Systemic Safety and Accident Modelling of Complex Socio-technical Systems

Zahid H. Qureshi and Alistair Campbell
Defence and Systems Institute, University of South Australia
zahid.qureshi [alistair.campbell]@unisa.edu.au

Abstract. Modern systems such as transportation, defence, telecommunications, nuclear power plants, robots and autonomous vehicles are increasingly becoming more complex. This is leading to new kinds of system failures, safety issues and severe accidents. The traditional approaches to system design and safety analysis are not adequate to capture the complexities and dynamics of modern socio-technical systems. This paper focuses on new approaches to safety and accident modelling of socio-technical systems based on systems theory and cognitive systems engineering. We examine the contributions by organisational sociologists to safety in complex organisations managing and operating high-risk technological systems. This paper recommends interdisciplinary research encompassing technology, human factors, and organisational sociology, 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 accident causation.

Introduction

Modern systems such as transportation, defence and aerospace, chemical and petroleum industry, healthcare and patient safety, and robots and autonomous vehicles are increasingly becoming more complex. The complexity is exacerbated by the use of advanced technologies, in particular, automation, artificial intelligence and digital technologies. This is leading to new kinds of system failures, safety issues, and potentially disastrous failure modes which can result in severe accidents. Notable disasters and accidents such as the Bhopal toxic gas disaster (Srivastava 1992) and NASA Challenger shuttle explosion (Vaughn 1996) are among many examples of system failures in complex systems that lead to serious loss of material and human life.

Bhopal is probably the site of the greatest industrial disaster in history. In the early hours of 3rd December 1984, a pesticide plant owned by Union Carbide, a US-based multinational company, released a cloud of deadly gas into the atmosphere (Srivastava 1992). It resulted in thousands of people dying within the first few days, and affecting the health of many thousands of families to date. The Bhopal disaster was a result of a combination of legal, technological, organisational, and human errors (Rasmussen 1997).

One of the worst air-to-air friendly fire accidents involving US aircraft in military history occurred on April 14, 1994 over northern Iraq (AAIB 1994) during Operation Provide Comfort. A pair of F-15Cs of the 52nd Fighter Wing enforcing the No Fly Zone mistakenly shot down two UH-60 Black Hawk helicopters, killing 26 American and United Nations personnel who were carrying out humanitarian aid to Kurdish areas of Iraq. The major reasons for this accident were organisational factors and the human operational use of technical systems that were embedded in a complex Command and Control structure (Leveson 2002).

The main goals of system safety are to prevent the occurrence of accidents in engineered systems and to reduce their consequences if they occur. An accident model provides an understanding of

system behaviour and associated cause-effect relationships between various components. They are used as techniques for hazard identification and risk assessment during system development in order to influence a safe design, and for post accident analysis to provide recommendations and countermeasures to avoid the occurrence of similar accidents.

Traditional safety analysis and accident models (e.g. Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA)) are based on a linear notion of causality, and consider an accident as arising from a single root cause. These models could adequately explain the failures of simple electro-mechanical systems that existed prior to the introduction of digital technology. Technological advancements and particularly digital technology (hardware and particularly software) is creating new safety problems and changing the nature of accidents. Thus, new accident models are needed: to capture the complexity and dynamics of modern complex systems; to provide new causal explanatory mechanisms to understand system accidents; and to support the development of new risk assessment techniques to prevent their occurrence (Leveson 2004).

The traditional sequential and epidemiological accident models are inadequate to explain the dynamics and nonlinear interactions between system components in complex systems. New systemic accident models, based on systems theory and cognitive systems engineering 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).

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 complex socio-technical systems. We examine the human, social, cultural and organisational factors in system accidents, and discuss organisational theories on safety and accident causation, and interdisciplinary trends in the application and development of systemic accident models that consider the human, technical and organisation factors.

Limitations of Traditional Safety Models

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 (Heinrich et al. 1980). An initiating domino is related to an adverse event or condition (the root cause), which produces an effect (another domino), which in turn leads to another adverse event and this sequence of dominos hit each other and cause an accident. FTA and FMEA are typical techniques based on this model that are employed for investigating technical failures in engineering systems (Leveson 1995). This model implies that an accident is the result of a single cause, and if that single cause can be identified and removed the accident will not be repeated. Industrial research has shown that accidents have multiple causes and contributory factors (Rasmussen 1997).

Sequential models are based on the premise that failures of a physical component or human error in a system are the abnormal events that cause accidents. In this approach, the human is considered as a component of the system similar to a technical component, and human error occurs when there is a deviation from a standard operating procedure. However, human behaviour is much more complex and this approach is inadequate for modelling human error in complex situations such as control and decision making in aviation.

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 (Leveson 1995). Sequential models assume that the cause-effect relation between consecutive events is linear and deterministic; whereas in complex socio-technical systems the relationships are complex and non-linear. The first event in the chain is often considered the "initiating event"; however, the selection of the initiating event is arbitrary and previous events and conditions could always be added (Leveson 2004). A particular event may be selected as the cause because it is the event immediately preceding the accident. The friendly fire shoot down of the two US Black Hawk helicopters in Iraq (AAIB 1994) could be blamed on the F-15 pilots (human error), since the last condition before the accident was the firing of the missiles. However, the accident report has identified several factors and events that contributed to the accident, such as organisational, human and technological factors. Occasionally, an accident investigator will stop at a particular event or condition that is familiar and can be used as an acceptable explanation of the accident (Leveson 2004). There are no guidelines on the stopping rules or objective criterion for identifying the initiating event from amongst the several contributory factors.

Epidemiological Accident Models

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 (1997) emphasises the concept of organisational safety and how defences (protection barriers e.g. 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. The latent conditions (arising from management decision practices or cultural influences) combine adversely with local triggering events (weather, location) and with active failures (errors and/or procedural violation) committed by individuals or teams at the sharp end of an organisation, to produce the accident.

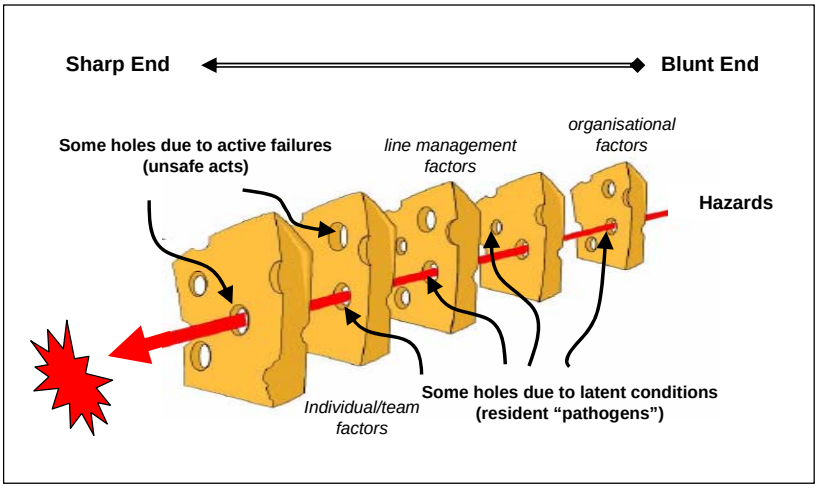

Figure 2: Swiss Cheese Model of Defences (Reason, 1997)

The dynamics of accident causation are represented in the Swiss cheese model of defences (Figure 2), where each slice represents a barrier to an adverse event. The holes represent weaknesses or failures in their respective barriers, and when the holes in the barriers align (shown by the arrow) an accident emerges due to these holes (failures) in barriers and safeguards.

A major advantage of this model is that by introducing the concept of latent factors, it can explain accident causation by including events that occurred at a remote time and space and linking them to events at the time of occurrence of an accident. 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 due to the dynamic and adaptive nature of the organisation.

Socio-technical Complexities in Industrial Systems

The design and operation of modern complex engineered systems is significantly influenced by the advances in technology, dynamic operational environments, economical and social environmental constraints, and legal and safety regulations. In particular, digital technology and automation haves augmented the complexity of technological systems by creating new kinds of system failures, and particularly where software errors have been attributed to many aerospace and transportation accidents (Leveson 2004).

A complex system is composed of many components that interact with each other in linear and non-linear manners. In contrast to loose coupling between system components, a component failure in tightly coupled systems has an immediate impact on the interacting component. The property of interdependence between components gives rise to system-level (emergent) behaviours, which cannot be inferred completely from the behaviour of individual components. The interactive complexity and tight coupling and their emergent affects, especially in systems which have many dynamically interacting components, are difficult to comprehend at the design stage. Perrow (1984) argues that these two properties, in particular, can make a complex system (technological or organisations) susceptible to accidents.

Modern complex systems generally involve human interaction with the technical system, such as a pilot flying an aircraft. The behaviour of the pilot is equally important as is the proper functioning of the technical system, where the pilot-aircraft forms the "unified whole" that constitutes the system (Kroes et al. 2006) which is necessary to perform its intended function of flying. Such systems, composed of human agents and technical artefacts, are often embedded within complex social structures such as the organisational goals, policies, legal, and political elements. For example, civil aviation is a complex public transportation system comprising technological artefacts (e.g. aircrafts, luggage transport, communication equipment); these artefacts have various interconnections and they all play an essential role in the functioning of the system as a whole (Kroes et al. 2006). These technical artefacts and systems operate in a social-organisational environment which influences the joint system behaviour. Kroes et al. argue that 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 systems.

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. Traditional accident models are unsuitable to capture the dynamics of the heterogeneous elements of the socio-technical system, i.e. the interdependencies between the technical systems, software, humans, and organisational elements. New models, such as systemic accident models, should now be employed that are more capable of providing causal explanations of socio-technical accidents.

Systemic Accident Models

Systems Theoretic Approach

New approaches to accident modelling adopt a systemic view which considers the performance of the system as a whole. In systemic models, an accident occurs when several latent and proximate 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 and cybernetics, which includes the principles, models, and laws necessary to understand complex interrelationships and interdependencies between technical, human, organisational elements.

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

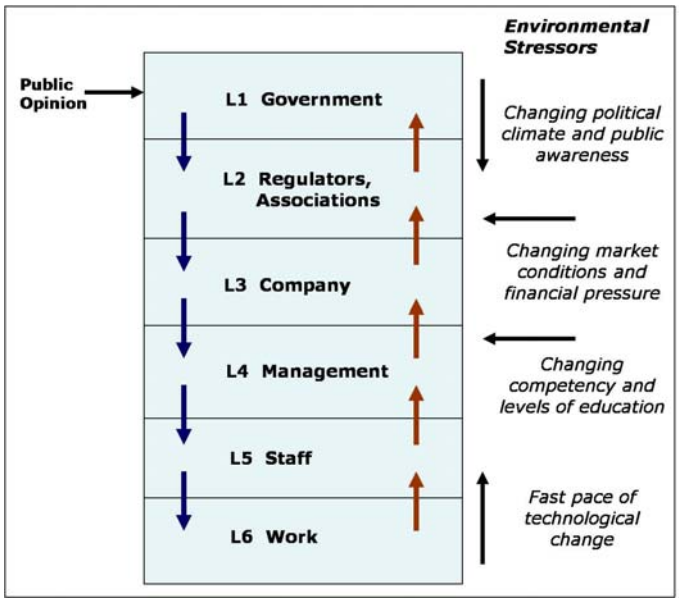

Figure 3: Model of Socio-technical System (Rasmussen 1997)

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 such as nuclear power plant and aviation.

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 highlights the need for "vertical" alignment across the levels in Figure 3. The organisational/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. These external influences should be considered at each level along with the dynamic constraints from other levels.

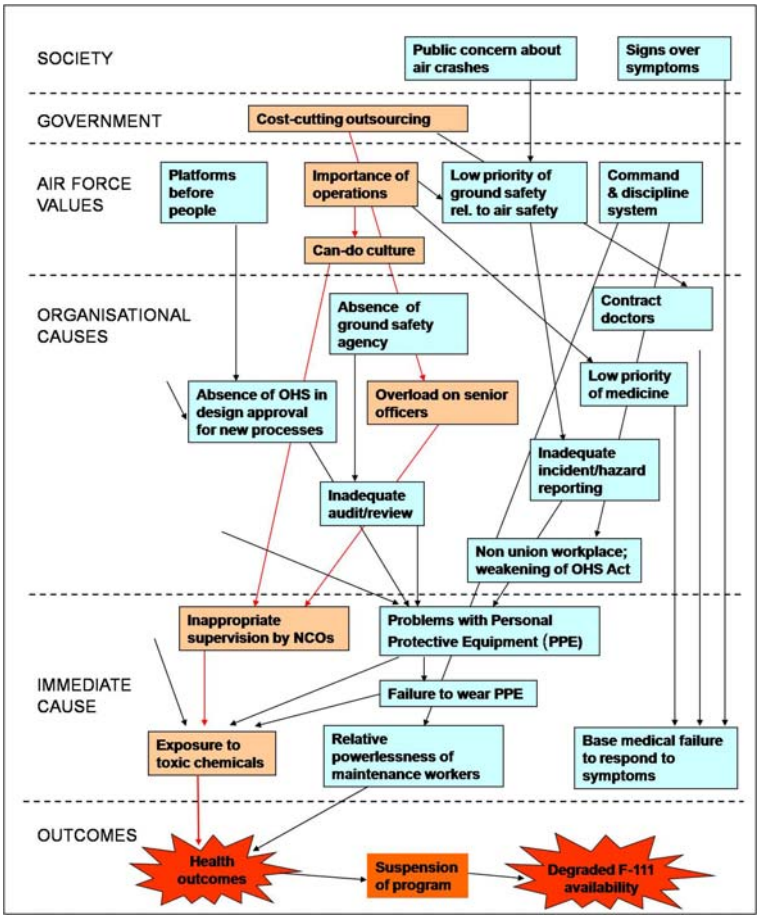

Figure 4: AcciMap Extract of F-111 Program (Clarkson et al. 2001)

AcciMap is an accident analysis technique is based on Rasmussen's risk management framework, which captures the various causes of an accident at each level of the socio-technical system and shows the interrelationships between them (Rasmussen 1997). An AcciMap analysis of the F-111 chemical exposure of Royal Australian Air Force (RAAF) workers was conducted in the official F-111 Board of Inquiry report (Clarkson et al. 2001). It uses counterfactual reasoning to establish the relationships between causal factors at all levels of the organisational hierarchy. The AcciMap causal flow diagram (Figure 4) explains the organisational and other systemic factors that contributed to the final outcome. This analysis shows that the focus should not be directed solely at the human factors or other errors, and concludes that the factors that lead to the final adverse situation include the values and culture of RAAF, cost-cutting and down-sizing of employees, and social attitudes such as the focus on air safety and low priority to ground safety.

In the STAMP (Systems-Theoretic Accident Model and Processes) 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 (Leveson 2004). "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, 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. Failures can be broadly attributed to: the controller issuing or executing inadequate or inappropriate control actions; or there may be missing or inadequate feedback.

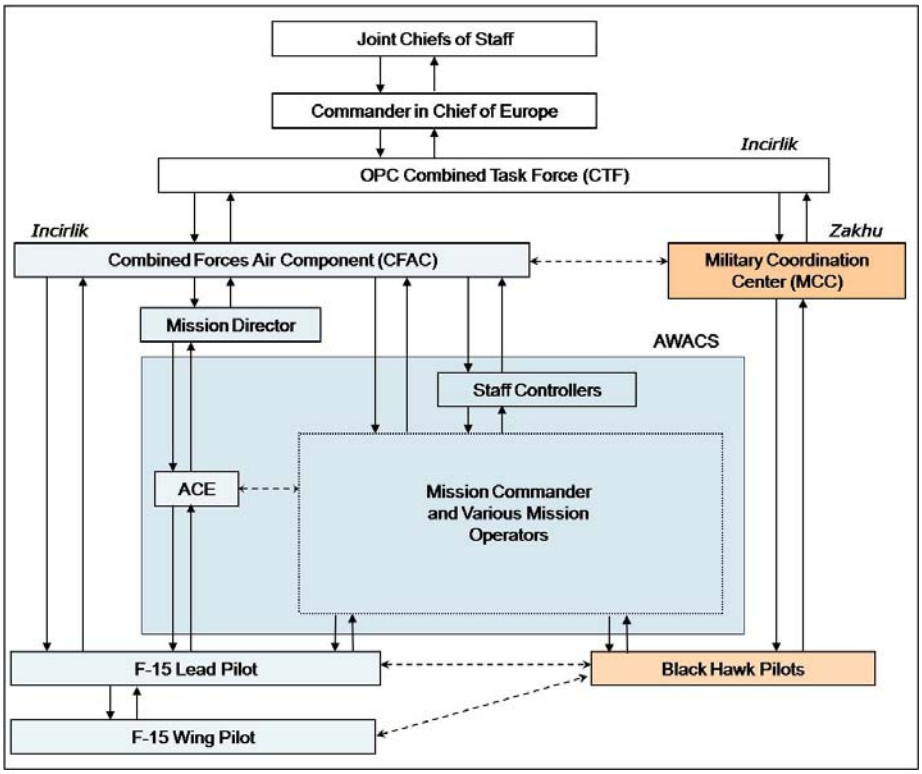

Figure 5: Blackhawk Fratricide C&C Structure (Leveson 2002)

In the STAMP analysis of the Black Hawk fratricide (Leveson 2002) in Iraq in 1991, first, the hierarchical command and control structure of the Black Hawk accident is developed starting from the Joint Chiefs of Staff down to the aircraft involved in the accident (Figure 5). The safety constraints and flawed control are analysed at each level in the hierarchical control structure to obtain a system-wide understanding of the contributory causal factors. For example, at the lowest level in the control structure, the pilots directly control the aircraft (operator at the sharp end). There were, however, several dysfunctional interactions and communication inadequacies (shown by the dotted lines) 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. 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. The use of the STAMP analysis provides a richer causal explanation as compared with the official investigation report. STAMP was also effective in analysing a Canadian public water safety system, and provided explanations of the dysfunctional interactions between different levels of the organisation that led to the water contamination (Leveson 2004).

Cognitive Systems Engineering Approach

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 & Riley 1997). Human error is generally considered as the main cause of accidents in complex engineered systems, and current Human Reliability Analysis (HRA) techniques arrive at this conclusion as they consider human behaviour similar to technical component failures (Hollnagel 1998). Human behaviour cannot be studied in isolation of the environment and the context of the particular situation in which work takes place. There are several factors in the context/environment, such as technical design, economical, procedural, cultural and organisational, which influence and shape human performance (known as performance shaping factors - PSF). Cognitive Systems Engineering (Hollnagel & Woods 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. Hollnagel & Woods (2005) propose a new paradigm of how humans and technology function as joint (cognitive) systems. They argue that “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”.

A number of systemic accident models for safety and accident analysis have been developed based on the principles of cognitive systems engineering such as: Cognitive Reliability and Error Analysis Method (CREAM); Driving Reliability and Error Analysis Method (DREAM), 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), with particular consideration of the context and impact of contextual factors on human reliability. The first step in analysing an accident is defining the context in which the error conditions and events occur. The conditions that shape context are called “Common Performance Conditions” (CPC), and are similar to the traditional PSFs. The CPC is a limited set of factors (Hollnagel 1998; Table 6, p.

113) containing the general determinants of performance, which assists in identifying the more likely action paths. The contextual conditions guide the selection of causes that are more likely to have contributed to the particular accident, such as on a rainy day the causes relating to driver alertness and car speed are more likely to have caused the accident.

A classification scheme is used that lists possible causal factors which can contribute to the performance of the human and machine leading to the accident. The scheme provides a clear distinction between the observable consequences or effects (phenotypes) of a dysfunctional behaviour, and the causes (genotypes) of those consequences. . Hollnagel (1998) provides a listing of error modes (Table 19, p. 179) as general consequents, each having several general antecedents, which is used to identify the most likely error modes (phenotypes) in the context of the accident. The classification scheme also provides a link between a particular phenotype and possible causes, for example, if the observed consequence of an accident is high speed, then possible causes may include communication failure, equipment failure, and driver distraction. After choosing a general antecedent e.g. communication failure, a general consequent is searched in other tables. The tables in CREAM are formally called 'groups', and the listed consequents and antecedents fall under a broader classification. At a higher level, the groups are separated into three major categories of causes relating to human, technological and organisational factors. CREAM shows the links between the possible set of causes in these categories to the consequent of failure. If enough information is available to choose a specific antecedent, then the analysis can stop for that branch.

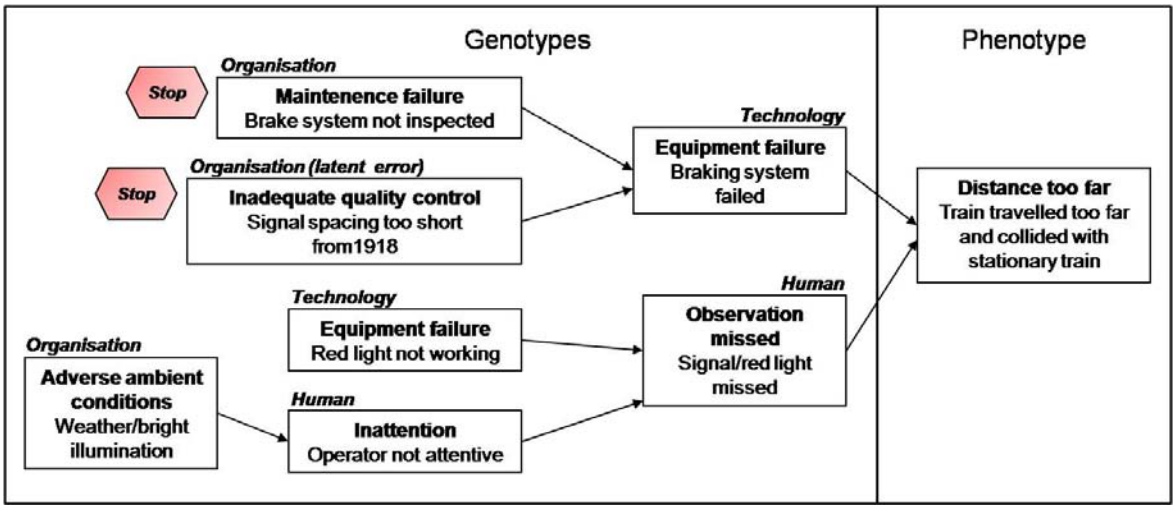

Figure 6: CREAM analysis of a train accident (Adapted from, Hollnagel 1998)

CREAM was applied for retrospective analysis of the New York City subway train accident that occurred in June 1995 (Hollnagel 1998). A subway train crashed into the rear end of a stationary train at a speed of about 14-18 mph. Initial causes of the accident were attributed to: 'train driver missed the red warning light' (human error) and 'automated emergency brakes malfunctioned' (technical error). Using the CREAM method, the observable consequence was the train collision which is due to the error mode regarding distance travelled by the first train was too far (selected as the phenotype in Figure 6). The error mode of 'distance' (Table 19, p. 179) lists several general antecedents and specific antecedents, and two possible general antecedents 'equipment failure' and 'observation missed' are selected as they support the context of the accident. In the classification group for 'equipment' (Table 25, p. 1182), the likely antecedents that could explain the failure of brakes are 'maintenance failure' and 'inadequate quality control'. The two nodes

belong to the Organisation group and are the stopping points since there are no general antecedents to follow. Note that ‘inadequate quality control’ is a latent error, since it occurred much earlier at a remote time and space. From the ‘observation’ group table (Table 20, p. 180), the likely antecedents for ‘observation missed’ are ‘equipment failure’ and ‘inattention’, shown in Figure 6. Similarly in the ‘temporary person related functions’ group table (Table 23, p. 181), the antecedent for ‘inattention’ is ‘adverse ambient condition’.

The official investigation determined that the train driver did pass the stop light and the emergency brake had worked. Thus the cause ‘maintenance failure’ can be excluded as an antecedent for ‘equipment failure’. The stopping distance specified earlier in 1918 for train speeds at that time, was quite inadequate in 1995 for trains travelling at higher speeds. This is related to an organisational error ‘inadequate quality control’ since attention was not paid to this factor. CREAM identifies the various socio-technical causal factors (human, technical and organisational) and shows their inter-relationships to the final accident occurrence. This example shows how the method and classification scheme of CREAM can be applied, and how a systematic use can assist greatly in identifying and explaining the likely causes of an accident.

The classification scheme described in CREAM is of a rather general nature which limits its application to many industrial domains. This method is quite difficult to use especially when several tables need to be searched, and lacks a well documented guideline for accident analysis.

DREAM is an adaptation to the traffic safety domain of the generic CREAM method, and it has been used for the analysis of several road accidents (Sagberg 2007). An important advantage of DREAM is the use of the classification of predefined causal factors that are involved in the majority of road accidents, which enables the aggregation of analysis results from individual cases to discover causation patterns among different groupings of accidents (for details see, Sagberg 2007).

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). Hollnagel argues that the performance variability of the system is analogous to the concept of resonance, where the system performance variability arises as a result of variability of the functions in the system. Furthermore, in order to understand system performance variability leading to failures and accidents, it is important to understand the normal variability of functions, and system failure occur as a resonance of the normal variability of functions. Functional resonance provides a useful analogy to model underlying mechanism in accidents and in understanding the emergent effect of undesirable system performance variations. This can also provide insights into developing remedial policies for the prevention of similar future accidents.

Hollnagel (2004) proposes a hexagonal representation for the functional components (Figure 7) of the socio-technical system, with six connectors which provide the linking of the various functions in different ways. FRAM analysis has been applied to conduct risk assessment of RNAV operations which is a method for navigation of aircraft flights (Hollnagel & Goteman 2004). Nine functions for the RNAV approach system are identified, and represented by their respective hexagons. Next the normal couplings between the nine functions are identified. The potential for variability of a function was rated using a number of common performance conditions: stable or variable but adequate; stable or variable but inadequate; and unpredictable. The normal coupling of all functions, along with their performance conditions, shows that the system RNAV approach is susceptible to performance variability that may affect the outcome. This analysis identified

several cases where normal connections between functions might fail, and also a number of potential unexpected connections. The analysis concluded that there were four possible failures in the RNAV operations which could lead to a risk for collision with other aircraft, and recommended a barrier to provide defences to failure modes.

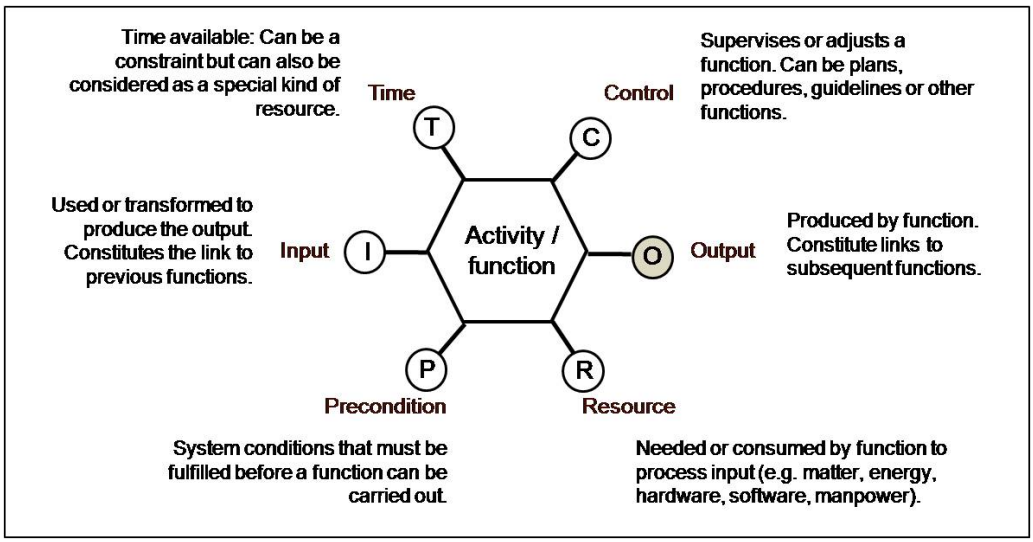

Figure 7: FRAM Functional Unit (Hollnagel & Goteman, 2004)

The analysis concluded that there were four possible failures in the RNAV operations which could lead to a risk for collision with other aircraft, and recommended a barrier to provide defences to failure modes. Sawaragi et al. (2006) applied FRAM to conduct a retrospective analysis of the aircraft accident that occurred at Cali airport in Columbia in 1995. FRAM analysis greatly contributed to modelling and understanding the emergence of the complex behaviours due to the interactions of the air traffic controllers and the different roles of two pilots.

Organisational Analysis of Accident Causation

Organisational Causes of Accidents

Organisations managing and operating high-risk technologies can be considered as complex socio-technical environments with systemic dependencies and tight coupling in the organisation structure, management policies, humans and technology. Industrial accident research has shown that, besides technical failures and human errors, organisational factors contribute significantly to a gradual drift of the socio-technical system to failure and unsafe state. Hopkins (2000) analysed the Royal Commission findings 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. Many cultural and organisational causes of the F-111 chemical exposure to RAAF workers were also identified using AccMap technique (see Figure 4).

NASA's Space Shuttle Challenger disintegrated in a ball of fire 73 seconds after launch on 28 January 1986. The Rogers Commission Report (1986) identified the cause of the disaster: the

O-rings that seal the Solid Rocket Booster joints failed to seal, allowing hot gases at ignition to erode the O-rings, penetrate the wall of the booster, which finally destroyed Challenger and its crew. The Commission also discovered an organisational failure in NASA. In a midnight hour teleconference on the eve of the Challenger launch, NASA managers had proceeded with launch despite the objections of contractor engineers who were concerned about the effect of predicted cold temperatures on the rubber-like O-rings. Further, the investigation discovered that NASA managers had suppressed information about the teleconference controversy, violating rules about passing information to their superiors; NASA had been incurring O-ring damage on shuttle missions for years. Rogers Commission also identified "flawed decision making" as a contributing cause of the accident, in addition to other causal factors such as production and schedule pressures, and violation of internal rules and procedures in order to launch on time.

Vaughn (1996) presents an alternative sociological analysis of the Challenger shuttle accident, and argues that traditional safety analysis techniques were limited in their capacity to go beyond technical component 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 identified 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, which silenced people. These elements had shaped shuttle decision making for over a decade, they occurred simultaneously and were focused on a single decision to meet the Challenger launch deadline.

A group of social scientists examined NASA's organisational, historical and cultural factors and provided insights into how these factors contributed to the Columbia shuttle accident (CAIB 2003). In the Board's view, NASA's organisational structure and culture was equally a causal factor of the accident as the physical cause (the foam debris strike). In particular, Vaughan highlighted the similarities of organisational system failures in both Columbia and Challenger accidents, and presented a causal explanation that links the culture of production, the normalisation of deviance, and structural secrecy in NASA. (CAIB 2003: Chap. 8).

There are two main schools of thought in sociology that have addressed the social, cultural and organisational aspects of safety and risk; they are identified as Normal Accident Theory (Perrow 1984) and High Reliability Organisation Theory (see for example, Roberts 1989). These theories provide different explanations on safety and accident causation in complex organisations and offer alternative strategies for safety and risk management. The main premise of Normal Accident Theory is that even though risk prevention is taken seriously, there are several cognitive, social, cultural and system characteristics that over time accidents are inevitable. According to this theory, the organisations managing hazardous technologies exhibiting both high interactive complexity and tight coupling are candidates for accidents which cannot be avoided. High reliability theorists argue that accidents in the modern world can be prevented by complex organisations if appropriate organisational designs and management techniques are employed (Sagan 1993). Sagan argues that organisation theories on accidents and risk are necessary to understand and address the social causes of an accident and in enhancing performance in technologically complex organisations to safely operate and manage high-risk technological systems.

Discussion and Conclusion

The underlying models of accidents can typically be grouped into three types (Hollnagel 2004): sequential models, epidemiological models, and systemic models. 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 FTA and FMECA, 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. 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.

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 in diverse domains.

Similarly, STAMP has been applied to a number of case studies for *post hoc* accident analysis (e.g., Leveson 2002; Johnson & Holloway 2003). 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.

Normal Accident Theory and High Reliability Organisation Theory, have addressed the social, cultural and organisational aspects of safety and risk These theories generally emphasise the organisational aspect of accidents and tend to overlook the technical aspects, oversimplify the causes of accidents by focusing only on simple redundancy, and not considering accidents where component failure is not the cause (Marias et al. 2004).

System theoretical approach to safety provides a framework for modelling the technical, human, social and organisational factors in socio-technical systems, including complex 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).

Systemic models should be further developed to include detailed organisational and cultural factors and to conduct multidisciplinary research incorporating macroergonomics and organisational sociology in particular. In order for industrial applications of the various systemic

models, analysis techniques should be automated and computer tools developed to facilitate the evaluation and application of these models.

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, Royal Australian Air Force.

Heinrich, H. W., Petersen, D. & Roos, N. (1980). Industrial Accident Prevention. New York: McGraw-Hill.

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

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

Hollnagel, E. & Goteman, O. (2004): The Functional Resonance Accident Model. Proceedings of Cognitive System Engineering in Process Plant 2004, CSEPC 2004, pp. 155-161.

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.

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

Johnson, C. & Holloway, C.M. (2003): 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.

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

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. & Riley, V. (1997): Humans and Automation: use, misuse, disuse, abuse. Human Factors, 39(2): 230-253.

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.

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

Roberts, K. H. (1989). New Challenges in Organization Research: High Reliability Organizations. Industrial Crisis Quarterly, 3(2): 111-125.

Rogers Commission Report (1986). Report of the Presidential Commission on the Space Shuttle Challenger Accident. June 6, Washington, D.C.: NASA. `http://history.nasa.gov/rogersrep/genindex.htm`

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

Sagberg, F. (2007): A Methodological Study of the Driving Reliability and Error Analysis Method (DREAM), TOI Report 912/2007, Oslo: Institute of Transport Economics.

Sawaragi, T., Horiguchil, Y. and Hina, A. (2006). Safety Analysis of Systemic Accidents Triggered by Performance Deviation. SICE-ICASE International Joint Conference 2006, Oct. 18-21, Bexco, Busan, Korea.

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

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

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

Weick, K. E. (1987). Organizational Culture as a Source of High Reliability. California Management Review, 29(2): 112-127.

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.

BIOGRAPHY

Zahid H. Qureshi is a Senior Lecturer in the Defence and Systems Institute at the University of South Australia. He graduated with a B.Sc. in Electronics Engineering from the University of Engineering and Technology, Lahore, Pakistan and a Ph.D. in Systems Science from the University of Wollongong, Australia. Dr. Qureshi's current research interests are in system safety of complex socio-technical systems, interdisciplinary research in the design and management of socio-technical systems in complex organisations. Dr. Qureshi has previously worked in the Australian Defence Science and Technology Organisation, and in industry on rail transportation and safety-critical software. Dr. Qureshi has also lectured in software engineering at undergraduate and postgraduate levels at the Nanyang Technological University, Singapore.