A Review of Accident Modelling Approaches for Complex Socio-Technical Systems

Zahid H. Qureshi

Defence and Systems Institute
University of South Australia
Mawson Lakes Campus, Mawson Lakes 5095, South Australia

zahid.qureshi@unisa.edu.au

Abstract

The increasing complexity in highly technological systems such as aviation, maritime, air traffic control, telecommunications, nuclear power plants, space missions, chemical and petroleum industry, and healthcare and patient safety is leading to potentially disastrous failure modes and new kinds of safety issues. Traditional accident modelling approaches are not adequate to analyse accidents that occur in modern socio-technical systems, where accident causation is not the result of an individual component failure or human error. This paper provides a review of key traditional accident modelling approaches and their limitations, and describes new system-theoretic approaches to the modelling and analysis of accidents in safety-critical systems. This paper also discusses the application of formal methods to accident modelling and organisational theories on safety and accident analysis.

Keywords: accident analyses, safety-critical, socio-technical systems, systems theory, sociological analysis, organisational theory, systemic accident models.

1 Introduction

System safety is generally considered as the characteristics of a system that prevents injury to or loss of human life, damage to property, and adverse consequences to the environment. The IEC 61508 (1998-2000) safety standard defines safety as, "freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment".

Highly technological systems such as aviation, maritime, air traffic control, telecommunications, nuclear power plants, space missions, chemical and petroleum process industry, and healthcare and patient safety are exceedingly becoming more complex. Such complex systems can exhibit potentially disastrous failure modes. Notable disasters and accidents such as the Bhopal toxic gas release disaster (Srivastava 1992), the NASA Challenger shuttle explosion (Vaughn 1996), the US Black Hawk fratricide incident during the 1994 Gulf War Operation Provide Comfort (AAIB 1994), and critical aviation accidents such as the 1993 Warsaw accident (Höhl & Ladkin 1997) are clear examples of system failures in complex systems that lead to serious loss of material and human life.

Large complex systems such as the Bhopal chemical plant and the Operation Provide Comfort Command and Control System are semantically complex (it generally takes a great deal of time to master the relevant domain knowledge), with tight couplings between various parts, and where operations are often carried out under time pressure or other resource constraints (Woods et al. 1994). In such systems, accidents gradually develop over a period of time through a conjunction of several small failures, both machine and human (Perrow 1994, Reason 1990).

Accident models provide a conceptualisation of the characteristics of the accident, which typically show the relation between causes and effects. They explain why accidents occur, and are used as techniques for: risk assessment during system development, and *post hoc* accident analysis to study the causes of the occurrence of an accident.

One of the earliest accident causation models is the Domino theory proposed by Heinrich in the 1940's (Ferry 1988), which describes an accident as a chain of discrete events which occur in a particular temporal order. This theory belongs to the class of sequential accident models or event-based accident models, which underlie most accident models such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis, and Cause-Consequence Analysis (Leveson 1995). These models work well for losses caused by failures of physical components or human errors in relatively simple systems. However, they are limited in their capability to explain accident causation in the more complex systems that were developed in the last half of the 20th century (Hollnagel 2004).

In the 1980s, a new class of epidemiological accident models endeavoured to explain accident causation in complex systems. Epidemiological models regard events leading to accidents as analogous to the spreading of a disease, i.e., as the outcome of a combination of factors, some manifest and some latent, that happen to exist together in space and time. Reason's (1990, 1997) Swiss cheese model of defences is a major contribution to this class of models, and has greatly influenced the understanding of accidents by highlighting the

relationship between latent and immediate causes of accidents.

Sequential and epidemiological accident models are inadequate to capture the dynamics and nonlinear interactions between system components in complex socio-technical systems. New accident models, based on systems theory, classified as systemic accident models, endeavour to describe the characteristic performance on the level of the system as a whole, rather than on the level of specific cause-effect "mechanisms" or even epidemiological factors (Hollnagel 2004). A major difference between systemic accident models and sequential/epidemiological accident models is that systemic accident models describe an accident process as a complex and interconnected network of events while the latter describes it as a simple cause-effect chain of events. Two notable systemic modelling approaches, Rasmussen's (1997) hierarchical socio-technical framework and Leveson's (2004) STAMP (Systems-Theoretic Accident Model and Processes) model, endeavour to model the dynamics of complex socio-technical systems.

Modern technology and automation has significantly changed the nature of human work from mainly manual tasks to predominantly knowledge intensive activities and cognitive tasks. This has created new problems for human operator performance (such as cognitive load) and new kinds of failure modes in the overall human-machine systems. Cognitive systems engineering (Hollnagel 1983) has emerged as a framework to model the behaviour of human-machine systems in the context of the environment in which work takes place. Two systemic accident models for safety and accident analysis have been developed based on the principles of cognitive systems engineering: CREAM - Cognitive Reliability and Error Analysis Method (Hollnagel 1998); and FRAM - Functional Resonance Accident Model (Hollnagel 2004).

During the last decade many attempts have been made on the use of formal methods for building mathematically-based models to conduct accident analysis. Formal methods can improve accident analysis by emphasising the importance of precision in definitions and descriptions, and providing notations for describing and reasoning about certain aspects of accidents.

As the understanding of industrial, transportation and aerospace accidents has evolved, they are no longer considered as simply the failures of technology alone, nor solely arising from the ubiquitous "human error", but also as a result of a historical background and an unfavourable organisational context (Vaughan 1996). Sociological analysis of accident causation is gaining momentum as an effective approach towards understanding the social and organisational causes of accidents (see, for example: Perrow 1984, Vaughn 1996, Hopkins 2000).

The *Columbia* investigation Report identifies a "broken safety culture" as a focal point of the accident's organisational causes (CAIB 2003). The report examines how NASA's organisational culture and structure weakened the safety structure that created structural secrecy, causing decision makers to miss the threat posed by successive events of foam debris strikes. Organisational culture has an influence on the overall safety, reliability and effectiveness of the operations in an organisation. Safety is a part of the organisational culture, and it is the leaders of an organisation who determine how it functions, and it is their decision making which determines in particular, whether an organisation exhibits the practices and attitudes which make up a culture of safety (Hopkins 2005).

This paper is organised as follows: in the following section, we discuss the traditional accident models; in Section 3, the issues and complexities of socio-technical systems are delineated; in Section 4, systemic accident modelling approach and models are described; a brief review of the application of formal methods to accident modelling is given in Section 5; sociological and organisational theories and research on accident analysis is discussed in Section 6; and finally, in the last section, we summarise the work on accident modelling and discuss future research trends.

2 Traditional Approaches to Accident Modelling

2.1 Sequential Accident Models

Sequential accident models explain accident causation as the result of a chain of discrete events that occur in a particular temporal order. One of the earliest sequential accident models is the Domino theory proposed by Heinrich (Ferry 1988). According to this theory there are five factors in the accident sequence: 1) social environment (those conditions which make us take or accept risks); 2) fault of the person; 3) unsafe acts or conditions (poor planning, unsafe equipment, hazardous environment); 4) accident; 5) injury. These five factors are arranged in a domino fashion such that the fall of the first domino results in the fall of the entire row (Figure 1). This illustrates that each factor leads to the next with the end result being the injury.

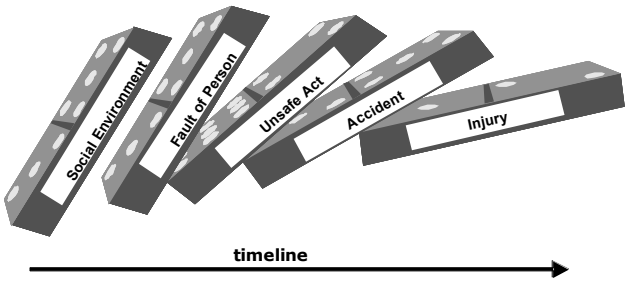

Figure 1: Domino model of accident causation

An undesirable or expected event (the root cause) initiates a sequence of subsequent events leading to an accident. This implies that the accident is the result of a single cause, and if that single cause can be identified and removed the accident will not be repeated. The reality is that accidents always have more than one contributing factor.

Sequential models work well for losses caused by failures of physical components or human errors in

relatively simple systems. While the Domino model considers only a single chain of events, event-based accident models can also be represented by multiple sequences of events in the form of hierarchies such as event tree and networks (see, for example: Leveson 1995, Ferry 1988).

Sequential models assume that the cause-effect relation between consecutive events is linear and deterministic. Analysing an accident may show that cause *A* lead to effect *B* in a specific situation, while *A* may be a composite event (or state) in turn having numerous causes (Hollnagel 2001). Thus, these models cannot comprehensively explain accident causation in modern socio-technical systems where multiple factors combine in complex ways leading to system failures and accidents.

2.2 Epidemiological Accident Models

The need for more powerful ways of understanding accidents led to the class of epidemiological accident models, which began to gain in popularity in the 1980s (Hollnagel 2001). Epidemiological models regard events leading to accidents as analogous to the spreading of a disease, i.e. as the outcome of a combination of factors, some manifest and some latent, that happen to exist together in space and time. An excellent account of this work has been provided by Reason (1990, 1997), which emphasises the concept of organisational safety and how defences (protection barriers such as material, human and procedures) may fail. In this approach the immediate or proximal cause of the accident is a failure of people at the "sharp end" who are directly involved in the regulation of the process or in the interaction with the technology (Reason 1990, Woods et al. 1994). Reason (1997) defines organisational accident as situations in which latent conditions (arising from management decision practices, or cultural influences) combine adversely with local triggering events (weather, location, etc.) and with active failures (errors and/or procedural violation) committed by individuals or teams at the sharp end of an organization, to produce the accident. The dynamics of accident causation are represented in the Swiss cheese model of defences (Figure 2), which shows an accident emerging due to holes (failures) in barriers and safeguards.

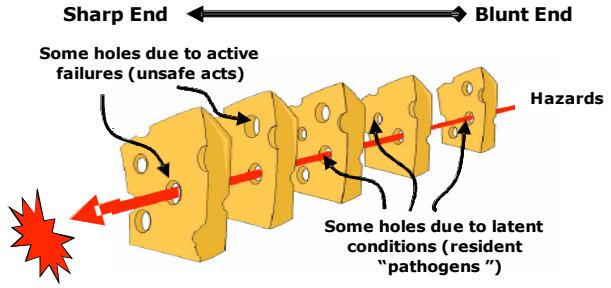

Figure 2: Swiss cheese model of accident causation (Reason 1997)

The notion of latent factors supports the understanding of accident causation beyond the proximate causes, which is particularly advantageous in the analysis of complex systems that may present multiple-failure situations.

However, epidemiological models still follow the principles of sequential models (Hollnagel 2004) as they show the direction of causality in a linear fashion. Furthermore, the causal links between distant latent conditions (organisational factors) and the accident outcome is complex and loosely coupled (Shorrock et al. 2003). Reason's model shows a static view of the organisation; whereas the defects are often transient i.e. the holes in the Swiss cheese are continuously moving. The whole socio-technical system is more dynamic than the model suggests.

3 Complex Socio-Technical Systems

In modern complex systems, humans interact with technology and deliver outcomes as a result of their collaboration; such outcomes cannot be attained by either the humans or technology functioning in isolation. Such systems, composed of human agents and technical artefacts, are often embedded within complex social structures such as the organisational goals, policies and culture, economic, legal, political and environmental elements. Socio-technical theory implies that human agents and social institutions are integral parts of the technical systems, and that the attainment of organisational objectives are not met by the optimisation of the technical system, but by the joint optimisation of the technical and social aspects (Trist & Bamforth 1951). Thus, the study of modern complex systems requires an understanding of the interactions and interrelationships between the technical, human, social and organisational aspects of the system.

For example, civil aviation is a complex public transportation system comprising technological artefacts (aircrafts, runways, luggage transport systems, communication equipment, etc.); these artefacts have various interconnections and relationships and they all play an essential role in the functioning of this transport system as a whole (Kroes et al. 2006). These technical artefacts and systems operate in a social-organisational environment which constitutes various policies and procedures, the air traffic control system, legal and economic aspects. Thus, the functioning of this transport system is also dependent on the functioning of social elements and on the behaviour of various human agents, and not purely on the functioning of the technical artefacts.

Charles Perrow's seminal work on normal accident theory (Perrow 1984) provides an approach to understanding accident causation in complex organisations managing hazardous technologies such as nuclear power plants, petrochemical plants, aircraft, marine vessels, space, and nuclear weapons. Perrow analyses many notable accidents involving complex systems such as the 1979 Three Mile Island nuclear power accident, and identifies that the characteristics that make a technological system or organisations more prone to accident are complex interactions and tight coupling.

A complex system is composed of many components that interact with each other in linear and complex manners. Linear interactions are those that are expected in

production or maintenance sequences, and those that are quite visible even if unplanned (during design), while complex (nonlinear) interactions are those of unfamiliar sequences, unplanned and unexpected sequences, and either not visible or not immediately comprehensible (Perrow 1984). Two or more discrete failures can interact in unexpected ways which designers could not predict and operators cannot comprehend or control without exhaustive modelling or test.

The type of coupling (tight or loose coupling) of components in a system affects its ability to recover from discrete failures before they lead to an accident or disaster. Perrow (1984) discusses the characteristics of tightly and loosely coupled systems. Tightly coupled systems have more time-dependant processes, so that is a failure or event in one component has an immediate impact on the interacting component. Tightly coupled systems have little slack, quantities must be precise and resources cannot be substituted for one another. For example, a production system must be shutdown if a subsystem fails because the temporary substitution of other equipment is not possible. In contrast, loosely coupled systems are more forgiving.

4 Systemic Accident Models

4.1 Systems Theoretic Approach

New approaches to accident modelling adopt a systemic view which consider the performance of the system as a whole. In systemic models, an accident occurs when several causal factors (such as human, technical and environmental) exist coincidentally in a specific time and space (Hollnagel 2004). Systemic models view accidents as emergent phenomena, which arises due to the complex interactions between system components that may lead to degradation of system performance, or result in an accident.

Systemic models have their roots in systems theory. Systems theory includes the principles, models, and laws necessary to understand complex interrelationships and interdependencies between components (technical, human, organisational and management).

In a systems theory approach to modelling, systems are considered as comprising interacting components which maintain equilibrium through feedback loops of information and control. A system is not regarded as a static design, but as a dynamic process that is continually adapting to achieve its objectives and react to changes in itself and its environment. The system design should enforce constraints on its behaviour for safe operation, and must adapt to dynamic changes to maintain safety. Accidents are treated as the result of flawed processes involving interactions among people, social and organizational structures, engineering activities, and physical and software system components (Leveson 2004).

Rasmussen adopts a system oriented approach based on a hierarchical socio-technical framework for the modelling of the contextual factors involved in organisational, management and operational structures that create the preconditions for accidents (Rasmussen 1997, Rasmussen & Svedung 2000). Leveson (2004) proposes a model of accident causation called STAMP (Systems-Theoretic Accident Model and Processes) that considers the technical, human and organisational factors in complex socio-technical systems.

4.2 Cognitive Systems Engineering Approach

Modern technology has changed the nature of human work from mainly manual tasks to predominantly knowledge intensive activities and cognitive tasks. Technology-driven approaches to automation have created new problems for human operator performance and new kinds of failure modes in the overall human-machine systems, which have led to many catastrophic accidents in the fields of aviation, nuclear power plants and military command and control (Parasuraman 1997). This has influenced the development of new approaches for human performance and error modelling, and accident analysis of joint human-machine systems.

Cognitive systems engineering (Hollnagel 1983) has emerged as a framework to model the behaviour of human-machine systems in the context of the environment in which work takes place. The traditional view is that "human errors" represent a *post hoc* rationalization (Woods et. al. 1994), which is based on the inverse causality principle: "if there is an effect, then there must be a cause". Cognitive systems engineering instead suggests that we cannot understand what happens when things go wrong without understanding what happens when things go right (Hollnagel & Woods 2005). Hollnagel & Woods introduce a new paradigm on Joint Cognitive Systems which describes how humans and technology function as joint systems, rather than how humans interact with machines. Efforts to make work safe should start from an understanding of the normal variability of human and Joint Cognitive Systems performance, rather than assumptions about particular, but highly speculative "error mechanisms" (for a detailed discussion see: Hollnagel & Woods 2005).

Two systemic accident models for safety and accident analysis have been developed based on the principles of cognitive systems engineering: the Cognitive Reliability and Error Analysis Method (CREAM); and the Functional Resonance Accident Model (FRAM).

CREAM is based on the modelling of cognitive aspects of human performance for an assessment of the consequences of human error on the safety of a system (Hollnagel, 1998). Two versions of CREAM have been developed for accident modelling: DREAM (Driver Reliability and Error Analysis Method) for analysis of traffic accidents; and BREAM for use in maritime accident analysis (Hollnagel 2006).

FRAM is a qualitative accident model that describes how functions of system components may resonate and create hazards that can run out of control and lead to an accident (Hollnagel 2004). FRAM is based on the premise that performance variability, internal variability and external variability are normal, in the sense that performance is

never stable in a complex socio-technical system such as aviation.

4.3 Rasmussen's Socio-Technical Framework

The complexity and rapid advancements in technology have led to the development of high-risk socio-technical systems, which are managed by complex organisations operating in highly volatile and dynamic environmental conditions such as market competition, economic and political pressures, legislation and increasing social awareness on safety (Rasmussen 1997). Rasmussen postulates that these factors have transformed the dynamic character of modern society and continuously influence the work practices and human behaviour in the operation of complex systems. Deterministic (e.g. sequential chain-of-events) causal models are inadequate to study failures and accidents in highly adaptable socio-technical systems. Rasmussen adopts a system oriented approach based on control theoretic concepts and proposes a framework for modelling the organisational, management and operational structures that create the preconditions for accidents. Rasmussen's framework for risk management has two parts: Structure and Dynamics.

Structural Hierarchy:

Rasmussen (1997) views risk management as a control problem in the socio-technical system, where human injuries, environmental pollution, and financial disasters occur due to loss of control of physical processes. According to Rasmussen, safety depends on the control of work processes in the context of the pressures and constraints in the operational environment.

The socio-technical system involved in risk management includes several hierarchical levels ranging from legislators, organisation and operation management, to system operators (Figure 3).

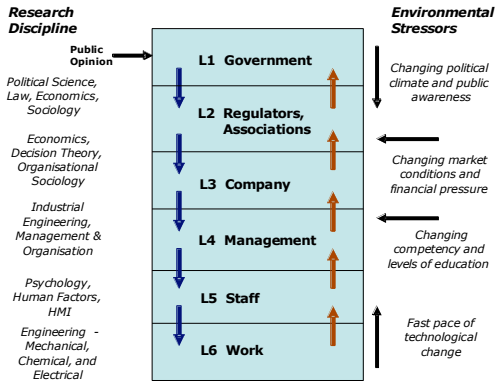

Figure 3: Hierarchical model of socio-technical system (Rasmussen 1997)

The top level L1 describes the activities of government, who through legislation control the practices of safety in society. Level L2 describes the activities of regulators, industrial associations and unions (such as medical and engineering councils) that are responsible for implementing the legislation in their respective sectors. Level L3 describes the activities of a particular company, and level L4 describes the activities of the management in a particular company that lead, manage and control the work of their staff. Level L5 describes the activities of the individual staff members that are interacting directly with technology or process being controlled such as power plant control operators, pilots, doctors and nurses. The bottom level L6 describes the application of engineering disciplines involved in the design of potentially hazardous equipment and operating procedures for process control.

Traditionally, each level is studied separately by a particular academic discipline, for example, risk management at the upper levels is studied without any detailed consideration of processes at the lower levels. This framework points to a critical factor that is overlooked by all horizontal research efforts, that is, the additional need for "vertical" alignment across the levels in Figure 3. The organisational and management decisions made at higher levels should transmit down the hierarchy, whereas information about processes at lower levels should propagate up the hierarchy. This vertical flow of information forms a closed loop feedback system, which plays an essential role in the safety of the overall socio-technical system. Accidents are caused by decisions and actions by decision makers at all levels, and not just by the workers at the process control level.

As shown on the right of Figure 3, the various layers of complex socio-technical systems are increasingly subjected to external disruptive forces, which are unpredictable, rapidly changing and have a powerful influence on the behaviour of the socio-technical system. When different levels of the system are being subjected to different pressures, each operating at different time scales, it is imperative that efforts to improve safety within a level be coordinated with the changing constraints imposed by other levels.

System Dynamics:

In complex dynamic environments it is not possible to establish procedures for every possible condition, in particular for emergency, high risk, and unanticipated situations (Rasmussen 1997). In nuclear power plants, where tasks and procedures are strictly prescribed, violations of instructions have been repeatedly observed (Vicente et al. 2004). Vicente argues that operator's violation of formal procedures appear to be quite rational (sensible) given the actual workload and timing constraints. The behaviour of operators is context dependent and is shaped by the dynamic conditions in the work environment.

Decision making and human activities are required to remain between the bounds of the workspace defined by administrative, functional and safety constraints. Rasmussen argues that in order to analyse a work domain's safety, it is important to identify the boundaries of safe operations and the dynamic forces that may cause the socio-technical system to migrate towards or cross these boundaries. Figure 4 shows the dynamic forces that can influence a complex socio-technical system to modify its behaviour over time. The safe space of performance within which actors can navigate freely is contained within three boundaries: individual unacceptable workload; financial and economic constraints; and the

safety regulations and procedures. The financial pressures produce a cost gradient that influences individual human behaviour to adopt more economically effective work strategies; while workload pressures result in an effort gradient motivating individuals to change their work practices to reduce cognitive or physical work. These gradients induce variations in human behaviour that are analogous to the "Brownian movements" of the molecule of a gas.

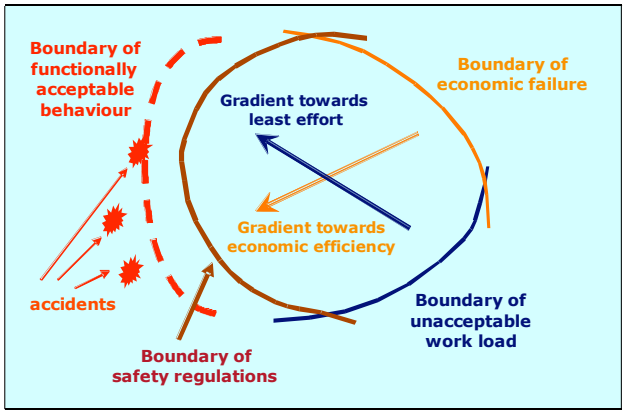

Figure 4: Boundaries of safe operation (Rasmussen 1997)

Over a period of time, this adaptive behaviour causes people to cross the boundary of safe work regulations and leads to a systematic migration toward the boundary of functionally acceptable behaviour. This may lead to an accident if control is lost at the boundary. Rasmussen asserts that these uncoordinated attempts of adapting to environmental stressors are slowly but surely "preparing the stage for an accident". Reports from several accidents such as Bhopal and Chernobyl demonstrate that they have not been caused by coincidence of independent failures and human errors, but by a systematic migration of organisational behaviour towards an accident under the influence of pressure toward cost-effectiveness in an aggressive, competitive environment (Rasmussen 1997).

Rasmussen's approach for improving safety and risk management raises the need for the identification of the boundaries of safe operation, making these boundaries visible to the actors and giving opportunities to control behaviour at the boundaries.

4.4 AcciMap Accident Analysis Technique

The AcciMap accident analysis technique is based on Rasmussen's risk management framework (Rasmussen 1997, Rasmussen & Svedung 2000). Initially, a number of accident scenarios are selected and the causal chains of events are analysed using a cause-consequence chart. A cause-consequence chart represents a generalisation that aggregates a set of accidental courses of events. Cause-consequence charts have been widely used as a basis for predictive risk analysis (Leveson 1995). The choice of set to include in a cause-consequence chart is defined by the choice of the critical event, which reflects the release of a well-defined hazard source, such as "loss of containment of hazardous substance", or "loss of control of accumulated energy". The critical event connects the causal tree (the logic relation among potential causes) with a consequent event tree (the possible functional and temporal relation among events) explicitly reflecting the switching of the flow resulting from human decisions or by automatic safety systems (Rasmussen & Svedung 2000).

The focus of this analysis is the control of the hazardous process at the lowest level of the socio-technical system in Figure 3. In order to conduct a vertical analysis across the hierarchical levels, the cause-consequence chart representation is extended which explicitly includes the normal work decisions at the higher levels of the socio-technical system. An AcciMap shows the contributing factors in an accident mapped onto the levels of a complex socio-technical system identified in Figure 3.

An AcciMap of the F-111 chemical exposure of Royal Australian Air Force (RAAF) maintenance workers is shown in Figure 5, which is based on the official F-111 Board of Inquiry report (Clarkson et al. 2001). The AcciMap causal flow diagram looks at the culture of RAAF as well as factors that lie beyond the organisational limits of RAAF. This analysis concludes that the failure of the chain of command to operate optimally predominantly lies at the values and culture of RAAF.

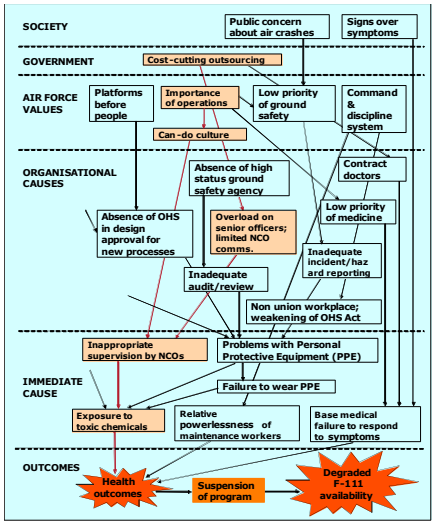

Figure 5: AcciMap of F-111 Seal/Reseal Program (Clarkson et al. 2001: Chap. 11)

In this way, the AcciMap serves to identify relevant decision-makers and the normal work situation in which they influence and condition possible accidents. The focus is not on the traditional search for identifying the "guilty person", but on the identification of those people in the system that can make decisions resulting in improved risk management and hence to the design of improved system safety.

4.5 STAMP Approach

Leveson (2004) proposes a model of accident causation that considers the technical (including hardware and software), human and organisational factors in complex socio-technical systems. According to Leveson, "The hypothesis underlying the new model, called STAMP (Systems-Theoretic Accident Model and Processes) is

that system theory is a useful way to analyze accidents, particularly system accidents." In the STAMP approach, accidents in complex systems do not simply occur due to independent component failures; rather they occur when external disturbances or dysfunctional interactions among system components are not adequately handled by the control system. Accidents therefore are not caused by a series of events but from inappropriate or inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system. "Safety then can be viewed as a control problem, and safety is managed by a control structure embedded in an adaptive socio-technical system" (Leveson 2004).

A STAMP accident analysis can be conducted in two stages: 1) Development of the Hierarchical Control Structure, which includes identification of the interactions between the system components and identification of the safety requirements and constraints; 2) Classification and Analysis of Flawed control (Constraint Failures), which includes the classification of causal factors followed by the reasons for flawed control and dysfunctional interactions. Here we summarise the STAMP analysis of the Black Hawk fratricide during the operation Provide Comfort in Iraq in 1991 (Leveson et al. 2002, Leveson 2002).

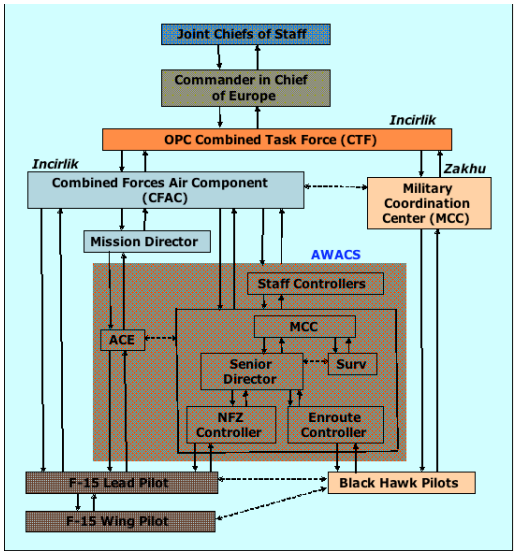

Figure 6: Hierarchical Command & Control Structure of the Black Hawk fratricide

The hierarchical control structure of the Black Hawk accident is shown in Figure 6, starting from the Joint Chiefs of Staff down to the aircraft involved in the accident. At the lowest level in the control structure are the pilots who directly controlled the aircraft (operator at the sharp end).

The AWACS mission crew was responsible for tracking and controlling aircraft. The AWACS also carried an Airborne Command Element (ACE), who was responsible for ensuring that the larger OPC mission was completed. The ACE reported to a ground-based Mission Director. The Army headquarters (Military Coordination Center) Commander controlled the U.S. Black Hawk operations while the Combined Forces Air Component (CFAC) Commander was responsible for the conduct of OPC missions. The CFAC Commander had tactical control over all aircraft flying in the No Fly Zone (NFZ) including both Air Force fighters and Army helicopters, but operational control only over the Air Force fixed-wing aircraft.

In addition to the formal control channels, there were also communication channels, shown in Figure 6 as dashed lines, between the process components at each level of the hierarchy.

The hierarchical control structure (Figure 6) is then analysed to identify the safety constraints at each level in the hierarchy and the reasons for the flawed control. Leveson (2004) provides a general classification of those flaws:

- the controller may issue inadequate or inappropriate control actions, including inadequate handling of failures or disturbances in the physical process;
- control actions may be inadequately executed; or
- there may be missing or inadequate feedback.

Using this classification, Leveson (2002) describes the analysis at each of the levels in the Hierarchical Control Structure. For example, at the Physical Process Level, a safety constraint required that weapons must not be fired at friendly aircraft. All the physical components worked exactly as intended, except perhaps for the IFF (Identify Friend or Foe) system, which gave an intermittent response (this has never been completely explained).

There were, however, several dysfunctional interactions and communication inadequacies among the correctly operating aircraft equipment (for details, see: Leveson 2002). A major reason for the dysfunctional interactions can be attributed to the use of advanced technology by the Air Force, which made the Army radios incompatible. The hilly terrain also contributed to the interference in the line-of-sight transmissions.

However, it is also important to analyse the safety constraints and flawed control at the higher levels in the hierarchical control structure to obtain a system-wide understanding of the contributory causal factors. For a detailed analysis at all levels see Leveson (2002). Leveson attributes the organisational factors at the highest levels of command for the lack of coordination and communication, as a key accident factor, which led to the failures at the lower technical and operational levels.

5 Formal Methods and Accident Analysis

5.1 Logic Formalisms to Support Accident Analysis

The structure, content, quality, and effectiveness of accident investigation reports have been much criticised (e.g. Ladkin & Loer 1998, Burns 2000); they do not accurately reflect the events, or are unable to identify critical causal factors, and sometimes conclude with incorrect causes of the accident. Omissions, ambiguities, or inaccurate information in a report can lead to unsafe

system designs and misdirected legislation (Leveson 1995). Thus, there is a critical need to improve the accuracy of the information found in conventional accident investigation reports.

Formal methods can improve accident analysis by emphasizing the importance of precision in definitions and descriptions, and providing notations for describing and reasoning about certain aspects of accidents. Formal methods are mathematically-based techniques which provide a rigorous and systematic framework for the specification, design and verification of computer systems (both software and hardware). Formal methods essentially involve the use of a formal specification language composed of three main components: rules for determining the grammatical well-formedness of sentences (the syntax); rules for interpreting sentences in a precise, meaningful way within the domain considered (the semantics); and rules for inferring useful information from the specification (the proof theory) (Lamsweerde 2000). This provides the means of proving that a specification is realisable, proving that a system has been implemented correctly, and proving properties of a system without necessarily running it to determine its behaviour. There are comprehensive accounts of experience on the use of formal methods in industry and research (e.g. Hinchey & Bowen 1995).

During the last decade many attempts have been made to use of formal methods for building mathematically-based models to conduct accident analysis. A comprehensive survey on the application of various formal logics and techniques to model and reason about accident causation is given by Johnson & Holloway (2003a) and Johnson (2003). They discuss the weakness of classical (propositional) logic in capturing the different forms of causal reasoning that are used in accident analysis. In addition, the social and political aspects in accident analysis cannot easily be reconciled with the classical logic-based approach.

Ladkin & Loer (1998) describe a formal method, called Why-Because Analysis (WBA), for accident modelling and rigorous reasoning; and have demonstrated benefits in the application of this method to a number of case studies in aviation and rail transportation (for example: Höhl & Ladkin 1997, Ladkin & Stuphorn 2003, Ladkin 2005). The development of deontic action logic as a language for constructing formal models (Burns 2000) has demonstrated that the methodical construction of a formal model of the accident report improves the accuracy of accident reports.

A number of research groups are investigating the use, extension and development of formal languages and methods for accident modelling and analysis, such as the Glasgow Accident Analysis Group (GAAG 2006) and the NASA Langley formal methods research program on accident analysis (LaRC 2004). The research program at NASA Langley is investigating the suitability of using one or more existing mathematical representations of causality as the basis for developing tools for:

- explaining causes and contributing factors to accidents;
- analysing causal explanations for consistency, completeness, and other desired characteristics;
- storing causal explanations for retrieval; and
- using previously stored causal explanations in the design of new systems.

Formal methods have been applied successfully to the design and verification of safety-critical systems; however, they need to be extended to capture the many factors and aspects that are found in accidents and accident reports. A single modelling language is unlikely to model all the factors and aspects in an accident (Burns 2000). Also scaling up, formal methods have limitations to model complete socio-technical systems, they need specialists in mathematics, and not everything can be formalised.

5.2 Probabilistic Models of Causality

The accident modelling approaches discussed so far are based on deterministic models of causality. These models focus on the identification of deterministic sequence of cause and effect relationships, which are difficult to validate (Johnson 2003), for example, it cannot be guaranteed that a set of effects will be produced even if necessary and sufficient conditions can be demonstrated to hold at a particular moment. Johnson argues that the focus should be on those conditions that make effects more likely with a given context, and examines the application of probabilistic models of causality to support accident analysis. Probabilistic causation designates a group of philosophical theories that aim to characterise the relationship between cause and effect using the tools of probability theory (Hitchcock 2002). The central idea underlying these theories is that causes raise the probabilities of their effects.

Johnson & Holloway (2003a) discuss the use of Bayesian Logic (which exploits conditional probabilities) for accident analysis, as an example to reason about the manner in which the observation of evidence affects our belief in causal hypothesis.

The probabilistic theory of causality has been developed in slightly different ways by many authors. Hitchcock (2002) conducts a review of these developments and discusses the issues and criticism to the probabilistic theories of causation. A major contribution is the mathematical theory of causality developed by Pearl (2000), which is a structural model approach evolved from the area of Bayesian networks. The main idea behind the structure-based causal models is that the world is modelled by random variables, which may have causal influence on each other. The variables are divided into background (exogenous) variables *(U)*, which are influenced by factors outside the model, and endogenous variables *(V)*, which are influenced by exogenous and endogenous variables. This latter influence is expressed through functional relationships (described by structural equations) between them.

Formally, Pearl (2000) defines a **causal model** as a triple $M = (U, V, F)$ where: F is a set of functions $\{f_1, f_2, \ldots, f_n\}$ such that each f_i is a mapping from (the respective

domains of) $U \cup (V \setminus V_i)$ to V_i and such that the entire set F forms a mapping from U to V . Symbolically, the set of equations F can be represented by writing: $v_i = f_i\,(pa_i; u_i)$, $i = 1, \ldots, n$, where, pa_i is any realization of the unique minimal set of variables PA_i in $V \setminus V_i$ (connoting parents) sufficient for representing f_i. Likewise, $U_i \subseteq U$ stands for the unique minimal set of variables in U sufficient for representing f_i.

The relationship between the variables of a causal model $M = (U, V, F)$ can be associated with the *causal graph* for M, which is the directed graph that has $U \cup V$ as the set of nodes and the directed edges point from members of PA_i and U_i towards V_i (Pearl, 2000). This graph merely identifies the endogenous and background variables that have direct influence on each V_i; it does not specify the functional form of f_i.

Pearl (2000) uses the structural causal model semantics and defines a **probabilistic causal model** as a pair $(M, P(u))$ where M is a causal model and $P(u)$ is a probability function defined over the domain of the background variables U. Pearl (2000) has also demonstrated how counterfactual queries, both deterministic and probabilistic, can be answered formally using structural model semantics. He also compares the structural models with other models of causality and counterfactuals, most notably those based on Lewis's closest-world semantics.

5.3 Why-Because Analysis Method

Ladkin & Loer (1998) developed the formal Why-Because Analysis method to represent and analyse causal sequences found in accident investigation reports for failure analysis in safety critical systems. This formal technique is based on formal semantics and logic, and separates the various explanatory domains: time, causation, and deontics (regulations, obligations and operating procedures). WBA is primarily concerned with analysing causality, and allows objective evaluation of events and states as causal factors. It is based on David Lewis' formal semantics for causality (Lewis 1973) and is intended to put accident analysis on a "rigorous foundation".

In general, the term "cause" is not well defined and there is little consensus on what constitutes a cause. One philosophical approach to causation views counterfactual dependence as the key to the explanation of causal facts: for example, events c (the cause) and e (the effect) both occur, but had c not occurred, e would not have occurred either (Collins et al. 2004). The term ''counterfactual'' or ''contrary-to-fact'' conditional carries the suggestion that the antecedent of such a conditional is false.

David Lewis (1973) developed a number of logics to capture counter-factual arguments that provide a formal semantics for causation. Lewis's semantics can be used to state that A is a causal factor of B (where A and B are two events or states), if and only if A and B both occurred and in the nearest possible worlds in which A did not happen neither did B. This implies that A is a cause of B or A is a necessary causal factor of B.

Ladkin & Loer (1998) introduce notations and inference rules which allows them to reduce the Lewis criterion for counterfactuals in the form (Figure 7) in which they use to explain the causal-factor relation between facts A and B. This logic provides a semantics for informal concepts such as "cause".

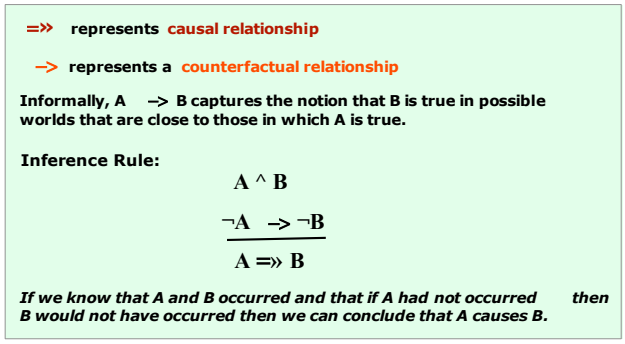

Figure 7: WBA notations and rules for causal relation

Lewis's semantics for causation in terms of counterfactuals, and the combination of other logics into a formal logic, called Explanatory Logic, form the basis of the formal method WBA. WBA is based around two complementary stages: i) Construction of the WB-Graph; and ii) Formal Proof of Correctness of the WB-Graph.

WBA begins with a reconstruction phase, where a semi-formal graphical notation models the sequences of events leading to an accident. The significant events and states are derived from the accident investigation report in their proper time order. These sequences can be represented in a form of temporal logics and then each pair is iteratively analysed to move towards a causal explanation using Lewis's counterfactual test. The graph of this relation is called a WB-Graph (see Figure 8 as an example).

The WB-Graph is subjected to a rigorous proof to verify that: the causal relations in the graph are correct, that is they satisfy the semantics of causation defined by Lewis; and there is a sufficient causal explanation for each identified fact that is not itself a root cause. A detailed development of the formal proof of correctness and the EL logic is described in Ladkin & Loer (1998).

The WBA method has been used for analysing a fairly large number of accident reports, mainly for aircraft and train accidents. In the Lufthansa A320 aircraft accident in Warsaw, the logic of the braking system was considered the main cause of the accident. The accident report contained facts that were significantly causally related to the accident. However, these facts were not identified in the list of "probable cause/contributing factors" of the accident report. The rigorous reasoning employed in the WB-Method enabled Höhl & Ladkin (1997) to identify two fundamental causes (source nodes in the WB-graph) that occurred in the report but were omitted as "probable cause" or "contributing factors": the position of the earth bank, and the runway surfacing. Once the position of the earth bank was identified as an original causal factor, it can be concluded that had the bank not been where it is, the accident that happened would not have happened. Thus the WB-Graph (Figure 8) helped to identify logical mistakes in the accident report, and has illustrated rigorous reasoning in the WB-method.

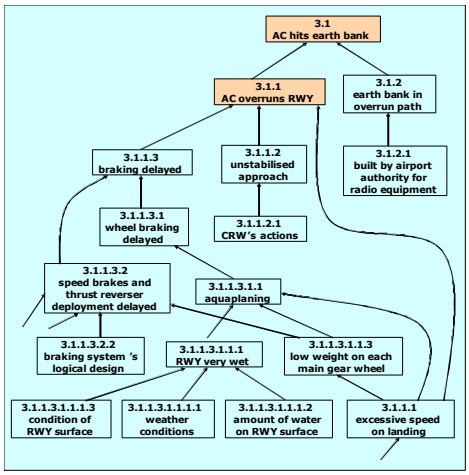

Figure 8: Extract of WB-Graph for Lufthansa Accident at Warsaw (Höhl & Ladkin 1997)

6 Sociological and Organisational Analysis of Accident Causation

Major accidents such as Bhopal and *Challenger* have highlighted the fact that in seeking the causes of complex system accidents we must now consider the interaction and interdependence between technological and organisational systems. Shrivastava (1992) argues that industrial accidents have identifiable causes, namely, human, organisational, and technological, and their consequences demand new policies designed to prevent such crises in the future. Bhopal is only one dramatic example of how the rapid and haphazard infusion of new, sophisticated technologies put stress on the economic and social infrastructure of a community.

A number of studies on aviation and maritime accidents have shown human and organisational factors as major contributors to accidents and incidents. Johnson and Holloway (1997) analysed major aviation and maritime accidents in North America during 1996-2006, and concluded that the proportion of causal and contributory factors related to organisational issues exceed those due to human error. For example, the combined causal and contributory factors in the USA aviation accidents showed 48% related to organisational factors, 37% to human factors, 12% to equipment and 3% to other causes; and the analysis of maritime accidents classified the causal and contributory factors as: 53% due to organisational factors, 24-29% as human error, 10-19% to equipment failures, and 2-4% as other causes.

Hopkins (2000) examines the findings of the Royal Commission, from a cultural and organisational perspective, into the Esso gas plant explosion at Longford, Victoria in September 1998. This accident resulted in the death of two workers, injured eight others and cut Melbourne's gas supply for two weeks. Hopkins argues that the accident's major contributory factors were related to a series of organisational failures: the failure to respond to clear warning signs, communication problems, lack of attention to major hazards, superficial auditing and, a failure to learn from previous experience. Hopkins identified many cultural and organisational causes of the F-111 chemical exposure incident (see Figure 5). This emphasises the need for attention to be paid to organisational factors and their influence to safety in the workplace.

Vaughn (1996) rejects the prevalent explanations (provided by traditional safety engineering techniques) of the cause of the *Challenger* shuttle accident and presents an alternative sociological explanation that explores much deeper cause of the failure. Vaughan discusses how common errors and violation of procedures can be seen as a normal occurrence, a concept known as *normalisation of deviance*. She reveals how and why NASA decision makers, when repeatedly faced with evidence that something was wrong, normalised the deviance so that it became acceptable to them. She identifies three major elements behind the *Challenger* accident:

- An enacted work group culture, that is how culture is created as people interact in work groups;
- A culture of production built from occupational, organisational, and institutional influences; and
- A structure induced dispersion of data that made information more like a body of secrets than a body of knowledge – silenced people.

These elements had shaped shuttle decision making for over a decade. What was unique in this particular situation was that this was the first time all three influences came together simultaneously across multiple levels of authority and were focused on a single decision to meet the *Challenger* launch deadline.

Vaughan draws parallels between *Columbia* and *Challenger* accidents, establishes that both accidents resulted due to organisational system failures, and presents a causal explanation that links the culture of production, the normalisation of deviance, and structural secrecy in NASA. (CAIB 2003: Chap. 8).

Sagan's (1993) study of nuclear weapons organisations found them to be infused with politics, with many conflicting interest at play both within the military command and control, and between military and civilian leaders. Power and politics should be taken seriously and necessary not only to understand the organisational causes of accidents, but also to start the difficult process of designing reforms to enhance safety and reliability in organisations (Sagan 1994).

7 Discussion and Conclusions

The sequential and epidemiological models have contributed to the understanding of accidents; however, they are not suitable to capture the complexities and dynamics of modern socio-technical systems. In contrast to these approaches, systemic models view accidents as emergent phenomena, which arise due to the complex and nonlinear interactions among system components. These interactions and events are hard to understand, and it is not sufficient to comprehend accident causation by employing the standard techniques in safety engineering alone, i.e. by analysing the failure modes of individual components using techniques such as FMEA, or relating the accident to a single causal factor. Since the standard safety techniques concentrate on component failure, they

cannot adequately capture the dysfunctional interactions between individual components operating without failure.

Accident models generally used for the prediction of accidents during the development of safety-critical system, in particular, are based on sequential models. Furthermore, traditional safety and risk analysis techniques such as Fault Tree Analysis and Probabilistic Safety Analysis are not adequate to account for the complexity of modern socio-technical systems. The choice of accident model has consequence for how *post hoc* accident analysis and risk assessment is done, thus we need to consider the extension and development of systemic accident models both for accident analysis and for risk assessment and hazard analysis of complex systems.

Rasmussen's framework has been comprehensively and independently tested on the analysis of two Canadian public health disasters (Woo & Vicente 2003) and on the Esso gas plant explosion accident in Australia (Hopkins 2000). These case studies demonstrate the validity of Rasmussen's framework to explain the accident causation *a posteriori*. Further research is needed to extend this framework to predict accidents and to explore the applicability to risk and safety analysis of critical socio-technical systems.

Similarly, STAMP has been applied to a number of case studies for *post hoc* accident analysis (e.g. Leveson et al. 2002, Johnson & Holloway 2003b). There is a need for a methodology for the development of the STAMP model including guidelines for developing the control models and interpretation of the flawed control classification.

Some advances have been made in extending the STAMP model to conduct a proactive accident investigation in the early stages of system design. Leveson & Dulac (2005) discuss the use of STAMP model for hazard analysis, safety (risk) assessment, and as a basis for a comprehensive risk management system.

Organisational sociologists have made significant contributions to the understanding of accidents in complex socio-technical systems. They emphasise the organisational aspect of accidents and tend to overlook the technical aspects. System theoretical approach to safety provides a framework for modelling the technical, human, social and organisational factors in socio-technical systems, including interactions among the system components. The socio-technical system must be treated as an integrated whole, and the emphasis should be on the simultaneous consideration of social and technical aspects of systems, including social structures and cultures, social interaction processes, and individual factors such as capability and motivation as well as engineering design and technical aspects of systems (Marias et al. 2004) .

The recent advances in new systemic accident models, based on cognitive systems engineering, such as the Functional Resonance Accident Model (Hollnagel 2004), should be investigated further and applied to the modelling of complex socio-technical systems to understand the variability in human and system performance and how this relates to accident causation.

Although, formal methods have been applied successfully to the design and verification of safety-critical systems, they need to be extended to capture the many factors including human behaviour and organisational aspects that are found in accidents and accident reports. Further research is needed to develop languages and semantics for modelling the various aspects of accidents in modern complex systems, such as: organisational, cultural and social properties, and human performance. WBA is probably the most mature formal method for accident analysis. WBA has also been compared with other causal analysis methods; in particular the comparison with Rasmussen's AcciMap technique showed that the methodical approach employed by WBA produces greater precision in determining causal factors than does the informal approach of the AcciMap (Ladkin 2005).

Future research is needed to comprehensively analyse the applicability of the new systemic models across a broader class of socio-technical systems, particularly in the safety-critical sector such as patient safety, transportation, nuclear power, maritime, defence, and aerospace. A number of studies have conducted comparisons of systemic accident models, particularly STAMP and Rasmussen's risk management framework (e.g. Johnson et al. 2007). Further studies should be conducted to compare and contrast the new systemic accident models in a variety of complex socio-technical domains.

Resilience Engineering is emerging as a new paradigm in safety management, where "success" is based on the ability of organisations, groups and individuals to anticipate the changing shape of risk before failures and harm occur (Hollnagel et al. 2006). Complex systems exhibit dynamic behaviour and continuously adapt their behaviour to account for the environmental disturbances. Such system adaptations cannot be pre-programmed during system design (Hollnagel et al. 2006). According to Rasmussen's model (Figure 4), a system may become unstable or lose control at the boundary of safety regulations. Thus resilience is the ability of organisations to maintain control in order to stay outside the accident region. Resilience engineering requires powerful methods, principles and tools that prevent this from taking place. Systemic accident models support the analytical aspects of resilience engineering, and STAMP has been applied to analyse the resilience of organisations confronted by high hazard and high performance demands (Hollnagel et al. 2006: Chap. 8). For the predictive part, resilience engineering can be addressed, e.g., by means of a functional risk identification method, such as proposed by the functional resonance accident model (Hollnagel 2004).

The complexity of modern socio-technical systems poses a challenging interdisciplinary research in the development of new safety analysis and accident models involving researchers from engineering, social sciences, organisational theory, and cognitive psychology. Thus, there is a compelling need for researchers to step outside their traditional boundaries in order to capture the complexity of modern socio-technical systems from a broad systemic view for understanding the multi-

dimensional aspects of safety and modelling socio-technical system accidents.

8 Acknowledgements

This research was initiated at the Defence Science and Technology Organisation, under the Critical Systems Development Task JTW 04/061, sponsored by the Defence Materiel Organisation. I am particularly indebted to Dr. Tony Cant, DSTO for his encouragement and stimulating discussions on safety-critical systems, and to the anonymous reviewers for many helpful comments.

9 References

AAIB (1994): *U.S. Army Black Hawk Helicopters 87-26000 and 88-26060: Volume 1*. Executive Summary: UH-60 Black Hawk Helicopter Accident, 14 April 1994, USAF Aircraft Accident Investigation Board. http://schwabhall.bigwindy.org/opc_report.htm

CAIB (2003): *Columbia Accident Investigation Board Report Volume I*. Washington, DC, Government Printing Office.

Clarkson, J., Hopkins, A. & Taylor, K. (2001): *Report of the Board of Inquiry into F-111 (Fuel Tank) Deseal/Reseal and Spray Seal Programs, Vol. 1*. Canberra, ACT, Royal Australian Air Force. http://www.defence.gov.au/raaf/organisation/info_on/units/f111/Volume1.htm

Collins, J., Hall, N. & Paul, L.A. (2004): Counterfactuals and Causation: History, Problems, and Prospects, In Collins, J., Hall, N. & Paul, L.A. (Eds.), *Causation and Counterfactuals*, Chapter 1, Cambridge, MA, MIT Press.

Ferry, T.S. (1988): *Modern Accident Investigation and Analysis*. Second Edition, New York, Wiley.

GAAG (2006): *Glasgow Accident Analysis Group*, Dept. of Computer Science, University of Glasgow, Scotland. http://www.dcs.gla.ac.uk/research/gaag/ (accessed: 21 December 2006).

Hinchey, M.G. & Bowen, J.P. (Eds.) (1995): *Applications of Formal Methods*, International Series in Computer Science, Herts, UK, Prentice Hall.

Hopkins, A. (2000): *Lessons from Longford: The Esso Gas Plant Explosion*. Sydney, CCH.

Hopkins, A. (2005): *Safety, Culture and Risk: The Organisational Causes of Disasters*. Sydney, CCH.

Hitchcock, C. (2002): Probabilistic Causation, In Edward N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy (Fall 2002 Edition)*, http://plato.stanford.edu/archives/fall2002/entries/causation-probabilistic

Höhl, M. & Ladkin, P. (1997): *Analysing the 1993 Warsaw Accident with a WB-Graph*. Report RVS-Occ-97-09, 8 September, Faculty of Technology, Bielefeld University. http://www.rvs.uni-bielefeld.de

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

Hollnagel, E. (2001): Anticipating Failures: What should Predictions be About? In *The Human Factor in System Reliability - Is Human Performance Predictable?* RTO Meeting Proceedings 32, RTO-MP-32, January, Cedex, France, RTO, NATO.

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

Hollnagel, E. (2006). *CREAM - Cognitive Reliability and Error Analysis Method*, http://www.ida.liu.se/~eriho/CREAM_M.htm

Hollnagel, E. & Woods, D.D. (1983): Cognitive Systems Engineering: New wine in new bottles. *International Journal of Man-Machine Studies*, **18**:583-600.

Hollnagel, E. & Woods, D.D. (2005): *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*, New York, Taylor & Francis.

Hollnagel, E., Woods, D.D. & Leveson, N. (2006): *Resilience Engineering: Concepts and Precepts*. Aldershot, Ashgate.

IEC 61508 (1998-2000): *Functional safety of electrical/electronic/programmable electronic safety-related system*. Parts 1 to 7, Geneva, Switzerland, International Electrotechnical Commission.

Johnson, C.W. (2003): *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. Glasgow, Scotland, University of Glasgow Press. http://www.dcs.gla.ac.uk/~johnson/book

Johnson, C.W. & de Almeida, I.M. (2007): An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03. *Safety Science*, In Press, doi:10.1016/j.ssci.2006.05.007.

Johnson, C.W. & Holloway, C.M. (2007): A Longitudinal Analysis of the Causal Factors in Major Maritime Accidents in the USA and Canada (1996-2006). *Proceedings of the 15th Safety-Critical Systems Symposium*, Bristol, UK, 13-15 February, F. Redmill and T. Anderson (Eds.), The Safety of Systems, 85-94, Springer.

Johnson, C. & Holloway, C.M. (2003a). A Survey of Logic Formalisms to Support Mishap Analysis. *Reliability Engineering & System Safety*, **80**(3):271-291.

Johnson, C. & Holloway, C.M. (2003b): The ESA/NASA SOHO Mission Interruption: Using the STAMP Accident Analysis Technique for a Software Related 'Mishap'. *Software: Practice and Experience*, **33**:1177-1198.

Kroes, P., Franssen, M., van de Poel, Ibo. & Ottens, M. (2006): Treating socio-technical systems as engineering systems: some conceptual problems. *Systems Research and Behavioral Science*, **23**(6):803-814.

Ladkin, P.B. & Loer, K. (1998): *Why-Because Analysis: Formal reasoning about incidents*. Technical Report

RVS-Bk-98-01, Faculty of Technology, Bielefeld University. http://www.rvs.uni-bielefeld.de

Ladkin, P.B. & Stuphorn, J. (2003): Two Causal Analyses of the Black Hawk Shootdown During Operation Provide Comfort. *Proceedings of the 8th Australian Workshop on Safety Critical Software and Systems,* Peter Lindsay and Tony Cant (Eds.), Conferences in Research and Practice in Information Technology, Volume 33, Canberra, Australian Computer Society.

Ladkin, P.B. (2005): *Why-Because Analysis of the Glenbrook, NSW Rail Accident and Comparison with Hopkins's Accimap*. Report RVS-RR-05-05, 19 December, Faculty of Technology, Bielefeld University. http://www.rvs.uni-bielefeld.de

Lamsweerde, A.V. (2000): Formal Specification: A Roadmap. *Proceedings of the Conference on The Future of Software Engineering*, Limerick, Ireland, 147-159, ACM Press.

LaRC (2004): The CAUSE Project, Research on Accident Analysis, NASA Langley Formal Methods Site. http://shemesh.larc.nasa.gov/fm/fm-now-cause.html (accessed: 18 December 2006).

Leveson, N.G. (1995): *Safeware: System Safety and Computers*. Reading, MA, Addison-Wesley.

Leveson, N.G. (2002): *System Safety Engineering: Back to the Future.* Aeronautics and Astronautics Department. Cambridge, MA, Massachusetts Institute of Technology. http://sunnyday.mit.edu/book2.pdf

Leveson, N. (2004): A New Accident Model for Engineering Safer Systems. *Safety Science*, **42**(4): 237-270.

Leveson, N.G., Allen, P. & Storey, Margaret-Anne. (2002): The Analysis of a Friendly Fire Accident using a Systems Model of Accidents. *Proceedings of the 20th International System Safety Conference*, Denver, Colorado, 5-9 August.

Leveson, N.G. & Dulac, N. (2005): Safety and Risk-Driven Design in Complex Systems-of-Systems. *1st NASA/AIAA Space Exploration Conference*, Orlando.

Lewis, D. (1973). Causation. *Journal of Philosophy*. **70**: 556-567.

Marais, K., Dulac, N., & Leveson, N. (2004): Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems, *ESD Symposium*, Cambridge, MA, Massachusetts Institute of Technology.

Parasuraman, R. (1997): Humans and Automation: use, misuse, disuse, abuse, *Human Factors*, **39**(2):230-253.

Pearl, J. (2000): *Causality: Models, Reasoning, and Inference*. Cambridge, Cambridge University Press.

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

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

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

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

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

Sagan, S. (1993): *Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, NJ, Princeton University Press.

Shorrock, S., Young, M. & Faulkner, J. (2003): Who moved my (Swiss) cheese? *Aircraft and Aerospace*, January/February, 31-33.

Shrivastava, P. (1992): *Bhopal: Anatomy of a Crisis*. Second Edition, London, Paul Chapman.

Trist, E.L. & Bamforth, K.W. (1951): Some Social and Psychological Consequences of the Longwall Method of Coal-Getting, *Human Relations*, **4**:3-39.

Vaughn, D. (1996): *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago, University of Chicago Press.

Vicente, K.J., Mumaw, R.J. & Roth, E.M. (2004): Operator monitoring in a complex dynamic work environment: A qualitative cognitive model based on field observations. *Theoretical Issues in Ergonomics Science*, **5**(5):359-384.

Woo, D.M. &. Vicente, K.J. (2003): Sociotechnical systems, risk management, and public health: comparing the North Battleford and Walkerton outbreaks. *Reliability Engineering & System Safety*, **80**:253-269.

Woods D. D., Johannesen L. J., Cook R.I. and Sarter N. B. (1994): *Behind Human Error: Cognitive Systems, Computers and Hindsight*. SOAR Report 94\-01, Wright-Patterson Air Force Base, Ohio, CSERIAC.