switch opening,** the left-hand switch rail was struck by the inner faces of passing train wheels, giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15) “Residual switch opening - the gap between the rail heads of adjacent switch and stock rails on the closed side of points.” (page 200) “The residual switch opening measured at the right-hand switch rail at the time of the accident **was probably the value set when the half-switches were renewed in 2001.** The records from the *Omnicom* train showed that in 2004 the value of the residual switch opening was already in excess of 1.5 mm. The residual switch opening of the right-hand switch rail was not deliberately changed over this period.” (79/285) See also:

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
	9/14 57/182 127/515 incorrect set up of the points with excessive *residual switch opening*
Arrow between C4&E5	“The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. **As a result of this,** **and** **the excessive residual switch opening,** **the left-hand switch rail was struck by the inner faces of passing train wheels,** **giving rise to large cyclic forces.** As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15)
E7:Trains pass over Lambrigg 2B between12-23/02/07	“The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, **the left-hand switch rail was struck by the inner faces of passing train wheels,** giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15)
Arrow from E7 to E5	The bolts holding the third permanent way stretcher bar to the right-hand switch rail became loose, and subsequently completely undone. As a result of this, and the excessive residual switch opening, **the left-hand switch rail was struck by the inner faces of passing train wheels,** giving rise to large cyclic forces. As a consequence, rapid deterioration of the condition of the remaining stretcher bars and their fasteners occurred. This led to the left-hand switch rail becoming totally unrestrained.” (9/15)

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
C8: No action taken by NR to repair 3rd PW stretcher bar between 18 -23/02/07	"A supervisor carrying out a scheduled basic visual inspection of the track on Sunday 18 February 2007 did not include 2B points. He had originally only intended to carry out a supervisory inspection, but then agreed, on 12 February 2007, the Monday preceding the inspection, also to perform the basic visual inspection, which extended further north to include the points. **During the week he forgot that he had agreed to extend his inspection** **to cover the extra length.** **As a result, the opportunity for a basic visual inspection to discover the degraded points, and for remedial action to be taken was lost."** (14/29)
An arrow from C8 to E4	"The April 2006 SMS PF01, clause 2.8, required that 'Should any cracked or broken bars or brackets be found, the signaller must be informed immediately and a 20 mph emergency speed restriction shall be imposed for up to 36 hours, providing all nuts were secure and tight. If these conditions cannot be met or if it is considered unsafe, blocked (sic!) the line." (226/7)
C9: Track section manager does not detect degraded state of 3rd PW stretcher bar on 18/02/07	"The deterioration in the condition of the third permanent way stretcher bar and its joint, and possibly some aspects of the deterioration of the second permanent way stretcher bar, should have been visible to a basic visual inspection on 18 February 2007, had it passed 2B points. The omission of the basic visual inspection of 2B points on 18 February 2007 was a causal factor." (127/516) **See also:** 9/14 14/29
Arrow from C9 to C8	"**The deterioration in**

Event/condition/arrow	**Evidence** **(Page/paragraph in the 2011 RAIB report)**
	the condition of the third permanent way stretcher bar and its joint, **and possibly** **some aspects of the deterioration of the second permanent way stretcher bar,** **should have been visible to a basic visual inspection on 18 February 2007,** had it passed 2B points. The omission of the basic visual inspection of 2B points on 18 February 2007 was a causal factor.” (127/516) “A supervisor carrying out a scheduled basic visual inspection of the track on Sunday 18 February 2007 did not include 2B points. He had originally only intended to carry out a supervisory inspection, but then agreed, on 12 February 2007, the Monday preceding the inspection, also to perform the basic visual inspection, which extended further north to include the points. During the week he forgot that he had agreed to extend his inspection to cover the extra length. **As a result, the opportunity for a basic visual inspection to discover the degraded points, and for remedial action to be taken was lost.”** (14/29)
E8: Track manager does not perform basic visual inspection on 18/02/07	“A supervisor carrying out a scheduled basic visual inspection of the track on Sunday 18 February 2007 did not include 2B points. He had originally only intended to carry out a supervisory inspection, but then agreed, on 12 February 2007, the Monday preceding the inspection, also to perform the basic visual inspection, which extended further north to include the points. During the week he forgot that he had agreed to extend his inspection to cover the extra length. As a result, the opportunity for a basic visual inspection to discover the degraded points, and for remedial action to be taken was

Event/condition/arrow	Evidence (Page/paragraph in the 2011 RAIB report)
	lost.” (14/29) 45/136 67/227 68/230 72/247 127/516 128/517 70/239 71/246 72/247
Arrow from E8 to C9	“A supervisor carrying out a scheduled basic visual inspection of the track on Sunday 18 February 2007 did not include 2B points. He had originally only intended to carry out a supervisory inspection, but then agreed, on 12 February 2007, the Monday preceding the inspection, also to perform the basic visual inspection, which extended further north to include the points. **During the week he forgot that he had agreed to extend his inspection to cover the extra length.** **As a result, the opportunity for a basic visual inspection to discover the degraded points, and for remedial action to be taken was lost.”** (14/29)