The Flight of Information: New Approaches for Investigating Aviation Accident Causation

A thesis submitted for the degree of
Doctor of
Philosophy

by
Thomas G C Griffin
School of Engineering and Design
Brunel University
May 2010

"There is no problem so complex that it cannot simply be blamed on the pilot."

Dr. Earl Weiner, Human Factors Society President.

Abstract

The investigation and modelling of aviation accident causation is dominated by linear models. Aviation is, however, a complex system and as such suffers from being artificially manipulated into non-complex models and methods. This thesis addresses this issue by developing a new approach to investigating aviation accident causation through information networks. These networks centralise communication and the flow of information as key indicators of a system's health and risk. The holistic approach focuses on the system itself rather than any individual event. The activity and communication of constituent elements, both human and non-human agents, within that system is identified and highlights areas of system failure.

The model offers many potential developments and some key areas are studied in this research. Through the centralisation of barriers and information nodes the method can be applied to almost any situation. The application of Bayesian mathematics to historical data populations provides scope for studying error migration and barrier manipulation. The thesis also provides application of these predictions to a flight simulator study in an attempt of validation. Beyond this the thesis also discusses the applicability of the approach to industry. Through working with a legacy airline the methods discussed are used as the basis for a new and forward-thinking safety management system.

This holistic approach focuses on the system environment, the activity that takes place within it, the strategies used to conduct this activity, the way in which the constituent parts of the system (both human and non-human) interact and the behaviour required. Each stage of this thesis identifies and expands upon the potential of the information network approach maintaining firm focus on the overall health of a system. It is contended that through the further development and application of this approach, understanding of aviation risk can be improved.

Contents

Figures

Tables

Acknowledgements

I would like to start by expressing sincere thanks to my supervisors Dr Mark Young and Prof Neville Stanton. It is they who introduced me to the world of research and gave me the opportunity to embark on this thesis. Their continued guidance and support has been invaluable and I sincerely hope to continue working together in the future.

There are many others who deserve thanks for their unwavering support, or simply tolerating me as I undertook this journey and they include: My Mum, Dad, Andrew, Matthew, Alastair and all my family and friends who discussed, debated and supported my work. Without them all it would have been a very different experience.

Many thanks to Patrick Davis, of British Airways (BA), for inviting me to work with his Safety Management Team. The chance to work with a key-organisation in the aviation industry has really cemented my passion for aviation and provided such a great opportunity. Additional thanks go also to Kate Robinson at BA for all of her help as an SME in the production and testing of the distance from disaster methodology.

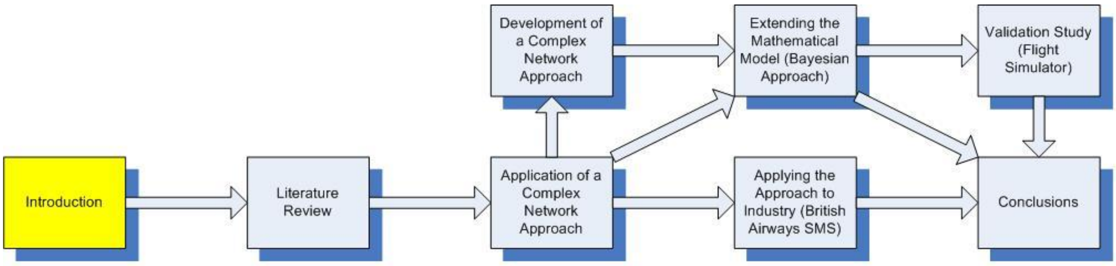
Thanks are also due to all of those who took time to correspond about the conference presentations or journal publications. Final thanks to all of the experimental participants who gave up their time to take part in the studies described in this thesis.

Commonly used Acronyms and Initialisms

The following is a reference list of acronyms and initialisms used within the thesis.

AA	American Airlines
AAIB	Air Accidents Investigation Branch
ASR	Air Safety Report
ASRS	Air Safety Reporting System
ATSB	Australian Transport Safety Bureau
BA	British Airways
BASIS	British Airways Safety Information System
CAA	Civil Aviation Authority
CCPS	Center for Chemical Process Safety
CHIRPS	Confidential Human factors Incident Reporting
CIRAS	Confidential Incident Reporting & Analysis System
DSA	Distributed Situation Awareness
EASA	European Aviation Safety Agency
EAST	Event Analysis of Systemic Teamwork
EGT	Exhaust Gas Temperature
EPR	Engine Pressure Ratio
FDR	Flight Data Recorder
GA	General Aviation
HFR	Human Factors Report
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IOSA	IATA Operational Safety Audit
JAA	Joint Aviation Authority
MOR	Mandatory Occurrence Report
N1	Gas Generator Section of Engine’s RPM
NTSB	National Transportation Safety Board
QF1	Qantas Flight 1 Accident Case Study
SA	Situation Awareness
SME	Subject Matter Expert
SMS	Safety Management System
SNA	Social Network Analysis
WESTT	Workload, Error, Situational Awareness, Time and Teamwork

1 Introduction



1.1 The field of "Human Factors"

Human Factors encompasses a large area of study within the realm of engineering and design. The basic premise of the research in this area is to increase performance, and especially in the last two decades performance in increasingly complex socio-technical systems.

Performance is a term that needs clarification due to its 'catch all' nature. Simply to increase performance within a system does not tell us too much; rather performance may be increased through increasing two main factors: Safety and productivity. Increasingly these two factors are seen as mutually exclusive; indeed Reason (1997) revisits several times the idea that in the 'battle' between productivity and protection of a system, it tends to be resolved in favour of the former due to the innate commercial nature of the areas where these systems exist e.g., Aviation, Rail, Nuclear, Chemical, Gas and Oil industries. This is not surprising in light of the discussions throughout Reason's book as a facet of human nature where increases in productivity have very positive results to individuals and to the collective but "by contrast, successful protection is indicated by absence of negative outcomes" (Reason, 1997, P.4). To management at all levels the former is indeed the more aspirational aim. In the system itself, however, these items are not at all exclusive; more so they are one and the same. As one is increasing the other by default will decrease but does not necessarily guarantee a negative. Rather, the level of 'absence' noted by Reason is diminished.

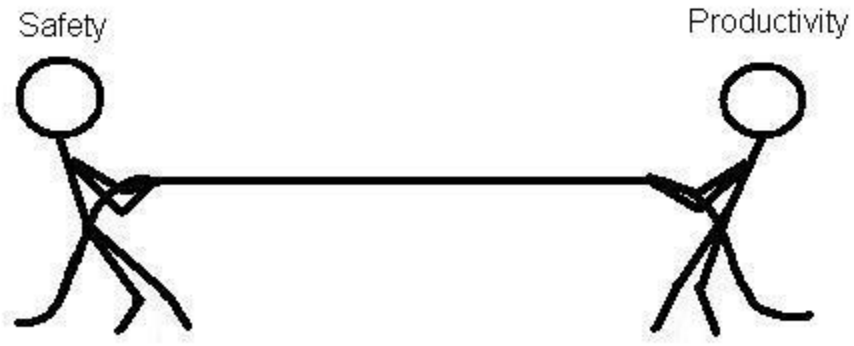


Figure 1-1 - The 'Battle' between performance characteristics within a system

In light of this, Human Factors has a very important role to play when looking at accident causation and investigation. As technology has become more reliable over time so the role of the human in the system has started to become the 'weak link' in a complex system, i.e., the human can act as pivotal between safety and productivity. There is nowhere more illustrative of this than the rapid development of aviation since its inception a century ago. For many years the accident rate was being reduced by increases in technological and industrial ability; the increase of structural integrity and reliability of the aircraft being flown and in particular the development of their propulsion, avionic and safety systems. However, in the last two decades, the serious accident rate[1] in commercial aviation has remained relatively stable at approximately one per million departures (Boeing Commercial Airplanes Group, 2000) and, as the continual increases in reliability etc. do not appear to be moving the statistics from this equilibrium, the focus to reduce these figures still further has become the human involved. For this reason, the field of Human Factors has evolved to play a major role in aviation accident investigation and its sole aim as stated in ICAO Annexe 13; "…the prevention of accidents and incidents[2]."

The 'accident pyramid' in Figure 1-2 was first developed by Heinrich (1930) and illustrates the comparable frequency of events in terms of magnitude. From this the human factors literature has developed comparisons with fatal accidents being the 'tip of the iceberg' and attempts to control the events at the larger base of the triangle in order to reduce those at the upper levels. The lower level of 'no-injury' accidents includes the largest group; that of 'near-misses' which have become a larger and more

---

[1] ICAO define a Serious accident as involving at least one serious injury/fatality, substantial damage or complete destruction of aircraft and fire (pre or post-crash)

[2] The term "incident" is taken to include near-misses and non-fatal/lesser-damage occurrences

important part of safety systems recently whereas the very tip may signify fatal accidents and these thankfully have reduced over time.

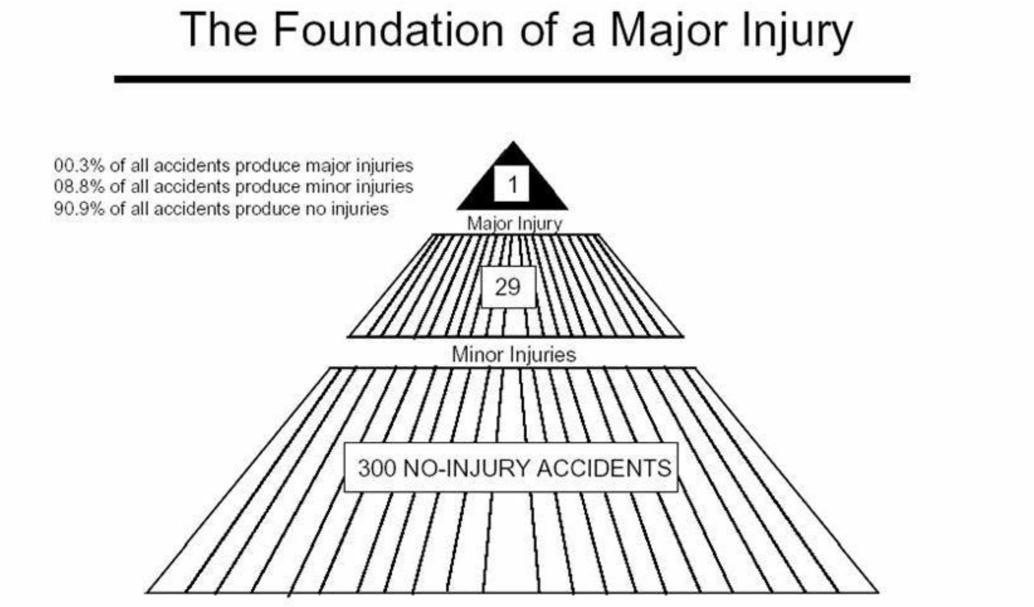


Figure 1-2 - Accident Pyramid (Adapted from Heinrich, 1930)

This Human Factors evolution was primarily hinged around the term human error: the errors committed by the operator of the system that 'caused' the accident or incident. The term Human Error itself has been well defined by Reason (1997) "as failure of planned actions to achieve their desired ends – without the intervention of some unforeseeable event." This in itself limits the areas of interest to those which can be affected directly by humans and possibly those which are proximal enough to have remedial actions possible and immediately effective. It is within this field that this project is based.

This thesis aims to address how we might go about improving the way in which we attempt to understand and investigate the complex world of aviation accidents and safety. More specifically this thesis explores the use of information networks to support improved risk mitigation.

1.2 Objectives and aims of the thesis

As highlighted above, and further discussed in the subsequent chapters of this thesis, the complexity of aviation accidents presents significant challenges both in academia and industry. Traditional models will be shown to be too linear that any representation of the real-world is artificial and limits usefulness. There needs to be a shift to understanding the system in which accidents (and equally normal-work events) take place rather than an improper emphasis on the end-result itself.

The thesis aims to address how information networks can be used to develop our understanding of complex system accidents and in particular those within the aviation domain. Through its focus on the system holistically and elements that are present within normal work, incidents and accidents it is hoped that artificial limitations are reduced and ultimately removed from risk mitigation methods.

The aims of this thesis are three-fold. Firstly a new method is to be developed and tested that **moves away from the linear models that currently dominate aviation risk investigation and reduction**. Full and real understanding of the complex aviation domain can only truly be realised if the models used in investigation reflect the non-linear complexities of the real world.

Secondly, the thesis looks to **incorporate general aviation** and make any method usable within this part of aviation equally as well as within the more heavily studied and discussed commercial world. Any new method would need to be able to address the sometimes very different issues which underlie these aviation types.

Thirdly, the thesis sets out to address **whether there is a fundamental difference between accidents and incidents**. Due to the reduction in aviation accidents, data are often not sufficient to develop system understanding. For this reason it would seem appropriate to turn to the more common incidents. However, it is important any method is able to cope with each type of event and does not preclude the use of incidents or oversimplify any relationship that they may have with actual aviation accidents.

A singular method is sought, therefore, that can address all of these issues. Complex network models are central to the work within this thesis and their many facets investigated in order to determine their true value within the field.

1.3 Structure of the thesis

This thesis has been constructed so that it can be read from beginning to end by readers new to this specific subject area. An attempt has also been made to maintain a simple writing style to aid understanding and inclusiveness. Later chapters are also designed to be read individually for those readers interested in specific areas of the research. In order to aid in the reading of this thesis signposting is included at the beginning of each chapter and in other positions as required. Figure 1-3 illustrates the outline of the thesis and helps in maintaining the central themes expanded upon below.
The themes developed in chapter 2 of the thesis, the literature review, are continued throughout the remaining chapters. In particular the central crux of this work is the

movement away from linear analysis of aviation events in chapters 3 to 8 (thesis aim). Chapters 3 and 4 identify information networks as a suitable tool to apply to aviation with the potential for integration with complex mathematics to provide both a qualitative and quantitative element (thesis aim). Chapters 5 and 6 build on the research and development from previous chapters in applying Bayesian mathematics to the information networks and testing this. In particular general aviation is the domain tested in order to provide a more comprehensive view of aviation that doesn't just centre on commercial operations (thesis aim). Chapter 7 then looks to firmly place the work in an industrial context (thesis aim) by working with a legacy airline and developing a brand new risk rating methodology based on a model consisting of networks. Finally chapter 8 looks to tie up some loose ends, look at possible further work and conclude the central thread of the thesis.

An overview of each chapter in slightly more detail is provided for the reader here:

Chapter 2, Modelling a dynamic world – The thesis commences with a scene setting chapter that sets out to explain the development of accident investigation models to date. Some of the key issues associated with these models and ways of thinking are explained and the foundations for the aims of the thesis identified.

Chapter 3, A complex approach to a complex scenario – In order to illustrate the usefulness of the information network approach, two polarised aircraft accident case studies are investigated with the technique. These case studies were selected as they illustrate two very different situations which led to very different events. It was considered important to show how applicable the method is to aviation accidents in their many guises. Each analysis, in this and subsequent chapters, may not be fully comprehensive on its own but throughout the thesis different aspects of the novel methodology are brought to the reader's attention and expanded upon.

Chapter 4, Development of a study – In this chapter the methods of developing information networks into a more comprehensive and useful approach are investigated. The chapter aims to draw quantitative measures to work collaboratively with qualitative aspects of the information networks. Bayesian mathematics are introduced as a potentially powerful ally of information networks and this forms the basis for the subsequent two chapters.

Chapter 5, Extending the potential of information networks; a Bayesian Approach – This chapter introduces the integration of Bayesian mathematics with the information network approach. A program was written to allow for a network to be investigated and potential error migration calculated in a novel way. Central to this chapter is addressing the thesis aim of developing a method that can not only be applied to commercial aviation, as is so often the focus of safety management, but also to general aviation. For this reason, data from general aviation accidents is used to populate probability information networks and potential uses investigated.

Chapter 6, Can we validate networks derived from incident data through simulation? A Pilot Study – Following on from the promising results of chapter 5, a flight simulator study was developed to validate the possible use and effectiveness of the Bayesian information network approach. Chapter 6 focuses on the planning and implementation of this flight simulator study together with statistical analysis of the resulting data. These data allow predictions of error migration to be tested and results discussed. Despite the study size being limited it is in the validation of the approach that the emphasis is on.

Chapter 7, Incidents versus Accidents; an Industrial Study – A central tenet of this thesis is the applicability of any developed methodology to industry. The key to applicability in a domain that is suffering from the sheer number of complex and time-consuming methods available is one that can be seen by industry to be of benefit and implementable. This chapter addresses these issues and reports on two years' work with an international legacy airline. The applicability of the information network approach to incidents and accidents allows for the development of a long-term plan to integrate the method into the airline's safety management system. Limitations of working in industry are also discussed and the past, present and future methods of risk management for the airline outlined. An interim method is tested against commercial aviation incident data to highlight the pertinence and usefulness of the approach. The method has now formed the core of the working practices of a new safety management system.

Chapter 8, Conclusions – the final chapter concludes the study with discussion of the aims and objectives. Areas for further research are also identified.

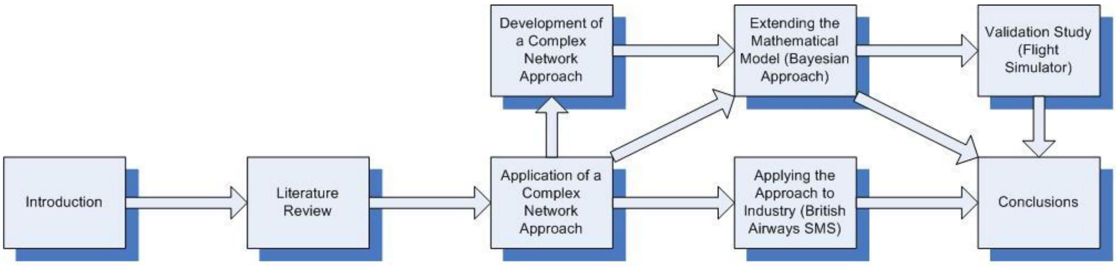
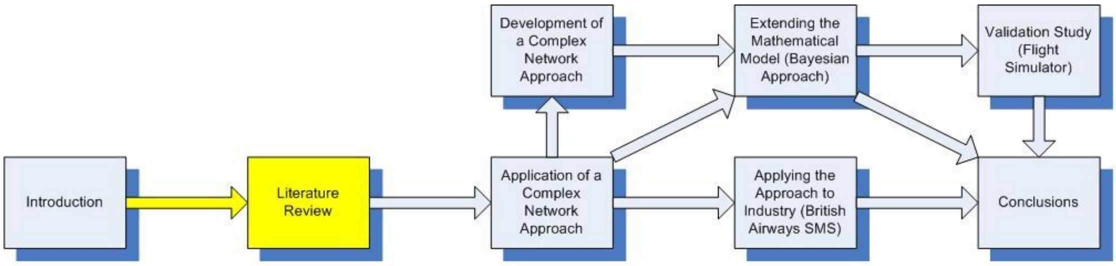


Figure 1-3 - Project Pathway Diagram

2 Modelling a dynamic world



2.1 Accident Causation Models

As chapter one outlines, this project focuses on accident causation models and in particular their application to the field of Human Factors in aviation. In order to fully understand the current position and trends of accident causation modelling it is important to acknowledge the developments and history of the area and where there may be room for further investigation and work. This chapter aims to provide a comprehensive analysis of the history and development of models and where opportunities and validation for this project arise.

The next section begins with an aviation accident case study. This is then referred to at salient points of the chapter in order to maintain a rooted discussion. It is appropriate to look at the history of accident investigation models by way of illustrating them with a contemporary accident case study.

2.2 Runway Overrun at Bangkok (QF1)

At about 2247 local time on 23rd September 1999, a Qantas Boeing 747-438 aircraft registered VH-OJH (callsign Qantas One, enroute from Sydney to London) overran runway 21 Left (21L) while landing at Bangkok (Don Mueang) International Airport, Thailand. The aircraft landed long and aquaplaned due to the runway being affected by water following very heavy rain.

The first officer was the handling pilot for the flight. The crew elected to use the 'normal' company practice configuration for the approach and at various stages during the approach to runway 21L, the crew were informed by air traffic control that although there was a thunderstorm and heavy rain at the airport, visibility was 4 km (or greater).

At 2244:53, the tower controller advised that the runway was wet and that a preceding aircraft (which landed at approximately 2240) reported that braking action was ‘good’. As the aircraft descended through the 200ft point, it started to deviate above the 3.15 degree glideslope, passing over the runway threshold at 169 kts at a height of 76 ft. Those parameters were within company limits but both high and fast. When the aircraft was approximately 10 ft above the runway, the captain instructed the first officer to go around. As the first officer advanced the engine thrust levers, the aircraft’s main-wheels touched down and the captain immediately cancelled the go-around by retarding the thrust levers, without announcing his actions. This resulted in confusion amongst the flight crew and reverse thrust was not selected or noticed to be absent during the landing run. The aircraft came to rest some 220m after the end of the stopway with its nose resting on an airport perimeter road. The aircraft sustained substantial damage during the overrun. None of the three flight crew, 16 cabin crew or 391 passengers reported any serious injuries. (ATSB Investigation Report 199904538, 2001)

2.2.1 **Single Perception Theory**

1890s

The birth of modern research into accidents and causation is mostly attributed to the work of Bortkiewicz (1898). He concluded, from limited studies, that accidents occurred at random and were therefore inexplicable. This view luckily did not restrain further research into accidents but instead opened the gates for years of investigation, conjecture and argument.

↓

1910s and 20s

The majority of the work and investigation into accidents was at first set with a pivotal view of a single event perception whereby an accident or incident is regarded as a solitary event for which there must be a solitary cause. The job of an Air Accident Investigator was to find this cause and by eliminating it would stop an accident from reoccurring. There are still elements and often mistaken use of the idea of a ‘single event’ when working with aviation, or other complex systems. However, it was soon realised that these environments spawn much more complex interactions between human-human, human-system and system-system components. This view of accidents also allowed for a blame culture to flourish whereby there was a party responsible as a ‘cause’ to the ‘event’. An accident had to have someone or something at fault, to blame so that it was not purely an ‘Act of God’ that could not be explained. This rather simplistic view and the work of, for instance Greenwood and Woods (1919) from the industrial fatigue research board (IFRB), gave rise to the ‘Accident Proneness’ model. This focus solely on the individual (rather than the system) came to dominate the research and accident reduction exercises for the first half of the twentieth century.

Further work within the IFRB and clinical studies of reactions, coordination and distraction amongst other elements, concluded that accident proneness existed. It was considered related to nervous instability and poor aestheto-kinetic coordination (Farmer and Chambers, 1926 and 1929). The uncritical acceptance of such an accident proneness model by the community at the time is almost fully attributed to this work. This view precipitated for many years to come although it can be seen that other work such as that of domino theory was already being developed realising the shortfalls of the current theory. Indeed, studies have continued long after this time examining the concept and working around the broad theory base of accident proneness in individuals e.g., Mohr and Clemmer (1988). During their study they find no real evidence for a proneness that is measurable or useful in accident causation analysis and conclude that “...it is unlikely that overall injury rates in the workplace can be effectively reduced by screening out workers with excessive number of injuries”. (Mohr and Clemmer, 1988, p. 127) This work illustrates the shortfalls of this model of accident investigation and as such highlights the limits of application to our QF1 study. If accident proneness were the case then the pilots should have been involved in other incidents prior to and following on from this event. These ideas can not be substantiated given the evidence. This view also suggests that these people can be selected out and therefore all accidents can be prevented by removing the accident prone individual either at the selection or training stage, or additionally after any incident has occurred. This is now, almost universally, accepted as a flawed theory. Dekker (2006) describes this ‘Bad Apple Theory’ as the ‘Old View’ and contends that safety progress was made mainly from technological advances and not as the result of the application of these theories. Thus, further models were needed to attempt to explain accident causation.

The main problems with the simple explanation of single perception theories, other than the realisation that more complex interactions occur, is that it assumes an innate replicability in incidents. If a ‘cause’ can be removed then the accident could not happen again. Were this applied to QF1 and the event investigated in the 1920s, the pilots could be sacked and as such the incident should not reoccur. This does not address any of the real issues and would have a devastating effect on morale and reporting behaviour were it enacted. The inherent fact is that accidents are viewed now at least as being so complex that many different ‘causes’ could have produced an incident. It is very difficult often to identify a certain cause or produce an effective barrier to similar accident types. The single event perception is very much suited to the type of investigation predating Human Factors influence as often that conclusive 'part' of an aircraft etc. could be found and blame attributed to structural facets of the system. However, a systems view had to be developed and adopted.

1930s and 1940s

2.2.2 **Domino Models and their development; the Demise of 'Proneness'?**

In his book *Industrial Accident Prevention* (1931), Herbert William Heinrich elaborated for the first time on his Domino Theory of industrial accidents. For the first time in Human Factors literature, accidents were attributed to a sequential chain of events rather than a single causal factor (normally an employee). In order to illustrate this he used the idea of a series of dominoes falling over causing the final event. (Figure 2-1)

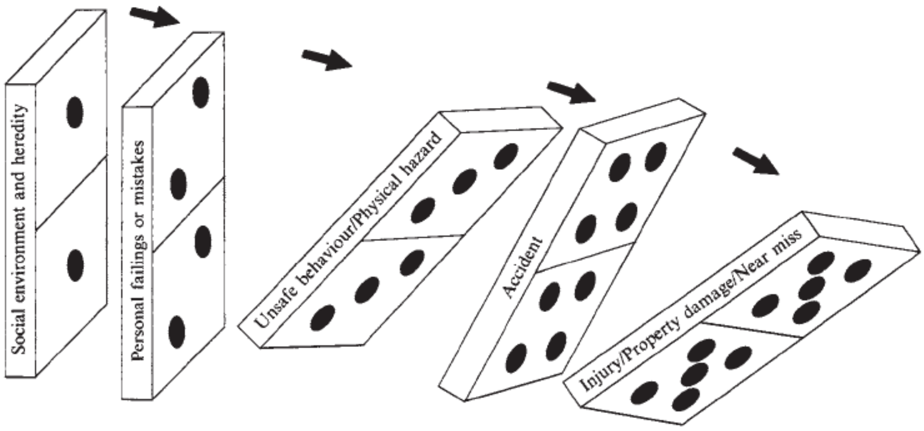


Figure 2-1 - Heinrich's Domino Model of Accident Causation – Adapted from H. Heinrich, D. Peterson and N. Roos (1980) Industrial Accident Prevention (5th Edition) New York, McGraw-Hill.

Inherent in this model of accident causation, Heinrich labelled each of the dominoes with causes that may lead to an accident. It can be contended that this resulted in the basis for modern accident causation models.

Heinrich's first domino was entitled "Social Environment and Heredity". This referred to the believed personality traits that are born from inheritance or the social environment that the worker is in influencing the likelihood of being involved in an accident. This in particular echoes elements of accident proneness theory whereby internal facets of a human contribute towards accidents regardless of external factors. This in a way shows a development on accident proneness rather than a complete deviation but with the other dominoes bringing in factors being discussed in all the research of the time.

Second, and inherently linked through the chain of events basis of the theory, is the “Fault of Person”. This refers to the effect a worker’s life (as an outside influencer) is having on them e.g., family problems, fatigue etc. This also includes flaws developed in the context of the social environment and system in which the worker operates. This is a significant drawing together of ideas that external influences on an individual and accident causation are equally, if not more, significant as internal ideas of proneness. Still today this is an important area in the investigation of accidents and incidents. These ‘soft issues’ are often easier to gain from those involved in an incident or accident on a surface level. It can be contended that approaching Human Factors via the ‘soft issues’ of family life and social life allows the industry to merely tick a box and not truly understand the more complex facets of system interaction with humans at all levels. However, referring again to QF1, at least had the event occurred in the 1930s there would be some form of defence for the flight crew. For the first time in an investigation outside influencers would be considered and from this the potential for changes to regulations, training and standards existed.

The second domino was also developed in Heinrich’s later expansions to include the actual expression ‘mistake’ as a result of these personal factors. The third domino illustrates Heinrich’s direct cause of accidents/incidents. This domino was termed either an unsafe act or unsafe condition. The very idea that this domino is required in order to ‘knock’ over the fourth, “accident”, shows that Heinrich postulated that one or both of these must be present for an accident to occur. This model was the first to really develop the importance of behaviour on influencing safety and accident causation and Heinrich felt that this third domino was the most important, and also easiest to remove from the picture in order to prevent accidents. The presence of this domino means that for the first time in investigating QF1 it would be necessary to dig deeper into the behaviour and rationale of the flight crew’s actions; a movement towards truly integrating behaviour.

The final domino, the fifth, was termed “Injury/Property Damage” and later included “Near Miss”. If one of the first four is removed, then the idea is the fifth “event” is avoided. At last there was a gateway into the complex world of system accident causation.

This was a significant step in the right direction for the study of causation and for modelling the Qantas incident more comprehensively. Any analysis is, however, still limited by the problems of a linear causal chain. If one domino is not present then theoretically the event would not occur and yet it is arguable from the report whether, for example, there were any significant outside influences (e.g., personal life) that affected the crew. Also, in the instance of the first domino, heredity is somewhat questionable and the social environment was the same for the first officer and captain and yet it is possible to suggest it was the captain who made the first mistake. A major problem with this, and one that has been brought to light particularly in recent years (e.g., Young *et al.* 2004), is that it may result in the search of answers to fit the model so that the chain is not broken. Although this does appear to answer some of the complex issues involved in the QF1 incident, the model is too reliant on the linear chain and on ideas of the individual. This takes little or no account of, for example, training and management. Arguably, had Domino Theory predicated the QF1 investigation the responsibility would again fall on the flight-crew as this is the most ‘resolvable’ course of action.

If we take the third domino, which is arguably the most important issue in Human Factors, it can be broken down into Heinrich’s terms of unsafe conditions (or reasons to commit unsafe acts). Expanding upon this idea of unsafe conditions is that they are caused by: physical unsuitability, lack of knowledge or skill, poor attitude and an unsafe working environment. This today still holds very true as precursors to complex incidents with just new ‘buzz’ terms being added to the bare-bones structure of the seminal framework. Heinrich goes on to distinguish between underlying and direct conditions within this domino. Although Heinrich suggests that the first two dominoes combine to produce the third, Vincoli (1994) puts it rather neatly that these unsafe conditions in the third domino are in fact “symptoms of root causes” from the first two dominoes so modernising the view on the unsafe act being a result not cause in itself of underlying factors.

Whilst the domino theory had already been published by Heinrich, the movement within the area still centred on theories of single perception. There was however a growing disillusionment with the studies that led to the theory of accident proneness. Johnson (1946) criticises over two hundred studies working on accident proneness citing invalid, inadequate or inappropriate statistical methods and conclusions. Indeed much of the work defending the theory from the IFRB and others was statistical argument on whether patterns of accident rates fit poisson and other distributions effectively. The major flaw with this work, though, was that it was based on a presumption of a homogenous exposure to risk. This polarised the work from recognising a difference in hazard exposure to individuals or effects on the individual such as those mentioned in domino theory - e.g., family problems, depression etc. It is this basis of a homogenous exposure to risk that fails to explain how aircraft only minutes prior to QF1 managed to land or go-around safely. Adelstein (1952) too was intrigued by the idea of accident proneness and its application to hazardous work. His study of 1,452 accidents of shunters on South African railways concludes that chance factors explain a lot more than proneness. He went on to conclude that there was no significant correlation between individuals and the repeat of accidents or accident rates over five years. He did not try to explain any new theory to explain the patterns but merely sought to apply accident proneness theory into a truly empirical situation.

1950s and 1960s

A 'new view' was developed based on the work of Cresswell and Froggatt (1963) amongst others. In their study of the causation of bus driver accidents, they coined the term 'Accident Liability' as a more developed addition to single perception theory. This reflected a propensity of individuals being prone to take risks rather than being accident prone directly and allowed for a new focus for research and behaviour adaptation.

To reflect these developments of theoretical knowledge and beliefs, further work was carried out throughout the period by a number of individuals to develop single perception theories; i.e., those holding the individual fully responsible in a Human Factors sense (as an alternative to an object failing). Clark Kerr in particular based his work around the premise of the single perception theories but reflecting on current research moving away from the rigid accident 'proneness' suggestion developed his Goals-Freedom Theory (GFT) (Kerr, 1950). The fundamental concept behind this theory is that unsafe behaviour leading to an accident is due to an unrewarding psychological climate in the workplace that leads to a lack of mental alertness. This is still centred on a single cause of accidents but begins to take into account fully the idea that external factors, or internal problems, may influence an individual so takes it away from some innate proneness. These developments begin to attack at the heart of the investigation into the Bangkok runway overrun. There is still very much lacking when addressing such an event though as this is still ultimately single-perception oriented and can easily over-simplify an incident. This case study is a prime example of where a relatively simple looking incident on the surface could all too easily be classified as such but if the surface is broken, as in the accident report, much more (and more meaningful) information can be retrieved.

In 1957 Kerr developed on his idea of GFT with his Adjustment Stress Theory. In this he reflects on the negative work environment contributing to accident causation and highlights stress as a factor that manipulates an environment, preventing the individual from concentrating fully on their work. This stress covers a multitude of areas including personal situations, time pressures, poor relationships in work and workplace hazards.

Whilst this work was going on in the background of industry, the 1960s, 70s and 80s brought technical advances and observable reductions in accident rate so the fighting force of Human Factors was arguably reduced during this period. Indeed, the pendulum had swung somewhat away from the human involved in an incident directly to a view of making the technology accept this ‘inevitability’ of accidents. Haddon (1961) commanded the design of fail-safe vehicles given the inevitability of accidents for some time into the future. This concept has again come to the forefront of study in recent years under the new label: Resilience Engineering (e.g., Hollnagel *et al.*, 2006). Even though Human Factors work, in the form carried out to date, was slightly dwindling there were still a number of notable developments in the standpoint of cause with respect to the bigger picture.

1970s

2.2.3 **Development of a Domino Idea**

By the 1970s in particular, the theory had come to be broadly acknowledged and many based their work on the domino theory such as Weaver (1971). He put more emphasis on the poor supervision afforded by management levels and stressed still further the importance of identifying the unsafe act and developments around this occurring. Bird and Loftus (1976) too reflected the direct management relationship on incidents and accidents and added an extra domino based on lack of control by the management to the original Domino process. (Figure 2-2) However, by merely adding a new domino, it could be assumed that (as no uncontrollable factors are considered in such a model) all incidents are avoidable if the management asserts enough control of the system. This almost blanket assertion that management is to ‘blame’ can not be justified for the QF1 case study presented. Beaty (1995) has repeatedly praised the management at Qantas and presented it as a model in many ways for airline operations worldwide.

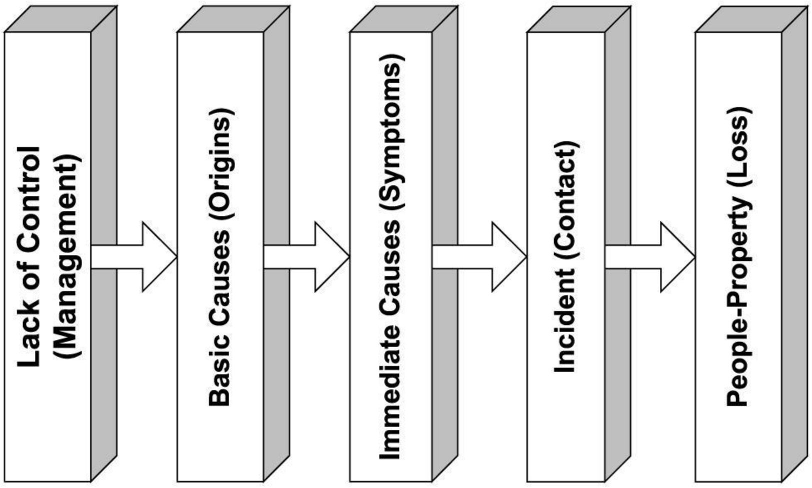


Figure 2-2 – Bird and Loftus' (1976) Loss Causation Model

Adams (1976) took this one step further and recognised the complex interaction of management strategy further up the chain using the term "Organisational errors" (a term still greatly extant today) to encompass the first three dominoes of the chain. Both worked to advance the model but neither made a giant leap in investigating accident causation as they were still bounded by limits in the applicability of a framework or model to the dynamic world in which it would be applied.

One of the first, and originally influential, attempts to apply this theory to the 'real' world was Johnson's Management Oversight and Risk Tree (MORT) (1975). Johnson recognised the interaction between personal, organisational and physical (environmental) aspects of the system or situation (Figure 2-3).

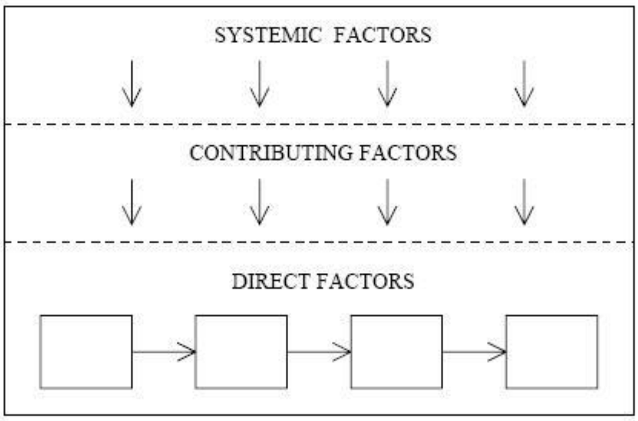


Figure 2-3 - Johnson's Three Level Model of Accidents (From Leveson, 2002)

Moreover Johnson's attempts to indicate that several accident pathways may develop over time led to this being a highly researched area of Human Factors and in particular to the rise of frameworks such as Reason's GEMS or "Swiss-Cheese" model.

MORT therefore encompasses not only Human Factors in terms of the individual but also a systems perspective in accident analysis. The first stage of a MORT analysis involves the 'standard' investigation into 'failures' by equipment or individuals that could have contributed to the event but also influences on these individuals and teams and some coverage of post-accident events including the response and availability of emergency services etc. It is at the second stage that MORT begins to look in more detail at accident causation by viewing "management system factors" (Johnson, 1975). In this, the general situation at the time of the accident is considered and failures within management and even other organisations are investigated. This happens even if there is no apparent direct link to the actual accident. MORT assumes a level of responsibility for accidents at the management level as it is said that they should create an organisation that would not allow situations such as these through directives and conditions. MORT looks for actions by the management level that could have prevented an incident at the event or in the pre and post event timelines. These are encapsulated into a standardised MORT fault tree to illustrate the development and causation issues of the event (Figure 2-4).

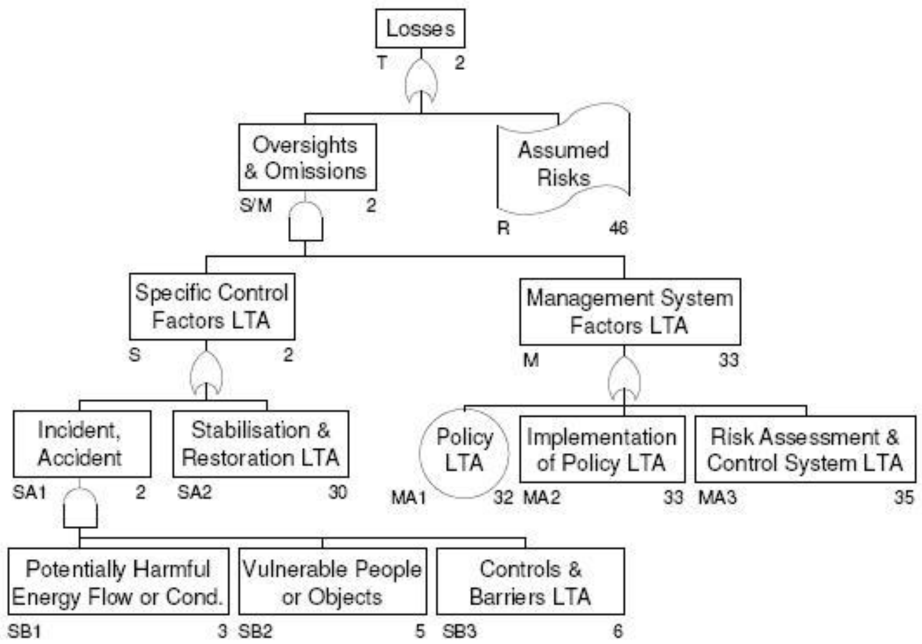


Figure 2-4 - An example of the MORT Fault Tree (From Bandener, 2005)[3]

[3] Labels to boxes: Left (e.g., SB1) is a unique identifier in investigation. Right (e.g., 3) is the MORT page number in the handbook. Further details of shapes etc. see Johnson, 1975.

As is clear from this summary of the application so far, MORT is heavily management oriented and almost appears to hold a level of blame but merely shifts this up the organisational structure. MORT does however allow some risks to be termed “assumed risks” and these do not hold management responsible as it would not be viable to do so for the smallest of factors in a real-life organisation. Possibly one of the most significant results of the work into MORT was the development of the idea of ‘barriers’ in a system. These can include simple physical barriers such as guards on machines or implementing a procedure to avoid an accident within the workforce; e.g. the go-around procedure for our QF1 case study. It is said that an accident occurs when one or more of these barriers is broken through either human action or some form of technological failure. Working the QF1 case study towards MORT, the points hold about the management being important, especially in terms of the barriers that were put into place but also the problems that resulted from incorrect approach procedures or weather training being implemented. These do not however account for the actual decisions made by the flight crew and to an extent neglects the direct influence of the conditions and actions despite a reference to assumed risks. This model most comfortably encompasses the case study this far and has moved itself slightly further away from the restrictive linear flow models. In itself though, the model fell foul to its own complexity and inflexibility for use as an investigative tool; a problem that can be argued is still present with many of today’s frameworks.

↓

1980s and 1990s

By the late 1980s and 1990s, the effect of technology improvements on accidents had diminished and again the rate plateaued. With this in mind, the greatest leap towards more investigation into organisational contributions to incidents has to have come from James Reason’s “Swiss Cheese” model of accident causation (e.g., Reason, 1990 and Reason, 1997). This model has been adopted by individuals, companies and world regulatory bodies such as ICAO (International Civil Aviation Organisation), the global aviation body as the basis of their investigative efforts and understanding of accidents. This includes the application of the model during the course of the Flight QF1 investigation itself.

Investigations into accidents outside the realm of aviation have also moved the concentration of investigation into the system as a whole e.g., Three Mile Island, The Herald of Free Enterprise and Piper Alpha. These incidents are discussed elsewhere in the literature but all illustrate the movement towards an organisational view of complex events. Indeed some years earlier, Perrow (1984) argued in his text that it was the nature of complex, tightly-coupled systems to suffer unforeseeable socio-technical breakdowns. This appears to have formed the basis for the movement such as Reason's work. This does, however, take any power away from the possibility of predictive work of accidents and incidents if the breakdowns are truly 'unforeseeable'.

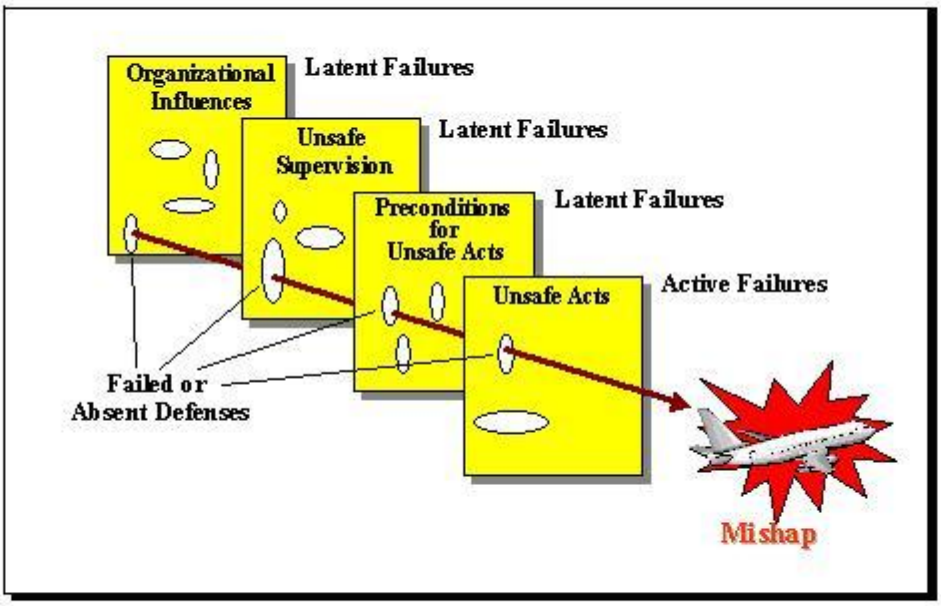


Figure 2-5 - Reason "Swiss Cheese" Model of Accident Causation (Reason, 1997)

As can be seen from Figure 2-5, Reason has identified several layers within which 'holes' are always present and where these align the result may be a catastrophic event. In the majority of cases, a layer will stop an event resulting in catastrophe and holes are fluid in that they may appear and disappear or change in magnitude depending on the psychopathology of the system or organisation. Most important to Reason's model is the distinction of latent errors versus the active errors of those at the 'sharp end' of the system. Arguably though (e.g., Young *et al*. 2004) this would suggest that human error, in either latent or active form, would be a contribution in 100% of incidents and accidents. This discussion of the percentage of accidents and incidents 'caused' by human errors has long been contentious with many views being put forward from Heinrich's (1931) discussion of an 80:20 split to Boeing's (1996) two-thirds, to this plausible view of 100%. Even in his book Reason (1997) says that although there will always be a presence of active failures, due to defences most will be caught and not lead to negative outcomes. This in itself, however, appears to highlight a major problem of Reason's work which is that without a predictive element some active and latent conditions will continue to exist and this leads to problems. This does tend to limit the model's applicability to a post-mortem investigation into the pathology of an organisation rather than a context-specific and applicable method of investigating all precursors to an incident or accident before or after the event. Therefore, it can be suggested that the danger lies in the way this model has been adopted and applied by rote and this needs further work.

Reason (2000) when discussing his developments and model states that we "…cannot change (the) human condition, but we can change the conditions under which people work" (p768). In other words he seems to allude to the fact that the understanding of thinking or 'why' of an individual's action at any cognitive level may well be of little or no use as it is an inevitability that error will occur. But is this too simplistic and almost fatalistic? Even in a conference presentation from late 2003 (p. 26), Reason suggested "…perhaps we should revisit the individual (the heroic as well as the hazardous acts.)" These appear to be significant words in re-highlighting the importance and relevance of active error.

This model has made a significant jump in the field of human error investigation and drew the attention of investigators and companies away from solely studying and blaming individuals. Through methods such as TRIPOD DELTA (e.g., Groeneweg, 1998) organisational identifiers of latent factors are centralised. The method, based on Reason's model, aims at controlling latent factors within an organisation through identification, categorisation and the use of compensating factors. Indeed we only have to look at the example of the Challenger accident that led to the loss of life and shock across the globe to see this movement more towards organisational errors being placed at the core of an investigation. In her very in depth and intelligent review of this event, Diane Vaughan (1997) shows how applicable Reason's model is to a timeline of events stretching back 9 years of latent pathogens and arguably no active error[4].

Despite the massive developments that this new view on accident causation and investigation undoubtedly caused, the movement appeared to remain central to the fundamental domino theory of a single causal chain but with the addition of factors and influences into the model. Even the "Swiss Cheese" model appears to be an extension of this and it is contended that such event chain models encourage limited notions of linear causality that make it difficult to incorporate non-linear relationships such as those of feedback (Leveson, 2002). Some worries also occur when such a model of causation is applied as an accident investigation method and model as in the ATSB's

[4] Even this is contentious however and the "launch decision" has been suggested as an active error. This re-highlights the issue of errors being the cause or result of events as the launch was the cause of the event but also the result of many events previous to it e.g., the meetings with engineers etc.

investigation of the Bangkok overrun. The distinction between the two appears to be fuzzy at best in real world application. Following an illustrative model such as this could lead to latent factors or non-important issues being searched for or found at the expense of others in order to complete the 'required' model of the accident chain.

Reason (1997) argues that latent errors are always present in any accident or incident but active errors may or may not be present - i.e. the active errors may well be the consequence and not the cause of incident pathways and are not a requirement if enough latent conditions exist. This helped to emphasize the concentration of industries on searching relentlessly for latent errors which have proved to be very difficult to find pre-event and too easy to find (or at least search for dogmatically) post-mortem due to factors such as hindsight bias. Fischoff (1975) emphasised that we rebuild the past into a linear and a logical fashion in our minds but such a linear progression is not possible in the real world; it is thus almost an oversimplification which magnifies the problem of searching for latent conditions in order to satisfy an abstract requirement for an unnatural cut off point in the investigation. That is, there is no natural point in a post-mortem accident investigation at which to stop searching when looking at latent conditions further and further up the organisation - but where do we start to get non-returns, or unrealistic returns, for effort? Sidney Dekker (2005) points out that Reason's model is limited by the confines of structuralism and although works well post-mortem (hindsight notwithstanding) it lacks function in the fluid pre-event world. This limitation is still prevalent today.

Perrow (1999) too emphasised this effect of latent conditions in a system which are most succinctly described by Reason (1990) in his seminal resident pathogen metaphor. This complimented all of the work that has led to many in depth discoveries of the salience and importance of latent errors. There are occasions, however, such as the Chernobyl disaster that have arguably been attributed to purely active errors by the operators at the plant. These appear to go against the grain of a wholly Perrow or Reason oriented approach to accident investigation. It should be remembered that this model is an illustration of an idea not a direct application for the accident investigators to rigidly adhere to. The relevance of these developments to those of a blame culture is discussed in section 2.3.2 especially with reference to Reason's (1997) fundamental attribution error and surprise errors.

It seems pertinent to point out that Reason's organisational model of human error is not being said to have never been useful. One example of a methodology in regular use and based upon his ideas, especially within aviation accident literature, is the Human Factors Analysis and Classification System (HFACS) (Shappell and Wiegmann, 2001).

HFACS has been applied to numerous aviation accidents and can identify useful relationships between active and latent factors (e.g., Li *et al.*, 2008). However, there are many limitations associated with such a methodology. Shorrock and Chung (2010) studied the links between research and practice and found gaping holes in the success of models such as HFACS.

It was during this time, however, that work was also being carried out to bring a completely new perspective to accident causation. An early example was the work of Hendrick and Benner (1987) in their development of the Sequentially Timed and Events Plotting (STEP) method from their earlier work on Multilinear Events Sequencing (MES) (Benner, 1975). Not only did these theories aim to help investigators in the actual carrying out of an accident investigation but they also moved significantly away from Domino Theory rebirths. Both of these methods are based upon Peturbation Theory (P-Theory) which is based on a system homeostasis being maintained and if this is disturbed by a perturbation then an accident sequence will develop if the system does not adapt (Benner, 1975).

The STEP method uses cards to consolidate event information including the actors and actions involved as well as a description and source of information. Events are then placed in a tabulature with time along the x-axis and actors along the y-axis and causal links drawn between events where required. This gives an investigator the details of the accident sequence and can highlight where defences or barriers have failed in relation to, for example, the Bangkok overrun event and where further developments may reduce further incidents. When applied to a case study such as QF1 it appears that STEP provides a useful method for illustrating and investigating both active and latent issues. However, there would appear to be a facet missing from making STEP a tool suitable for use within complex systems and that is the focus on a single event (and its immediate surrounding events) rather than at the system as a whole. There needs to be development in these tools that allows them to reflect a system space during normal and abnormal work.

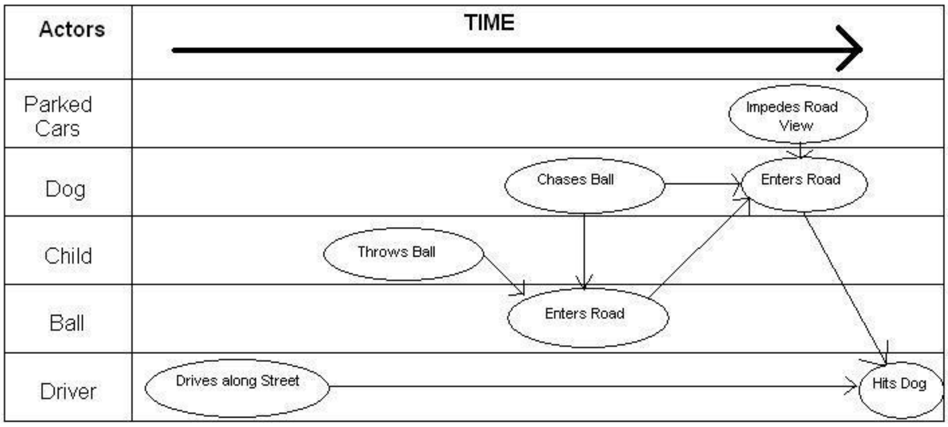


Figure 2-6 - A Simplified STEP matrix for a car accident in an urban area

The STEP matrix (Figure 2-6) when completed illustrates nicely this birth of network approach to accidents built up of multiple causes, multiple actors and multiple events. This allows network models to be fluid (or at least dynamic) which counters the issues raised referring to Dekker's (2005) assertion that Reason's model cannot.

Rasmussen (1997) too developed work to step outside the constraints of single-chain causation albeit with added influences and factors. Rasmussen understood that to decompose behaviour into decisions and actions artificially isolated the phenomenon from the context in which those behaviours had taken place. This was, he concluded, an ineffective way of trying to understand behaviour (Rasmussen, 1997). He presented a systems approach looking at vertical integration between layers of a dynamic socio-technical organisation. Rasmussen (Figure 2-7) knew the importance of a closed loop feedback system to an organisation's success in a dynamic world so that, similar to STEPs P-Theory idea of adapting to changes in the system in order to prevent chains of events leading to an incident occurring, the system may remain stable. A lack of vertical integration between the various layers shown in Figure 2-7 can be blamed on this lack of feedback and the actors involved (human or machine components) not understanding fully the role of the other actors within the system but not in the immediate vicinity, i.e., actors at other levels.

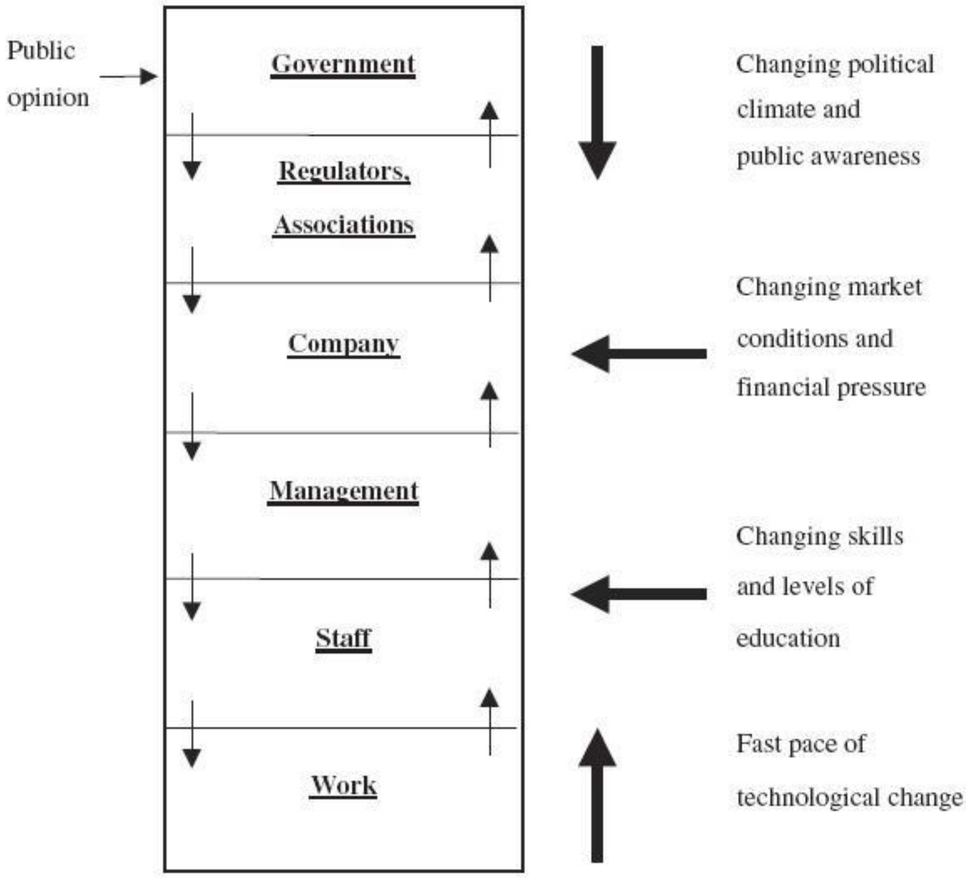


Figure 2-7 - Rasmussen's levels of a complex socio-technical system (Adapted from Rasmussen, 1997)

Vicente (2006) produced a paper illustrating how Rasmussen's framework for risk management in a dynamic society can fit the breakdown of a water supply system resulting in many injuries and deaths in Walkerton, Canada in 2000. Vicente's work was the first full-scale independent application of the framework to dynamic society. It was concluded in the paper that most of the predictions of the model were found to be true by the surrounding events. The defences are seen to erode not all at once but gradually over time as the interactions between the different layers degrade and feedback is reduced. The temporal pattern of events is not illustrated easily in this method but a descriptive map of factors can be derived and from this all the interactions and responsibilities of actors from all levels can be shown. Vicente illustrates the relevance of this approach to systems failure. This framework when applied to a case study such as QF 1, still lacks, however, elements of the network methods of STEP discussed above. Such facets as a temporal and more detailed event synopsis are lacking yet it gives a good overall basis for abstracting details about an incident and allowing generalisable conclusions.

2.2.4 **Human Reliability and Error Identification**

If accident investigation is one side of a coin, we can now turn our attention to the other side of that coin, which as we have seen has many unanswered or unanswerable questions and problems, which is accident prediction. Although not exactly new in the realm of Human Factors, methods such as Human Reliability Assessment (HRA) techniques are still in their infancy in terms of development. These methods use probabilistic risk assessment as a form of basis. This movement towards quantitative methods of accident investigation is often powered by a need to limit subjectivity. The quantity of historical data that is so often collected and perhaps not utilised to its full potential is also important since these often help develop probability relationships. This next section then, addresses the more quantitative aspects of accident investigation models which to date are often separated from their qualitative 'cousins'.

Human Error Identification (HEI) is fundamentally the initial part of HRA techniques and is used as the basis of Probabilistic Safety Assessments (PSAs) (Cox and Tait, 1991). HEI is a subjective technique that is method-specific. The aim is to illustrate the impact of human error on a system and also the recovery associated with that error. (Kirwan, 1998)

Kirwan (1998) highlighted the relevance of HEI to Human Factors and Ergonomics independent of HRA in that the identification of errors through the process is result enough in itself. These factors are further refined in Error Reduction Analysis (ERA) which can demonstrate the ways of reducing the likelihood of the error, or if it occurs, the impact on the system. This eliminates the dependence on probabilities and quantification of errors, the use of which is highly debated in the literature. Reflecting on previous discussion about the over-emphasis on chain type models of causation, Leveson (2002, p.14) states that the "limitations of event-chain models are also reflected in the current approaches to quantitative risk assessment. When the goal of the analysis is to perform a PRA, initiating events in the chain are usually assumed to be mutually exclusive. While this assumption simplifies the mathematics, it may not match reality."

In Kirwan's (1998) discussion of the HEI methods available he finds thirty-eight in the literature including well known examples such as SHERPA (Embrey, 1986), THERP (Swain and Guttmann, 1983) and HAZOP (Kletz, 1974). Almost half of these have been produced in the preceeding five years which demonstrates the emphasis shown on this area of study throughout the 90s and still today[5]. SHERPA (a flowchart based

[5] Stanton *et al.* (2006) find over 100 models in the literature

application) has had wide application and remained a popular tool in complex tasks it has been seen to become unwieldy and too resource intensive (Kirwan, 1998). 'Second Generation' HEI methods have been developed such as the Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel and Embrey, 1994) which was based upon SHERPA, Rasmussen's (1988) Skill, Rule, Knowledge framework (SRK) attempts to incorporate a cognitive level of analysis to HEI. This and the TRACEr method developed by Shorrock and Kirwan (2002) can be applied both retrospectively and prospectively which advances the usability of these tools greatly in accident prevention. An important point also is that these diagrammatic, or simply formalised, methods of investigation allow observers to view the basis upon which investigators make their conclusions and bring with it improved transparency.

As the design related to aircraft develops with time so must the means with which to qualify the design and analyse/investigate human related interaction with it evolve. The ERRORPRED Project (Stanton *et al*. 2006) is a great source of an investigation into the modern investigative tools available to Human Factors practitioners at present. All of the major models are covered and their positive and negative aspects discussed briefly. The problems found tend to be that despite the number of models available, many become too unwieldy to apply in complex situations and there still appears to be large scope out there to develop a framework, especially including some level of cognitive modelling of actors, that is not too general to use in investigation nor too specific to just one realm or particular situation. Stanton *et al.* (2006a) developed a toolkit approach to the problem of predicting error and this method faired favourably when compared with standalone methods, such as SHERPA and HAZOP mentioned above. The toolkit approach appears to deal well with the complexities of working with error and increased the sensitivity of error prediction and multiple-analyst validation compared to other HEI methods used in isolation (Stanton *et al.*, 2009).

During their development of this new HEI tool for aviation, Stanton *et al*. (2008) reflect that despite the number of techniques available the applicability in a number of situations is still questionable: "The goal for researchers now remains to investigate how these contemporary HEI methods can be improved and also the development and creation of new, aviation specific HEI methods." (Salmon *et al.*, 2002, p.129)

Present

2.3 Current Application of Human Factors in Aviation Accident Investigation

2.3.1 **Hindsight as a Barrier to the future**

Do we wish to address specifically the direct causes to an incident or accident or address the overall pathology of an organisation and system? This is the question that presents itself at this junction in Human Factors work in accident investigation. As discussed by Young *et al.* (2004) and Dekker (2002) many latent conditions or failings are found in current accident investigations, but the ability to attribute causality is only truly possible in hindsight. The relentless application of these top-down models of accident causation (e.g., Reason, 1997) although without doubt finding many important latent conditions within an organisation, may well be the barrier to any form of predictive and arguably more relevant investigation. The argument stands that searching back from an event there is no natural 'stop' point. Indeed, Braithwaite (2001), whilst discussing Moshansky's 1992 investigation of the F-28 Air Ontario icing crash from Dryden, put it rather well when he said that the "apparently vast number of errors was not indicative of a particularly bad accident, rather, a thorough investigation."

Since the concept of hindsight as a major problem with investigation is being discussed, let us first look at when the concept originally arose. Fischoff (1975) discussed this at length and concluded that hindsight was not equal to foresight but the movement at the time believed that by knowing how past events occurred and eliminating some element of this, they could not occur in the future. Although simplistic by today's standards this did set about a very important culture within industries to identify errors and problems within the system or individuals. Now the prevalent idea is that, as mentioned previously, the past is structured into a linear set of events. However, this simplification was not possible in a dynamic period of time so immediately we are behind in the 'war' on the factors involved in the lead up to an event. It is known that simply removing an element will not prevent future accidents. It is further understood that the use of ideas such as the fluid motion of the layers within Reason's model and the holes within those layers the situation can be viewed as ever changing. This forms two main camps of which those that feel the need for the acceptance of fallability in humans and the need for "resilience engineering" (e.g., Hollnagel *et al.*, 2006) appear to be the most forward thinking.

When looking at causation it is important to try and place ourselves in a position similar to that of the individuals and system at the time. In this way an attempt is made to not utilise our own biased view of what it may have been like with our new omnipotent knowledge. Woods (2003) put it very succinctly when he says that the future seems implausible before an event but after this the past seems incredible in a kind of ‘how could they not have seen that’ way. This surprise factor that must have been present by the individuals at the time is also discussed in Reason’s book Human Error (1990) and the truth is they did not ‘see it’ (whether aural, visual, tactile etc.) or else the event would not have occurred. This is further developed by Dekker (2005) in his discussion of the “banality of accidents”. Accidents are not the result, he and Perrow (1984) suggest, of a series of incidents leading up to an accident but are normal people doing normal work in normal organisations. From the point of view of an individual involved, the lead up to an accident may well appear that way to themselves. This gives extra weight to the importance of addressing ‘near misses’ and reporting programs such as CHIRP or BASIS.

What can be gleaned from accident investigations using the prescriptive method of adhering to a top-down model appears to be a great audit of a company and its pathology but may not realistically extract ‘causes’ of the event proximal enough for it to be usefully analysed and attacked. It is after all “workable remedial applications” (Reason, 1997) that we are searching for in accident investigation not an unmetered breakdown of all company failings. Therefore, as Young *et al.* (2004) suggest in their paper, maybe a bottom-up approach as discussed again in Dekker (2002) may be more useful and less biased in the hunt for true causes of accidents. Then, if acted upon appropriately, those causes may positively affect the future of the system.

2.3.2 **The Safety Culture and Blame**

All of the models discussed above have been used as the basis for investigations into accidents. The basis for the study of Human Factors in accident causation and in aviation, along with other complex socio-technical systems, is to increase safety within and across the industries. Surely the basis of this is to have an organisation that is safe. Looking at the organisation as a whole, what exactly can make a safe culture or background for a system in order to decrease the chance of incidents and accidents? This next section addresses some of the issues which are important regardless of the model or method chosen since they directly affect the reporting and investigative practices of organisations.

Westrum (1992) identified three major organisational cultures: Pathological, Bureaucratic and Generative (Table 2-1). It can be seen from the table produced that an airline, or other complex industry, should aspire to generative ideals. Things are not swept under the carpet but are addressed and ideas welcomed; a mainstay for risky and complex operations is the need to be adaptable and imaginative.

		Cultures		
		Pathological	**Bureaucratic**	**Generative**
Topics	**Information**	Don't Want to Know	May not find out	Actively Seek it
	Messengers	"Shot"	Listened to IF arrive	Trained & rewarded
	Responsibility	Shirked	Compartmentalised	Shared
	Failure	Punished or concealed	Lead to local repairs	Lead to far-reaching reforms
	New Ideas	Actively discouraged	Often present problems	Welcomed

Table 2-1 Westrum's Organisational Cultures and how they handle safety information (Adapted from Reason, 1997, P. 38)

Learning needs to become a priority within these organisations and the need is strong to remove the typical epitaph of complex socio-technical systems that there is always something else more important or pressing. (Reason, 1997)

There have been a number of prescriptions as to being a safe culture and a safe organisation mentioned through the literature over time such as Reason (1997) discussing organisation 'competence' in terms of collecting the right data, acting upon it and disseminating it a useful way to all concerned. Examples of this would include the incident data collection and safety information systems discussed later in the section on incidents and their importance. There is no definitive organisational safety health at present though and papers or companies will use whatever statistic or comparison suits their needs in order to shed positive light. Reason (1997, p.191) states rather importantly that most commercial airlines today have almost uniform training, operational and regulatory procedures and even similar aircraft types so the difference around the globe of flying an airline with 1:260,000 chance versus 1:11,000,000 chance of an accident with at least one death may in some part at least be down to the culture of that airline. This again should be comparable with other industries and indeed in the UK's report on the incident at Chernobyl the head of CEGB at the time, Lord Marshall, amongst others (Reason, 1990) went so far as to state that the accident could not have happened in Britain due to its safe nature. Identifying and quantifying what actually makes a safe culture is an area in which much work needs to be done in order to make effective use of good examples worldwide. This is shown to be hard though when an individual from any particular state or inclination, be it eastern, western or other, looks as if to compare with their own 'way' rather than from a perspective of objective total outsider.

A significant illustration of this is found in Braithwaite's discussion of safety culture within Qantas and other airlines where he compares crews from different parts of the world and within different national carriers. Firstly, though, before discussing such a question it is important to look at what culture means in the argument. Again, Reason (1997, p.192) covers this rather well and states succinctly that "whereas national cultures arise largely out of shared values, organisational cultures are shaped mainly by shared practices." If we take this as doctrine, then this would imply that regardless of where in the world or which airline or dominant social culture, if one implemented a practice such as giving out incident reports/briefing safety procedures or newsletters etc., will always lead to a better safety culture. This rather simplified things a bit too much but looking back, as did Reason to Uttal (1983), it can be seen that an organisational culture is "shared values (what is important) and beliefs (how things work) that interact with an organisations structure and control systems to produce behavioural norms (the way we do things around here)".

Braithwaite (2001) proposed that Australian crews may well have success in a safety environment due to their openness to speak out against each other regardless of 'seniority'. This may well be the opposite of well-established Far Eastern airlines or those from countries that can be considered as having a far more 'hierarchical' social culture. In these organisations superiors are significantly more autocratic with their subordinates signifying a large power divide. This has been associated with poor crew resource management in certain parts of the world (Harris, 2008). However, safety in these more rigid environments has been attributed to a high level of sticking to the SOPs (Standard Operating Procedures) that may also be relevant to the Qantas model of Aviation safety. It can be seen yet again that these areas have many unanswered question but the major foreseeable problem with this, and even the studies that stand so far, are that they rely on input from the pilots in the form of questionnaires or interviews both of which struggle to get the response levels that would provide truly reliable information or scope for the entire airline/nation/environmental culture.

It can be argued, as Reason does, that safety (or any other aspect for that matter) culture is something that an organisation ‘has’ not ‘is’. By this, the organisation is malleable and facets may be added to or subtracted from such a culture in order to improve it. It is these facets that need to be identified and examined as to whether they will be integrated with other cultural facets to work in a positive manner. Indeed, Braithwaite (2001) makes an interesting discussion of the need for a comprehensive set of system safety indicators similar to the Flight Safety Foundation’s CFIT checklist. This would need to be a proactive and simple checklist style procedure to assess an organisation and look for obvious areas that may need improvement, or indeed can be proved to be even better than the previous believed norm at any level and thus integrated to other organisations or at least argued for or against. Reason (1997) again points out that prescriptive feed-forward only methods can never fully control safe behaviour. Therefore, use of such a system safety check would allow a continuous feedback process for the development of the safe culture within an organisation. This would require processes to be carried out periodically and all individuals made to feel that all comments or reports (e.g., through incident reporting) are welcome and acted upon. The problem is in the level at which it is aimed as if too general its usefulness will be limited but if too fine-grained it may become prohibitive to use. The essence of the argument is for ‘loops within loops’ integrating levels of the system through feedback (Figure 2-8).

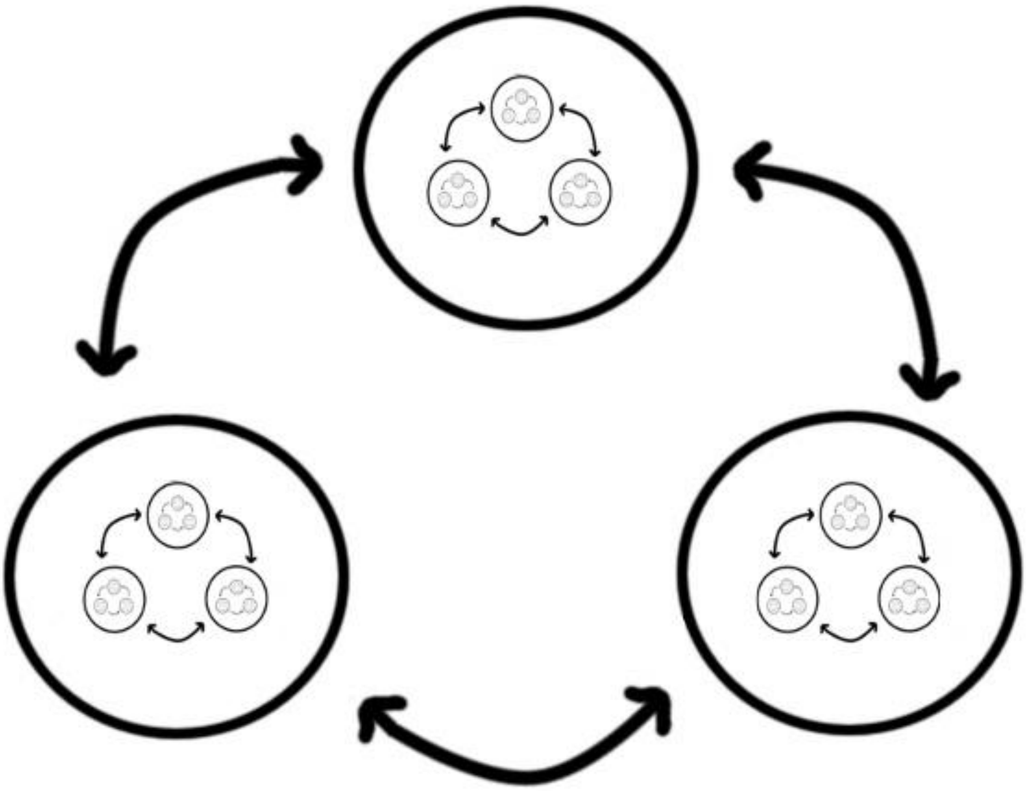


Figure 2-8 – Illustration of interconnected feed-back and feed-forward loops through levels of a system

Intrinsic to any organisation is the presence of a blame culture whether it be a true blame culture or one of no-blame, or even positioned in between (such as the 'just' culture). Certainly for the development of incident reporting programs blame is particularly important. This is also the case in the author's argument for a redressing of the balance of emphasis that has led to active error playing second fiddle to latent pathogens in investigations and prevention of incidents; i.e., it is not the intention to return to a period of blame and shaming individuals for their actions but merely to concentrate on the 'whys' and 'hows' of an individual's actions. Aside from this though, blame has been a major factor in moving the concentration of investigations away from the individual even though attribution to individuals at the sharp end, according to Reason (1997), deflects the blame from the organisation as a whole. It is contended in fact that an organisation cannot simply uncouple culpability of an event from itself to an individual; they are an internal factor and a part of the organisation from which blame should not be sought to be removed. It has oft been the culture to blame individuals due to the satisfaction, both to conclude an investigation where looking at an organisation may involve a never ending search, and also to fulfil our possible innate requirements. However, this must be avoided if a high level of safety culture is to be gained. Blaming an individual and acknowledging the effect of an active error by an individual, or group of individuals, should not be one and the same; they should be treated as mutually exclusive for the purposes of investigation. Only if terms such as 'gross negligence' are fulfilled should one then look to sanction an individual; beyond that training and correction must come first. After all, it is known that all activities have some form of inherent risk therefore it would be unfair to punish an individual for falling for this risk. The emphasis must become not on blaming and not on ignoring the fact that an individual can have a profound effect on accident causation but on the 'whys' and 'hows' at a cognitive and organisational level, i.e., A Systems View.

2.4 Incidents; a tool for proactive safety

Central themes of this research coming to the surface in the review thus far have included the comparison and use of both commercial and GA aviation and the need to address dominant linear models. Additionally in reviewing the literature and in particular the practical use of methods relating to aviation accident investigation there appears to be scope to increase the use of non-accident scenarios to understand the aviation system better. In particular feedback has been discussed as an important issue within an organisation that will be safe and incident reporting programs are one area where this usefulness can be capitalised on.

Incidents, or "near-misses", can be defined as ranging from partial penetration of defences to situations in which all the available safeguards were defeated but no actual losses were sustained. As such they cover a whole multitude of sins and would hopefully therefore promulgate a multitude of information for safety development. This section sets out to discuss the way in which industry is currently working with accidents. This will also address the issue of using incidents for safety management and more particularly understanding incidents more fully with information networks.

2.4.1 **What place for incidents?**

In his editorial to a special edition of Interacting with computers, Chris Johnson (1999) highlights an important factor in Human Factors; a "…bias towards major accidents". He goes on to suggest that this is a barrier to the uptake of Human Factors in industry and the full utilisation of techniques. These are the high profile, high cost (in monetary and life terms) accidents that cover the front pages and can send the public into frenzy. Thankfully, the majority of "events" involving human error result in an incident (or even non-event) rather than a catastrophic accident and these can be considered by many to be "Free Lessons". Reason (1997) spends some time discussing the idea that safety awareness and defence is highest post-accident. This may then dwindle over time as accidents are expected to happen to someone else and, as per his "surprise attribution", not happen to themselves. Ideally, incidents should be used to create a safer environment within these systems and organisations to a similar extent that accidents have been in the past. Safety systems such as CHIRPS (the Confidential Human Factors Incident Reporting System) or BASIS (British Airways Safety Information System) attempt to do this. Reason (1997) again rather cleverly relates incidents to inoculations that may be protective measures for a period of time after the event. This of course is reliant on useful interpretation, investigation and dissemination.

As the number of catastrophic accidents in aviation, and other highly complex industries, decreases over time due to increases in safety, so the lessons that can be learned from them also decrease. This results in the awareness of what can happen also passing out of the current mindset. It must become that incidents do not only receive the cursory or routine attention in investigation that they have to date; they must be the new "accident", in investigative terms, until we fully learn all the lessons they may have to offer us. This movement to fully utilise incidents due to the falling accident numbers has been discussed as far back in the literature as Rasmussen in 1988 yet we are still not fully taking advantage of the resource available to us. The concentration of investigation also must develop in order to truly utilise these incidents to their utmost. We must begin to look at where incidents went right and the positive circumstances that may be developed into preventative measures in the future. There are, of course, caveats to any statement such as this and care must be taken not to return to a "throw more regulations at it" type attitude. Within this, it appears something is being done about safety but such counter-measures may have negative implications for some aspects of work or elsewhere within the system. Incidents may be a true step towards proactivity in safety management until such a time as fully proactive error prediction techniques, which are admittedly in their infancy, can make a larger contribution to complex systems.

2.4.2 **Common Cause**

In order to get the most from incidents, this research intends to analyse them to the same extent as accidents (and even look to predict potential outcomes based on incident investigation) in order to ascertain whether lessons are being missed. However, before we can do this another hurdle must be addressed. The whole premise on which the usefulness of investigating incidents in order to reveal information about accident causation is balanced around what is commonly referred to as the Common Cause Hypothesis. This dictates that the causal pathway leading to an accident is fundamentally the same as that leading to an incident, or near miss, with the significant alteration of one or several factors that lead to a changed outcome (one not of an accident).

This was first discussed in Heinrich's (1931) *Industrial Accident Prevention*. Although there has been some work to assess the validity of such a common cause, it appears as if the similarity of causal pathways for incidents and accidents has become confounded with issues of severity and frequency of incidents and accidents (Wright and Van der Schaaf, 2004). Perhaps the basis of this confusion is in the way Heinrich and others (e.g., Bird, 1996 and Salminen *et al.*, 1992) carried out ratio based studies in order to try and prove or disprove the relationship between incident and accident. In fact, in Wright and Van der Schaaf's paper they go on to discuss the confusion found in all the studies they found (of pertinence) that suggested an argument for, or against, the common cause theory. In other words, the theory itself has never really been proven and yet it is the basis for so much near-miss based work.

Dekker and Hollnagel (1999) several times allude to an evolution towards failure that releases pre-cursor events to an accident and signal the vulnerability of the system. They suggest that the sequences of events leading up to an incident or accident are almost identical and they share traits of human-automation breakdown. This holds firmly in view the common cause for accidents and incidents in the most complex of socio-technical systems and human-computer interactions. Indeed there appears to be much empirical evidence (although the link not proven or attempted to be proven) to suggest that correct investigation of incidents could prevent accidents. Woods et al's (1994) analysis of a 1992 Strasbourg crash showed that a previous British Airways incident had many of the same details but the information did not get to those who needed it in order to prevent the accident. This is one of many articles in the literature that illustrate the previous existence of incidents that did not have a catastrophic end yet accidents followed with too many of the same precursors. Indeed this again emphasises the communication issues that the details of incident investigations and reports need to be directed to the correct people. Working with Orasanu and Connolly's (1993) concept of Naturalistic Decision Making we can see that people tend not to bring situations back to first principles for knowledge based behaviour when novel. Instead, they rely on comparisons with previous encounters and from this we can surmise that the more knowledge of previous events we can give our crews, the higher the possibility that comparisons may be correct.

This is not to say that all cases of remedial action following on from an incident result in a totally positive outcome. Reason (1997) discusses a couple of case studies where this is not true including one from Three Mile Island in 1979. There are also cases in aviation such as that involving the introduction of takeoff monitors during the 1950s following a number of accidents on contaminated runways. This device directed pilots to the “correct” takeoff attitude for the conditions in order to resolve problems identified in previous incidents of flight crews demanding the incorrect attitude. Following the failure of a retaining screw within the unit, an unusually high angle of attack was commanded by the device and following the instructions, the flight crew stalled the aircraft and crashed back onto the runway. This illustrates succinctly the danger of merely introducing new guidelines, practices or regulations in not actually identifying and preventing the problem and cause of accidents. As Don Norman (1990) concludes, if analyses are isolated so the improvements that result from them may also be isolated potentially leading to new problems at the system level.

Wright and Van der Schaaf’s study worked at a very general level and in very limited conditions within the railways using data from CIRAS (Confidential Incident Reporting and Analysis System). It is, however, the only paper of its kind in a search of the literature that appears to address the actual assumption of common cause. This does introduce the idea of further significant work possibly using BASIS, CHIRPS and other reporting systems in different industries to get a multi-level study of common cause presence. This would give a clear grounding to further work in promoting the use of incident data to prevent accidents.

There are proponents, such as Dekker (2005), of the banality of accident theory. This suggests that incidents do not in fact precede accidents in systems safer than 1 in 10^{-7} events. Before this point he suggests that indeed incidents may be precursors of an event and useful as such. Dekker says that normal work precedes accidents in these states and this in itself goes against the ideas discussed by Reason and those defending common cause. Leveson (2002) too refers to papers by Edwards (1981) and Kjellen (1982) claiming “data on near-miss (incident) reporting suggest that cause for these events are mainly attributed to technical deviations while similar events that result in losses are more often blamed on human error.” (Leveson, 2002, p. 21) This however, may be due to reporting practices and characteristics of human reporting procedures rather than true causation difference. This is a different view of the coin that may be answered with further study on the core of common cause theory.

2.4.3 **Realising the potential**

We have already mentioned a diminishing return through accident investigation alone. Accidents are rare events leading to a population size that is not good enough for any form of statistical analysis to show the state of the system (Waldock, 1992). It could be more useful to start treating incidents in this way; ‘incident’ becoming the new 'accident'. Westrum's (1992) organisational cultures illustrate quite clearly that those organisations with a generative nature would be most likely not just to collect incident data and reports, which is not enough in itself, but also to act on them appropriately. They would also treat those making the report fairly and in a positive manner (notwithstanding the discussions centred around blame or misconduct).

Incidents, when properly examined, may also allow us to get past the hurdle of hindsight. A chain of events have occurred that may be interrogated and the individuals are still present to discuss their feelings and position at the time; we can actually ask what and who was aware of what at any time. Incidents are in short, all of the negative, common cause withstanding, events which allow positive investigation returns without the completely negative and destructive end. Although Reason (1997) feels accidents are indeed necessary for the development of an organisation it is contended that the answer should be no; if incidents are given the precedence accidents received in the past twenty years or so then the number may be reduced and the safety of the industry increased as a whole.

Reason (1997) goes on to discuss how redundancy in systems may hide mistakes or errors. This, he suggests, may be negative to safety evolution within an organisation as the ability to learn from them is diminished. However, this is also true whereby incidents if not used to their full extent also makes these complex systems more opaque to users. Information that may prove useful if attacked in the right way is being wasted. One cautionary note at this point, however, is that if incident data are to be utilised fully, and as such shared in the public domain for researchers and other companies to view, they must not form the basis for a new 'league-table' of safe airlines, crew, or industries as this will have only negative effects on the reporting side of incident data.

In order to glean the highest standard of information from our incident data we first need a system for collecting and investigating data. This is far from simple as the literature discussions to date have pointed out. In recent years we have seen the development of some very exciting and useful incident reporting tools such as the UK CAA's CHIRPs (Confidential Human factors Incident Reporting Program), the USA NTSB AIRS (Aircraft Incident Reporting System) and British Airway's BASIS programs to name but a few. These systems are an amalgamation of data, with voluntary and mandatory reporting procedures for incidents and accidents set out by national authorities or airlines themselves. In order to gain as much information as possible systems such as BASIS use voluntary reporting forms from pilots then engage the crew by telephone, or no-blame inquiries in Qantas' INDICATE proactive safety program

(Braithwaite, 2001). In using open-ended and specific questions, investigators try to work out not just what happened but also why. This 'why' has become more important to these systems in recent times as the data are increasing. As a result, the data was useful for a while showing trends of 'what' is occurring but struggled to show 'why' an event or situation may have occurred. Concentration on the latter may lead to a better safeguard than event logs per se. CIRAS too, the confidential reporting system for the UK railways (Davies *et al.*, 2000) has been struggling with large quantities of data but limited information on why the events are occurring. Some of this may be due to the way in which the comparatively immature reporting system is approached by employees in the railways and may develop in time. Here a development towards looking at the bigger picture of the safety of the system and what the reports are telling the analysts is crucial. This is not to say that it would be an easy task with such a large number of data and a possible entire culture shifts being required.

2.4.4 **Reporting Issues**

At the heart of these reporting systems, as already mentioned, is normally the word 'voluntary'. Even in 'mandatory' schemes, the crews involved are relied upon to not only 'own up' to an event or 'error' but also to be prepared to think about how, what and why this happened so that lessons can be learned. This is asking a lot from commercial airline crews especially as they already feel their time is under pressure. Many see these duties as more paper-work taking them away from their principal flying role. There is also the issue of embarrassment that Braithwaite (2001) picks up on so clearly.

Mentioned in chapter 2, the idea of blame is even more prevalent in a society where voluntary means possibly putting yourself forward for "the chop". De-identification of the individuals involved is the simplest step taken towards encouraging individuals to come forward. It is important and widely acknowledged in the literature (and thus feeding into organisations slowly) that although there is emotional satisfaction in blaming individuals there is little or no effect on future fallibility of that individual if blamed. Again, we are unable to change the human condition but must work with it. There is still a long standing question with the legal position though, especially as Braithwaite (2001) points out in the USA where litigation is a serious business (now also becoming overused in the UK and around the globe). Much of the literature around this area at first encouraged the position of a 'no-blame' culture. However, this can be just as negative as a 'blame' culture. With 'no-blame', there can be no come back or remedial measures taken for truly culpable acts of negligence or acts extremely removed from training. This is where the idea of a 'Just' culture was developed. It was correctly recognised that although a system was needed to encourage the reporting of incidents, where individuals were truly responsible or negligent then action could be taken whether it be remedial training, merely a union representative talking to the crew involved (as in BASIS after any important reports submitted) or even legal proceedings. There are bases in the literature such as Neil Johnston's substitution test (1996) to assess whether blame is a fair or necessary element to a situation. In this psychological test, it is suggested that where an individual's actions are judged to be possible unsafe acts in relation to an event, the individual concerned is replaced by someone of similar qualifications and experience. The following question is then posed: "In the light of how events unfolded and were perceived by those involved in real time, is it likely that this new individual would have behaved any differently?" If the answer is "probably not" then Johnston asserts that "…apportioning blame has no material role to play…." This allows a simple comparison between peers and allows for a just analysis of the need for blame or not.

There is also important cautionary recognition throughout the literature that indeed the most poorly reported incidents, whether due to embarrassment or non-detection, may well be the most dangerous "latent pathogens" out there in the system. Indeed, Dekker (2005) elaborates at great length about the difficulties of relying on an individual to recognise one's own mistakes. This is particularly poignant when working in a complex environment whereby one believes they are doing normal work and nothing special is occurring. Even an outsider viewing a 'mistake' may not be correct in that it is a mistake to them but inside the head and 'world' of the individual it is a normal action at that time. This is an interesting area, in attempting to use incident data, which may be worth investigating further together with its implications on incident reporting. This is a new idea compared to the work of Woods (1984) showing how individuals or their co-workers in nuclear industries identified the errors they had made. If there is an innate difficulty in identifying errors, especially at the rule and skill based levels, then this is going to leave incident and accident investigation with an almost unconquerable chasm in attaining our goals. In a similar vein, Guastello (1996) cited a Swedish study which illustrated a need to train individuals in what to report and what not to report in terms of what actually is an incident; i.e., the quality of reporting is just as important as the quantity.

The story doesn't end there however, and the literature has examples of the need for action on whatever reports are made in order to encourage future reporting by crews or individuals (Dekker and Hollnagel, 1999).

2.4.5 **The future for Incident Use**

Once again though, even if we do collect enough of the right information and are able to apply thorough investigative techniques it is effectively useless unless that information is communicated to those that matter: individuals within organisations at all levels. Indeed, beyond simply disseminating the information within the company, Christopher Hart (FAA Assistant Administrator for System Safety) "…believes that the only way of further reducing airline accident rates is the sharing of safety information." (Male, 1997, p. 24) Inherent in this sharing of information though would have to be an evolution in inter-company relations. This would particularly be with respect to commercially sensitive or confidential information and data. Safety cannot afford to take a back seat to company secrecy but this is of course an idealist view.

I think it is also time for the industry to begin really concentrating on the elements in incident reports that lead to successful outcomes; these are a truly positive and proactive element to investigating near-misses. Reason (2008) too believes it is time to return to the 'heroes' of events rather than treating all involved as 'villains'. Johnston's substitution test again has scope for application here. Would, for example, another pilot have saved flight UA232 (an engine failure resulted in damaged and unusable flight controls leaving the crew to use the two remaining engines for control) given the same circumstances. What is the heroic element either of individuals who avert accidents or of a system that does so? As appears to be standard amongst this research though there are warnings such as from Habberley *et al.* (1986, p.50) suggesting that near-misses resulting in a successful outcome may cause crews to be more daring in the future and believe they can "get away with it". The crux of the argument with incidents is that organisations in high-risk situations must develop a 'learning culture' and continually reflect upon their practices through monitoring and feedback (Pidgeon and O'Leary, 2000). This requires flexibility of organisations that comes right back to the opening arguments of the "tug of war" between cost/production and safety. Braithwaite (2001) discusses how Qantas allow their crews access to practice onboard simulators whilst not in use for training. As such, he points out, pilots have a natural quality that they want to improve and be the best so flexibilities like this can make a very big difference within the organisation. This determination to improve, I would argue, has even overtaken the feeling discussed by Beaty (1995) that safety was viewed as a feminine attribute discouraging pilots from taking it too seriously. This, linked with improved dissemination of the result of these investigations and analyses, will aim to improve the accident rate beyond its almost twenty year plateau. As Reason put it: "Errors arise from informational problems. They are best tackled by improving the available information – either in the person's head or in the workplace." (Reason, 1997, p.154)

2.5 The Influence of Modern Technology

In the past twenty years or so automation has had significant effects on the role and job of flight deck crew but despite this, the accident level as we have seen has remained relatively constant. With the advent of increased automation and redundant safety in complex flight systems, the role of the pilot is oft quote in the literature as becoming more of a monitoring role removed from the physical control of the aeroplane. Indeed, through this increase in automation (and possibly a significant factor in encouraging it) is the decrease in slips made by the human actor in the system. This, however, comes at a price as the errors made tend to be of a higher order and therefore can be much more serious. There is still not enough known about the issues of new 'sharp-end' technology and their effect on a system. More concerning than this is the reluctance of commercial aviation manufacturers to fully integrate and adopt Human Factors perspectives in products (although this may partially due to the fact that designs tend not to be 'new' but rather 'developed' from past models) (Harris, 2007 and 2009). The following section introduces some of the issues that will need to be addressed in order for the crossover from academia to be realised in the commercial aviation industry in particular.

The importance of Human Factors is not reduced because of an increase in system reliability and complexity; indeed it is effectively increased. As Woods *et al.* (1994, p.181) quotes a director of safety at an aircraft manufacturer, "you can incorporate all the human engineering you want in an aircraft. It is not going to work if the human does not want to read what is presented to him, and verify that he hasn't made an error." Although a slightly harsh summary of the role of humans and Human Factors it does reinforce the issue that humans are, more often than not, the limiting factor (Harris, 2006). Sarter, Woods and Billings (1997) put in focus the situation by describing 'the substitution myth'. This contends that simple substitution of people by machines to improve system safety whilst retaining previous standards is an oversimplification and a fallacy (Harris, 2006). Instead the substitution has a far-reaching effect on the system and changes the role of human operators. In other words, machines cannot simply replace humans and humans must rely on interaction with machines for jobs at which they perform better. In any given situation both are affected by the other; a linked system. This means the system works on the basis of function allocation and playing to the strengths of the interaction is of the utmost importance. Arguably where things may fail more than not are at the interfaces of this interaction; the points of information transfer.

The development of more advanced systems brings about new varieties of pitfalls for the human actor in the system. Errors resulting from mode-errors, abnormal situation recoveries and monitoring duties simply did not exist until the technology to create these pitfalls was present and integrated to modern air transport.

The problem of human-machine interaction has many layers to it that increase in complexity to model and understand. One such layer discussed by Rasmussen (2000; cited in Woods and Dekker, 2000) is attempting to predict the way in which humans will react to new technologies and in particular to that natural human facet of work: The work-around that may lead to errors or problems. Woods and Dekker also point out that, although an answer to the problem is not so easily identifiable, it is hard to study current world technology and effects of introducing new technology. They argue that this introduction effectively changes the world into which it enters; an almost paradoxical situation that may only be changed with greater emphasis on predictive models and improved understanding of the system working and interacting as a whole. (Figure 2-9)

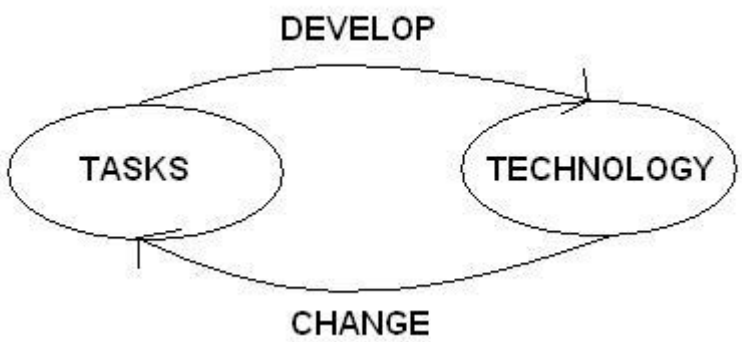


Figure 2-9 – Illustration of the interaction between technology and task (Carroll *et al.*, 1991)

Many studies and papers have been written looking at the effects of increased automation on pilot performance. Wood (2004) carried out a review for the CAA on "Flight Crew Reliance on Automation" and from this learned that indeed pilots have become more reliant on systems especially as those systems have become more reliable. This harks back to the idea mooted by Reason that lack of an accident draws people's attention away from safety issues; in the same way the lack of the systems failing draws people into a false illusion of safety. Another interesting point that arises from this paper, and one that has recently resurfaced in popular aviation media and academia (e.g., Ebbatson, 2009), is that of whether commercial pilots have indeed lost manual flying skills due to their over-reliance on automation. A spin off of this may well be related to points discussed in the GA section about relevance of training for commercial pilots on manual flying skills.

2.6 Conclusions

This review of current literature has identified several areas where improvements can be made to the methods, tools and underlying models for aviation accident investigation. It can be seen throughout the chapter that the dominant theory behind many methods and current viewpoints is a model developed from linear domino style research. There are, however, more recent developments which have begun to evolve from a new and exciting approach which tries to combat any linearity. It is in this area that much future work must be carried out to refine and hone current and novel methodologies.

Stanton *et al.* (2006), discussed in section 2.2.3, confirm the need for aviation specific models of investigation that are usable yet flexible enough to be applied to the polarised spread of incidents occurring. It has also been discussed that there is scope for improvement and modification of current techniques rather than necessarily having to develop a brand new method (of which there are arguably already too many!).

The central problem that has surfaced from this review of the literature is that many of the tools that are currently in use are very good at certain aspects of the job but given the complexity of the world in which they are being applied they are often found lacking. There is also the balance between a complex method reflecting a complex system versus the desire to keep a method simple and this is proving problematic for many current methods.

2.7 Chapter summary

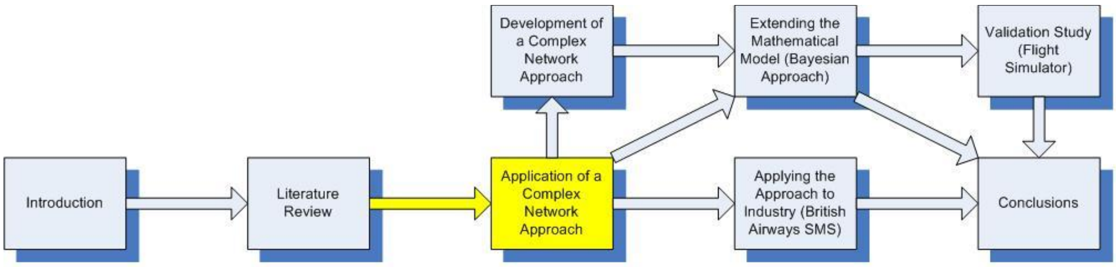
This research has identified the need for a method that can not only handle the complex sociotechnical systems it aims to investigate, but can also progress beyond being reactive to proactive and even predictive. The chapter began exploring the history and development of accident investigation techniques, it then introduces more complex non-linear theories that may provide further development and finally addresses the needs of the aviation community in terms of a suitable tool.

The aims of this thesis, therefore, can be summarised as follows:

This project will aim to look at developments of bottom-up investigative models. This will concentrate on looking into an area of merging predictive modelling into investigation so that we might reach a goal of proactive investigation and accident reduction. This chapter has highlighted significant gaps in current practice and these include the need to develop a method that draws from the positive aspects of both qualitative and quantitative methodologies and incidents in addition to accidents. The need has also been revealed for a method which can be universally applied across aviation (general and commercial) to understand both catastrophic events but also near-misses and ideally normal-work. Most significantly is the requirement for a method which can better reflect the dynamic and complex real-world events that it is trying to understand more fully. This requires a movement away from linear models and a return to understanding the importance of the 'sharp-end' of Human Factors. The most viable way to address these issues is to begin to look at more complex network type approaches to accident investigation. This new method would need to embrace the multi-causal, non-linear system in which these aviation events take place.

The subsequent chapters identify and apply a novel methodology within aviation and then look to refine and develop that model before applying it with an industrial partner. It is hoped the work will help progress past a stagnant level of safety in complex socio-technical organisations.

3 A complex approach to a complex scenario[6]



3.1 Chapter introduction

In order to truly understand and begin to move forward within the field of accident mitigation it is the opinion in this project that it is important to break down accident causation into its constituent elements without losing the dynamic properties of the real world situation. This allows us, as discussed in chapter 2, to highlight not only the negative elements resulting in accidents or near-misses but also gives us the opportunity to begin to study the positive elements of any event and how these avoided worsening situations.

It is not enough to simply create a timeline of tasks carried out by actors within a scenario and suggest those actions contributed or otherwise to the resultant outcome (akin to 'Domino' style cause and event chains). Whilst aviation accident analysis has traditionally been dominated by linear models of causation (e.g., Heinrich, 1931), the complexity of factors in many accidents, including increasing levels of design complexity, make it difficult to fit them to a simplistic 'domino' model. Even the current 'world standard' for aviation accident investigations (Reason's 'Swiss cheese' model; Reason, 1990, 1997), despite being highly successful over years of application, is still limited by a linear approach which cannot capture the full complexity in the chain of events and relies too heavily on a post-mortem analysis (Dekker, 2005). In this chapter, more fluid, non-linear representation of the system space is adopted. This illustrates

[6] This chapter is the basis for the following journal publication: Griffin, T. G. C., Young, M. S., Stanton, N. A. (2010). Investigating accident causation through information network modelling. Ergonomics, 53: 2. 198-210. (Attached in Annexe 1)

where decisions were made and the event took place emphasising the dynamic interaction between agents and the central role of information transfer - communication - in optimising complex systems.

One must look further into the dynamic world that we have already discovered: “Even relatively simple aviation tasks involve multiple agents (human or non-human), dispersed throughout time and space (pilots, air traffic controllers, flight management systems etc.), working together towards a common goal, and with emergent properties which may not be easily predicted from the task inputs. Thus the analysis of such tasks warrants a multi-causal, multi-linear and multi-agent approach.” (Griffin *et al.*, 2007, p.1)

3.2 Event Analysis of Systemic Teamwork (EAST)

The first challenge was to find a suitable method to break down accidents and incidents into their constituent parts. It is proposed that a new model based on methods of complex system analysis may be applied to aviation accidents. One such framework which appeared to analyse the events in a suitable way was The Event Analysis of Systemic Teamwork method (EAST; Stanton et al., 2008). EAST was originally developed as a “toolkit” Human Factors method fusing several other well known and published methods in order to examine the role of actors and groups of actors to gain a more complete picture of complex socio-technical systems. This multifaceted approach has the potential, when all aspects are interlinked, of providing a more comprehensive representation of the system. This focus on the system in which an event takes place rather than the event (or agents within that event) itself is something that no model reviewed in chapter 2 attempted and could elicit major benefits. It has been applied to a number of domains, including military vessels (Gregoriades & Sutcliffe, 2006), rail (Walker *et al*., 2006) and ‘command, control, communications, computers and intelligence’ (C4i) scenarios in the military (Stanton *et al.*, 2006), all of which have parallels with aviation tasks. However, it has not yet been applied to accident analysis.

Through this novel application, EAST could allow for the causal events to be deconstructed into three major networks and it was hoped that from this conclusions could be drawn and links between the layers of the networks made to form a fully three-dimensional model of the accident build-up. EAST breaks down events into three major networks: Task, Social and Information (Figure 3-1; for a more detailed review of the methodology see Stanton *et al*, 2008). This network approach allows for the study of a system in a dynamic and complex way rather than a linear chain in that it covers the ‘who’ (agents), the ‘what’ (tasks), the ‘how’ (communication/teamwork), the ‘why’ (knowledge), the 'when' (by a timeline) and the 'where' (through an operations sequence diagram). EAST therefore allows a detailed view of the complexity of the system and a comprehensive examination of information flow across the networks. It opens an opportunity to investigate *where* things go wrong, particularly from the multi-causal perspective - errors or weak links within the networks can migrate onto other pathways and ultimately lead to a system failure. This multi-causal approach is in complete contrast to the linear models that dominated the literature review. This could allow for a more natural deconstruction of a system and a system's events removing many of the artificial and over-simplified aspects of previous methods.

In order to accomplish this, the three networks described above are firstly created for 'snapshots' in time, and can then be animated over a period to illustrate the changes within the networks. The changes over time are equally informative as the status of the network on each snapshot.

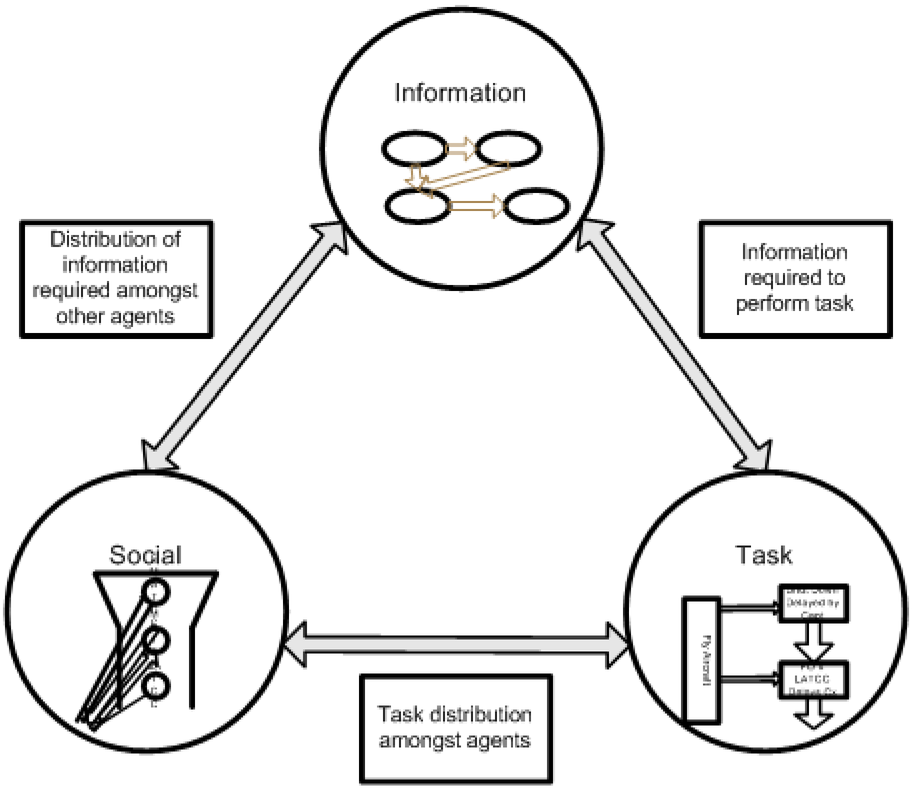


Figure 3-1 Interrelationship between Task, Social and Information networks (adapted from Stanton et al., 2008)

One major area where EAST differs to a number of well-published methodologies in aviation safety, e.g., STAMP (Leveson, 2004) and HFACS (Wiegmann and Shapell, 2003), is its non-taxonomic approach. This is obviously not to say that taxonomic approaches are any less valid or useful in their own right; indeed their number is greater than any other form of model. However, EAST attempts to represent the system "as is". From this EAST allows identification of issues arising from decisions made and the information that is or is not available to the correct person at the correct time thus centralising the concept of situation awareness (SA) and beyond that introducing measures of team SA (Salmon *et al.*, 2008).

Situation awareness (SA) is often used as a blanket causal term for accidents involving pilots (i.e., Human Factors issues) within the aviation industry. In fact, some studies have concluded SA, or loss of it, is a leading causal factor in aviation incidents (e.g., Hartel, Smith and Prince, 1991). SA, however, remains a contentious topic within the human factors community. Despite much work into the SA of individuals, there is much to be learned about how individuals work together as teams in complex systems and how their SA is shared, or distributed (Salmon *et al.*, 2008). Information networks may allow a more in depth understanding of this phenomenon.

To date, EAST has not been applied to accident analysis; in this thesis the methodology is used to describe an aviation accident case study for the first time, and from there we explore the potential for prospective use of the information networks in particular.

The crux of this study then, is the idea that inter-network and intra-network communication (both verbal and non-verbal) forms the basis of effective performance and as such reduces the likelihood of an accident or negative event from occurring or going uncorrected. Under this assumption the primary network of concern was the knowledge network – who owns what knowledge, and how is it being communicated around the network?

In order to assess the suitability of EAST as a method for accident analysis in aviation a case study is described in the following section. This case study provides the basis for a comprehensive review of the EAST method and then opens up pathways for development and improvement.

3.3 The Kegworth Air Disaster

Central to this study was the issue of identifying a suitable case study to analyse. This needed to balance a relatively simple causation with enough depth of knowledge of the events that led to the accident. Since this project predominantly focuses on the Human Factors of accident analysis it was also important that these factors were reported by the investigating body as being of significance to the outcome rather than purely mechanical or other facets (this of course does not preclude any factor being involved in addition to the human agents).

The crash of a Boeing 737-400 near Kegworth in Leicestershire on the 8th January 1989 was identified as being suitable for a preliminary application of the novel accident analysis technique, in particular because the official Air Accidents Investigation Bureau (AAIB) report included enough detail to populate the networks (including interviews with the crew themselves). The Kegworth crash is also noteworthy as it is one of the first involving the new design of cockpit instrumentation known as glass-cockpits, hailed as one of the greatest single leaps in pilot-machine interaction.

The synopsis below is taken from the official AAIB Report (Aircraft Accident Report Number 4/90 (EW/C1095)):

> “G-OBME left Heathrow Airport for Belfast at 1952 hrs with 8 crew and 118 passengers (including 1 infant) onboard. As the aircraft was climbing through 28,300 feet the outerpanel of one blade in the fan of the No. 1 (left) engine detached. This gave rise to a series of compressor stalls in the No. 1 engine, which resulted in airframe shuddering, ingress of smoke and fumes to the flight deck and fluctuations of the No. 1 engine parameters. Believing that the No. 2 engine had suffered damage, the crew throttled that engine back and subsequently shut it down. The shuddering caused the surging of the No. 1 engine ceased as soon as the No. 2 engine was throttled back, which persuaded the crew that they had dealt correctly with the emergency. They then shut down the No. 2 engine. The No.1 engine operated apparently normally after the initial period of severe vibration and during the subsequent descent.
>
> The crew initiated a diversion to East Midlands Airport and received radar direction from air traffic control to position the aircraft for an instrument approach to land on runway 27. The approach continued normally, although with a high level of vibration from the No.1 engine, until an abrupt reduction of power, followed by a fire warning, occurred on this engine at a point 2.4 nm from the runway. Efforts to restart the No. 2 engine were not successful.
>
> The aircraft initially struck a field adjacent to the eastern embankment of the M1 motorway and then suffered a second severe impact on the sloping western embankment of the motorway some 2 nm from the runway.
>
> Thirty-nine passengers died in the accident and a further eight passengers died later from their injuries. Of the other seventy-nine occupants, seventy-four suffered serious injury.”

It is evident, even from such a brief summary, that this event was entwined with complex Human Factors issues. It was not just the flight crew who were involved in this situation, as the ‘team’ extended to air traffic controllers, flight operations personnel, cabin crew and the passengers themselves. Confusion arose on the flight deck over which engine had suffered damage and the flight crew were unable to elicit the correct information from their instrumentation or from the cabin crew and passengers, some of whom had witnessed the damage occurring. This multitude of factors, still relevant to aviation today, makes the Kegworth crash, despite being quite dated, a good candidate for the multi-causal, multi-agent analysis offered by a network approach. Indeed, due to the age of this accident a number of studies have been published investigating the accident (e.g. Johnson 1995, and, Besnard 2004) and also the method of investigation and reporting itself (e.g. Johnson 1997). This results in a significant amount of data and information to work with. Therefore, since the aim of this chapter is to introduce the application of a methodology to an aviation accident rather than attempt to deduce new knowledge from the event, the previous investigation of this case study allows for a greater comparison of techniques and findings.

3.4 Data Gathering

The EAST methodology uses an Hierarchical Task Analysis (HTA) as the foundation of information retrieval from a defined scenario. In the case of this study, a formal report was used and as such an HTA-type technique could be used to analyse the text of a report. However, as a preliminary study, it was decided to keep the analysis at a macro level and the analysis was carried out by the author under the supervision of EAST specialists. The text was used in its original state to collate the information required for the formation of the networks. From the report and event transcript (i.e., the documentation pre-discussion and conclusion) it was possible to break the scenario down into three easily distinguishable action snapshots:

1. Realisation of problem and immediate actions

2. Engine Shutdown

3. Descent and Final Approach

Within each of these sub-scenarios, separated temporally, task networks were developed to encompass the actions of the agents onboard the aircraft and those involved outside of the aircraft (e.g., ATC and Flight Operations). The tasks were identified from their coverage in the report and the author’s knowledge of the phases of flight and are illustrated in Figures 3-2 to 3-4.

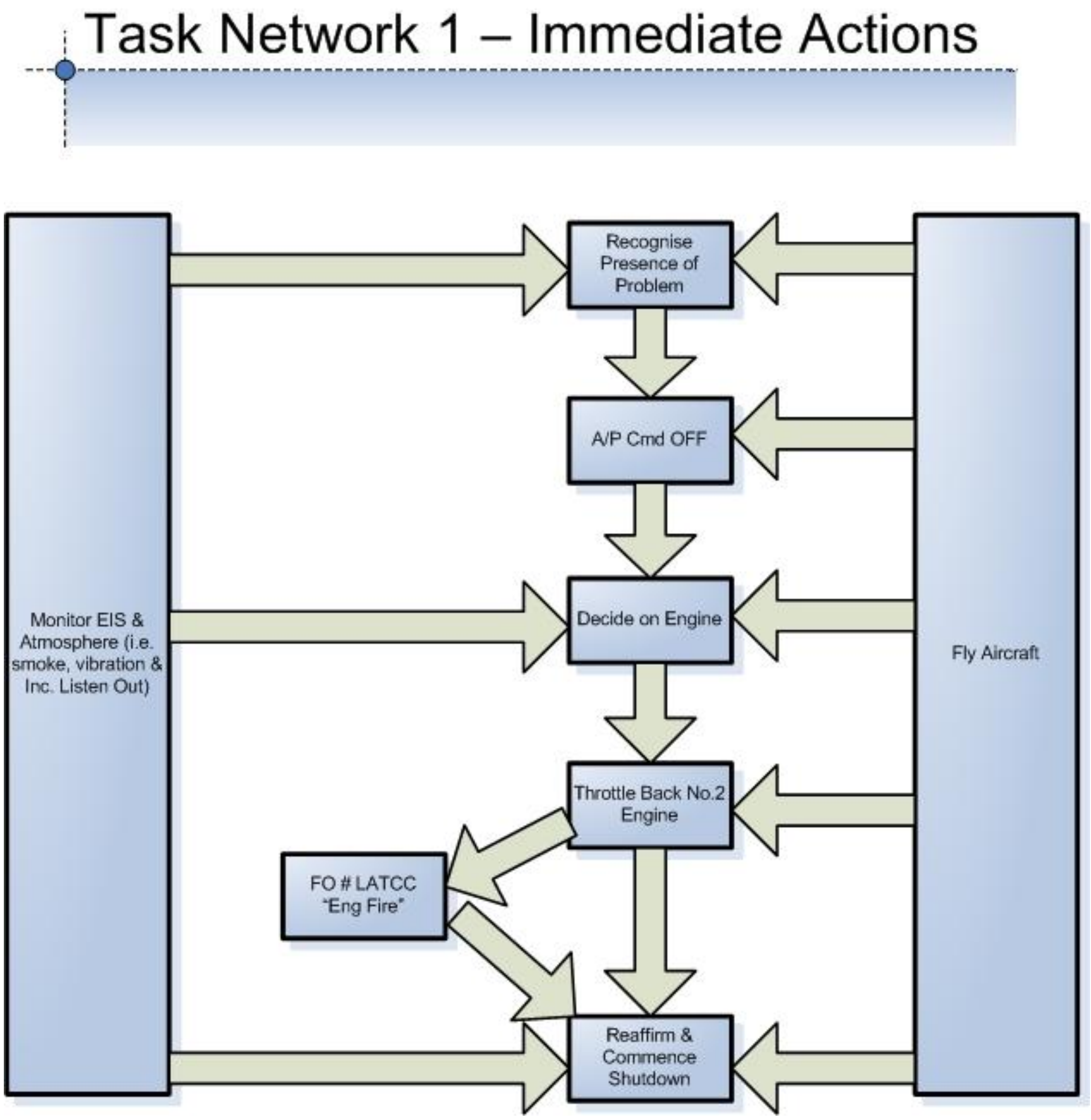


Figure 3-2 – Task Network in Snapshot 1

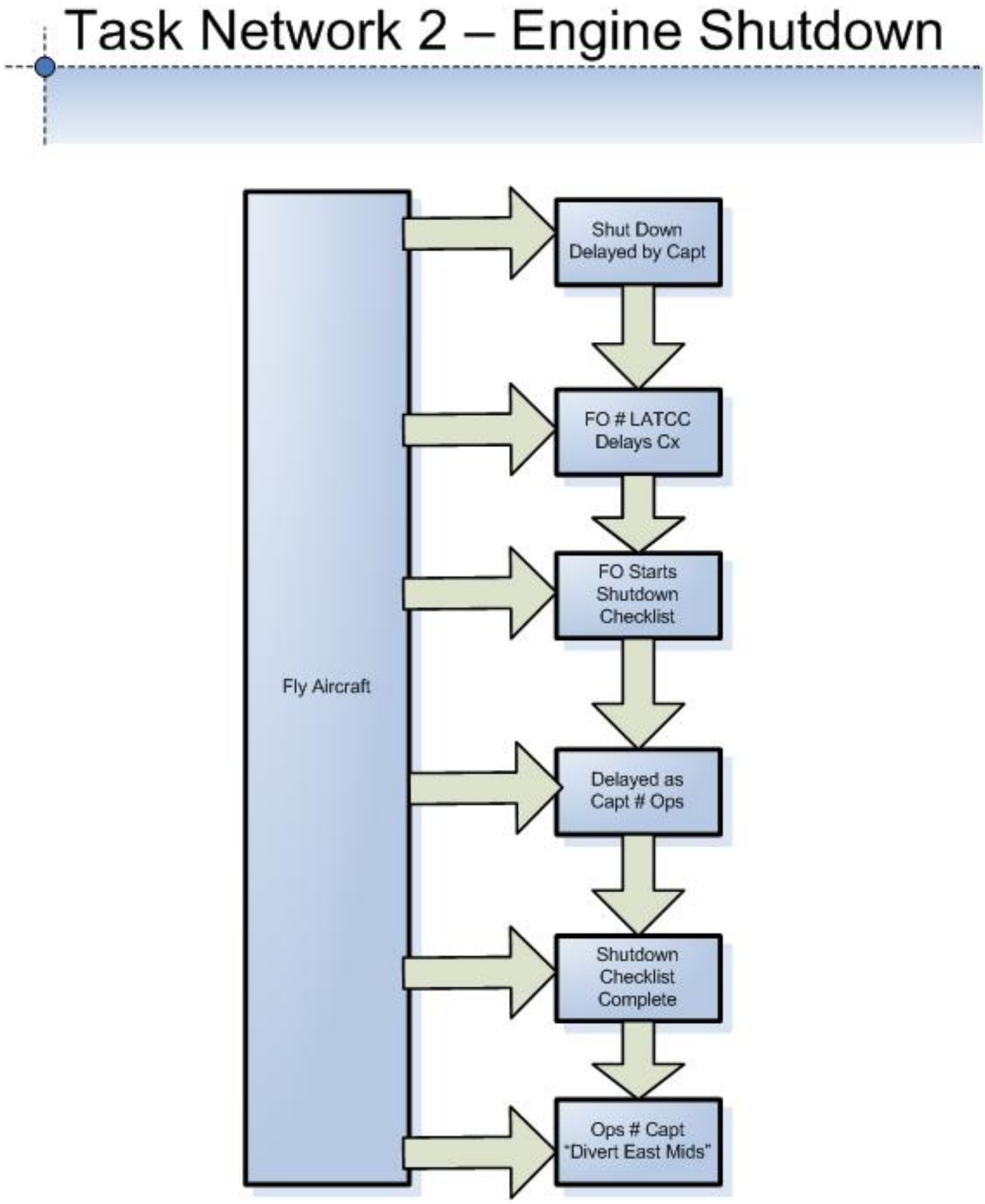


Figure 3-3 – Task Network in Snapshot 2

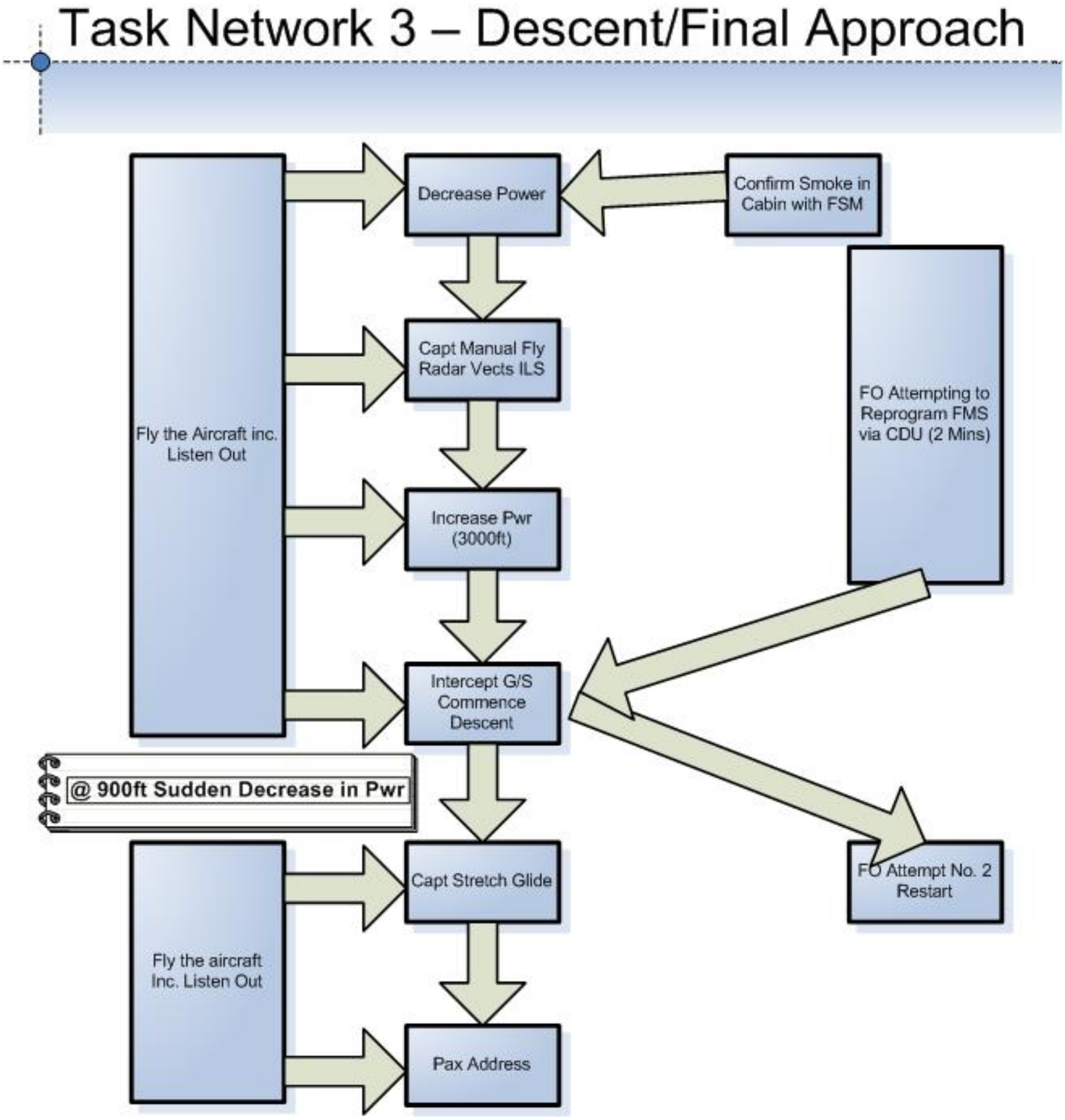


Figure 3-4 – Task Network in Snapshot 3

EAST uses the HTA and other information gathered about the scenario to develop Communications Usage Diagrams (CUDs) and a Social Network Analysis (SNA), which illustrates the social network present at the time. In the same vein, the AAIB transcripts available through the formal report were analysed to construct communications diagrams (in the same sense illustrating the social set-up) for each of the three action sequences (Figures 3-5 to 3-7). The arrows represent the level of communication between agents; high, medium or low. These terms are based on the number of interactions recorded in the accident data (from the report stating an interaction between flight crew for example or recorded transcript evidence of a radio communication) and show the relative passages and levels of communication.

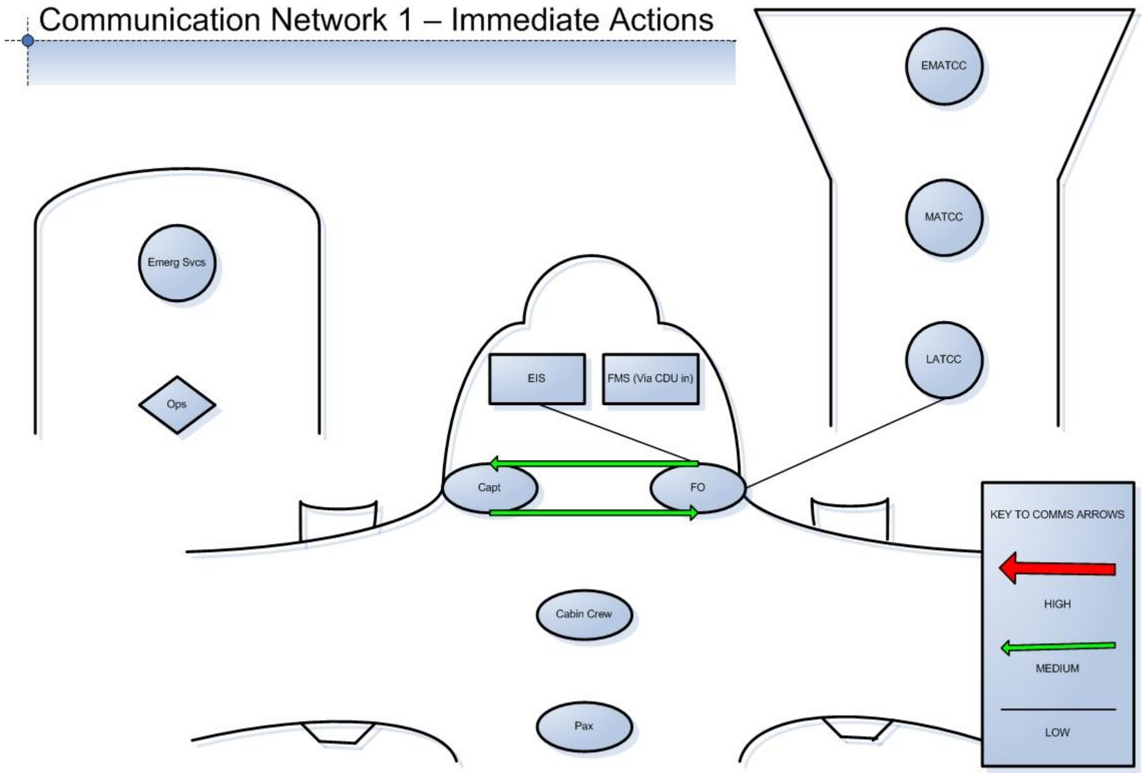


Figure 3-5 – Communication Network in Snapshot 1

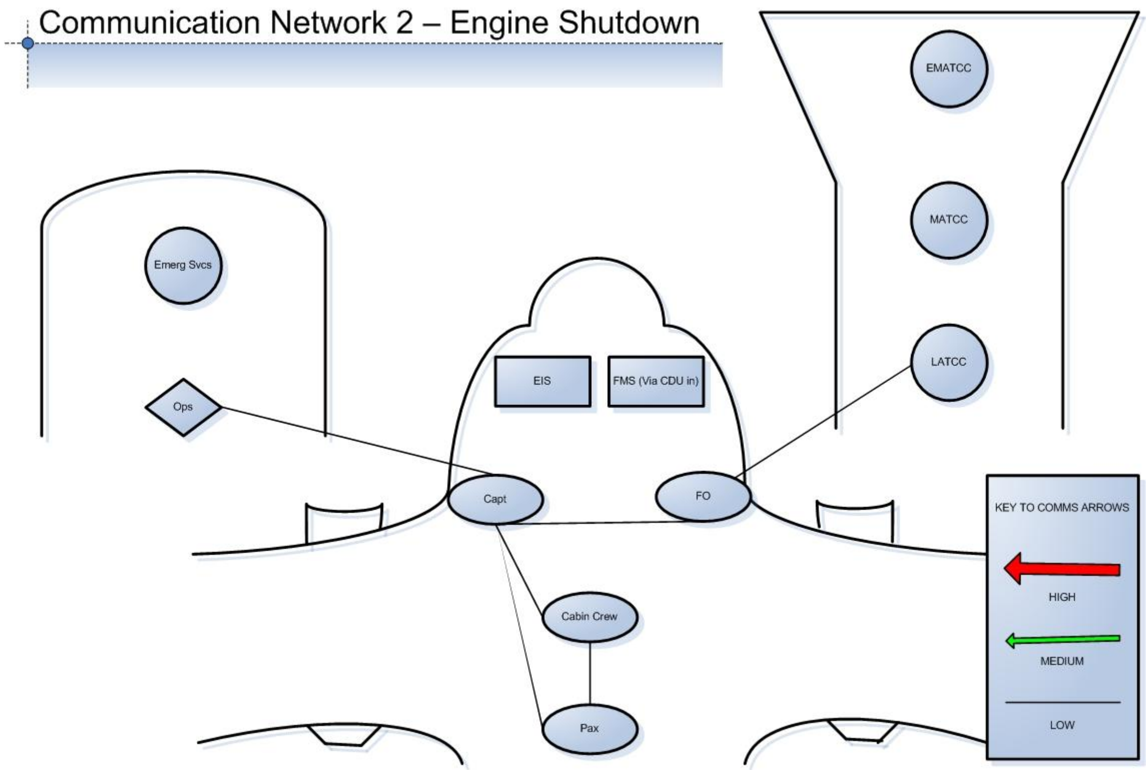


Figure 3-6 - Communication Network in Snapshot 2

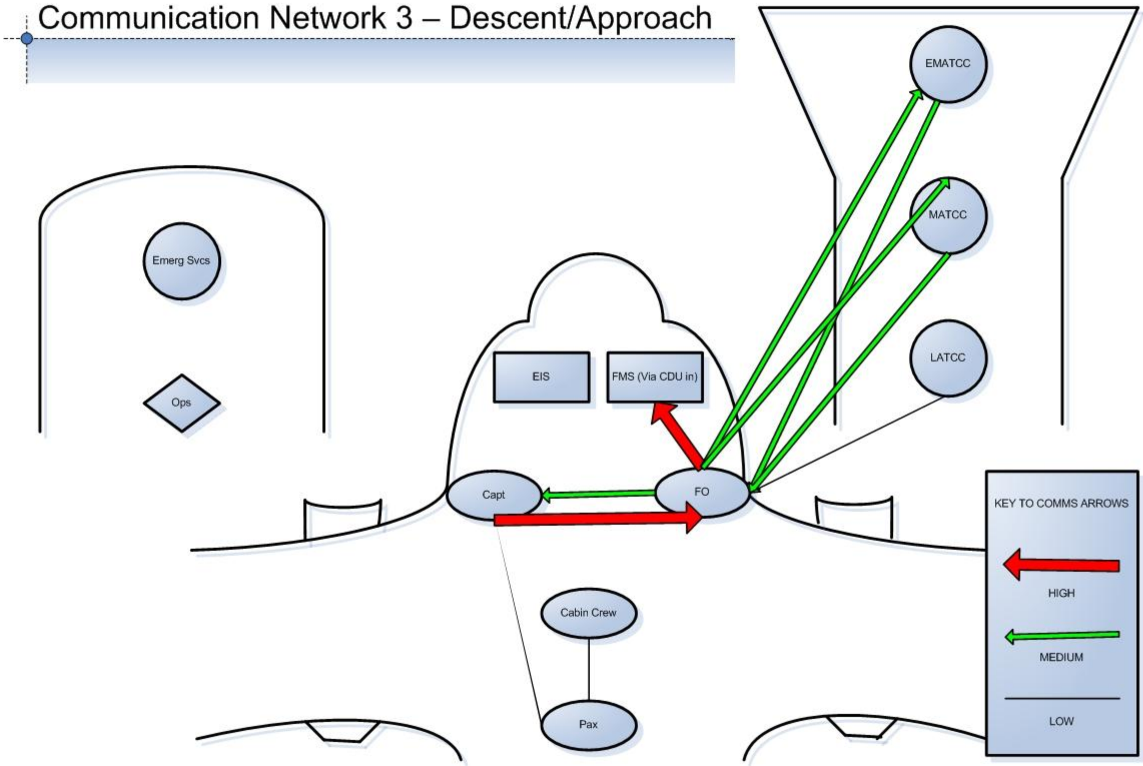


Figure 3-7 - Communication Network in Snapshot 3

The third network that completes this total system view of the aviation event is similar to EAST's Information Network. There is much discussion in the literature (e.g., Ogden, 1987; Collins and Loftus, 1975) about specific uses of the terms and networks that are used to denote knowledge and the presence or lack of it. As such, it is important to clarify the exact representations illustrated in this approach to a knowledge network to work in conjunction with the CUD and Task type networks above. For the purposes of this study, the nodes present within the information network are words or terms taken directly from the AAIB report similar to methods used in task analysis techniques (including the narrative and transcript) to represent 'available information elements' (i.e., raw information that is present within the system at any particular time). These information element words were identified in a novel way compared to the original EAST methodology. Information element nodes were populated through analysing the report text and compiling a list of noun-like words (i.e. those that name a person, place or thing (Allen, 1984)).

These elements are then connected to each other using propositional terms such as 'has', 'displays', 'causes' or 'senses' to create the networks. Walker *et al.* (2009) identify, in the construction of information networks, this process as akin to practices common in linguistics research.

The EAST methodology then attempts to use the results of each of the three networks to create a theoretical 3-dimensional interconnecting network. However, in order to develop the method further, in this study the networks are further refined by highlighting those information elements that are 'owned' or activated by any particular actor, human or machine, at any particular time (cf. Sarter and Woods, 1991). The author, again with guidance if required from the team that developed EAST, worked through the AAIB document and identified occasions when a node was referred to by an actor or in relation to a non-human agent. Examples of this would include where the first officer spoke of a fire; this would identify conscious ownership of the information element relating to fire. Additionally from the data recorders on board the aircraft details of the vibration indicator readings and fuel flow etc. could be gathered and from this it could be decided whether the aircraft systems owned the information or not.

This ownership is denoted by colour in the networks. In this way, the network allows us to view which information elements *could* (or even *should* in an ideal world) be consciously owned, and which ones *are* actually owned. This allows us to identify where communication breakdowns can occur - that is, where crucial information is not being shared throughout the entire network. As such, it is the aim that in a prospective sense, this eventually shows us where the major problems and faults may arise to lead to an accident or incident.

Due to the nature of the information gathered from aviation accidents it was not possible to use primary sources of information other than those reproduced, in part, in the accident report. However, the method has been developed so that analysis can be based upon evidence directly available to investigators at the time of any event including witness reports, flight data recordings and crew reports.

Figures 3-9 to 3-11 represent the spread of information in the three separate action tasks for the events leading up to the crash of G-OBME at Kegworth (A key is provided as Table 3-1). The information networks presented here have moved on from the traditional EAST approach in that elements of the task and communication networks are included through the coloured ownership of nodes. It allows the focus to remain on the information networks and remove the need to draw on all three networks at once.

Figure 3-8 guides the reader through the five-step methodology adopted to create these information networks:

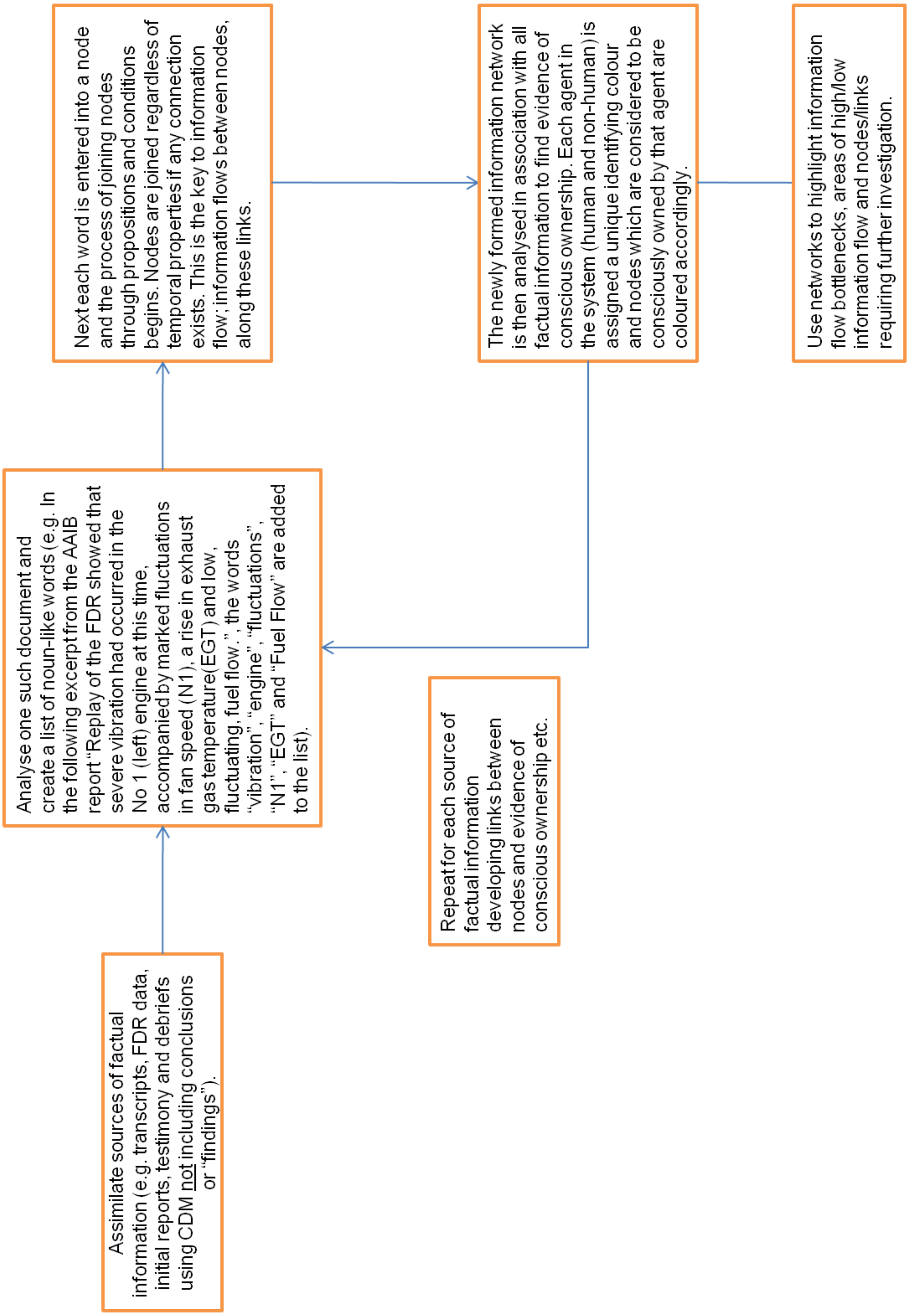


Figure 3-8 – The five-step methodology to create the information networks

Figure 3-9 – Information Network in Snapshot 1

Figure 3-11 – Information Network in Snapshot 3

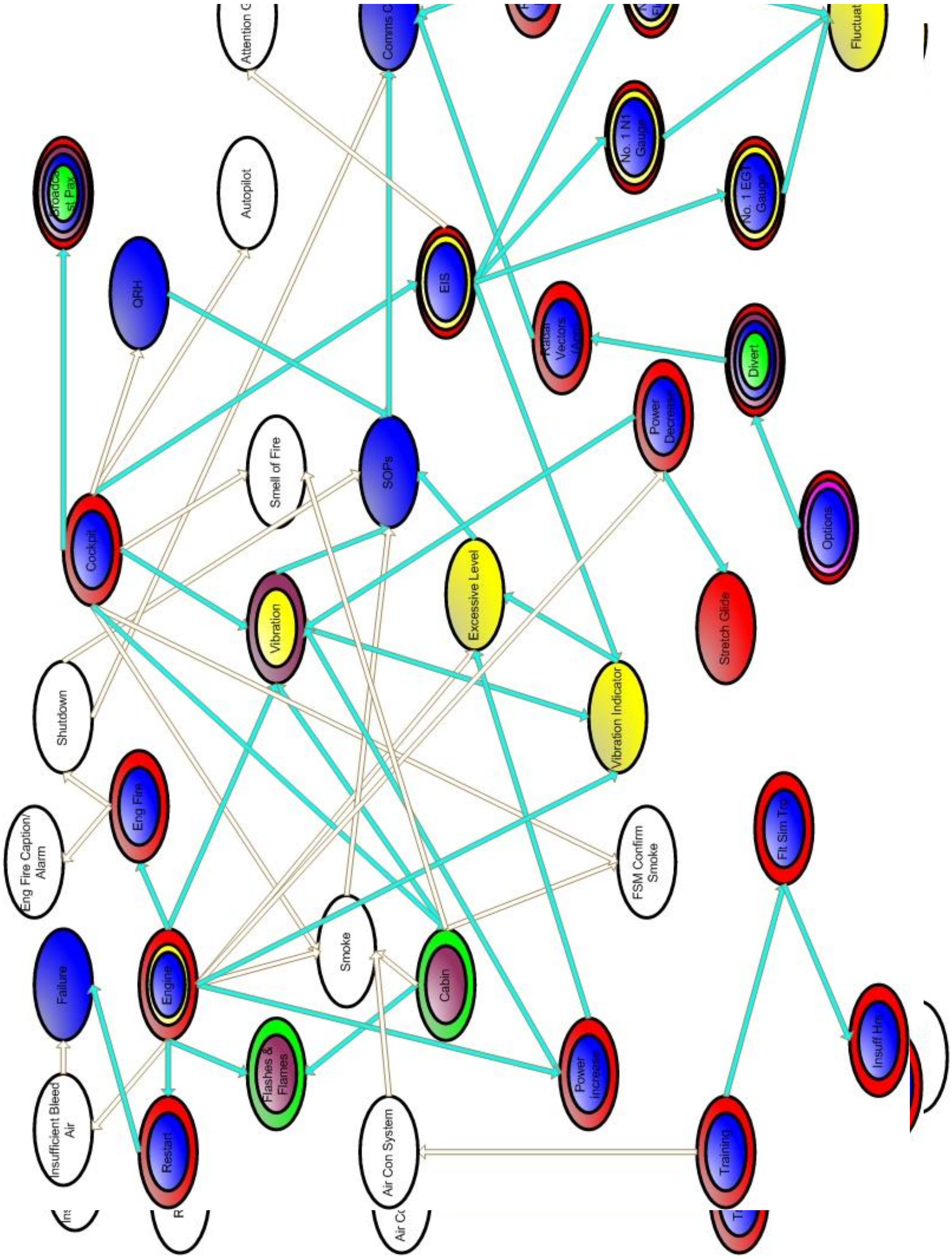
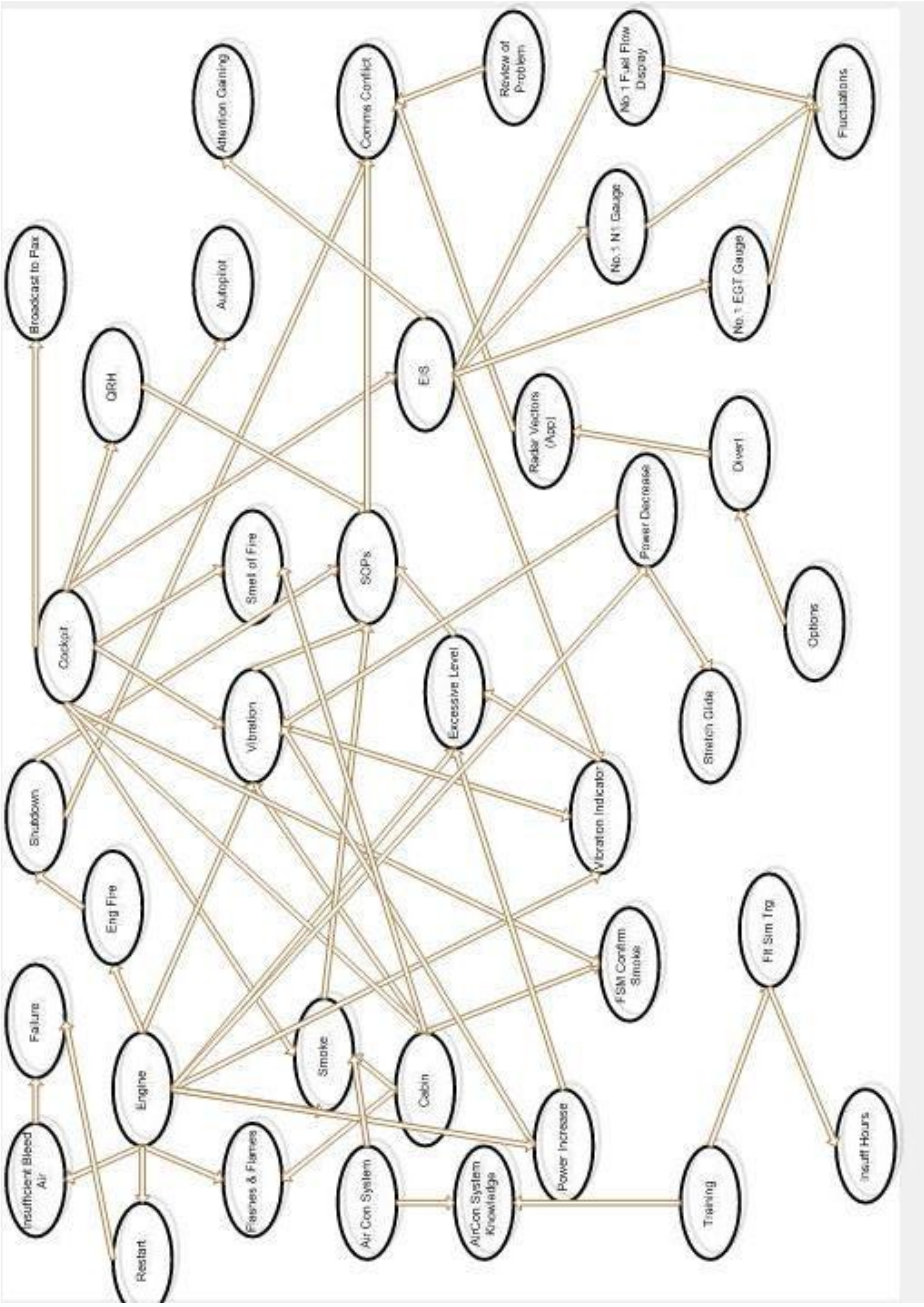


Figure 3-12 – Information Network uncoloured for clarity



Node colour (or part constituent)	Agent consciously owning information
Red	Captain
Blue	First Officer
Yellow	Engine Instrument System
Green	Cabin Crew
Purple	Passengers

Table 3-1 - Colour Key for Figures 3-8 to 3-10 (Figure 3-12 has also been included in the thesis without ownership colouring to make the node labels easier to read)

3.5 Analysis of networks

This section begins to draw conclusions from the networks that have been developed. Key to this section is the concept of ownership and where two nodes that are linked do not share the exact same colours (i.e. are owned by the same agents) there is an issue of information loss or gain that needs to be investigated further. Equally where a node is not active (or owned) where it may well be expected to be that too is an issue for further investigation. Later in the chapter the issue of time is also addressed as networks can be animated over time (snapshots or ideally continuously in future versions) and where nodes change colour (ownership) so again an issue of information entering or leaving the system between networks is identified.

The task network for each snapshot illustrates the actions that are being carried out by all actors within the scenario and is a reference point from which to understand the communication and knowledge transfer that is in progress. The communication network too helps to ground the knowledge elements in the wider picture and allows for us to relate the transfer (or not) of these elements between humans and machines. These two networks in particular are envisaged to come into their own when further work is carried out to integrate and link the three networks together forming an inter-network and intra-network three dimensional network model of the accident sequence.

The network of particular interest at this stage in the thesis is that of the information elements. Immediately visible, even without a detailed knowledge of the events, are elements of information that are present and “owned” at any particular time. This in itself is a novel approach to accident investigation and a new method with which to illustrate the information space in which the decisions were made and actions taken that led to the events reported. It allows for a positive visualisation of the particular time at which the networks are formed and by comparing a series of networks it shows the changes over time of communication, tasks and most importantly conscious information within the system. The analysis highlights which aspects of communication between human and machine agents underpinned the event – that is, which information elements were present or absent for key agents at the right times. The analysis highlights which aspects of communication between human and machine agents underpinned the event – that is, which information elements were present or absent for key agents at the right times.

The stylised network diagram immediately draws to the eye of an investigator the presence, or lack, of relevant pieces of information to a particular agent at any time during the event. Take, for instance, the node 'vibration indicator' (Figure 3-13) from the overall network. Information elements linked with the indicator (e.g., 'vibration' and 'engine') are present for all of the agents on the aircraft. However, only the Engine Instrument System (EIS) has ownership of this important node, and as such the communication has not effectively been transmitted to pilot and first officer. This is also true of other nodes and links within this knowledge network. It may be pertinent at this point to revisit the concept of ownership within the information networks. A key foundation of the EAST approach is that it does not differentiate between human and non-human agents as both are key to the flow of information within complex systems. Within human agents it can be said that an individual owns a piece of information within the system when they have conscious knowledge of it. With a non-human agent the definition is required to be slightly more flexible in meaning. In the case of the EIS, engine parameters are received via an airborne vibration monitor which analyses and converts engine vibration to a displayable reading. In the sense that the information "vibration level" has been recorded and is being displayed via the EIS on a vibration gauge it can be argued that the EIS has ownership of that information. This information is owned (being that it is present and correct) and displayed within the system.

So from simply looking at this network structure we can deduce that communication has failed to bring the vibration indicator to the conscious awareness of the flight crew and as such highlights this node as a possible contribution towards the resultant situation. This in itself is a novel illustration and approach to highlighting design failures and where further investigation is required to assess management of the situation.

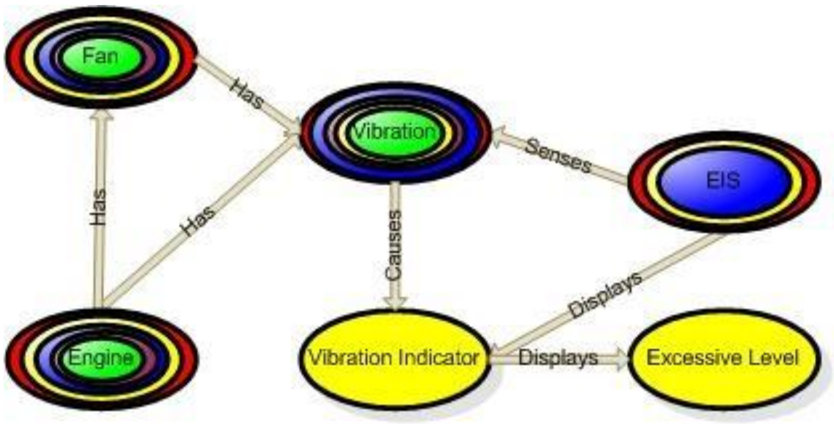


Figure 3-13 - Details of Nodes surrounding “Vibration Indicator” (See key Table 3-1)

Taking this one step further, at the other end of the network (Figure 3-14) we can see that the captain and first officer both have ownership of the engine instrument gauges (Engine Gas Temperature (EGT), N1 Fan Speed, Fuel Flow) information nodes. However, neither of the pilots had ownership of the information node ‘fluctuations’; i.e., they at no time acknowledged the fluctuations of values within these gauges despite having recollected awareness of having looked at these instruments and presumably their individual values.

Together from this, we can see that neither the captain nor first officer were consciously aware of the high level of vibration indicated on the vibration indicator or the fluctuations of the engine instruments. Communication of information from the instruments to the flight crew has thus flagged itself as an important issue in the network and as such is a possible contributing factor towards the accident.

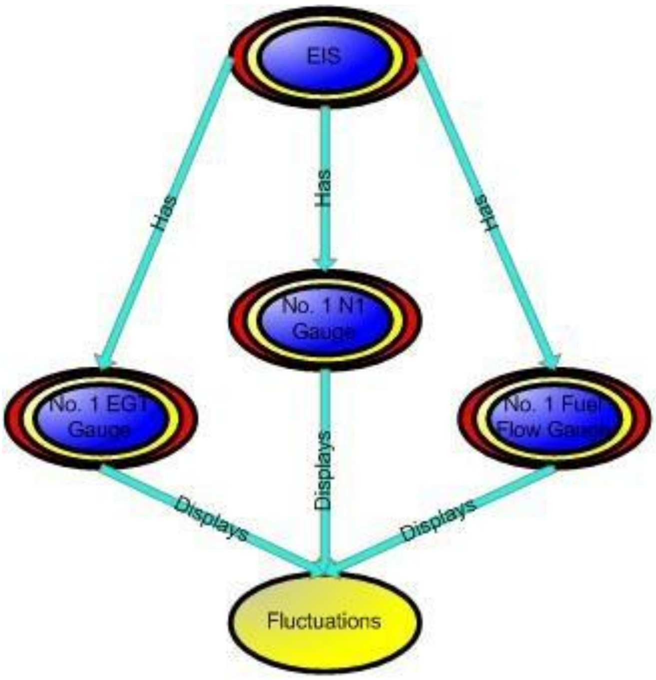


Figure 3-14 - Details of Nodes surrounding “Fluctuations” (See key Fig. 3-8)

It is possible to study these findings in more depth. It is important to designers not only to be given information on when a system design has failed but also how and why it may have occurred and any risk management factors that were involved or could be incorporated. That is, it is not enough to highlight a problem but it is necessary to provide some options for risk reduction. The EAST networks allow us to identify where system design elements may be a central cause in erroneous events - whether that is through technically-designed machines or training-designed humans. The following extract from the analysis highlights an example of not just what has gone wrong but also looks at the interaction of networks to understand why.

At time 2005.05 hrs (the onset of vibration) until 2005.31 hrs, the Captain had ownership of the node ‘vibration’ (if not ‘vibration indicator’) and knew something was obviously wrong with an engine, although unsure of what or which engine it was. During this time it can be seen, by stepping the information network through different periods of time, that neither the nodes ‘engine fire’ nor ‘shutdown’ were owned by the captain until at, or after, 2005.31hrs. At this time, the first officer uses the phrase ‘…looking like an engine fire…’ in a radio communication to London Air Traffic Control Centre (LATCC) (AAIB Report Appendix 4a, 1990). By viewing the corresponding communication diagram, we see that this leads the captain to the assumption of an engine fire despite the absence of usual cues (e.g., fire alarm visual warning or bell). Thus in the latter network the captain takes ownership of the nodes for both ‘engine fire’ and ‘shutdown’ (Figure 3-15).

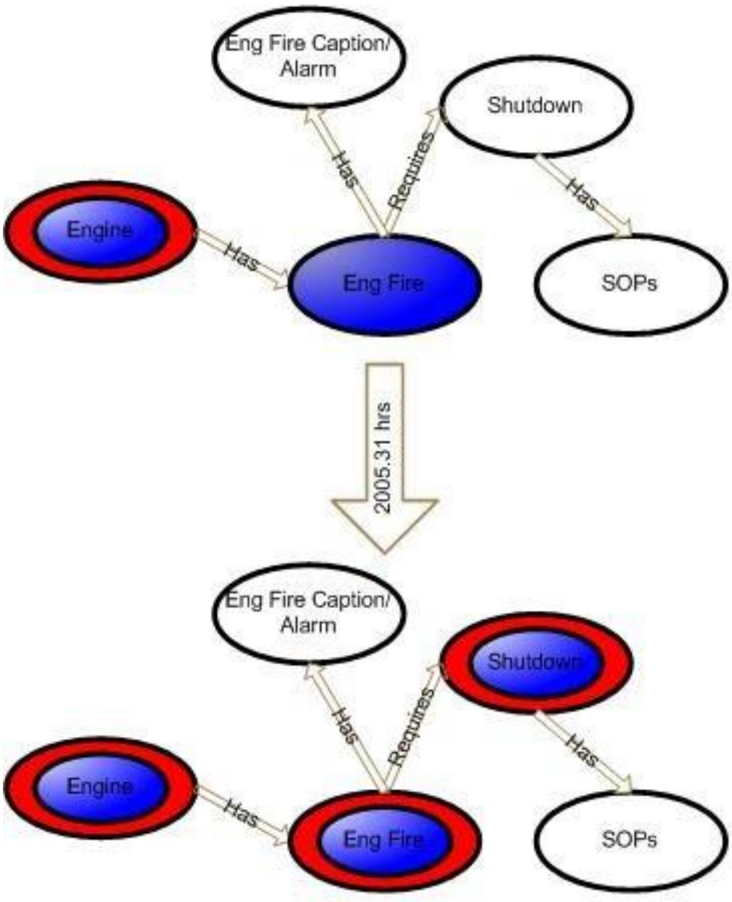


Figure 3-15 The erroneous transfer of information on the flight-deck

This example crudely illustrates the connection between the information networks for the pilot and first officer. By applying the terminology of signal-detection theory (Table 3-2; Green & Swets, 1966) we are able to fully describe the system situation at the time of these decisions and the false alarm that was the basis for many of the following incorrect actions. This communication failure is very different to the examples centred on engine instrument fluctuations above. The successful passage of erroneous information causes a false alarm as opposed to the unsuccessful passage of correct information (a 'miss') in those previous examples. All of these instances have an effect on the system and hence on the outcome. Examples such as these can direct further study into specific elements of an incident and understanding, for example, possible latent issues of expectancy in this particular example. In this way, the method does not solely focus on the active issues of an event but can additionally elude to the latent factors beneath.

	Response "Absent" (Carry out vibration	**Response "Present" (Carry out engine fire**

	Check list actions)	actions)
Stimulus Present (Engine fire auditory or visual alarms)	**Miss**	**Hit**
Stimulus Absent (No engine fire auditory or visual warning)	**Correct Rejection**	**False Alarm**

The use of these information networks in the analysis of an event allows a clearer picture to be developed for designers, highlighting those times or pieces of equipment with which higher than normal levels of confusion, communication, clutter or workload

Table 3-2 Categories of signal detection (adapted from Green & Swets, 1966)

are related. It would appear that higher numbers of information nodes present, or active, within a system would relate to an increased workload in assimilating the information and 'owning' it. The graphical depiction of such information bottlenecks, or areas of intense communicative activity, allows for easier interpretation and identification of risk factors for system breakdown.

In the particular example of the 'engine fire', we can see from the information networks of both pilots that the captain had no ownership of this information until such a time as the first officer passed his (erroneous) ownership of this node to air traffic control (ATC) – when the captain also assimilated it. This illustrates most clearly the relevance of these network models in identifying how situation awareness propagates across the system. Despite being a negative (false alarm) event for the system, this particular instance depicts how not all individual agents must own the same pieces of information (nodes) for it to become the team SA (Salmon *et al*, 2008). Even where all team members own the same information, such as conscious awareness of certain instruments, each individual's conclusions from that information may be unique and lead to differences in resultant behaviour. (Stanton *et al,* 2009).

3.6 Implications for further work and limitations

It is the ultimate aim of this new approach in accident causation investigation to link the separate networks and use the interaction between them to interrogate system events and produce possible prospective analysis. Therefore this preliminary study only begins to address the issues that must be resolved in order to develop a fully working model and fulfil the brief.

It is worth noting that the full accident transcript was not available to study (rather the significant portions were included in the report) so it is obvious that were this possible more work could be done to validate and make use of the communication/social network and then from this look for ways of integrating the three into a three-dimensional model. This is of course a goal that further development of the modelling methods and techniques will work towards. There are also limitations associated with the use of a case-study born from official accident report documentation. The Kegworth accident was a complex event and the investigation no less so. Although it is rational to argue, as in section 3.4, that some validation is received from gaining similar conclusions to that of the official accident report it is possibly cyclical in nature. However, it can also be seen that to come up with the same conclusions as a hugely in depth investigation from a novel method is integral to the life of this model. Beyond this validation exercise though, this chapter works as a feasibility test. Despite there not necessarily being any new findings or lessons it does showcase a new method. Chapter 4 of this thesis looks more at new findings and applications whilst later chapters then address predictability and application of methods.

What this new method brings to the table is a formalised method for investigating an accident whether from primary (and immediately after the event) information, secondary data or even elements of predictive data as long as information networks can be created. The network aspect of the approach removes the reliance on linear timeline approaches that dominate attempts to investigate and discuss an event. The networks have shown that equal measures, if not more, of information can be displayed and relationships between nodes and routes of information processing are clearer. This method is the first to truly centralise the theme of communication (information flow) and use that as a basis for analysing and describing an event but more importantly the whole system within which the event took place. This draws less artificial boundaries into an investigation and opens up the possibility of identifying communication channels or routes of information flow that are not obvious from the outset. The non-linear approach also prevents narrow-minded investigations from the point of view that it requires the investigator to follow up on the broader system as it is unlikely nodes do not develop links reflecting and directing analysis towards the broader system. This leads, as intended, to a more comprehensive accident analysis. It can be seen that further to this formalised method (something championed by the likes of Johnson *et al.*, 1995) the networks also continue to remove individual fault as a conclusion. The networks identify where the correct information was not available to the correct agent at the correct time; a system fault to a system event.

The repeatability, and usability, of the methodology between users needs to be studied as further work. This method is applied, at a base level, to live accident/incident scenarios with primary source data used to populate the networks in later chapters. Furthermore, this method is very much grounded in the ergonomic principles of accident investigation and work is ongoing to integrate effectively the more technical (or hardware) issues within the system model by studying parallels with methods well-tested in this area, e.g., Fault-trees and Risk Assessment Tools.

An HTA-type technique could be developed and utilised to analyse the text of a report, or used post-accident to analyse the scenario. This technique may also be employed for prospective analysis situations where communication of knowledge elements is very important. It wasn't necessary to use an HTA, as EAST would prescribe, in this study due to the macro nature of investigation and some limitations again with the full transcript etc. not being available for viewing.

In a real life scenario application of this method, it would be possible to use a CDM for post-event interviews etc. but this was effectively done by the AAIB investigation team in order to gain crew statements for the report used. Further work also needs to be carried out to incorporate elements of organisational structure into the networks and thus model. This may be implicitly, i.e., implicit in a breakdown of communications is an organisational issue to be addressed, or, explicitly, i.e., incorporated into organisational nodes and thus into the model physically.

3.7 Chapter summary

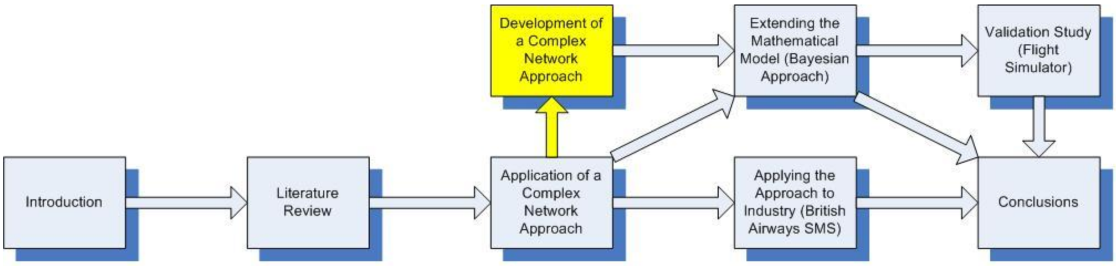
This chapter has discussed the novel application of information networks as a methodology for understanding a complex event more holistically. The method improves the illustration and analysis of the information present within a system (represented by all the nodes), the information readily available to human agents (non-human agents e.g. EIS owning information) and the information consciously received and processed by agents (i.e. owned nodes). In this way, the approach allows us to study not only communication and information within a system but also the concept of situation awareness (SA); both individual and team (Salmon *et al.*, 2008). This concept is taken further in chapter 4.

Chapter 2 highlighted shortfalls in the current resource bank of accident analysis models. A dominance of artificial linear chain models together with many subjective classification techniques left requirements for the field to change. Central to the gaps in current models was the need to understand more fully the system in which events took place rather than just the events themselves. In order to begin to achieve the removal of these gaps, information networks have been developed within this chapter to incorporate elements of ownership and centralise this theme of communication (information transfer) that underlies the events. Central to the conclusions of this chapter then is that this new method of applying information networks to an aviation accident has gained results in several hours deskwork which are very similar to a high-profile full investigation by several bodies that lasted months (e.g., Besnard (2004) and Johnson (1995) referred to earlier). By highlighting individual nodes of interest to the investigation from using the network diagrams similar conclusions to the official investigation could be made. This is not a negative thing since it is the purpose of this chapter to assess the validity of applying the method to aviation accidents and that validity has been shown. If it were argued that there has been no improvement over current methods then that is where chapter 4 and the quantification of networks and its related SA comes in. This chapter has set the shape of the work in this thesis.

Key throughout has been the forward movement away from linear chain models towards something more dynamic and complex that retains the nature of the system reflecting the flow of information and bottlenecks that exist.

Chapter 4 investigates methods of quantitatively objectifying the process and possible avenues for using suitable metrics. Chapter 5 then develops the quantitative theory in order to capitalise on the potential of this complex systems model.

4 Development of a study



Chapter 3 applied a novel information network methodology to an aviation case study. Primarily, this resulted in the centralisation of communication as a theme of aviation accidents. The application of the method also highlighted many positive outcomes including improved visualisation of a system and avoidance of linear decomposition of the event.

This chapter sets out to extract more from the information network approach in more detail and introduce comprehensive comparisons with an 'ideal' scenario. Further than this, chapter 4 continues the work of chapter 3 by beginning to develop the approach and seeks to objectify the process. First non-accident scenarios are discussed so that there is a baseline to compare the accident networks from chapter 3 against. Next quantitative methods are discussed, evaluated and their integration into the information network model investigated. In particular social network analysis is used in this chapter before the evaluation of other methods and metrics results in a conclusion of how to take the work forward in chapter 5.

4.1 The importance of centralising communication

Where the EAST analysis provides qualitatively more information than its predecessors is in identifying the points at which information is not effectively being transmitted to the right people at the right time – that is, where the knowledge has not been salient enough. It is in their foundations as a truly systemic and holistic analysis tool that the information networks provide a new approach that envelop all areas of the system and not simply the design or human-element in isolation. From this it is possible to suggest ways of designing and developing systems (e.g., to increase relevant salience) and training procedures (e.g., the effect seen from limited conversion training above), feeding back to the design stages, to make the information more salient (or communication channels stronger) and thus improve information transfer. The ability of the networks to illustrate information propagation through a system clearly supports the application of the method to the study of situation awareness and in particular team situation awareness (Salmon *et al.*, 2008). This holistic use of networks to help understand Distributed Situation Awareness (DSA) in relation to developing training or designs is an important step in using SA as more than a label-cause of accidents and begins to address the requirements of the Human Factors community in this area (Salmon *et al*, 2008a). This is in itself a novel approach to accident investigation and a new method with which to illustrate the information-space in which the decisions were made and actions taken, thus centralising the construct of communication to any distributed and complex task.

Taking this idea of saliency of information within the networks further, it is clear that certain nodes that should have been owned in an 'ideal' situation but were not in the actual event can be described as being not salient enough for the relevant agents to have consciously locked onto them. If we take systems improvement to be akin to improving saliency of key information, these networks allow tidy observations from any post-event analysis and can easily highlight those areas where an increase in saliency is required in order to counteract possible communication failures which in turn can direct, or highlight, design related issues. Thus it appears as if there is scope for 'ideal' networks to be integrated into the approach to gain a deeper understanding of the study of an event or system. Further to this, this chapter acknowledges the importance of identifying salient nodes and connections within this network before addressing the connection between networks and further development therein. Moving back to what can be concluded from the method this far, it has become apparent that an important difference with this novel work is that it concentrates on communication as a cause of all events.

Much work has been carried out in recognising communication as a major contributing factor to risk in a number of domains, including aviation (see e.g., Gibson *et al*, 2006). In the current thesis, it is argued that communication failure can be seen as the basis of all aircraft accidents and incidents. Whether the communication is machine to machine, human to machine, or human to human, all are based on the passage of information between multiple agents (see **Error! Reference source not found.**). In the present analysis, it is crucial that we do not distinguish between human and non-human agents in the system in order to understand the impact of communication. Indeed, it appears that the humans involved in these complex domains view the holistic system in that way (Stanton *et al*, 2006). Optimising communication is thus of central importance to managing the risks in complex systems; in turn, the design of interfaces and communication channels is fundamental to avoiding failures that may occur in their use. Carvalho *et al.* (2007) discuss how through naturalistic decision making mechanisms, agents within complex systems often resort to using a number of heuristics to direct their decisions and how vague communication (in this chapter between human and non-human) often leads to incomplete situation awareness. Through identifying communication as key within the system space it is hoped that this method may identify, as in the Kegworth case-study, areas where saliency of information needs to be raised in order to govern the decision making process of agents.

From/To	**Human**	**Machine**	**Job Aid**
Human	Voice Written note	Keyboard Mouse	Writing Recording
Machine	Displays	Data	N/A
Job Aid	Checklist Procedure	N/A	N/A

Table 4-1 Example Taxonomy of System Communications

A new methodology based on network models of complex systems has, in this study, been applied for the first time to aviation accidents in order to elucidate the full aetiology of the incident and in an attempt to identify the complex factors involved in a system failure. Despite EAST's original development as a qualitative tool for understanding and improving system performance *in toto*, it does offer the possibility to analyse in detail the spatial and temporal development of an incident. These networks have been seen to allow a new pathway for preventing accidents focusing on the whole system and not any one part in isolation.

Individual situation awareness (SA) is often the centre of attention in accident analysis and yet we can see that any one agent, e.g., the pilot, is just a small part of a wider system, supporting and being supported by others, with information changing hands continuously. As the debate continues in the literature about models of individual situation awareness, team situation awareness has begun to attract increasing amounts of attention amongst ergonomists. The complexity of team SA being a concept beyond that of combined individual SA is clear in work across the community (e.g., Salas *et al*, 1995, Gorman *et al*, 2006 and Salmon *et al*, 2008). However, Stanton *et al* (2006b) introduce a concept that all relevant information is held within a system and individuals may have different views of that information, thus developing a compatible SA rather than a shared SA. Thus, it is the capturing of all the information present within a system that is central to this work and developing an understanding of DSA in accident scenarios.

Applying information networks to aviation accidents allows us to illustrate and understand more clearly the information space in which decisions were made and interactions between agents took place. In this way information networks provide an improved method of investigating the setting and 'why' of individual's actions which has been highlighted as an important issue in literature (e.g., Li *et al.*, 2009). Latour (1991) speaks of the use of networks to define the 'actants' within a socio-technical system in relation to incidents and suggests that once the description is saturated, the explanation emerges. The networks that have been introduced to aviation accident analysis in this chapter propose, in a more objective way, to describe a situation to this saturation point and not attempt to explain an accident. It should become evident from a thorough understanding of the system as it stands and works where situations have been less than 'ideal'.

By analysing the event through the application of information networks, we are able to highlight particular instances of verbal communication, such as that illustrated with the erroneous passage of the 'engine fire' node of information between the captain and first officer. Verbal communication has long been discussed in the literature and there is little debate about its importance in team, or complex, situations. So much so in fact that NASA's ASRS (Aviation Safety Reporting System; a voluntary confidential reporting program) related 70% of its first 28,000 reports to issues with communication. (Connell, 1995). Further than this though, the networks allow us to identify and address instances where non-verbal or non-human to human communication (e.g., passage of information from a display to the pilot) has played a significant role, whether negative or positive, in affecting the teamwork and team situation awareness within a complex system.

Most importantly we are now able to concentrate on the flow of information throughout a system and highlight the communication that does, or should, occur at any particular time. Through analyses of these networks, concentration on communication of information and further development to highlight significant nodes and saliency amongst nodes, the application will allow much better feedback to designers where a system might fail about what, how and why it failed. This will in turn inform the designer how to improve interaction between agents and in particular at points in time with peaks of workload.

As a method of mitigating risk not only through the design process (focusing on equipment) but balancing that with training (the people) and the task (job in hand), information networks, and their associated study of DSA, allows for a new form of feedback pivotal to the flow of information within the system environment. Accident investigation reports are often criticised as being too broad and that they 'are not primarily intended to be used directly by designers' (Brusberg *et al*, 2002). By visualising the information space, this method allows for the scope of an investigation to concentrate on selected areas of communication and information transfer. It is after this narrowing, when communication bottlenecks or information flow centres are identified, that communication taxonomies or social theories such as Activity Theory (cf. Bedny and Meister, 1999) or Actor Network Theory (Latour, 1987) can be applied to search the deeper issues. Where a methodology such as EAST drives the investigation and elicitation of information flow failures so human cognition models such as Naturalistic Decision Making models or Efficiency-thoroughness trade-off, ETTO, (Hollnagel, 2004) can be applied to those specific interactions. Such applications can in turn address the social, psychological, cultural and regulatory issues central to the overall aim (Carvalho *et al.*, 2009) that are often investigated but with the aid of such models can help better direct the search for significant factors.

Unlike many other frameworks that are in present use, this method and model is not exclusively about classifying errors. This is atypical to most developments in recent years and also allows for positive as well as negative issues to be highlighted and investigated in a situation. This is apparent where a positive link is found in an analysis of a particular situation and that may be of use to a different situation but under similar circumstances. In addition it is hoped as the model progresses, actions and links that help prevent or correct a negative event may become salient and be used to feed other similar situations.

Steering towards the use of these network models to investigate incidents and accidents is not to detract from or replace the holistic approaches adopted by many in risk situations (for instance, greater study at a behavioural level e.g., Bennett, 2004). The use of networks to describe and understand the system at the time helps focus the attention of investigative processes in eliciting *what* happened. These then have to be developed further into understanding the reasons *why*. In this way, the networks begin to rebuke the developing nature within aviation to avoid the 'sharp end' completely in an incident investigation in favour of focusing on an upper-echelon search for factors. Instead, this methodology directs an investigation from the sharp end up whilst adding much needed objectivity to the process.

It was discussed in chapter 2 that it is possible accident investigations (and thus the models and methods) have moved away from fully addressing the active factors to concentrate more on those latent issues and a possible explanation for this is a fear of blame. This approach, however, re-evaluates the digression from realising the potential of fully investigating the active factors and suggests a way of investigating active failures by dissecting the situation without the need for blame being intrinsically linked to failure (i.e., failure of communication at some point in a complex network system cannot be attributed to one person). The method allows us to concentrate on the actual event and not be drawn into a full audit of the airline's safety health for the sake of it. This does not however attempt to annul the importance of latent factors either. This model also directs and constrains an accident investigation; by creating networks of the situation an investigator is kept within the confines of the accident itself (which can, and will, include latent and socio-organisational factors) and this is beneficial to the process of accident investigation in my view. If these network models are animated over time then the investigator, or relevant person, has a storyboard of the event whilst retaining the dynamic and complex nature of a non-linear networking approach.

This far in the thesis, specific nodes central to the development of an accident have been identified leading to an increased understanding of the information flow and situation awareness within a system. A central theme that keeps returning is the need to develop a greater understanding of normal and abnormal situations without losing sight of the overall system. Therefore, the rest of this chapter looks to tie together the issues discussed so far and incorporate 'ideal' events in order to elicit differences and possible greater understanding of the negative outcome event.

4.2 Expanding on the idea of 'ideal' networks

Of primary importance to this study, with its relation to SA, is the need to objectively identify nodes of significance. The analysis of the crash at Kegworth highlights the aspects of communication present between human and non-human elements that underpin the event. By developing these network models from only the objective information within the narrative and transcript of the AAIB report (i.e., with no reference to their conclusions or discussion) it can be seen from the full results that very similar conclusions can be made using this method. Having identified some of the key contributing factors for the accident, the next step was to improve upon the standard method and investigate the possibility of developing the method to be more complete.

In order to further objectify the identification of information-flow issues, a set of non-accident scenario networks were constructed that could be used in comparison to those for the accident scenario and the detail of this process is covered next.

These ‘ideal’ networks (e.g., figure 4-1) were based on information from company operating procedures and the checklists that were made available in the formal report. A series of ‘ideal’ task, communication and information networks were produced by the author with reference to Boeing 737 Standard Operating Procedures (SOPs), the AAIB report which included extracts from the Quick Reference Handbook (QRH) for 737 pilots, observations from equally qualified pilots and checklists that were present on the aircraft at the time. The method of creating the information networks reflects the same process for the actual event in chapter 3. The emergency checklists and relevant pages from the QRH and SOPs were analysed and it is these that produced the nodes. As would be expected the nodes found were comparable to those identified in the actual analysis but the ownership of each node was inferred from either the pattern of work, communication practices and checks dictated in the literature rather than solely the AAIB report. An example of this is given in the following extract from the AAIB official report which refers to a drill in the British Midland 737 QRH:

“It defined 'high engine vibration' as a condition indicated by a reading on the vibration indicators in excess of 4.0 units accompanied by perceivable airframe vibrations. It introduced the following procedure:

Thrust lever........ RETARD

Flight conditions permitting, reduce N1 to maintain AVM below 4.0 units.

NOTE: Engine shutdown is not required as AVM indications will decrease with thrust reduction. If the AVM indication does not decrease when the thrust lever is retarded, other engine problems may be indicated.” (AAIB Aircraft Accident Report Number 4/90 (EW/C1095))

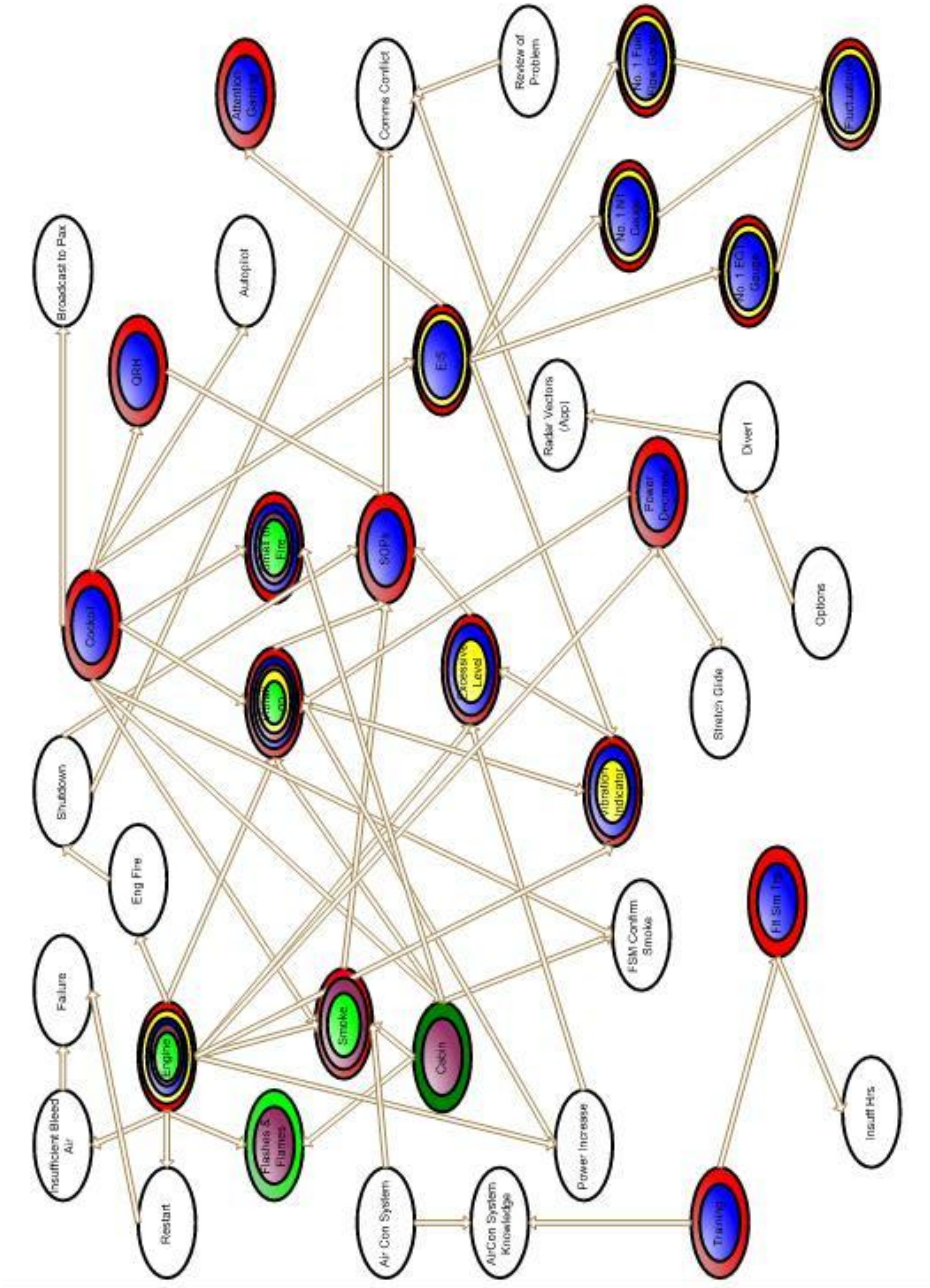
This drill would be assessed in the way Figure 3-1 dictates and deductions made. An example of these deductions would be that given this drill neither the first officer nor captain should have conscious ownership of the node “Engine Shutdown” given the note that it is an unnecessary action in an ‘ideal’ world. Conversely the node “QRH” should be consciously owned by both the flightcrew as they should be referring to it for drills such as this.

The author (a qualified commercial pilot) also validated the networks, albeit informally, with two current Boeing 737 pilots to ensure that no obvious mistakes or presumptions away from the factual report and pilot-literature had been made. This also served to overcome any ambiguities in terms of conscious ownership of nodes and who should have what information at what time. This method of detailing what steps should be taken in abnormal operations, what information should be gained and what actions should be taken and when are standard practise in aviation and the basis for training and operational flying. In future use, the regulatory authority or company conducting the analysis of an event or system will be able to dictate the 'ideal' scenario as they do already with the QRHs, SOPs and other literature they publish and adapt.

By comparing the task and communication networks and imposing the findings on the information networks it was possible to see where communication links have been added or lost. As such, possible routes into the system for misinformation, false alarms or missed knowledge objects can be identified. It is, however, in the information network that the most obvious differences are visible. In our example, comparing the ideal and accident scenarios reveals that the node "vibration indicator" should have been owned by the first officer and captain in addition to the EIS – whereas in actual fact it was only owned by the EIS. This supports one of the major conclusions from the AAIB report, in that the information was available on the flight deck to suggest a problem with engine No. 1, and that the shutdown of the wrong engine may have been prevented had this information been transmitted effectively to the flight crew. It is important at this stage to emphasise that at no point is the purpose of this study to lay the blame for any event with any individual or system component but to understand where the EAST analysis provides qualitatively more information. This is in identifying the points at which information is not effectively being transmitted to the right people at the right time – that is, where the knowledge has not been salient enough. From this it is possible to suggest ways of designing and developing systems and training procedures to make the information more salient (or communication channels stronger) and thus improve information transfer. In a prospective sense, it is hoped this method may eventually show us where major problems and faults may lead to an accident or incident without the negative event having had to occur.

Through comparing the actual and 'ideal' networks fully and removing those nodes that are owned and conscious elements in both, we can deduce that the remaining knowledge elements will have affected the outcome of the situation, the decisions made, and actions taken (figure 4-2). Since these nodes are the differences between an 'actual' and 'ideal' scenario they must play some part in the resulting event whether negative or positive. Elements including "standard operating procedures" (SOPs), the "quick reference handbook" (QRH), "vibration indicator" and "fluctuations" (in the

Figure 4-1 - 'Ideal' information network in snapshot 1



relevant engine instruments) were all highlighted in the comparison as being relevant to the decisions taken (all present in figure 4-2). These nodes may be described in signal detection terms as “False Alarms” or “Misses”. By animating the nodes over time to show ownership in a temporal sense, it is possible to display in a novel way the storyboard of information (together with communication and tasks) in the scenario and investigate in a step-by-step method that still encapsulates the complexity of the system and doesn’t break a dynamic reality down into an artificial linear chain; the crux of the model’s objectives.

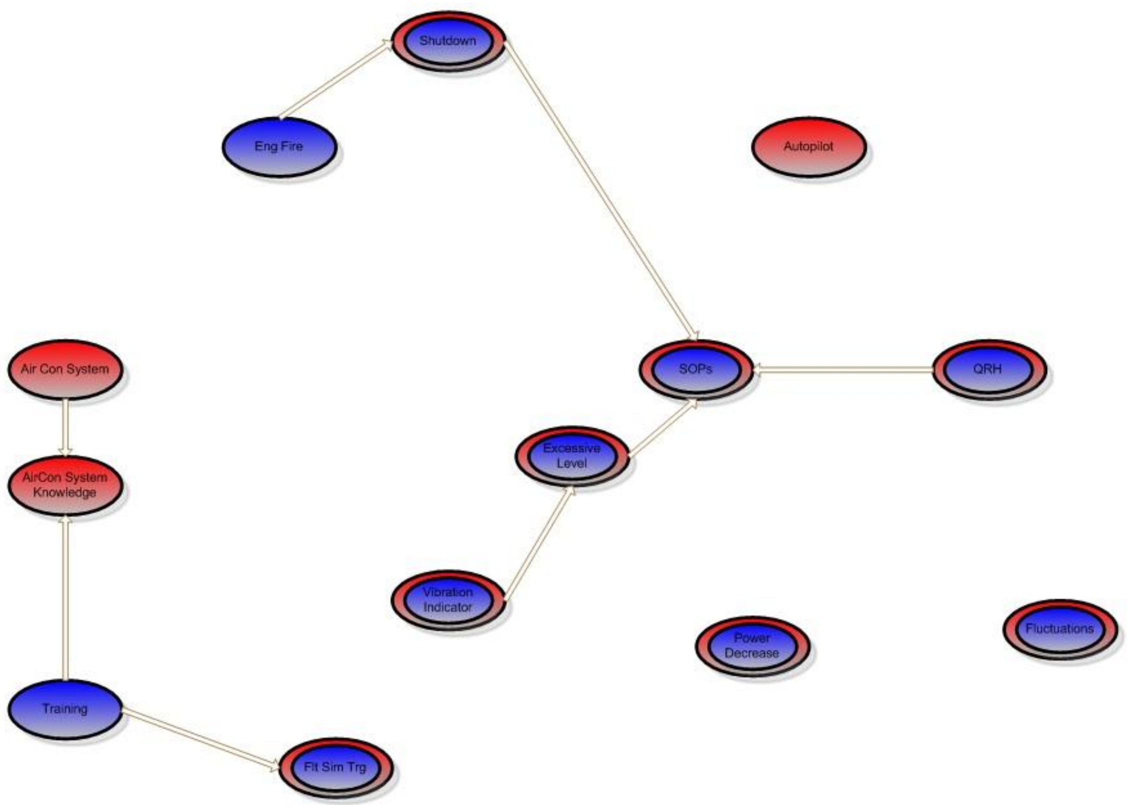


Figure 4-2 - Snapshot 1 with only nodes remaining that contained differences between ‘actual’ and ‘ideal’ scenarios

Figure 4-3 illustrates in a simplified manner one section of the snapshot raised by contrasting the ‘ideal’ scenario against the actual one which is developed from figure 3-14 above. By comparing the task and communication networks it was possible to see where communication links have been added or lost. From this comparison we can see where information may bottleneck, or conversely becomes over-salient, in an actual event compared with the ideal outcome that is central to the design of any system. As such, possible routes into the system for misinformation, false alarms or missed information objects can be identified. By comparing the actual with an ‘ideal’ scenario, it can be seen that in the ‘ideal’ situation the first officer would not mention an engine fire in his radio communication as there are no precursors for this assumption present in his information network. Alternatively, a second ‘ideal’ outcome would be that the first officer uses the same term but the captain assimilates the information present in the system to counter the theory (illustrated as “alternative ideal” in figure 4-3).

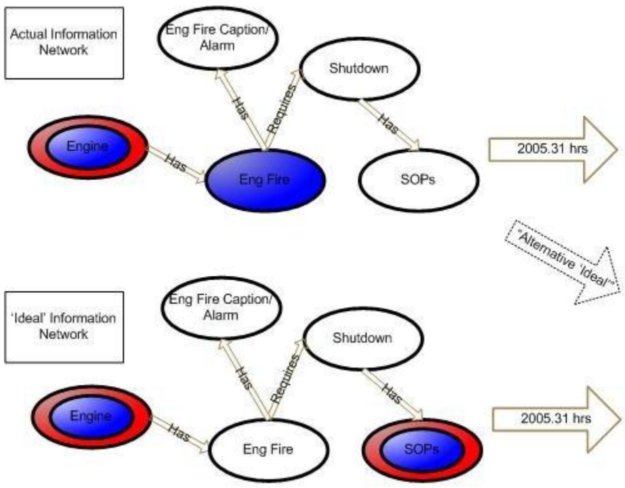


Figure 4-3 - Comparison of a section of actual and ‘ideal’ information networks relating to false-alarm with engine fire

The significance of the ‘vibration indicator’ node within the system, as discussed earlier, is mirrored through this new analysis as being a node of central importance within the ‘ideal’ versus actual comparison. In the AAIB formal report, it was concluded that all of these factors, and in particular the ‘vibration indicator’, were significant in the cause of the accident. This external validation, as discussed earlier, is an important point in the use of a new tool for analysing accidents in that the conclusions remain ecologically valid and the relationships to system design are made clear. Further than this though, these network models provide a springboard for prospective analyses of other scenarios and this idea is built on later in this thesis through looking at ‘ideal’ and actual modelling. This idea of validation is not to say, however, that had the AAIB investigated an identical accident today that the conclusions would have been identical. Methods of investigation, tools and even attitudes have changed and will continue to do so as we develop in the area of advancing safety (Ayeko, 2002). However, it could be argued that the central arguments of the conclusions would remain valid whilst the detail, emphasis and scope might change over time. More importantly, the information network method produced here removes a level of subjectivity associated with some of the linear models discussed in chapter 2 which would increase the likelihood of reproducibility.

The AAIB suggested if the crew had ‘sat on their hands’ and taken time to refer to their operating procedures and checklists, together with fully assimilating the information from the engine indications, the event may have been averted. This is an especially important conclusion given the increased chance of comprehension errors and expected limited capacity of pilot's memory under the high workload of an abnormal scenario (Morris and Leung, 2006). This is only at the superficial level, though, and the report goes on to explain that in the change from Boeing 737-300 to -400, limited conversion training took place and as such, the changes in design of instrumentation contributed to the communications breakdown (compounded by a view from older models that the vibration indicator was an unreliable instrument – which was not true of the -400). This is not to say the designs themselves were a cause of the accident but rather the lack of integration between the operators, the designs, the designers and the risk managers further up the line (Busby and Hibberd, 2002).

4.3 Statistical analysis of networks

In chapter 3, and again here in section 4.2, initial studies of aviation accident case studies using information networks resulted in an improved understanding of the system in which the events took place. Further to this, with communication centralised, the study acknowledges the importance of identifying salient nodes and connections within these networks. This can then be extended to the connection between networks and further development therein. In particular, metrics can be applied to the comparison of the networks in order to suggest key nodes or factors resulting in the event. In this way, it is hoped nodes can be identified as being those that may be present and result in normal operations or a near-miss but key factors, or breakdowns in communication, which may result in an accident and must be removed by prospective analysis at the design or training stages. Work in this vein approaches the theory of the biological sciences with similarities to the study of neural networks. The importance lies in identifying activation levels and transfer functions within nodes to highlight those which are key to an event. It may also be possible to identify those with high levels of redundancy through which an event can still occur despite nodes required not being present or others being present that should not.

It was important to identify a suitable metric for deducing node importance or salience for the information networks. Such a metric was sought and traditional methods of social network analysis (SNA) tested against the data to try and provide an insight into the results; adding the desired quantitative element. SNA has enjoyed multi-disciplinary use, for example, in helping to illustrate modes of communication and information flow, company structure and in medical environments (Houghton *et al.*, 2008).

In order to introduce these quantitative factors in the first instance, a software program developed by the EAST team called WESTT (Workload, Error, Situational Awareness, Time and Teamwork; Houghton *et al.*, 2008) was used. By entering the information network data (nodes and links) in to the computer program, statistics such as the Bavelis-Leavitt index of centrality and measurements of sociometric status can be applied to the networks produced. Sociometric status aims to identify the overall contribution of an agent to the communication (in all forms) within a network. Centrality is a metric that indicates the most central agent. This is calculated in terms of the smallest geodesic distances from all others, where a large geodesic distance results in a long period of communication and more chance for distortion of the information. Both of these metrics arguably attempt, in different ways, to identify key agents or nodes within the network graph.

Turning to the information network analysis of the Kegworth case study, it was decided to at first concentrate on the first snapshot only. The actual and ideal networks were focussed on in order to elicit as much detail as possible from one section before moving on and combining multiple network data. The results of the initial statistical analysis as carried out using Agna (Benta, 2003) are produced in a simple chart below for comparison (Figure 4-4).

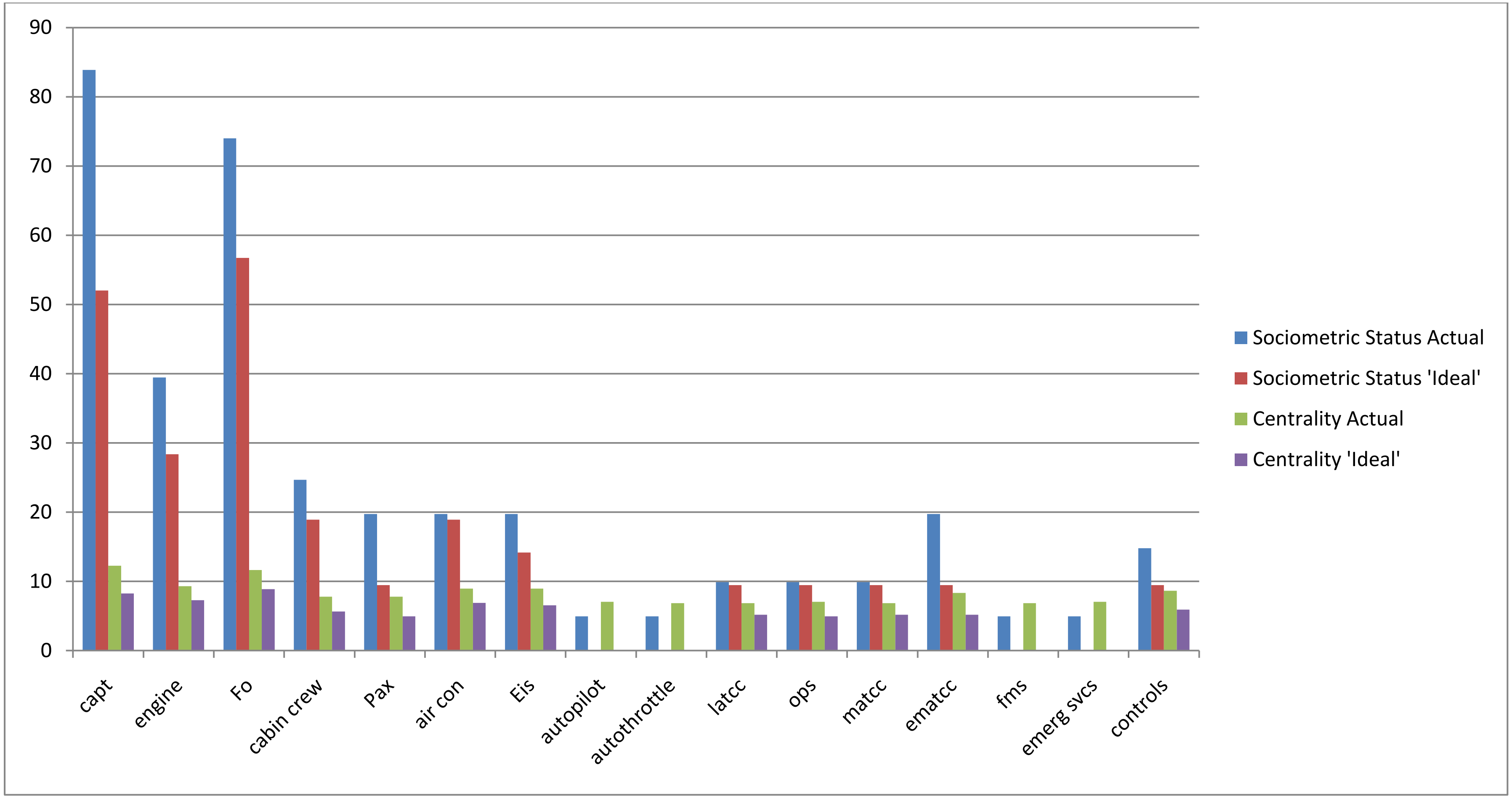


Figure 4-4 – SNA Analysis of Kegworth (snapshot 1)

This original data-mining used the information from the WESTT analysis and as such centred on the actors (e.g., Captain or First Officer) in the analysis. Since, in the application of the information network approach to Kegworth, agent's owner ship of a node could be identified within the network, the agents no longer needed to be considered independently for the SNA. Thus, it was then important to apply the metrics to only the nodes within the information networks which removed the actors from appearing in their own right for the remainder of the analysis. In this new way, instead of applying SNA to a communications network, it was applied to the information network with communication being implicit in the linkages between those nodes present within the system. This could help elicit what is central, or key, within the information network and what information is not being communicated effectively; an aim of the application of this methodology.

In the context of our information model, sociometric status appears to be a more valid metric with which to contribute towards node importance since it is this that illustrates the information communication power of any particular node most closely. The nodes identified in chapter 3 as being of most interest (i.e., those central to the development of the scenario) in this particular case study and their associated metric values are given in figures 4-5 and 4-6.

For the purposes of this first stage, all nodes that were active were given a value of 1 in the social network matrix used as the basis for the analysis (see Agna user guide for more details). We can see that this has had an effect to essentially mask some of the more subtle data within the network such as magnitude of ownership and position in the graph field.

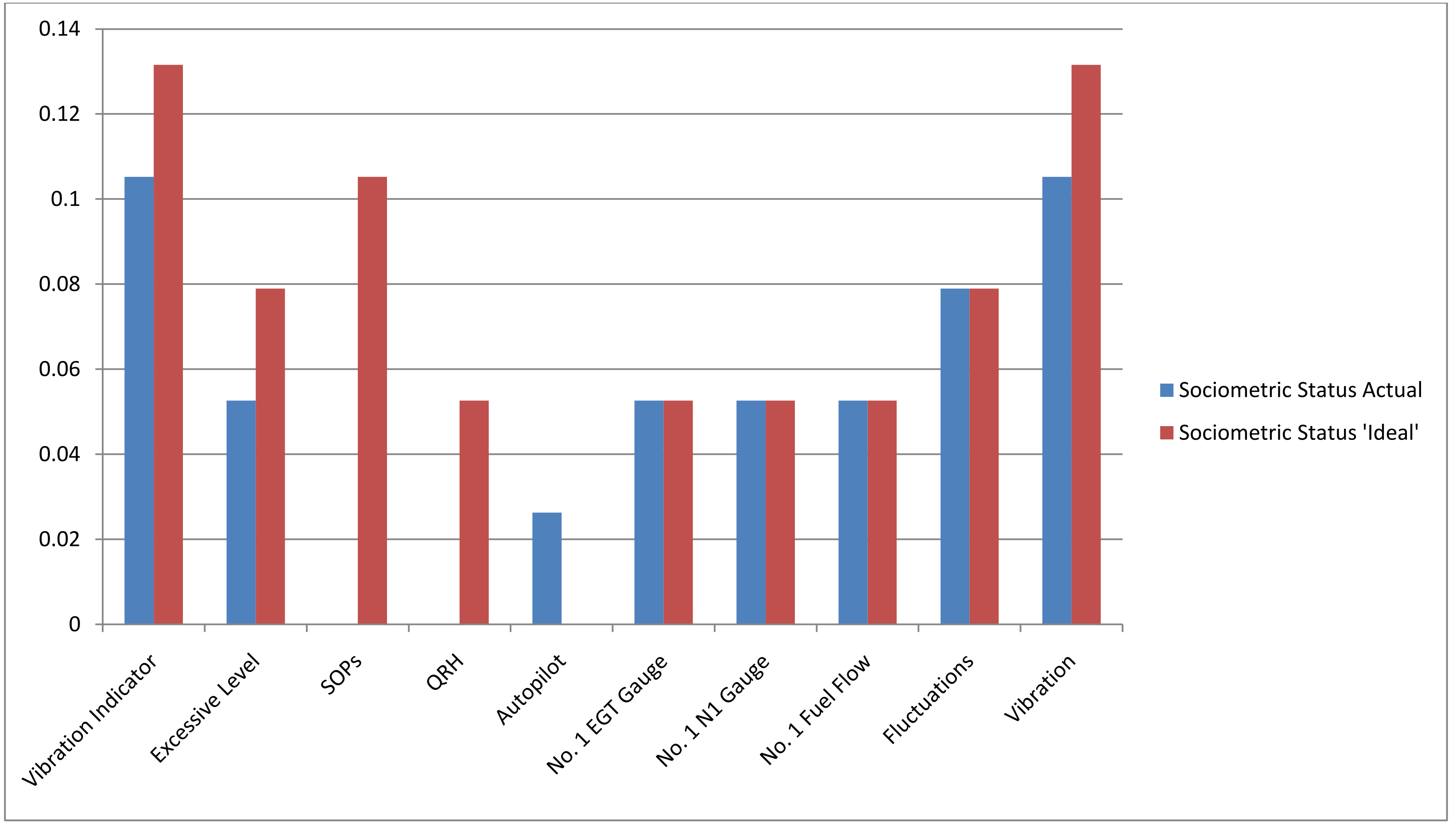


Figure 4-5 –Analysis of Sociometric Status of Key Kegworth Nodes (snapshot 1)

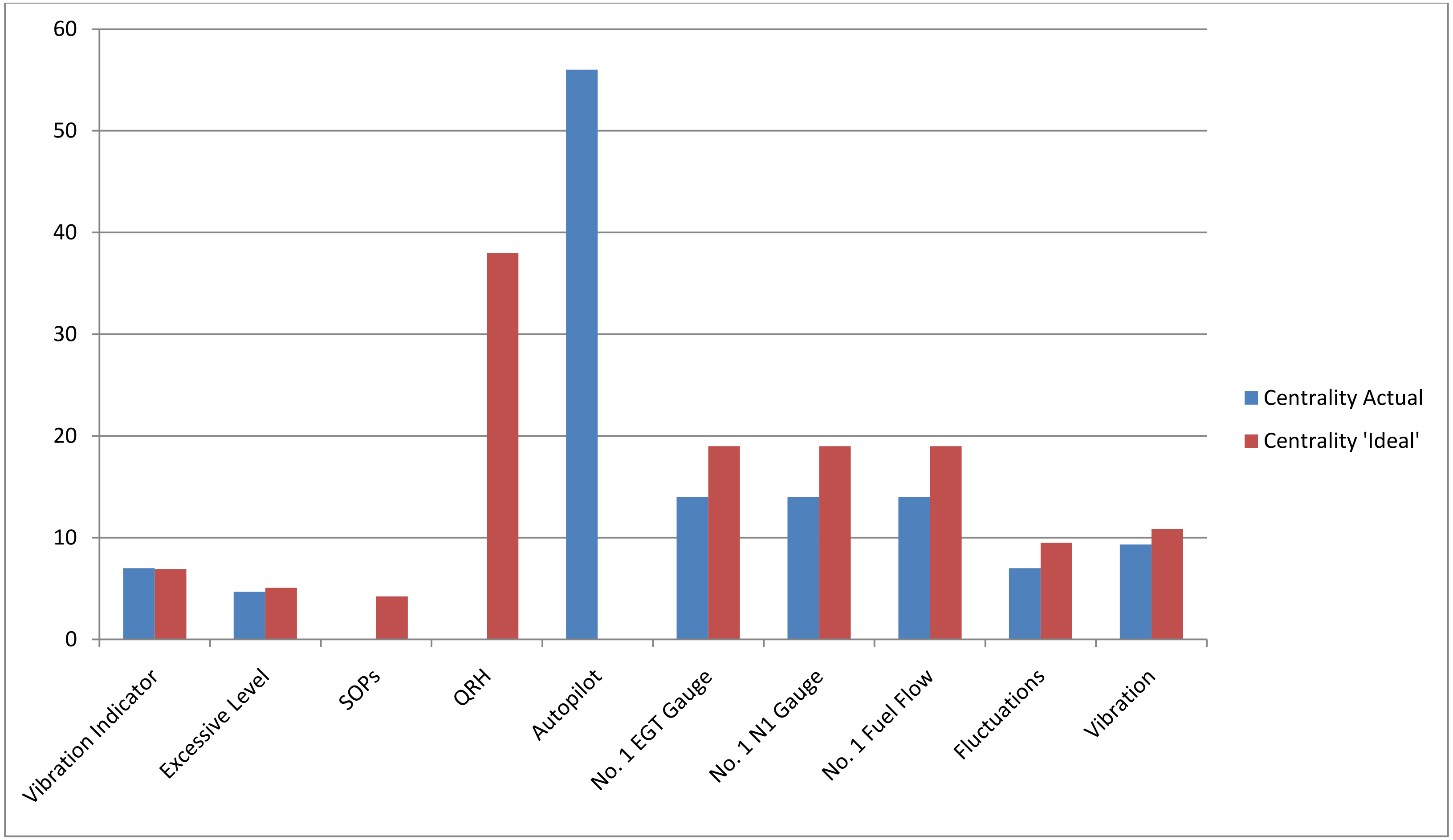


Figure 4-6 – Analysis of Centrality of Kegworth Key Nodes (snapshot 1)

From the graph, it can still be seen, however, that there are clear differences between the ‘ideal’ and actual in cases such as the inappropriate deselection of autopilot or the use of SOPs and the QRH. It is particularly interesting to see that this sociometric status metric does indeed show real differences in the importance of nodes between the two networks. The best example of this is the increase of information flow surrounding the vibration indicator (hence the higher sociometric status by definition), and its associated excessive level, in the ‘ideal’ versus actual case. The additional flow of information surrounding important nodes such as these are the probable basis for an ‘ideal’ opposed to the actual outcome and need further investigation.

In order to take this further and begin to incorporate the ownership of the nodes into the statistical analysis, methods of weighting the nodes and links between nodes were investigated. Following discussion with a graph theory specialist it was found that there is no formal method for attempting to do this in SNA. Instead, it is normal practice to define a relationship on the edges of the graph (the links) and establish whether a weighting system works. The second method of statistical analysis used therefore, was to weight the links in the analysis using the number of owners of the originating node (i.e., if three agents owned the originating node, regardless of the ownership of the receiving node, the link was weighted “3”).

Nodes	Sociometric Status (‘Actual’)	Sociometric Status (‘Ideal’)
Vibration Indicator	0.368421	0.473684
Excessive Level	0.157895	0.289474
SOPs	0	0.342105
QRH	0	0.105263
Autopilot	0.052632	0
No. 1 EGT Gauge	0.157895	0.157895
No. 1 N1 Gauge	0.157895	0.157895
No. 1 Fuel Flow Gauge	0.157895	0.157895
Fluctuations	0.236842	0.236842
Vibration	0.368421	0.5

Table 4-2 - Weighting Method 2 Sociometric Status of Key nodes

Unsurprisingly, the centrality remained unchanged between the un-weighted first method and this. This is due to the nature of the metric in that it does not centralise the information passing through it but its relative position in the graph. Sociometric status results were affected (table 4-1) but the relative comparison of figures was unchanged from the un-weighted graph.

The third method applied to this data was to weight a link dependent upon the number of owners of the originating node added to the number of owners of the recipient node. The comparison between actual and ‘ideal’ centrality figures revealed some differences in sociometric status values for the first time (table 4-2). Nodes such as “Excessive Level”, “SOPs” and the engine gauge instruments’ “Fluctuations” were all of a higher value in the ‘ideal’ as would be expected. This higher value would indicate the central importance of these nodes to an ‘ideal’ event outcome. For the first time however, the sociometric status of the engine instruments (No. 1 EGT, N1 and Fuel Flow Gauges) were not identical in the actual and ‘ideal’ situations. The sociometric status was higher in the ‘ideal’ than the actual scenarios. The ability of the model to pick up differences such as this quantitatively is what this testing sets out to do.

Nodes	Sociometric Status (‘Actual’)	Sociometric Status (‘Ideal’)
Vibration Indicator	0.473684	0.921053
Excessive Level	0.210526	0.5
SOPs	0	0.552632
QRH	0	0.210526
Autopilot	0.078947	0
No. 1 EGT Gauge	0.263158	0.315789
No. 1 N1 Gauge	0.263158	0.315789
No. 1 Fuel Flow Gauge	0.263158	0.315789
Fluctuations	0.315789	0.473684
Vibration	0.789474	1.026316

Table 4-3 - Weighting Method 3 Sociometric Status of Key nodes

With sociometric status weighted in this way then, the values identified for the nodes in the ‘ideal’ versus actual give credence to the observational results made in chapter 3 of the thesis.

There were, however, some anomalies in the centrality results. The node “Vibration Indicator” (a node seen to be highly significant to the events in the accident report and the initial findings of the network reports) had a lower value of centrality (6.91) in the “ideal” than the actual (7.38) using this weighting method (and similar results using the fourth method). Sociometric status has already been determined as a more suitable metric than centrality as its definition suits more closely what is trying to be established within these networks. That is, the information communication power of any particular node rather than its position within the network.

A fourth method was then applied to the case data (table 4-3). The weights for the links in this instance were derived from the number of owners of the originating node multiplied by the number of owners of the recipient node. The intention behind this was that any node with owners at the originator but not at the recipient would become zero due to the multiplication as opposed to addition in method three. This would eliminate values for links that in fact are not active and would highlight the importance of this state.

Nodes	Sociometric Status ('Actual')	Sociometric Status ('Ideal')
Vibration Indicator	1.157895	1.789474
Excessive Level	0.157895	0.789474
SOPs	0	0.684211
QRH	0	0.210526
Autopilot	0.052632	0
No. 1 EGT Gauge	0.315789	0.473684
No. 1 N1 Gauge	0.315789	0.473684
No. 1 Fuel Flow Gauge	0.315789	0.473684
Fluctuations	0.236842	0.710526
Vibration	1.842105	1.842105

Table 4-4- Weighting Method 4 Sociometric Status of Key nodes

Again it can be seen from table 4-3 that those nodes identified in chapter 3 as being of key importance have a higher sociometric status in the 'ideal' scenario. Further than this, the fourth method also identifies, as in the third, that the sociometric status of No. 1 engine's instruments is higher in an 'ideal' scenario (i.e., has a more important part to play in information transfer). One difference has resulted in the fourth method when compared with all others in that the sociometric status of the node "Vibration" is equal in both scenarios. This would appear initially to be a spurious result given the expected higher value in 'ideal'. The exact calculations carried out by Agna would have to be tested to be sure of the reasons behind this result but it may be indicating that the node had the same potential for information flow in both situations and was not a node that needed, or had, changes applied to it for the 'ideal' event.

	Correlation (sig.)	df	Sig. (2-tailed)
Paired Samples Test	.896 (.000)	9	.007

Table 4-5 – Paired t-test results for Sociometric Status (Method 4)

Table 4-5 illustrates one set of results from a statistical analysis of the Kegworth snapshot one actual versus ‘ideal’ sociometric status values. The significance value is below that of the required $p < 0.01$ leading to the acceptance of the hypothesis that there is a significant paired difference in values between the actual and ‘ideal’ scenario analyses. Each of the other methods were also subjected to the same statistical test but the results were less significant than the fourth method.

Through the majority of these methods and in the majority of cases, the results from the observations made of the network have been validated in quantitative terms. There also appears to be a statistically definitive advantage in applying these metrics when weighted. However, this area of graph theory is experimental and requires further work and foundation building. It is clear from the results of this application of the SNA metrics that sociometric status is the more suited to an information network method. However, neither centrality nor sociometric status appear to elicit the information completely from such a network analysis of accident causation that is required. In particular, sociometric status lacks the necessary abilities to identify potential, rather than existing, links. This is an area that requires exploring since this element of identifying all potential information paths is central to a comprehensive model.

The introduction to this chapter highlighted the potential this new method holds when looking to understand more fully SA within a system. The comparisons so far, both qualitatively and more latterly quantitatively, introduce the ability to not only identify when an agent’s SA is intrinsic in the event outcome but also where SOPs, QRHs and regulators etc. are unrealistic in their demands and reasonable expectations of what SA should be within a system. The method further defines where these shortfalls occur in terms of the information flow and links between nodes. What is certain is that the idea of a level of activation above (or below) which a particular node becomes critical is a developing theme in the research of metrics and the rest of this chapter reviews several alternative multi-disciplinary skills and research themes that have some relation to the ongoing work.

4.4 Selection of a suitable metric

Following the study of the statistical methods for the Kegworth disaster outlined above, it is noted that although they validate and give grounding to the network theory for mapping accident causation, there is still a fundamental flaw present in that no activation level or comprehensive statistical relationship can easily be identified between critical and non-critical nodes. It is a central aim of this thesis to develop an integrated qualitative and quantitative model with potential for developing a predictive nature. Sociometric status has shown that metrics can be applied successfully to the information network approach at the core of this work but that maintains use only in post-mortem investigation. In order to move forward towards proactive, or even a predictive methodology, avenues of data integration into the networks must be investigated.

This section describes briefly, a number of considerations made in the project journey to possibly apply to the information network model. These were investigated as to their suitability for purpose. A number of these considerations have had to be discarded due to the nature of the project or the nature of their irrelevance. Some may well be useful in the future beyond this thesis as the model evolves.

4.4.1 **Critical Path Analysis**

Critical path analysis (CPA) was developed in the 1950s as a project management tool to identify and predict those areas within a project which could not be delayed without an overall delay to the eventual goal. This mathematically based algorithm identifies critical activities and it is this idea of criticality that is relevant to the accident causation networks. The way CPA does this is by relating the order or activities, and their dependency to having preceding activities completed (or otherwise), to the overall project network and identifying potential bottle-necks in the process. Due to the sole dependence on time however, a value that has already been identified as one of the main restrictions to linear models, it has become apparent that this method will not develop the model any further.

4.4.2 **Information Theory**

Claude Shannon is attributed with the birth of information theory in the late 1940s. Originally developed in research into telecommunications it essentially incorporates data compression, coding of data and the passage of bits of data through noisy channels without loss.

Within this concept, information theory calculates the information content of data based on logarithms of the inverse probability of those data occurring. An example in language is that the word “the” has very little information contained in it and its probability is very high (Pierce, 1980). This idea may be interesting if applied to the ideas of the accident causation network whereby a node such as “vibration indicator” could have a lot of potential information associated with it as the relative probability of abnormal readings is rare. Information theory allows for analysis of communication channels between, e.g., air traffic controllers and pilots, and communication between towers and pilots can then be analysed based on entropies found to be associated with accidents as a possible prevention (or alerting) method. This concept includes highlighting possible information “bottlenecks” and may be applicable to the model at a later stage of its development if an acceptable association with probability theory is found to be suitable.

4.4.3 **Latent Semantic Analysis**

Latent Semantic Analysis (LSA), or Latent Semantic Indexing, is a technique developed in the 1980s by a team of psycholinguistic researchers and first published by Deerwester *et al.* in 1990.

LSA produces a measure of word-word, word-passage and passage-passage relationships to attempt to objectively predict the consequences of overall word-based similarity between different passages of text. In this way LSA could prove to be a useful methodology to apply to, for example, incident transcripts or reports in order to identify relationships or similarities in an objective way.

“LSA is a fully automatic mathematical/statistical technique for extracting and inferring relations of expected contextual usage of words in passages of discourse.” (Landauer *et al.*, 1998, p.263) LSA represents text in a matrix containing frequency of word use in a passage. A function then weights the frequencies expressing a measure of the word’s importance in that passage and the extent to which any particular word carries information in general. Further factor analysis is then used to identify key words or phrases within passages. For further information and more detailed explanation of the statistics involved the reader is directed to Landauer *et al.* (1998) as an introductory paper.

It is important in such a method to note that the “similarity estimates derived by LSA are not simple contiguity frequencies, co-occurrence counts, or correlations in usage, but depend on a powerful mathematical analysis that is capable of correctly inferring much deeper relations.” (Landauer *et al.*, 1998, p.260)

There are, however, many limitations currently discussed in the literature for LSA in current practice including suspicion of high levels of incompleteness or error (Landauer *et al.*, 1998).

Interestingly, though, it has been proposed that LSA constitutes elements of computational theory capable of further understanding the acquisition and representation of knowledge (Landauer and Dumais, 1997). This includes, they argue, developing further understanding of how individuals acquire more knowledge, or information, than is evident purely on the surface.

As mentioned above, there appears to be some scope to use LSA at initial stages of investigation instead of HTA particularly when dealing with transcripts and reports. However, current limitations and uncertainties within the method at this early stage ultimately preclude it from this project.

4.4.4 **Bayesian Theory**

> "Graphical models are a marriage between probability theory and graph theory. They provide a natural tool for dealing with two problems that occur throughout applied mathematics and engineering -- uncertainty and complexity. Probability theory provides the glue whereby the parts are combined, ensuring that the system as a whole is consistent, and providing ways to interface models to data. The graph theoretic side of graphical models provides both an intuitively appealing interface by which

> humans can model highly-interacting sets of variables as well as a data structure that lends itself naturally to the design of efficient general-purpose algorithms." (Jordan, 1998, p.1)

Bayesian networks are one such graphical model. Jordan (1998, p.1) goes on to say of such models that "many of the classical multivariate probabilistic systems studied in fields such as statistics, systems engineering, information theory, pattern recognition and statistical mechanics are special cases of the general graphical model formalism. Examples include mixture models, factor analysis, hidden Markov models, Kalman filters and Ising models. The graphical model framework provides a way to view all of these systems as instances of a common underlying formalism. This view has many advantages; in particular, specialised techniques that have been developed in one field can be transferred between research communities and exploited more widely." This last point is essential in this author's view where developing a method with real usability, multi-disciplinary application and real-world foundations is key to the thesis. "Moreover, the graphical model formalism provides a natural framework for the design of new systems." (Jordan, 1998, p.2)

Bayesian networks are complex diagrams that organise the body of knowledge within a system by mapping out cause-and-effect relationships. The key variables are coded with numbers that represent the extent to which one is likely to affect another. Bayesian networks hail from the work of Rev. Thomas Bayes and in particular his posthumously published essay of 1763. In the essay, Bayes produced a mathematical formula to calculate probabilities for causally related variables for which relationships can't easily be derived through experimentation due to their inherent complexity.

Social scientists worked on this idea much later and began using the theory to clarify which are key factors within a particular event and it is this potential usefulness of the theory that leads to the suitability of study within this project. During the 1970s and 1980s, neural nets were popularised as computers were able to deal with large amounts of data and identify patterns. There were limitations however where the neural nets couldn't predict as they couldn't be 'trained' as such and would therefore require an infinite source of data exclusively covering all possible outcomes; not realistic in aviation or other complex systems.

During the late 1980s, however, researchers in the field of Artificial Intelligence discovered that Bayesian networks offered an efficient way to deal with the lack, or ambiguity, of information that had hampered previous attempts. Eric Horvitz (a pioneer in the field working at Microsoft during the 1990s and producing papers over many years, e.g., Horvitz *et al.*, 2001) asserts that the approach "...was efficient because you could combine historical data, which had been meticulously gathered, with the less precise but more intuitive knowledge of experts on how things work to get the optimal answer given the information available at a given time." (Helm, 1996; from an interview with Horvitz) This intertwining of both historical data and specialist knowledge (utilising subject matter experts (SMEs) for instance) lends itself to the application of our information network models.

4.5 Conclusions

Chapter 4 has shown the direction of development that the research has taken since the successful application of information networks to aviation accidents. The introduction of an 'ideal' set of networks as a tool of comparison allowed for significant nodes to be more easily identified. Further than this it opened up the opportunity of a quantitatively comparable network to an actual system and thus smoothly transitioned into the second half of the chapter. Returning to Salmon *et al*. (2008a) introducing a quantitative element to the networks has really started to identify levels of situation awareness and introduced the concept of activation levels of particular nodes (i.e., information actively owned) within a system.

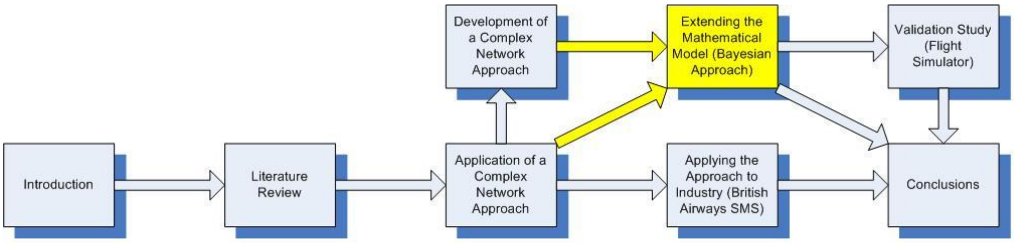
Social Network Analysis was adopted as a suitable starting metric to attempt to identify these key nodes and significant trends, or differences, between actual and ideal system networks. Together with weighting of nodes based on agent's ownership, sociometric status was found to be a way of identifying statistically significant differences between actual and 'ideal' scenarios. This method could be applied in situations where systems are compared in a current snapshot state to the 'ideal' for that system. From this, nodes that are statistically significantly different in terms of their information communication power can be highlighted and investigation of those nodes implemented. It is likely, given the central importance of communication, as discussed in the introduction in relation to Gibson *et al.* (2006), in understanding these events, that those nodes performing most differently from an 'ideal' scenario would stand the greatest chance of influencing a negative event (or at least an event not modelled by the 'ideal' scenario).

Technique	**Advantages**	**Disadvantages**
Critical Path Analysis	Used and tested in critical activities	Linear foundations
Information Theory	Centralises information transfer	Limited to analysis of qualitative networks
Latent Semantic Analysis	Addresses relationship of information	Currently limited to passages of prose
Bayesian Theory	Integrates SME knowledge and transferable between domains	Complex in large systems

Table 4-6 – Summary table of theories with potential for integrating into information network models

Several methods of looking to further analyse the information networks are discussed and despite promising aspects to more than one, the chapter unearthed a potentially very useful statistical methodology in Bayesian networks. Table 4-6 illustrates the major advantages and disadvantages discussed for each method. Despite the complexity that may occur in Bayesian networks, and this is something that needs addressing, the limitations of the other methods mean they are not suitable at this time for integration into the model. It is for the very reason that Bayesian methods appear to work well with information networks that the following three chapters of this thesis look at extending the application beyond accident investigation towards a proactive and even predictive methodology. Chapters 5 and 6 look at developing the information networks further by combining the theories of Bayesian statistics and testing against a situation-based study. Chapter 7 then looks at the real-world industrial application of the information network methodology with a legacy airline.

5 Extending the potential of information networks; a Bayesian Approach[7]



5.1 General Aviation; the 'unprofessional' genre?

In Chapter 4 we saw how the information networks can be analysed using social network-style metrics, and also looked into developing the method with a variety of subject-areas that may be applied. The aim of this chapter is to investigate the possibility of developing the quantitative power of the information networks on the basis of the findings from chapter 4. Bayesian networks have been identified as a potential method that could be integrated with information network theory in order to objectify the model further. This chapter looks at combining the two methodologies and making use of an oft-underused source of data.

It is undoubtedly a good thing that aviation accidents are incredibly rare. However, due to the lack of more Kegworth's, QF1's and other catastrophic events it makes it very hard to begin to develop a methodology based on probabilities and number of events. It is for this reason, and in the interests of

[7] This chapter is the basis for the following published paper: Griffin, T. G. C., Young, M. S., Stanton, N. A. (2009). Barriers and accidents: The flight of information. In D. De Waard, J. Godthelp, F. L. Kooi, and K. A. Brookhuis (Eds.). Human Factors, Security and Safety . Maastricht, the Netherlands: Shaker Publishing. (Attached in Annexe 1)

studying aviation comprehensively rather than solely commercial large-scale incidents that this chapter begins to turn to the world of General Aviation (GA). Although it would be untrue to suggest that there are a plethora of regular aviation accidents in GA, there are undoubtedly more than in commercial aviation and as such that makes this a useful, and comparable, area of study.

This chapter sets out to ensure that GA is a suitable area of study for information networks, and Bayesian application, before then discussing a move from taxonomic classification systems and increasing the amount of quantitative analysis. It is the author's opinion that these two aspects combined provide for real strength in the analysis of aviation accidents. Finally in the introductory section, Bayesian mathematics and their application to information networks and barriers is then discussed in relation to current, albeit limited, literature. This is not a negative thing though since that makes this a new, upcoming and exciting area of research.

5.1.1 Are GA accidents fundamentally different to Commercial Aviation accidents?

General aviation is defined, in the UK, as any aircraft in use excluding military or commercial air transport. There is no limitation on size or design within the legislation and yet GA is more commonly understood as light aircraft flying for non-commercial transport (including flight instruction). This still includes a wide range of operations, flying aims, roles, procedures, training levels and aircraft types.

In the twenty-eight year period of full record keeping, up to 2008, 359 fatal accidents occurred to UK GA aircraft (GASCo, 2010). This is not starkly in contrast, as would be expected were GA so very different in safety and professionalism, to commercial aviation fatal accidents (28 in 2009 and 34 in 2008 being typical figures (Learmount, 2010)). However, the majority of commercial aviation accidents (as opposed to incidents), by their very nature, result in fatalities whereas the majority of GA accidents do not (National Transportation Safety Board; NTSB, 2006). For this reason, GA provides many times more non-fatal accident reports which give a suitable number of events with which to work. Like with all figures it is often hard to get a clear picture of the 'market share' in aviation accidents (including non-fatal) but the Australian Transportation Safety Board (ATSB; 2007) studied American and Australian data from the nine years up to 2002 and reported that between 70% and 85% are from GA flying despite the number of flying hours being just under half of all hours.

Studies have shown that pilot error is identified as a key contributing factor in many more GA over commercial accidents (a difference of almost 50% of reports) and that this is likely to reflect differences in training and experience between crews (Li *et al.*, 2001). GA flying is identifiably different to commercial in a number of ways including the fact that the aircraft are hit harder by weather variances, there are different and less checked training (both initial and ongoing), less automation and systems management (although this is changing in light of new 'glass-cockpit' technology) and variable levels of maintenance. Lenne and Ashby (2006) carried out a study on GA aircraft in Australia and concluded that almost three-quarters of the crashes studied involved aircraft-handling or pilot-control errors. This is further supported by US data that identified 71% of accidents having those issues as central causes (NTSB, 2006). It is not enough, however, to merely report such issues and expect an improvement in safety. This are the tips of the iceberg in terms of accident causes and further work must be done to understand the whole system of GA flying and where interactions occur between causes and other factors. Lenne and Ashby (2006) report that there are many associated or explanatory factors reported alongside those accidents which had pilot control errors at the centre. Li and Harris (2006) take this further and highlight the importance of further data and investigation to really understand the importance of these explanatory or contributory factors; a true systems approach to GA accidents.

It is often argued that due to the implicit differences, some of which have been discussed, in GA as opposed to commercial aviation flying that they are not comparable. Although it is certainly true that the types of accidents tend to show different causal structures, it is not the aim of this thesis to suggest that the two types of accidents are comprehensively similar. Moreover, it is in removing this need to compare and contrast event 'types' within the different areas of aviation that information networks are investigated and applied to GA in the hope that they elicit suitable analyses of the system regardless of flight type. This also applies to the argument over fatal and non-fatal accidents being born from different event foundations.

5.1.2 A new approach that aims to remove the limitations of classification methodologies

Not only will this study look to use GA accidents to further the understanding of the system of flying and flying accidents in general, but non-fatal accidents will be used in addition to those that resulted in fatalities. The reason for this is simple; increased data with the hope that this leads to increased understanding of the GA system surrounding aviation accidents. This is in line with the ethos of applying information networks since the more comprehensive any network can be made, the more understanding can be comprehensively gained. The literature is far from conclusive as to whether non-fatal and fatal accidents are intrinsically different. It is clear that for many events, the factors and characteristics are very similar (Lenne and Ashby, 2006) and as such provide a great resource of data to be mined. However, it has also been shown that in some areas the factors and characteristics of non-fatal crashes can be at odds with those of fatal accidents (Haworth, 2003). In their discussion, Lenne and Ashby (2006) actually request future emphasis on using data to discern if non-fatal and fatal landing accidents are similar in the nature of development or whether differences are more than superficial. In the same way that the information networks should preclude the need to label an accident as GA or commercial it is hoped this novel network approach can remove the bias of fatality on any study. Through attempting to illustrate and understand the information-space within which any accident occurs (fatal/non-fatal, GA/commercial) the limitations imposed by classification of accidents can potentially be removed. The information space within the networks are created based on information present within the system and not restricted or enhanced by the particular outcome or classification of an end-result. This is an advantage over methods which limit themselves through inflexible grouping and fitting. There are often inconsistencies in the classification or labelling of accident types and consequences let alone the factors and causes behind them (Jarvis and Harris, 2009). Indeed, classification methods such as the Human Factors Analysis and Classification System (HFACS) have revealed limits in application to GA studies both in powered and non-powered flight (Lenne *et al.*, 2008; Jarvis and Harris, 2009) due to the lack of solid organisational structures further up the causal ladder. Wiegmann and Shappell (2003) take this a step further and suggest the unsuitability of methods that looks at higher level factors in GA accidents, doubting that they would be evident or comprehensive.

The information network methodology does not presume to replace a classification procedure but add an alternative and additional direction from which to attack the system and elicit areas, or issues, of concern and causality (or prevention in ideal terms) of accidents. The information networks focus not on the classification of definition of an event's outcome but on the system in which that event took place. The emphasis is shifted from an event (which has been shown to be difficult to classify and often full of slight variations that recurrence is limited) to the barriers and links between information nodes surrounding any event, or non-event.

In other words, communication is still purported to be central to any event and the information networks represent this flow of information (communication) well. It is true that in GA the types of information and communication will be different to commercial aviation. However, it is still effectively communication whether between the pilot and, the now more basic, instrumentation, pilot and visual cues (so often not necessary for commercial flying), pilot and the controls (which are mostly direct feedback controls with factors such as stickforce important) or between instrumentation and the environment. All information within the system may be consciously acknowledged and interpreted correctly (successful link), missed completely (failed link) or misinterpreted as seen in the case of Kegworth (chapter 3). Information networks do not differentiate the way in which information is processed but instead allow for the study of information in its more raw state regardless of environment or technical surroundings. In this way it is irrelevant whether the system being studied is GA or commercial so long as the respective information can be modelled comprehensively.

This step away from outcome-classification and event-by-event investigation removes the limits of reproducibility and the need to encompass varied small changes to look at the barriers within which remain constant despite the ultimate outcome. It is hoped the information network, with Bayesian mathematics, approach is more suitable to the analysis of GA accidents and works equally as well as with commercial accidents studied thus far.

5.1.3 **Quantitative and Qualitative methods; a balancing act**

Any comprehensive ergonomics method needs to balance the qualitative and quantitative aspects in order to be as complete as possible. As in the plan for this thesis as a whole, any method should also maintain an effective interaction between industrial practice and academia. Hignett and Wilson (2004) very neatly summarise this fusion of styles in order to produce the most effective and reflective view of a system (Figure 5.1).

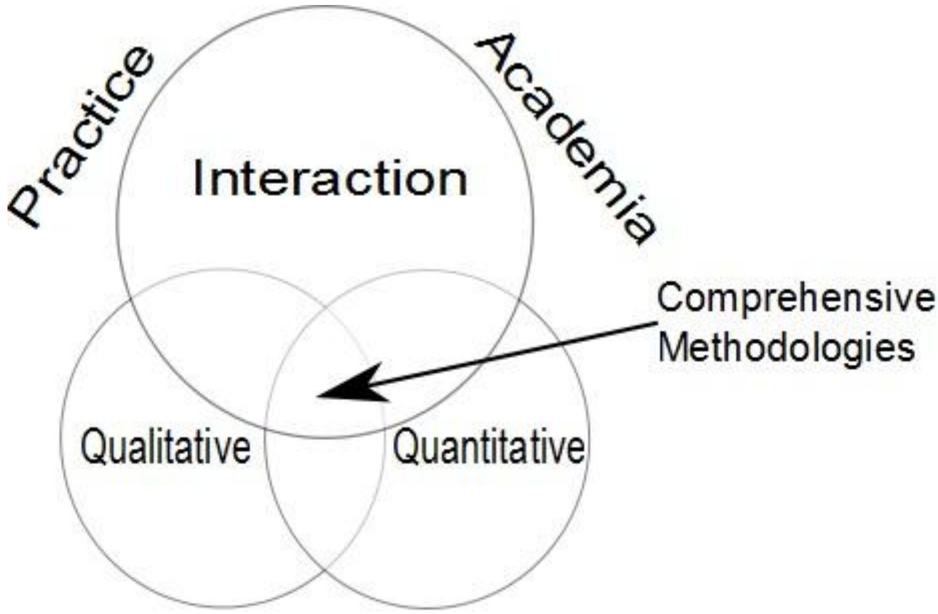


Figure 5-1 - The interaction of facets required for a comprehensive method (Adapted from Hignett and Wilson, 2004)

HFACS, for example, uses a qualitative approach for analysis but then quantitative methods are often applied to the data that are produced. A more complex methodology must delve further into really integrating the qualitative and quantitative aspects though. This chapter looks at a method of fulfilling the ideal set out in figure 5-1 where all aspects are integrated to form a more comprehensive and representative model. The method proposed, in using information networks, addresses the qualitative aspects of the accident reports without artificially simplifying or classifying and then looks to incorporate quantitative aspects by way of historic data and mathematical manipulation introduced in chapter 4. In this way the method attempts to strike a balance using both qualitative and quantitative data so as not to artificially adopt one method at the expense of the other. This is favourable since each represents different facets of the real-world system and therefore both need to be present in a usable and realistic model. Risk models incorporating both qualitative and quantitative qualities allow understanding of system design (through predominantly qualitative means) but also a visualisation of actual practice within the system (quantitative historical data for example) (Marx and Westphal, 2008).

There is no doubt that this area of ergonomics is developing and probabilistic risk assessment (PRA) is an area of study being swiftly advanced. However, much of the use of PRA has been with mechanical or engineered nodes and barriers since these mechanical systems have easily identifiable probabilities of failure etc. Over the past ten years there has been much research into the use of PRA with Human Factors (e.g., Marx and Westphal, 2008; Baybutt, 2002). This has centred on treating the human probabilities very differently to the non-human which is contrary to the approach that information networks may be able to provide. Information networks using historical data to compute probabilities of node occurrence and link success/failure remove the highly subjective probabilities currently associated with these other methods; resulting in a more objective, less ambiguous unified approach. Indeed, Ale *et al.* (2005) suggest the power of these types of models "can be greatly enhanced if probabilities and logical dependencies can be quantified" using a variety of methods (p.37). Additionally, in using historical data, the reliance on SMEs to calculate probabilities for hundreds and thousands of nodes is removed. This also removes a large amount of the subjectivism that is criticised in current methods (Trucco *et al*., 2007). The major difference in proposition of this study is that the aim would be to extend the method to the complex non-linear networks that are the ultimate aim of the approach. This would be a large step forward when compared to the current fault tree style linear approaches. How exactly these facets can be incorporated in the information networks is addressed next.

5.1.4 **Why Bayesian?**

Fault-trees are the bread and butter of current PRA techniques within industry and academia. This study proposes extending the application to non-linear information networks and this requires an advanced mathematical model. Chapter 4 introduced Bayesian modelling and highlighted significant potential that could be utilised with the information networks.

The information networks used in the thesis thus far are reminiscent of several graphical models used throughout maths, science and engineering. Since a quantitative measurement is sought and there is a large pool of historical data then probabilistic graphical models could offer the necessary facets required to improve the information networks still further. There are two significant groups of probabilistic graphical models; directed and undirected. Undirected models, also referred to as Markov networks or chains, are used to represent conditionally independent items, or nodes. Since this is an oversimplification and not reflective of the true nature of aviation accidents the alternative, directed graphical models, are of more interest.

Within this group of graphical models, a Bayesian Belief Network is referred to as a directed acyclic graph. The name, and underlying theory, of these networks stems from Thomas Bayes' theorem (Bayes, 1763). Bayes theorem takes into account the effect of the hypothesis occurring on the probability of the evidence actually being observed. In other words, it is not only the relationship between events that is taken into account but also the marginal probability of each event ever having occurred. This allows for more complex relationships to be illustrated and investigated. Due to the complexity of the relationships being reflected by Bayes, each network is built from a series of conditional probability tables (CPTs). Each node, in this case representing each node within an information network, within a Bayesian network has its own CPT and together with the arcs between nodes the graphical model represents causal influence.

Figure 5-2 illustrates a simple Bayesian network complete with CPTs for each of the binary (i.e. either true or false) nodes. Each node is connected by a link of singular direction indicating causality. As the variables are discrete, the CPT lists probabilities that the node is either true or false given each of the parent's nodes values.

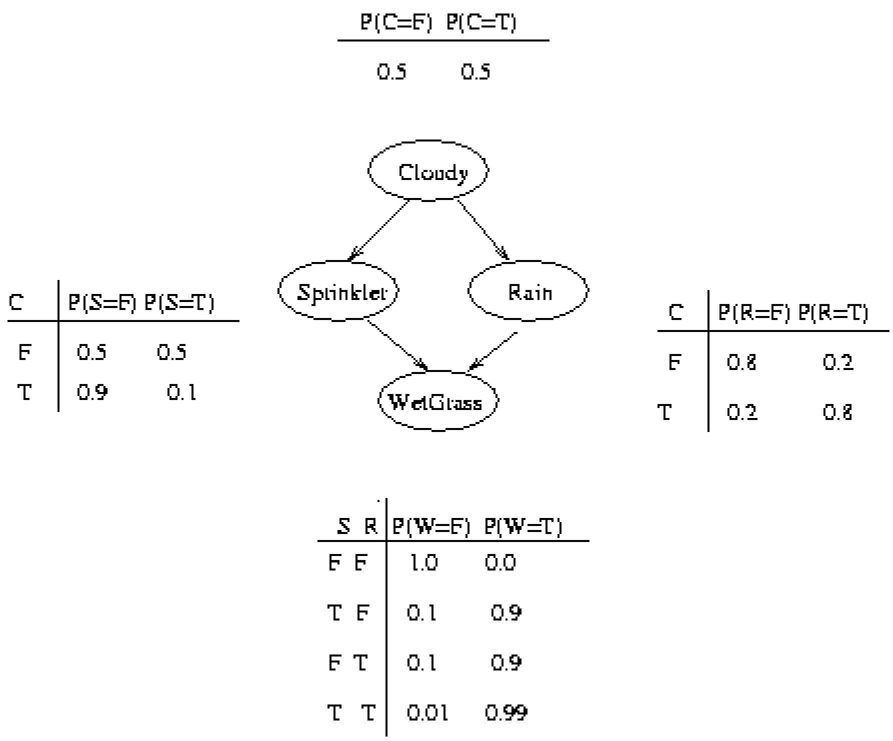


Figure 5-2 – Simple Bayesian Network (from Murphy, 1998)

In the bottom CPT it can be seen that the probability that the grass is wet (P(W=T)) is 0 if both the sprinkler and rain nodes are false (i.e., S and R = F). This makes sense since given this simplified network the grass can only be wet from either rain or a sprinkler. In this way all possible outcomes can be predicted given the evidence observed of parent nodes. This also illustrates the advantage gained from using a network even if it can be argued that it isn't comprehensive; lessons can still be learned and networks investigated.

CPTs are typically developed with a mix of historical data and subjective specialist knowledge. This allows know, or expected, relationships and effects to be modelled. This is particularly useful in areas such as aviation accident investigation where events are rare and historical data may not be a good predictor of future events, causes and outcomes. However, there is a certain amount of criticism that can be levelled at such an approach where the very foundation of a graphical model is based upon the subjective "belief" of an expert. Luxhøj and Coit (2006) level this criticism at Bayesian networks and suggest that in order "to achieve objective results, that expert judgement must be quantified through a structured and traceable process." They go on to suggest a system that relies partly on historical data, as does the approach adopted in this chapter, and partly on trying to objectify the process of the experts through frameworks such as HFACS. Where this work attempts to divert from previous applications is by not adhering to the rigidity and restrictiveness built in using taxonomic classification systems. Additionally, it is the aim of this study to remove the focus from causal factors (the basis of Luxhøj and Coit's approach) of a particular event (i.e. an accident) and instead look at a system regardless of outcome and removing the focus from catastrophic events alone (Ale *et al.*, 2005). It is interesting to note that although a Bayesian network is very capable of illustrating causal relationships there is no necessity for a directed edge (link between nodes) to signify a causal dependency. This opens up the use of the information networks where the links are propositional or identifying the flow of information rather than imposing a causal structure. In this way the approach tested here uses actual information nodes thereby delving deeper into any situation and system without attempting to artificially classify interactions.

Significantly, Bayesian networks are able to model feedback loops, exclusivity and probabilistic rather than simple strict causal relationships (Ale *et al.*, 2007) with unlimited variables given enough processing power. This type of manipulation would be required in order to apply quantitative theories to a complex 3D network with potentially thousands of nodes and links. Of real interest to this work is also the development of methods, as discussed, to remove the subjectivity of SMEs in applying probabilities to the networks. This continuing work in the field of Bayesian mathematics and modelling reveals the potential usefulness of the method and is central to this chapter. The next subsection revisits the idea of barriers within a network, a central theme of the thesis, and how this may provide a new way of looking at safety improvements combined with the methodology outlined here.

5.1.5 **Barriers and Error Migration**

Barriers are ubiquitously linked with safety in the literature and yet their use within aviation, outside physical barriers (e.g., engineering related or physical safety barriers), appears to be limited. Within network models of a system, it would be possible to change probabilities of occurrence of events, or probabilities of conscious ownership of information, by inserting (or removing) barriers into the links between nodes. It is these arrows, or links, that result in the flow of information within a system and any action to affect them should manifest itself as changes in outcome or changes in the probability of an outcome. Barriers, in this sense, can be seen as safety measures, i.e., the quality of a barrier defines the increased metaphorical ‘distance’ it creates from a negative outcome in this instance. Luxhøj (2002), a leader in the application of Bayesian networks, introduces new nodes into what he terms an ‘influence diagram’ (similar in form to a fault-tree) to represent potential barriers in a system. These nodes can take on structural type barriers or human acts such as inspection and management roles. Probabilities can then be applied in the same way as any other node to affect the overall probabilities of the system. Where this study looks to differ is by reflecting the effect barriers have on the links between information elements; being more reflective of the real-world system and not inserting superfluous nodes if they are not necessary. This is important since a particular barrier may in fact effect several links in different areas of a system in different ways and this would be hard to contain within a single additional node. The study discussed here is looking to investigate how barriers may be incorporated into an information network and whether the method is suitable for predicting the potential effects of the introduction of new, or adaptation of existing barriers. If a barrier effects the link between nodes then it would infer the probability of that node now occurring is affected.

However, if probabilities must add up to one (i.e., the event will occur on 100% of occasions) and the barriers are affecting the probability of any node occurring within a network, then the value of the probability difference cannot simply be lost, so we must therefore look at alternatives to this. An adiabatic process, in relation to thermodynamics, is one where there is no heat lost or gained from/to the system (e.g., a gas or fluid) despite changes occurring within. In a similar vein, the probabilities within our aviation network system also cannot be simply lost or gained to exceed a probability value of one leaving an adiabatic style information system. If these probability values cannot simply disappear then the only option is migration of probability around the network and, given that any network model developed is aimed to be as comprehensive as possible, this may give some scope as to predicting the migration of the values around the system. Ideally, of course, the simulations should allow us to identify what barrier implementation or changes would allow for maximizing the positive, or safe, outcomes within a system. This, the nature of barriers that are effective and methods of testing the prediction of such networks against simulation of a system are tested as novel methods.

5.2 Investigating GA Accidents

This design and method section identifies the source of historical data for use in this chapter and chapter 6. Additionally it outlines the method of database creation from a number of GA accidents by the author. The rest of the chapter is discussed following section 5.2.1 below.

5.2.1 **Data Repositories**

The Air Accidents Investigation Branch (AAIB) is an executive arm of the UK Department for Transport. It is the duty of the AAIB to investigate civil aircraft incidents and accidents both within and outside the UK where there are British interests. The Chief Inspector, David King, states that the aim of the AAIB is “to improve safety by determining the causes of air accidents and serious incidents and making safety recommendations intended to prevent recurrence...it is not to apportion blame or liability.” (AAIB Website, 2010)

The AAIB are responsible for investigating the majority of ‘reportable’ incidents to GA aircraft, i.e., those that do significant damage or injure people. The majority of these incidents are reported and dealt with by correspondence leading to the issuing of a report in a monthly bulletin. The more serious accidents, including those that are fatal, have dedicated investigation teams similar in composition to a commercial accident investigation.

It can often be considered difficult ground to investigate an accident, in particular at the ‘active’ end, and report without any perceived blame or liability. However, the information network approach demonstrated in chapter 3 re-evaluates the digression away from realising the potential of fully investigating the active factors. The approach suggests a way of investigating active failures, which has been shown to be applicable and useful in chapter 2, by dissecting the situation without the need for blame being intrinsically linked to failure since the central theme is failure of effective communication at some point in the system network.

In chapter 2 it was suggested that linear models lead towards a search focussing on latent factors at the expense of the often more controversial active factors. Linear chains draw the investigator’s attention away from the sharp end in an effort to understand the build up to an accident. It is suggested in this thesis that a dynamic network allows more comprehensive understanding of the entire system without necessarily separating nodes into latent and active (proximal and not). In this way we are not losing the link between “latent factors” a long way back in a chain. In having to draw the linkages between nodes in a network and having that visual and “solid” link present, it is easier to visualise the links between the active and latent nodes. This reintroduces the dynamic and complex concept of the active space - suggesting that latent and active factors are inextricably linked. Latent and active factors are one and the same in the dynamic world and should be addressed together as a single issue not separated into latent and active causes. It can be considered that the information network approach attempts to identify active failures yet leads to an understanding of latent reasons through study of the links.

In an attempt to apply this information network approach to GA accidents the rest of this chapter looks at developing a database and from that populating networks with historical data. In this way the focus, on the surface at least, is active factors and yet it is hoped the links that are defined between the nodes highlight the latent and underlying reasons behind any incident as has been introduced in chapter 3.

In order to create a Bayesian network to manipulate and learn lessons from the following steps will be taken:

1. 200 accident reports published by the AAIB will be studied and a series of factors (or information elements/noun-like words) will be recorded. (Section 5.2.2)

2. An information network will be built joining these factors whenever a propositional or information-flow link exists. (Section 5.3.1)

3. A section of this network will be modified and made suitable for conversion into a Bayes Network formula using computing language. (Section 5.3.1)

4. Probabilities will be applied to the nodes (or links) of the network as per the historical data collected in section 5.2. (Section 5.3.2)

5. MATLab will be used to code the Bayesian network that has been developed using a toolkit approach with all the algorithms necessary for successful calculations built in. (Section 5.3.3)

Section 5.4 then looks at the preliminary results and discusses the usefulness of this approach. Chapter 6 is where the method comes to life and a novel approach of validating a Bayesian network prediction using simulation studies is carried out.

5.2.2 **Creating a Database**

As described in section 5.2, GA events are released to the public in monthly bulletins and so in order to create a database of incidents these records were analysed for a period from January 2005 until January 2007. For the purposes of clarity, the accident scenarios used involved single-engine piston fixed wing light (5,700 kg maximum gross weight or less) GA aircraft, e.g., the Cessna 152 or Piper Warrior.

Due to the nature of current reporting methods, as described in section 5.2, and the limits of information released to the public it is not possible to create comprehensive information networks for individual, or grouped, events. However, the investigation of a new method should not be limited by current restrictions or shortcomings and instead should look to developing reporting based on the method and not vice-versa. As such, each of the AAIB formal report transcripts were studied and, using no additional external information so as to limit bias, a database of factors reported in the accident was developed. The constituent incidents were classified by the AAIB primarily in terms of ‘causative’ and ‘outcome’ events. Further data including date of flight, aircraft type, licence held, hours flown in recent time and total, nature of flight and stage of flight were recorded. Table 5-1 a sample of factors recorded for the accidents as playing a key role. The method of deducing the factors to be used can be likened to the method of retrieving noun-like words to create information elements in chapter 3.

Sample of Factors From the Accident Database		
Vibration	Bounce	Wind/Turbulence/Downdraft

Low Sun	Icing	Command G/A (Not command G/A)
EFATO	Inadvertent Stall	Complex Op Procs (e.g. noise abatement)

Table 5-1 – Example of GA Accident Factors

A sample of database entries is included in annexe 2 of this thesis. Of the 200 analysed incidents, 100 were during the landing phase of flight and so this area was focused on during the subsequent sections of this chapter. This choice, and the underlying data, also reflects the more general picture where the landing phase of flight has been found to have the highest proportion of GA crashes (Lenne *et al.*, 2008; Lenne and Ashby, 2006).

5.3 Developing a Bayesian-Information Network approach

5.3.1 Manipulating the Network

All of the landing incidents' causative and outcome factors were listed and an information-network style diagram built linking nodes where possible. Figure 5-3 shows a stage in this process of building a network from the nodes.

Originally, similar to those in chapter 3, information networks were modelled using knowledge objects taken from a Hierarchical Task Analysis for the nodes with propositions such as 'has' or 'causes' forming the links. However, for this study, the taxonomic labels, e.g., "too high/fast on approach", are entered as nodes into the information network and the links between nodes are drawn up to represent viable relationships, thus representing possible incident pathways. Due to the nature of these nodes, it is possible to consider some as 'influencing factors' (yellow nodes in figure 5-4), others further along the information network as 'intermediate outcomes' or 'further influencing factors' (grey nodes in figure 5-4) and finally as 'outcomes' (white nodes in figure 5-4). More importantly, though, each node represents information objects that are present within the system at that time. Further to this, an event cannot occur without the information being present in the system to indicate that event (even if that information goes unnoticed). The links, or arrows, between nodes represent the flow through this information network resulting in a specific outcome.

In order to begin formulating a workable network, i.e., one that could then be manipulated using Bayesian mathematics, all nodes with an occurrence value of one were either grouped together or moved into the node “other rare event”. This allowed for a more manageable network that still retains the potential to extend the networks to include hundreds or even thousands of accident pathways and additional nodes, limited only by computing power as will be seen later in the chapter. This resulted in the generic landing case illustrated in figure 5-3.

For development of the Bayesian element of the information network style scenario it was necessary to isolate a smaller portion. This would make the nodes more manageable to be manipulated with the conditional probabilities and a Bayes network produced. Therefore, to further limit the calculations required at this stage, a typical ‘influencing factor’, “too high/fast on approach”, was selected. Only the associated nodes were kept, and all others removed from the network. The ‘influencing factor’ “too high/fast on approach” occurs seventeen times out of the one hundred accidents. The nodes associated with this network pathway are: “approach to landing”, “too high/fast on approach”, “heavy landing”, “heavy landing & overrun”, “overrun” and “nosewheel collapse”. There are also the associated nodes of “go-around” (an approach that fails and results in another attempt), “decision to land” and “other rare event” included for completeness.

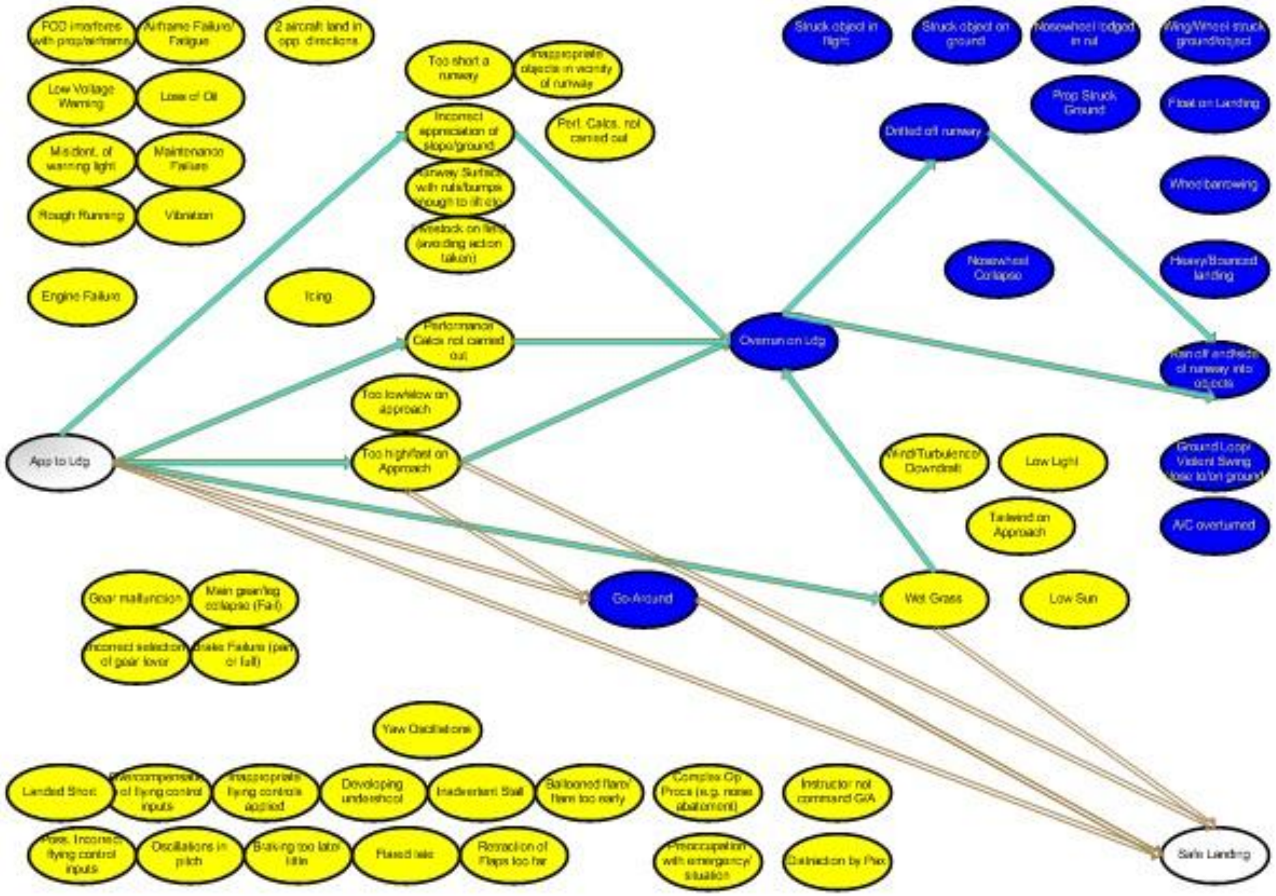


Figure 5-3 - Generic Landing Case for GA aircraft (sample step of linking)

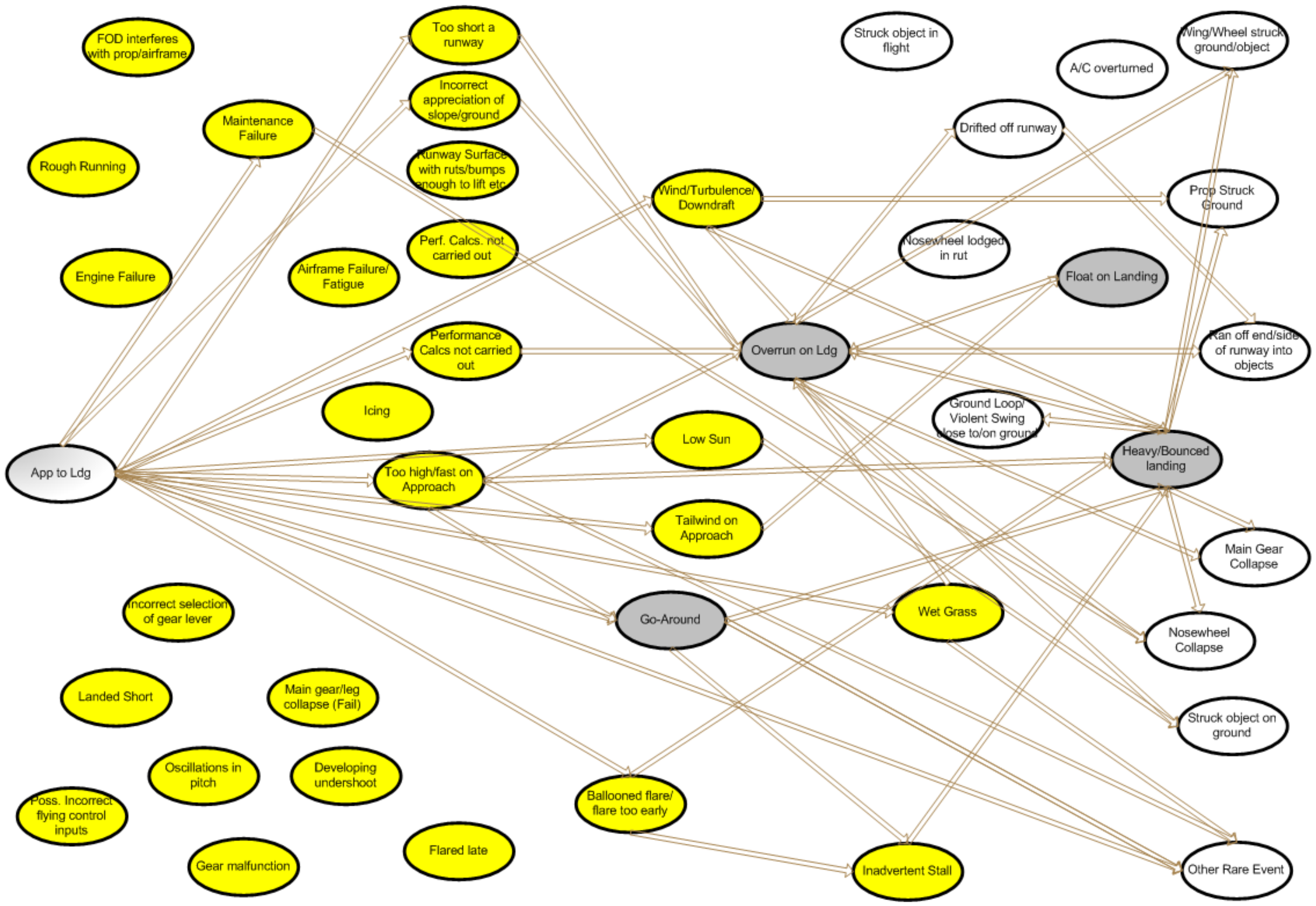


Figure 5-4 - Generic Landing Case for GA aircraft with singular nodes removed

5.3.2 **Probabilities and Possibilities**

The frequency of occurrence of each node was recorded and from this, conditional probabilities given the occurrence of the preceding node(s) were calculated using adjacency matrices. Figure 5-5 shows the simplified information network for a "too high/fast on approach" landing scenario. The probability of each node occurring in the one hundred accidents, non-conditionally, is given on each link. The additional node of "land decision" was created in order to allow statistical computation and comparison to the "go-around" node.

Once a network has been created, the conditional probability distributions of each node given their parent nodes are ascertained. By developing a series of equations in MATLAB (a numerical computing programming language) and populating them with the conditional probability data, it will be possible to use the software to manipulate the values and calculate the effect on occurrence probabilities of each node in a Bayesian style (allowing the investigation of barrier effects on a system).

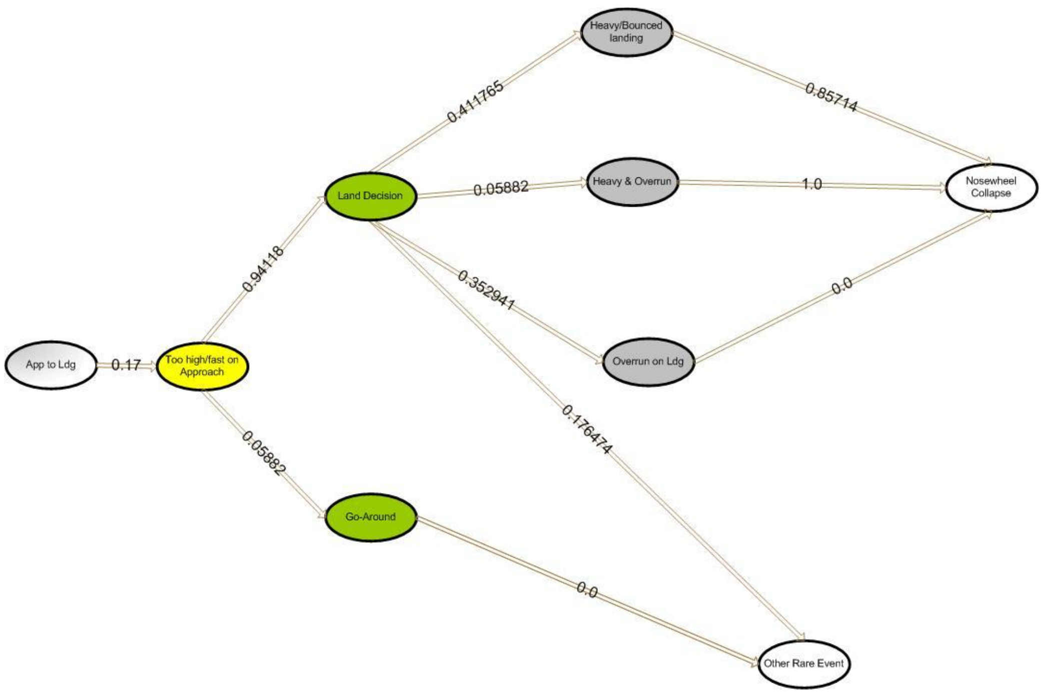


Figure 5-5 - Information network with non-conditional probabilities applied

These modified networks essentially allow a level of prediction of the effect on the whole network of manipulating event probabilities.

5.3.3 Building the Bayesian Network

It is important, if predictions and progress in the field are to be made, that the model and methods used in this study are qualifiable. Bayes networks allow all of the necessary facets discussed in earlier sections and so an approach that envelops the theory and algorithms is key to the method. MATLab has the ability to append toolkits to carry out complex calculations and as such becomes a workable solution when paired with Kevin Murphy's Bayes Net Toolbox.

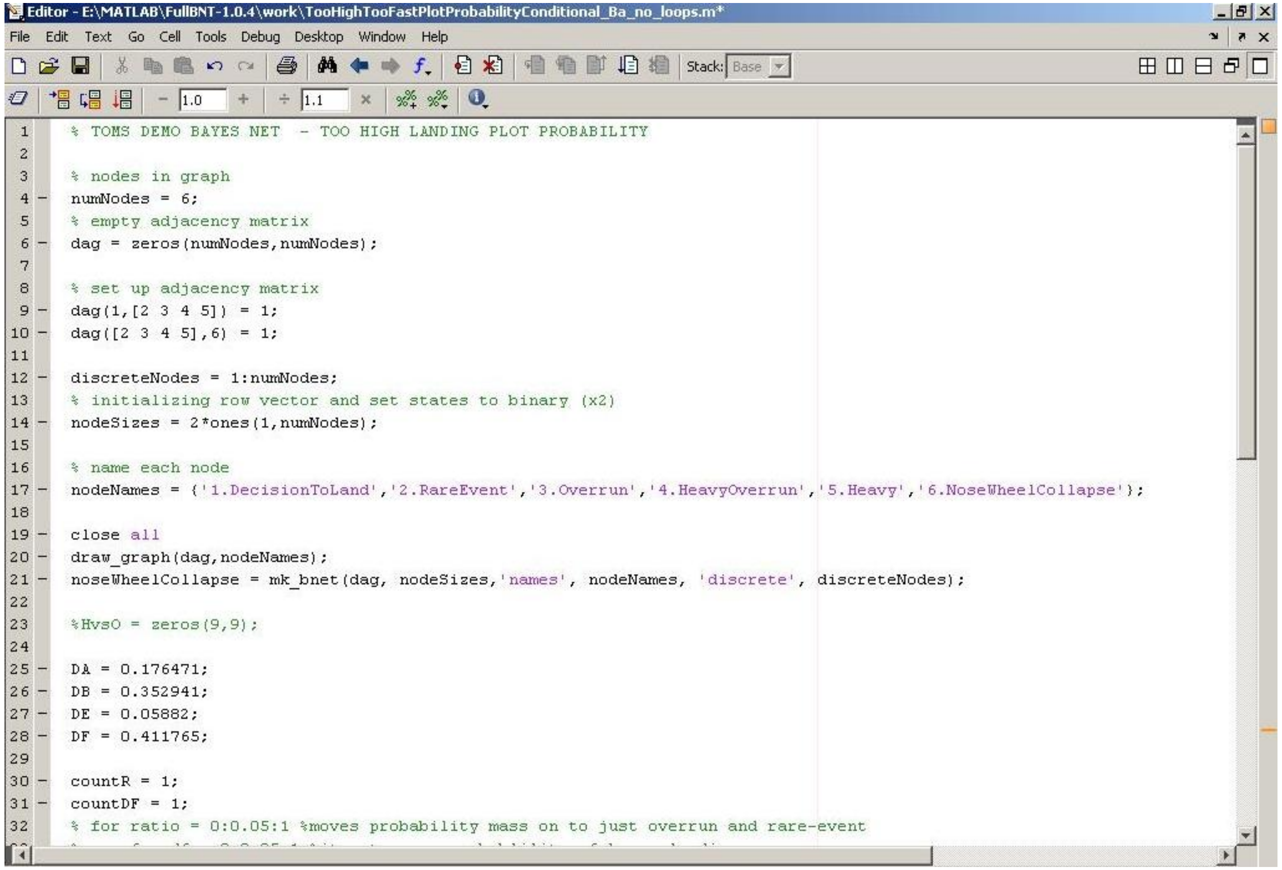
It was decided this was the best platform to create a Bayes network type methodology of identifying all possible outcomes (i.e., effects on probability of related nodes) from modifying a particular link's probability with the addition, or manipulation, of a barrier. This would comprehensively identify information, and hence error, migration routes created when attempting to mitigate the accident pathways described in the information network. The benefits of developing a semi-automated mathematical program are that the calculations for a simple network such as that described in this paper are extensive yet once developed it is hoped the system could work on a much larger scale.

The following describes the process of modelling a simple information network as a Bayesian network and populating that network with probabilities based on historical data as has been carried out for use in chapter 6.

The simplified information network shown in figure 5-5 now had to be coded to a Bayes network within MATLab. This process involves the specification of a directed acyclic graph. This converts the graphical network into a non-graphical model by identifying which nodes are related to others and in which direction (i.e. identifying parent and child nodes as in Figure 5-8). This is termed an adjacency matrix. Figures 5-6 and 5-7 show the code as it stands in the program and the following paragraphs explain its meaning.

In MATLab any line of code which is preceeded by a "%" symbol is considered a comment line and generally ignored when the program is being executed. These comment lines are included to make reading the code simpler. Line 4 simply tells the program how many nodes are present in the system; in this case 6. An adjacency matrix is a method of telling the program which nodes are linked and which are not. Line 6 empties the adjacency matrix so that lines 9 and 10 can inform the program where links are present in this case. A dag is a directed acyclic graph (a network of sorts) and, for example, line 9 states that node 1 is linked to nodes 2, 3, 4 and 5 as the link is “1”.

Line 12 then defines each node as discrete, i.e., having a certain number of possible values, and line 14 further defines the nodes as binary. This identifies the nodes as either being “true” or “false” which is a valid representation of the nodes within a system which are either present or not.



Editor - E:\MATLAB\FullBNT-1.0.4\work\TooHighTooFastPlotProbabilityConditional_Ba_no_loops.m*

```
% TOMS DEMO BAYES NET  - TOO HIGH LANDING PLOT PROBABILITY

% nodes in graph
numNodes = 6;
% empty adjacency matrix
dag = zeros(numNodes,numNodes);

% set up adjacency matrix
dag(1,[2 3 4 5]) = 1;
dag([2 3 4 5],6) = 1;

discreteNodes = 1:numNodes;
% initializing row vector and set states to binary (x2)
nodeSizes = 2*ones(1,numNodes);

% name each node
nodeNames = {'1.DecisionToLand','2.RareEvent','3.Overrun','4.HeavyOverrun','5.Heavy','6.NoseWheelCollapse'};

close all
draw_graph(dag,nodeNames);
noseWheelCollapse = mk_bnet(dag, nodeSizes,'names', nodeNames, 'discrete', discreteNodes);

%HvsO = zeros(9,9);

DA = 0.176471;
DB = 0.352941;
DE = 0.05882;
DF = 0.411765;

countR = 1;
countDF = 1;
% for ratio = 0:0.05:1 %moves probability mass on to just overrun and rare-event
```

Figure 5-6 - Screencapture of the MATLab code (Part 1)

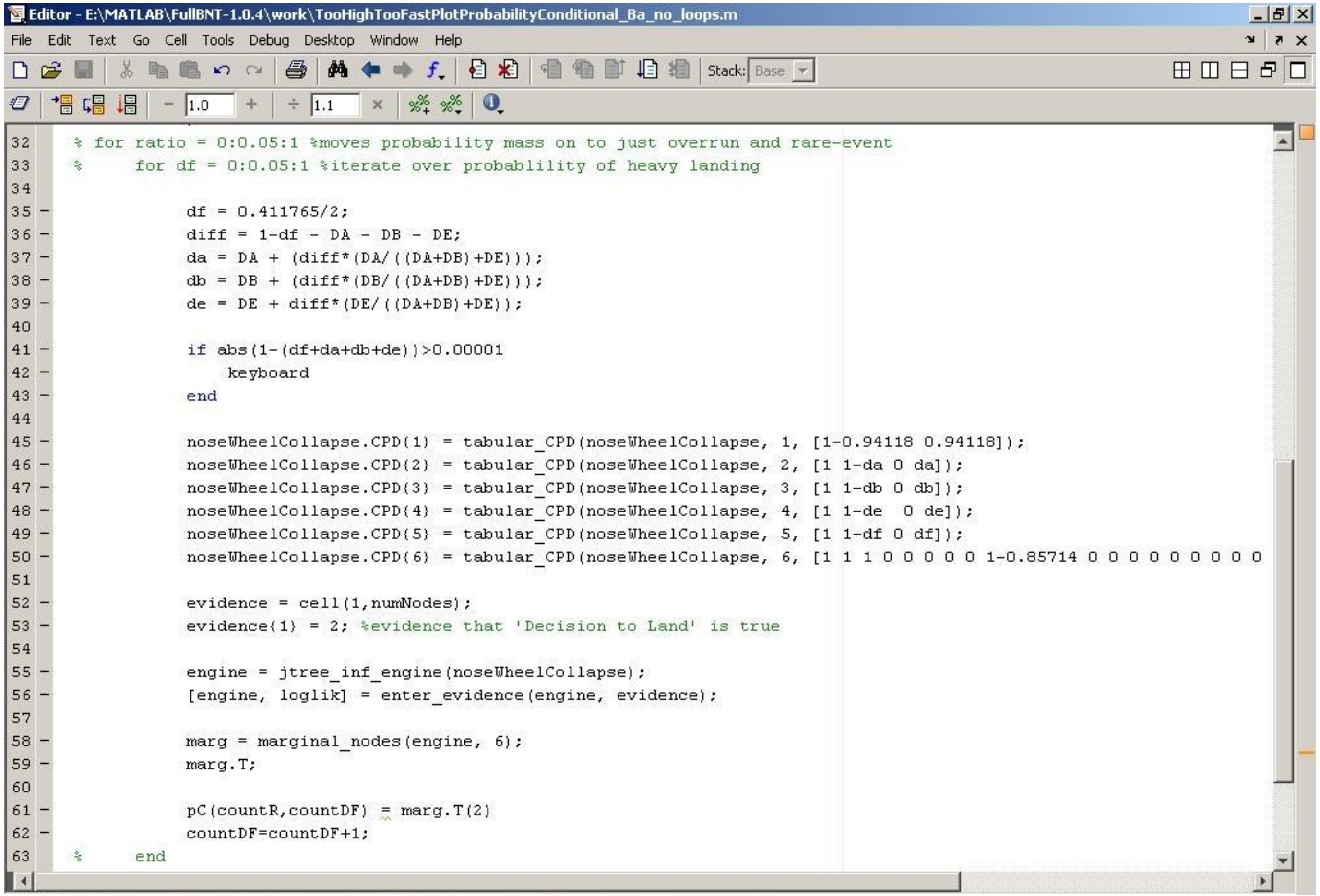


Figure 5-7 – Screencapture of the MATLab code (Part 2)

Line 17 then informs the program of each node's name before line 20 then instructs the program to draw a graph to display the network formed and this is shown as figure 5-8.

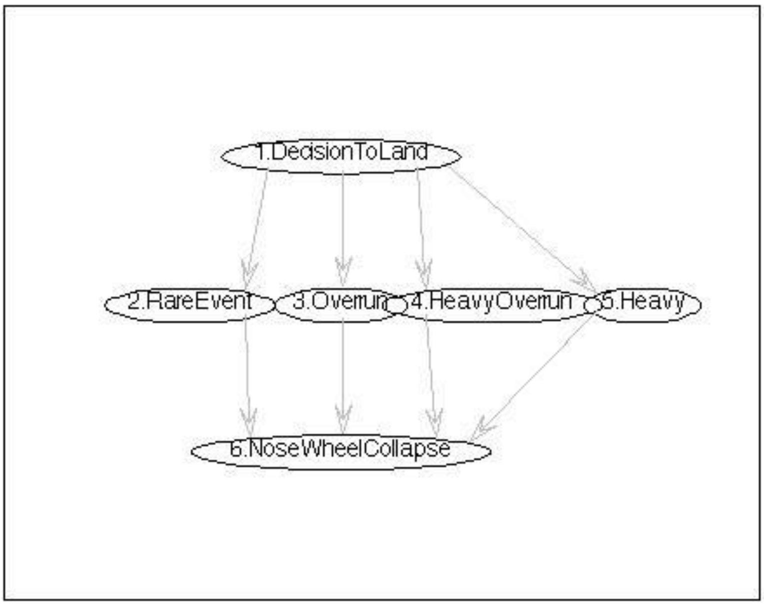


Figure 5-8 - The scenario network as programmed in MATLab

When compared with figure 5-5 it can be seen that this network is only modelling from the point at which the pilot decides to land. The method can be extended much further but it is important in this original exploratory study to maintain a reasonable level of understanding whilst limiting the number of additional errors or variables that might creep in through expanding the network tested.

Line 21 now instructs the program to make this Bayes net referring back to the previous lines in the script. Lines 25 to 28 inform the program of the probability of each node occurring in the historical data collected earlier in section 5.4. Each node has been assigned a letter to simplify the code. These are shown in figure 5-9.

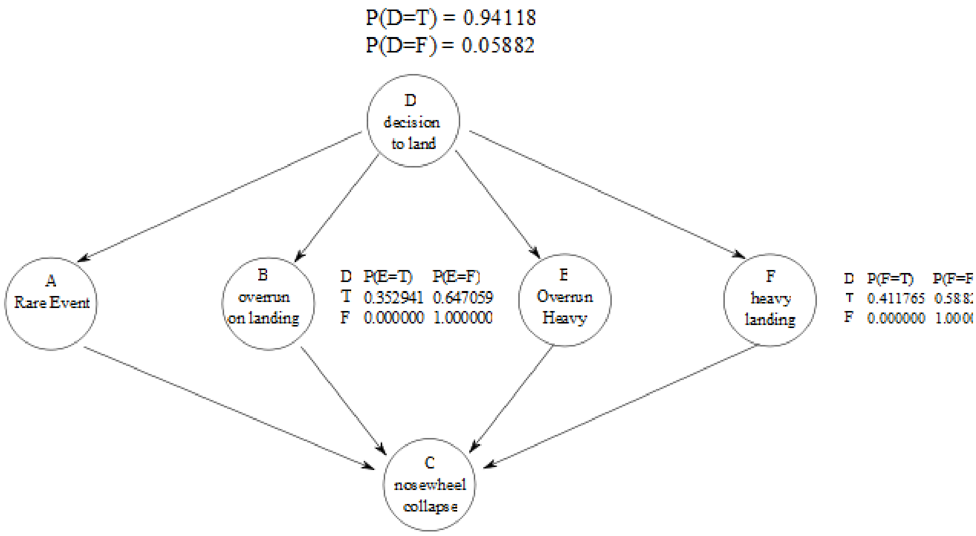


Figure 5-9 - Network diagram illustrates letters as used in MATLab code

Line 35 allows the user to define ‘df’ which is the new (and changeable) value of ‘DF’ shown in line 28. It is this value that represents the probability of a heavy landing occurring and as such changes to this value can be likened to changing the strength of the barrier leading up to the node ‘heavy landing’.

Lines 36 to 39 code the redistribution of any probability of occurrence ‘lost’ from the ‘heavy landing’ node. Line 36 ensures that the probability adds up to 1 at all times whilst 37 to 39 model the redistribution of probability according to the ratio of probabilities of the other nodes. In this way, the original model (as coded) infers that any probability value lost from the node ‘heavy landing (F)’ migrates to the nodes ‘overrun (B)’, ‘overrun and heavy (E)’ and ‘rare event (A)’.

Lines 45 to 50 are where the data from the GA database are entered into the program. Bayes nets use Conditional Probability Distributions (CPDs) to model the probability of each possible outcome. In order to make the model usable at this stage it was necessary to treat each node as mutually exclusive. This precludes the chance of an ‘overrun’ node being ‘true’ at the same time as a ‘heavy and overrun’ node. This should not, on the surface at least, affect the result of the network since each event had been classified as separate when harvesting the data. A 0 in the CPD is usually the result of two nodes being ‘true’ at one time. An example Conditional Probability Table (CPT; which is used to calculate the CPD) is given in table 5-2. The order of the CPT is important and the first column must begin with a 'false' and then work alternately with 'true'. In this way, each alternate line must add up to 1 if nodes are mutually exclusive. From the first and third rows of table 5-2 it can be seen that if there is no decision to land there can only be a 'false' for the node heavy since no landing is made. Row three therefore has a probability of 0. The data from the GA database have given the probability of a 'heavy landing' (given the decision to land being 'true') as 0.411765 (row 4) so in order for the CPT to work the probability for row two must be 1- row 4 which is equal to 0.588235.

Node D	**Node F**	
DecisionToLand	**Heavy**	**Prob**
F	F	1
T	F	0.588235
F	T	0
T	T	0.411765

Table 5-2 - CPT from line 49 (probability of node 'heavy landing')

Line 50 of the code illustrates the CPD for the node 'nosewheel collapse' and as such has the greatest number of possible options, thirty-two, although many of these are limited to zero by mutual exclusivity.

Lines 52 and 53 tell the program that the node 'decision to land' is true. This is a useful limitation for the purposes of the study in chapter 6 but open to manipulation in the future through the addition of many pieces of evidence prior to the node in question. The next four lines of code cause the program to run the scenario and produce, through inference, the marginal distribution of probability. The reason the results are considered marginal probabilities is that the analysis has artificially reduced the number of variables that are being considered compared to the real situation. This does not, however, necessarily result in inaccurate data since the quality of the historical data and any inferred relationships between nodes is what the inference engine uses to calculate probability relationships.

To test the coded network we can execute the program with line 35 (df) as the original value of DF 0.411765. In this case, the program calculates that the probability of nosewheel collapse is 0.2627. If, as in figure 5-7, we halve the probability of the heavy landing (df = 0.411765/2) then the resultant probability of nosewheel collapse is 0.1201. It is clear that this is not half of the previous probability and so there is a relationship that is being modelled within the network that is not strictly linear.

This value of df will be investigated in chapter 6 in a flight simulator study. If a barrier can be given a quantitative value, such as reducing the number of heavy landings by half, then the program can attempt to predict the effect on all other nodes. Although this is very limited at this point, in terms of the number of nodes being used, if the method is shown to work or produce at least positive results, then the expansion, as previously noted, is less problematic. It would be possible to produce a program capable of automatically filling such a Bayesian model as the numbers become too unwieldy to use first principles and manual CPTs.

5.4 Outcomes, Limitations and Future Work

5.4.1 **Current limitations**

It is important at this developmental stage of a novel method to acknowledge and address any limitations that are currently present. Methods for further work to overcome and combat these limitations are discussed here and further in chapter 6.

The analysis detailed in this paper uses only negative-outcome data (i.e., 100% of flights used resulted in an accident) and this currently limits the migration issues relating to a “safe outcome”; a central element of this work. The addition of positive-outcome data is not without its challenges but commercial aviation certainly has the equipment and ability to record and observe vast amounts of normal operation data should it prove useful to do so. This mixed-outcome data then can be incorporated to populate comprehensive networks. The acquisition of such data is harder in the GA environment but if the method proves useful then action can be taken to improve this. Once positive outcome data are included then it would become clearer which barriers are most likely to result in the migration of probability towards more positive results, or at least a result which results in the increase of activation of fewer negative outcome nodes than other network manipulations at the barrier level.

Within the Bayesian information network method itself the main limitation in this initial form is the treatment of all nodes as mutually exclusive. At this stage of the development it was necessary to limit the mathematics involved in order to test the nature of applying Bayesian theory to the information networks. In developing a program within MATLab it is possible to include nodes with feedback loops and also to introduce relationships of non-mutually exclusive events. The quantity of data required is significant in order to build the relationships to a level which is useful and for this reason the limit is predominantly processing related. This can therefore be conquered with larger data pools and more complex network programming.

In terms of this study and manipulation of the network, the primary limitation is the quantity of information available and used to populate the networks. This really is to identify the potential of a novel methodology and any increase in data can be catered for with more complex and automated programming processes retaining the base theory tested here.

Finally, the identification and use of factors and node elements would need further development in future studies. In particular, for the purposes of this study the author compiled the list of nodes from the accidents and in future repeats would develop a method of cross-validation both inter and intra-rater to improve quality.

With these limitations, and the potential methods for removing them, in mind the following addresses the outcomes and further developments that this study has resulted in.

5.4.2 **Chapter outcomes**

What this chapter has done is take the potential of Bayesian mathematics and combined that with the novel information network approach to understanding a complex system.

As discussed in section 5.1, the current literature tends to argue that GA and commercial accidents can not be compared successfully. Methods such as HFACS do suffer from these limitations but primarily this is due to classification of events and the difficulties in achieving the non-natural taxonomies required especially at the higher levels of taxonomic methods. This study has shown that GA accidents are not fundamentally different in that communication and information flow remain central to any system. As such, analysis can be carried out with networks which centralise the barriers and links of information rather than outcome. Despite the different types of information or methods of information transfer the fundamental process of communication can still be modelled through information networks. Failures in this communication can then be further investigated or potential leaks and weak points highlighted. In this way the approach detailed here based on information networks is argued to be more suitable than other methods for studying the breadth of aviation accidents. Unlike the main comparable work in the field, that of Luxhøj *et al.* (e.g., 2002 and 2006), the method is not restricted by limitations of classification/taxonomic techniques. For the first time Bayesian theory has been merged with systemic information theory and shown potential to overcome the restrictions associated with linear based fault-trees and methods that require causal taxonomies. This marks a first step in opening up the potential to study a system holistically without the prerequisite of an incident or causes.

This method has used historical data to populate the networks. It is very unlikely for historical event data to predict accurately a future event outcome due to the rarity and variability of aviation accidents and as such limited use has been made of such data. However, using data in a way that removes the need to compare ultimate outcomes or events and can instead compare the pathology of an aviation accident at a deeper level (i.e. information flow and individual information elements) has already been shown possible by information networks in chapter 3. This development in the field allows areas of particular concern to be highlighted by centring the barriers (and links) instead of the labelled or ‘classified’ event. Historical data of a particular link failing could lead to the further investigation of that link and associated barriers or factors. This would then develop a further understanding of exactly what that barrier or link is and how it is affected by, for example, training, regulations and propagation of relevance. This link may be implicit in a number of outcomes and as such by understanding the system at the information network level we are not limited to attempting to predict outcomes with historical outcomes; more relationships can be studied, modelled and potentially understood. A fully developed program using the methods above could result in a warning system as certain barriers are attacked more frequently than others or have potentially more far-fetching negative results than others. Crucially also, the same barrier may affect many different links and this is where the model would develop into a fully functional 3D network. This is explored in chapter 8.

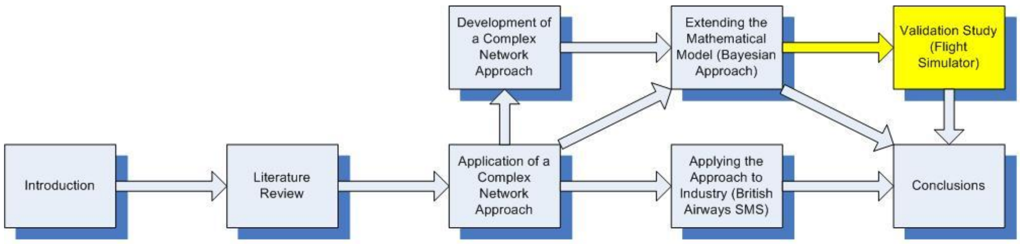
The strength of this model when compared to many PRA methods is that the aim is not restricted to needing exact predictions of outcomes. Instead, the focus is on highlighting and making salient relevant nodes, links, barriers, and, factors. The quantitative aspect of the approach give the method objectivity and make use of the large amounts of data that are far from useless despite the caveats given in the previous chapter. Further than simply predicting the probability of a particular node or barrier to be activated, this method has potential to really develop the understanding of the pathology of the system.

5.5 Summary

This chapter has taken information networks further as a comprehensive qualitative and quantitative model. By removing the limitations of classic taxonomic methods, information networks prove to be equally as useful in understanding GA accidents as commercial accidents. The availability of GA accident data, although limited in detail due to reporting issues discussed, meant that a sample network could be built and predictions made on the effects to other nodes within that network following a manipulation of a barrier. This idea can then be extrapolated to larger and more complex networks and where possible programming, studied further in later chapters, can overcome the limitations discussed above. This is where this method takes the leap from reactive to proactive and has definite elements of a predictive model; the ultimate aim of investigative models.

The Bayesian model developed in this chapter is the basis for the testing carried out during a flight simulator study in chapter 6. This chapter investigates for the first time whether a simulation study can be used to validate predictions from information networks embedded with Bayesian mathematics. Future application of this type of method is also possible with the commercial aviation industry based work detailed in chapter 7.

6 Can we validate networks derived from incident data through simulation? A Pilot Study



6.1 Can a validation approach be validated?

The thesis continues with Bayesian mathematics merged with the information networks because they allow us not only to define the probability of a hazard occurring but also encapsulate risk more fully by integrating the probability of an accident given any particular hazard (Luxhøj, 2002). Further than this, by integrating the information network theory the restrictiveness of this approach to hazards and accidents can be removed. Analysis can occur based on the deeper level of information nodes meaning the analysis can occur regardless of perceived blame, linear cause or even a negative outcome. Bayesian networks have been developed to indicate relationships within a system just as an information network does – therefore together these two methods have the potential to be a strong analytical tool.

The initial introduction sets the scene of the study and reinforces the strong link between this chapter and chapter 5. Next the idea of using a verbal instruction to participants as a barrier is introduced and validated with reference to previous literature and usability. Finally, the last part of the introduction looks at the use of simulators within aviation and identifies this as a novel study that attempts to validate Bayesian information network predictions using flight simulation for the first time.

6.1.1 Setting the Scene for Simulator Validation

Chapter 5 looked at how information networks can be developed along a very different path to exploit the quantitative potential of the method without limitation in terms of immediate applicability. The current Chapter looks at whether, for the first time, the quantitative predictions from the information networks being populated with conditional probability data could be validated given enough simulation, or real-life, data collection.

The aim of this study and chapter is to investigate the possibility of validating the predictive nature of Bayesian networks through laboratory experimentation. The landing sequence of a general aviation aircraft has been isolated in order that the data produced and tested do not become too unwieldy that any underlying lessons or potential is missed. It is not possible at this stage to model the entire flight within one thesis and so in order to maintain a constant approach, the landing phase has been isolated as in chapter 5.

It is beyond the scope of this thesis to attempt to validate an entire network or comprehensively the use of Bayesian theories applied to information networks. However, as the subsection title suggests, this chapter attempts to discover if historical data can, as used in chapter 5, help to predict and model real-life scenarios. This study attempts to begin this process and if successful, develop and increase the scope of application which is then more down to software development and data management. Ideally, with comprehensive information networks based on GA flying populated with historical data, changes to training or regulation of pilots and flight could be tested in the network probabilities and then possibly cross-checked through simulation. This chapter sets out to attempt to introduce the possibility of validation of this theory in order to capture the elusive idea of error-migration within networks and chart best or worst scenarios given specific changes.

6.1.2 **Bayesian Information Networks and Barriers**

Networks have been developed in chapter 5 based on General Aviation (GA) historical data collected from landing scenarios. The information networks' nodes were populated using this historical data from the Air Accident Investigation Branch (AAIB) without the use of taxonomies such as HFACS, a technique breaking protocol with the literature to date. The use of information networks instead of causal fault-tree based approaches provides potential for a deeper understanding of a complex system such as aviation without linear restrictions. Following the construction of information networks, similar in design to those found in chapter 3, the links between nodes were quantified with probabilities and in order to capture the full interrelationships between nodes a Bayesian network developed. Luxhøj *et al.* (2001) based the values within their Bayesian networks initially on subject matter expert assessments and then began to integrate historical data. In order to remove subjectivity as much as possible at this stage, the networks were populated with historical data. It is then hoped that this

Bayesian information network reflects accurately the real-world and the simulated world tested in this study. It is clear though that further work needs to be carried out to really quantify the interactions and models and this is continuing throughout the subject area (Ale *et al.,* 2005).

Further than this, developing upon ideas introduced by Luxhøj (2002), this chapter looks to introduce barriers into these Bayesian models and manipulate the values of nodes and links within a network resulting in the variation of any potential outcomes and node activation. In the future both the nodes and the barriers may be quantified in terms of "...distributions of values rather than point estimates wherever appropriate." (Ale *et al.*, 2007, p. 1432)

Luxhøj and Coit (2006) talk of introducing "technologies" or "interventions" into their Bayesian Belief Networks in order to affect the causal trees used. Luxhøj and Kauffeld (2003) used HFACS as the basis for developing a Bayesian network and attempted to assess relative risk post-barrier introduction based on the taxonomy. What this study looks to do is remove itself from any restriction of a classification or taxonomy technique and instead look to identify at a deeper level information (or error) migration; an issue that is to date not covered comprehensively in other literature. Methods have been published and used to attempt to qualify relationships within systems such as System Hazard Analysis (SHA). The FAA have published a handbook (2000) that details integrated SHA (ISHA) and MIL-STD-882E (US DoD, 2005) is a well known document detailing US military safety practice. Both of these identify the sort of work that must be done to understand the effect on the rest of the system of any new insertion and that "...insertions...are accomplished in a manner that maintains an acceptable level of mishap risk" (US DoD, 2005, p.13). Although positively addressed, these issues are raised at a very high-level, something this study attempts to overcome. Indeed, it is hoped that by adopting the information network methodology this study will show that information migration prediction can be validated with flight simulation as a starting point. Further to this the information network, by removing compartmentalisation of particular accidents or outcomes, has the potential to really show migration outside of the particular scenario which is being investigated; ideally highlighting nodes of interest that are not immediately apparent to the investigator. In this way the potential of the method will not be fully developed in this study but the foundations for this further research so will be born.

For the purposes of this study, it is not appropriate to develop and test a technology, or barrier as understood from a purely engineering perspective. Instead, using barrier theory to its fullest, barriers do not require a physical presence and in this case a strong instruction to a pilot (as long as it is unambiguous and possible) may act as an intervention; a barrier. MIL-STD-882E considers a wide range of barriers including modifications to equipment, insertion of new technologies or materials and changes to techniques and methods; this makes an instruction a suitable insertion. This strong instruction, in having an influence upon the information flowing between nodes and the presence or otherwise of a node within the network acts in a manner comparable with a physical barrier. This makes an instruction suitable for testing in this study where Bayesian predictions are compared to flight simulation results. Indeed, to "develop procedures and training" as a "mishap risk mitigation measure" (US DoD, 2005, p.11) is considered a fourth level, or lowest order of precedence, method to mitigate mishaps. Therefore, if a verbal instruction is shown to work in this method then it is reasonable to expect those mitigation measures with a higher precedence (design selection, safety devices and warning devices) would work to an improved extent. In this way, the method is testing the worst mitigation and its effect on the nodes and the network/Bayesian model.

6.1.3 **Is Simulation Suitable for Study?**

It is clear there would be serious implications, both financial and safety-related, if participants were asked to fly real aircraft in potentially difficult, or even dangerous, situations. In fact, aviation has been a forerunner in the use of simulators for training and practise since their early development when computer graphics and processors could satisfactorily reproduce facets of the real-world scenarios. Indeed Salas *et al.* (1998) discuss the centrality of simulators within almost every aspect of aviation training. It would appear appropriate, therefore, to turn to simulation for the testing of aviation centric models of accident causation.

Simulation in itself though is also incredibly expensive when looking at, for example, the high-fidelity, full-motion platforms that a company such as British Airways (BA) spends millions of pounds on. The running costs are also high, requiring specialised synthetic flight instructors (SFIs). It is not surprising then that just one hour in a BA simulator costs upwards of £400 to the general public in 2009. Conversely however, this is still significantly cheaper than an hour's cost of flying a BA aircraft given fuel, handling costs, approach fees and dual crew etc.

So the same is true for general aviation. The cost of hiring a light aircraft varies considerably depending on type, age, capability and location. But there are a small number of light-aircraft simulators which are being developed to provide cheaper solutions to training and testing of safety and aircraft performance. Brunel University has one such simulator; the Merlin MP521 (Figure 6-1).

This simulator provides a cost-effective platform for basic training and aeronautical testing. The graphics and fidelity of the simulator, despite being full-motion, are of course limited in comparison to the type used in large airlines but in the right situation they provide very valuable tools for research. This project is one such example. The aim of validating a section of the network for a light aircraft landing does not require high-fidelity and highly-graphical simulation. So long as visual cues similar to that of a normal approach, e.g., instrumentation, runway and surrounding visuals, are present, then the simulation is suitable for the type of study in this chapter. In fact, Dahlstrom *et al.* (2009), after some discussion of the literature surrounding the argument, even go so far as to say that sometimes "high levels of technologically driven fidelity can simply be wasteful in terms of costs and time...."

The aim of this project was to investigate the potential of using simulators to validate and test predictions made by the Bayesian style networks adapted and researched in chapter 5. It is hoped that the results from this study give support to the probabilities harvested through studying the GA accident archives. Further than this though, the study will allow for the manipulation of the pre "Heavy Landing" node barrier previously identified. Using an instruction to affect the behaviour of the participant pilots a measure will be taken of the reduction effect this has on heavy landings. Subsequently the factor of reduction can be entered into the Bayesian Information Network and a predictive value for changes in nosewheel collapse events elicited. The actual value of nosewheel collapse pre and post instruction will be compared with the predicted value from the network statistically and if found to be similar it can be concluded that the information networks do have strong potential to act as predictors of real-world events after manipulation of barriers within.

Figure 6-1 - Brunel University's Merlin MP521 Flight Simulator

6.2 Methodology

The reasons and theory behind the testing of Bayesian information network predictions by flight simulation have been discussed. Section 6.2 sets out the way in which this study was carried out. In particular it highlights the study variables and the experimental design including the equipment, procedure and participants involved.

6.2.1 **Design**

This study takes the form of a within and between subjects simulator test built up of 6 scenarios. The 3 scenarios had altered starting points from where the simulation would begin and the participants asked to execute a landing approach. In order to test the network predictions it was necessary for the study to elicit results of the aircraft overrunning a runway and carrying out a heavy landing. Therefore each scenario was developed to allow the participant to carry out an approach, and possible landing, to a runway of fixed length. The force of impact of the aircraft (heaviness of landing) and the landing distance (distance past the fixed threshold where the aircraft came to a complete stop) could be measured and stored for statistical analysis and comparison with the results from chapter 5. Within each scenario it was possible to carry out a successful and safe landing but with increases in speed and height at the starting point this would obviously become more of a test and reflect more realistically a high and/or fast approach to land.

Independent Variable One (Made up of 3 levels)	Independent Variable Two (Made up of 2 levels)	Dependent Variable One	Dependent Variable Two
Slightly High & Fast	No Instruction	Force on Landing	Overrun
High & Fast	Instruction Received		
Very High & Fast			

Table 6-1 – Summary of the study variables

Table 6-1 summarises the variables within this study. The independent variables are covered in detail in section 6.2.4. Force on landing (dependent variable one) was measured with reference to normal acceleration of the aircraft upon impact with the ground. This offered the best value reference for distinguishing which landings are considered heavy and those considered not heavy. The second dependent variable, overrun, was measured in relation to the distance past the threshold that the aircraft came to a complete stop. This could then be related to the overall length of the runway and thus a conclusion made as to whether the aircraft had overrun the runway. Since all participants completed all conditions so the manipulations of the scenarios are within-subjects.

The study was developed so as not to measure flying skill directly due to the limitations imposed by the hardware and software used. Instead the study deals with decision making, ability to interpret simple instructions, basic flying skills and allows for any improvement over the scenarios flown by using pseudo-random test order. Most pilot participants remarked that the simulator was just like converting onto a new type of aircraft (not necessarily totally realistic or as easy to fly as many aircraft). As such each volunteer was flying this “type” for the first time and each therefore is equally handicapped in that sense.

As in chapter 5, the network was broken down into a more manageable section concentrating on the “too high/too fast” scenario of landing approaches which could be modelled in the simulation (Figure 6-2).

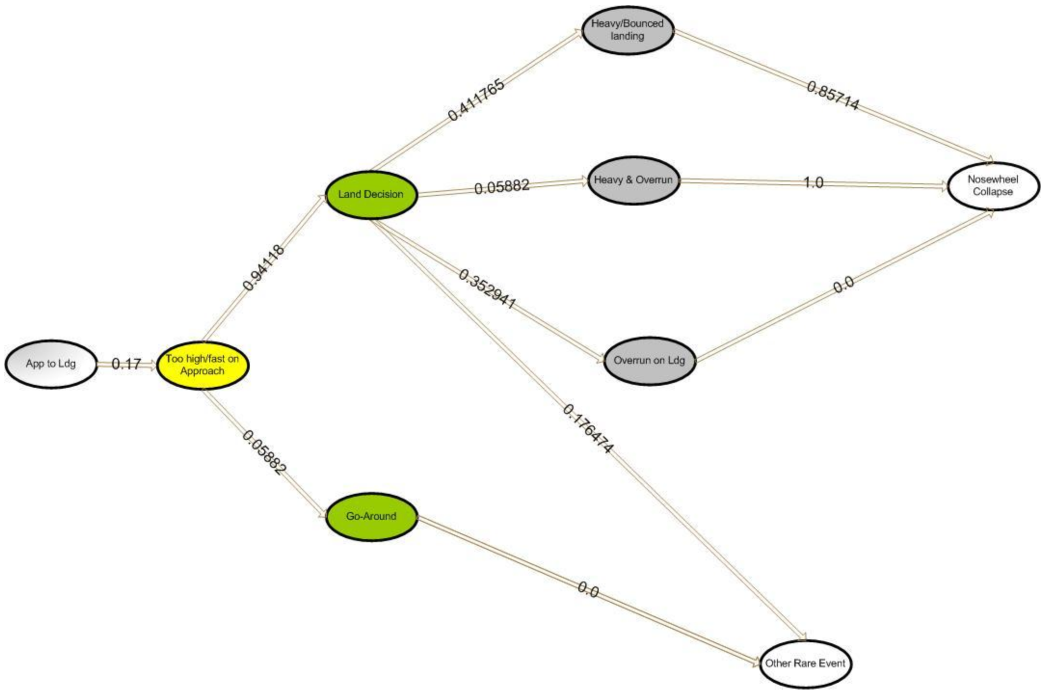


Figure 6-2 - Information network with non-conditional probabilities applied

6.2.2 **Equipment**

Figure 6-3 - Internal view of the Simulator

The Merlin MP521 full motion flight simulator was originally designed to teach all aspects of aircraft design principles including the evaluation of controls and aerodynamic models. The basis of the software is a non-linear transonic six degree-offreedom model. This allows reconfiguration of the module to almost any aircraft type from glider to airliner.

Due to the limited nature of simulator graphics it is usual to increase the amount of information available on screen in terms of data to make up for a lack of depth perception and other subtle cues. For the simulator study the Heads Up Display (HUD) was modified to remove the central crosshairs, g-reading, latitude and longitude readouts, height, speed and vertical speed. These were instead represented in standard format instruments (identical to Cessna light-aircraft) on the instrument panel to the side of the control-yoke. The screenshots of the simulator control-panel and pilot's view are included here to show the graphical capabilities of the simulator. Figures 6-3 and 6-4 illustrate the set up of the simulator cockpit, position of instruments, controls and visual display used.

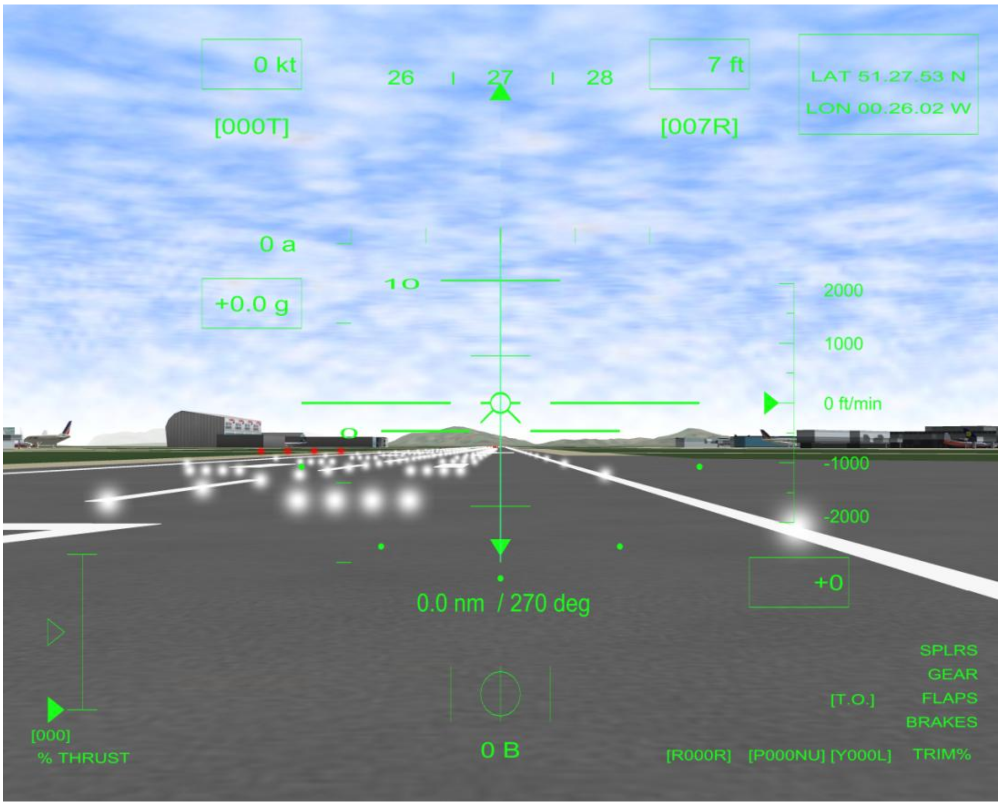


Figure 6-4 - Heads Up Display in standard format (This was adapted for sim study)

In terms of feel and control, the simulator uses compressed air to give feedback to the yoke control and also to control the full-motion experience. The simulator is fitted with a vernier throttle akin to that in a Cessna light aircraft, a yoke control, rudder pedals and a suite of instruments digitally representing measurements of altitude, speed, pitch, roll and yaw in a standard format. The aeronautical model underlying the behaviour of the aircraft model is similar to that of a Cessna 152 training aircraft (figure 6-5).

Figure 6-5 – Cessna 152 Landing

6.2.3 **Participants**

Participants were invited to take part voluntarily in the study. An email was sent to 500 members of a local flying club and replies received from 36 acceptable individuals as wanting to take part. An acceptable participant from the study was determined as a pilot holding at least a Private Pilot's Licence for aeroplanes (PPL(A)) so student pilots or enthusiasts were not accepted. Of the 36 individuals, 30 were able to make the days that the simulator was available for use and of those 30, 28 produced usable data. Of the 2 unusable participants' data, one set of data became corrupted on saving which was not recognised until after that individual had left and the other (due to the wish not to impose changes or restrictions on pilot's behaviour) carried out manoeuvres which impaired the ability of the data to be compared fairly with the other participants.

The 28 participants can be broken down into 26 males and 2 females. Ages varied from 25 to 63 with a mean age of 46. There was a range of hours as pilot of a light aircraft of between 54 and 1470 with an average of 383 (382.7143).

6.2.4 **Procedure**

The scenarios themselves were made to be simple due to the nature of the simulator used and in order to limit result variations. This is best achieved through simple scenarios and limited outcomes which would in turn reflect best the chance to validate, or not, the possible prediction values from the network models.

Due to a limited number of airfields available in the software, Gatwick was chosen as the airport to base the scenario at as it had less surrounding scenery than the alternative (Heathrow). The runway at Gatwick is too long to make the study valid for looking at runway overruns in light aircraft, therefore a straight taxiway parallel to the main runway was located in the South-Eastern corner of the airfield and this used as the “runway” for the practice and the scenarios. Figure 6-6 and Figure 6-7 show the location of this taxiway at London Gatwick. The length of the study “runway” is approximately 3,118 ft (950.5 m) of tarmac and this is comparable, albeit a very generous length within GA, to the home airfield of the participants where the main runway length is 3,330 ft (1,110 m) of grass.

Figure 6-6 - The Study "Runway" (© Google Maps)

Figure 6-7 - The Study "Runway" Enlarged (© Google Maps)

Each participant was given a guide of the simulator and its controls/instruments on arrival and then asked to read a preliminary brief:

"You are the pilot in command of this light aircraft and all decisions are yours to be made as if in command of your own aircraft on a 'typical' flight. Following an introductory circuit during which you can become familiar with the controls, you will fly a series of 6 approaches to the same runway. This first circuit is not being recorded for the purposes of this research. Each subsequent sequence is simulating the first approach to an airfield at the end of a flight. Each sequence will begin from a point on the final approach with the simulation frozen. When you are ready to continue, the simulation will begin and continue until you are told that the sequence is at an end. If you do decide to land from any sequence please land as short as possible and stop as near to the threshold as possible. After each sequence there is a short questionnaire to be completed; be completely honest in your responses. You will not be judged on your performance, no person outside of this laboratory will see details of your performance and we are unable to provide feedback on your flight.

Do you have any questions?"

Any questions were then answered although great care taken to ensure that any questions would not alter the behaviour or decision-making of the pilot; such as the use of a go-around.

Each pilot was then given the opportunity to fly a circuit from the runway to get used to the handling characteristics of the aircraft before attempting 3 landing approaches from a "normal" 600ft, 80kts starting point with the simulator frozen. This was the non-experimental task and carried out as follows:

<u>Non-experimental task:</u>

Task A

1. Initial Point: threshold of Taxiway at LGW, 0ft AMSL, hdg 080°, 0 KIAS.

2. Free-exercise to complete circuit and familiarise pilot with the aircraft. Following this allow 3 practice approaches to the taxiway to become familiar with task.

3. Identify with the participant approach and landing speeds as follows:

   V_{ref} = 65 V_{fe} = 80

Following on from this practice session, each participant was then presented with the simulator frozen in one of 3 starting positions:

<u>Experimental tasks:</u>

Task 1

1. Initial Point: 1nm finals for Taxiway at LGW, 600ft AMSL, hdg 080°, 80 KIAS.
2. Continue approach and aim for any landing within specified preferred landing zone (PLZ).
3. Measure normal axis impact force and distance from 08R threshold that landing occurred.

Task 2

1. Initial Point: 1nm finals for Taxiway at LGW, 800ft AMSL, hdg 080°, 90 KIAS.
2. Continue approach and aim for any landing within specified preferred landing zone (PLZ).
3. Measure normal axis impact force and distance from taxiway threshold that landing occurred.

Task 3

1. Initial Point: 1nm finals for taxiway at LGW, 1000ft AMSL, hdg 080°, 100 KIAS.
2. Continue approach and aim for any landing within specified preferred landing zone (PLZ).
3. Measure normal axis impact force and distance from taxiway threshold that landing occurred.

As mentioned, the order of these 3 tasks was pseudo-randomised (see full test profile in annexe 3 for full order). Participants, who were in two-way radio contact throughout, were then read the following brief before being presented, in a pseudo-random order, tasks 4 to 6:

"For the remaining 3 landing tasks you are required, as pilot in command of this aircraft, to avoid at all costs from making a heavy landing. A heavy landing is one described as being uncomfortable for your passengers, causing excessive bounce on touchdown, or, in danger of damaging your aircraft in any way."

This additional brief acts to modify the barrier within the Chapter 6 network before the node "Heavy Landing" and as such is key to any validation exercise. Tasks 4 to 6 had the same initialisation features as tasks 1 to 3 respectively and each participant was told when each had come to an end.

Any comments from the participants were then noted (anonymously) and age, gender and hours data noted on their completed questionnaires.

As this study is an attempt to see whether larger scale validation of the Bayesian inspired information networks is feasible it was important to limit the number of variables so as not to cloud the data. Since the test was interested in landing force and landing distance, not braking force or distance, the braking force was set at a moderate level for all participants and they could not increase or decrease the singular force. Each participant was given precisely the same brief and same practises before the experimental phase began. The runway and conditions of flight including control feel, visual cues and starting-points were all consistent. The pseudo-random order of scenarios was used as the most likely way of limiting improvement effects with time and practise. The fact that the aircraft was unlike any real GA aircraft in a number of ways in terms of feel and behaviour meant that no participant could have an advantage by flying a particular type in the past.

As discussed in chapter 5 it can be assumed that exact predictions will be very hard to come by given the extent and quality of current historical data. However, if trends can be identified and relationships studied then a lot can be elicited from this technique. There are a number of methods which can be applied to the data resulting from this study to identify and test any relationships and these will be looked at in the next section.

6.3 Results

The results of this study are addressed in this section on several levels. Firstly some general observations relating to heavy and overrun landings are made together with a high-level summary of all data collected. Next the data is grouped into alike sets and tested using the chi-square metric. Section 6.3.4 then looks at continuous data and applies a nested ANOVA (Analysis of Variance) to the results. Although it can be argued that the ANOVA takes credence away from the chi-square, both provide a slightly different slant on the results. Each is useful in order to validate the usefulness of the instruction as a barrier and then take that further to investigate the relationships further. Whilst an ANOVA statistical test might suggest one group or individual has made a heavier landing than another, chi-squared definitively says what a heavy landing is (defined later in the chapter) thus providing a definitive slant on the results versus the continuous metric's relative comparison. Finally in the results section, 6.3.5

returns to the Bayesian based predictions made in chapter 5 and relates them to the empirical data found in this study. It is hoped that the data from the flight simulation scenarios validates the relationships that have been modelled in the Bayesian information network.

6.3.1 **General observations**

168 scenarios were flown (28 participants with 6 scenarios each). Data was recorded via a datalog produced by the simulator's mainframe. This raw .asc file was then modified to a usable output. Relevant data have been harvested from the datalog and reproduced in annexe 4 to this thesis. Table 6-2 displays one participants data for explanation.

Participant	**Scenario**	**Ground roll (m)**	**Distance past T/hold (m)**	**Normal Accel.**
A	1	378.5786172	743.3316396	-26.97

Table 6-2 – Example of relevant data from simulator datalog

Table 6-2 shows an example participant and the recorded data for one of the 6 scenarios. Highest and lowest values for each dataset within the table in annexe 4 are highlighted in amber and green respectively. All scenarios highlighted in red resulted in an overrun of the runway which is discussed in section 6.4.2.

Within the annexe, column 3 records the longitude at touchdown. Participant AA touched-down closest to the threshold on scenario 3 with a value highlighted as -0.15018641 (4 metres into the runway). Conversely, participant C, scenario 6 had a touchdown point of -0.1398577 (819.5 metres down the 950 metre runway). The overall mean for touchdown longitude was -0.145708271 (358 metres into the runway) with a standard deviation of 0.002805892 (221.3 metres).

Column 4 displays the longitude at which the aircraft has come to a complete stop, taking into account a constant braking force for all participants. The longitude for the stopend of the runway is -0.138198 and any longitude in excess of this would result in an overrun which is discussed in the next section. The shortest full-stop of an aircraft was participant AA during scenario 1 with a longitude of -0.14598704 (336 metres). The longest full-stop was participant KR, scenario 6 at -0.13522286 (1185.3 metres). The overall mean for full-stop longitude was -0.141000321 (729.4 metres) with a standard deviation of 0.002607827 (205.7 metres).

Column 3 of table 6-2 (column 5 of annexe 4) gives a measure of ground roll in metres. This is calculated by comparing the longitudes and multiplying by a factor of 78895.2

metres per longitudinal value of 1. This is a distance calculated for longitude in degrees at a latitude of 51º 8’ 53” North (Gatwick airport). The shortest ground roll was participant C, scenario 1 at 219 metres. The longest ground roll was carried out by participant Z, scenario 6 at 651 metres.

As a more useful illustration of stopping distance, column 4 (column 6 in annexe 4) indicates the distance (in metres) that the aircraft is past the threshold when it comes to a complete stop. The basic observations are as explained above in column 3.

Column 5 (column 7 in annexe 4) is a measure of force of impact of the aircraft upon first contact with the ground. The unit of measure is m/s^2. The greatest force of impact is -54.91 m/s^2 (participant Y, scenario 2) and the least -10.24 m/s^2 (participant D, scenario 4). The mean force of impact is -19.6 m/s^2 with a standard deviation of 6.3 m/s^2.

In total, out of 168 scenarios, there were 30 go-arounds. This is where the pilot elected not to continue an approach and the height in feet and longitude value at which the pilot carried this out are given as columns 8 and 9 in annexe 4.

6.3.2 **Overrun Events**

In total 22 “overrun” landings were recorded out of a total of 168 scenarios (138 landing scenarios after removing go-arounds). As discussed previously the scenarios were developed to be challenging and to increase the chance of overrun height and speed was above ideal in two out of three scenarios therefore this value is artificially high for the purposes of this study. This is important since the section of network isolated was that surrounding a high and fast approach to land.

On the surface, scenario 1 had no overrun events, scenario 2 had 1 overrun, scenario 3 had 2 overruns, scenario 4 had 2 overruns, scenario 5 had 7 overruns, and, scenario 6 had 10. However, since the number of go-arounds varied the percentage of completed landings that produced an overrun event per scenario is given in table 6-3 below and this shows more clearly the increase in events for scenarios 3, 5 and 6.

Scenario & No. of Ldgs	Overrun events as a % of completed Landings
1 (26 ldgs)	0
2 (26 ldgs)	3.85

3 (18 ldgs)	11.1
4 (25 ldgs)	8
5 (25 ldgs)	28
6 (18 ldgs)	55.56

Table 6-3 - Percentage of overrun events per scenario

It is not sufficient to look at the raw data in terms of overrun events. Therefore, a chi-square test produced by the crosstabs procedure for multiple unrelated samples was carried out on the data.

	Value	**df**	**Asymp. Sig (2-sided)**
Pearson Chi-Square	33.051	5	.000

Table 6-4 – Results of Chi-Square for Scenario versus Overrun event

It can be seen that this chi-square statistical test shows the differences in the number of overrun events to be significantly different between scenarios ($p < 0.05$). However, since more than 20% of the expected frequencies are smaller than 5 (50% (6 cells) in this case) the chi-square test is not reliable. The best way to resolve this issue is to record more data in a future study. It is possible, however, to group some of the data together and rerun the test with scenarios 1,2 and 3 grouped versus 4, 5 and 6. This would elicit whether there is a statistically significant difference to back up what appears to be a significant number of overrun events after the instruction not to land heavy is made.

	Value	**df**	**Asymp. Sig (2-sided)**
Pearson Chi-Square	14.404	1	.000

Table 6-5 - Results of Chi-Square for grouped Scenario versus Overrun event

This value for chi-square shows that the number of overrun events in scenarios 1,2,3 versus 4,5,6 is significantly different ($p < 0.05$). This would suggest that the instruction not to land the aircraft hard for the second series of scenarios has indeed increased the likelihood of an overrun event. Again at this point it is pertinent to recall that a pseudo-random order of testing was used to avoid any developmental changes due to practise.

However, in order to eliminate the differences in speed and height at the starting point from being the cause of overrun event frequency changes those must be compared in the fashion: 1 and 4 vs 2 and 5 vs 3 and 6. The results are encapsulated as Table 6-6.

	Value	**df**	**Asymp. Sig (2-sided)**
Pearson Chi-Square	8.861	2	.012

Table 6-6 - Results of Chi-Square for scenarios grouped by starting speed and height

On this occasion it is clear that the difference between the groups in terms of number of overrun events is not statistically significant (p > 0.05). This confirms that the differences in overrun event occurrence are due to the instruction on heavy landings and not the starting point of the simulation. This statistic, therefore, validates the use of the verbal instruction as a barrier as it is clear this has had a statistically significant effect on the network and its outcome. Therefore, it can be concluded at this stage there were significant differences where the barrier appeared to affect the outcome.

6.3.3 **Heavy Landings**

So now it has been found that there is a statistically significant difference in the number of overrun events between the pre-instruction scenarios and post-instruction scenarios the same analysis can be carried out for those landings classified as heavy.

'Heavy landing' is not a label that can be applied quite so clinically as overrun. An overrun is an excursion from the runway which has a defined length so any landing that exceeds this distance is an overrun. A heavy landing, however, is not so clear-cut. The European Aviation Safety Agency (EASA) document CS-23 (Certification Specifications) outlines the acceptable means of compliance with the specifications required for aeroplanes. As part of this document, a requirement of approval for certification is that the aircraft is stressed to at least 4g. This, however, refers to the a9ircraft as a whole and undercarriage limits are lower. Certification requirements for light aircraft require the undercarriage to accept up to 2.75g (26.968 m/s^2) without structural damage (EASA, 2003). A perfect landing, in contrast, should be 1g normal acceleration as the force of lift transfers from the wings to the undercarriage undetected. For the purposes of this study, a 'heavy' landing is one where the normal acceleration exceeded a value of 2g (19.6133 m/s^2). This figure is based on requirements set out in EASA documents CS 23.473, CS 23.479, CS 23.483, discussion with an AAIB engineering inspector and a certified aircraft engineer.

As discussed above, there were 138 landings after go-arounds were removed from the data. Of these landings, 59 were classified as 'heavy' given the definition of the previous paragraph (leaving 79 considered satisfactory). Breaking those landings down further it can be seen that from scenarios 1, 2 and 3 there were 47 heavy landings (67.14% of successful 1, 2, 3 scenario landings). Scenarios 4, 5 and 6 produced 12 heavy landings (17.65% of successful 4, 5, 6 scenario landings).

As with the overrun data, this information about heavy landings was analysed using the chi-square test produced by the crosstabs procedure for multiple unrelated samples. The results are illustrated in table 6-7.

	Value	**df**	**Asymp. Sig (2-sided)**
Pearson Chi-Square	35.841	5	.000

Table 6-7 - Results of Chi-Square for Scenario versus Heavy Landing event

Table 6-7 shows that through the chi-square statistical test, the differences in the number of heavy landing events is significantly different between scenarios ($p < 0.05$). On this occasion there is no issue of cells having lower than expected counts so there is no need to group the samples together. It can be concluded that the instruction not to land heavy (an introduced barrier in the information-style network) has increased the number of overrun events and decreased the number of heavy landings to a statistically significant level ($p < 0.05$).

6.3.4 **Further Statistical Analysis**

Next, the data can be analysed in the context of being continuous beyond that of the discrete variable statistics used thus far. This eliminates the need for the data to be classified in qualitative terms such as good or bad landings and allows a greater range of statistical investigation to overcome some of the limitations associated with this. However, since the term overrun is a discrete title the following statistical measures will compare force of impact with the distance past the threshold at which the aircraft came to a complete stop. This is akin to measuring the likelihood of an overrun. Unlike the chi-square tests the ANOVA will compare two non-heavy or two heavy landings with each other thus providing an alternative slant on the testing.

Firstly Multivariate analysis of variance (MANOVA) was used to confirm that the independent variable (restricting heavy landings) did have a statistical significant effect on the dependent variables; i.e. the normal acceleration on landing (force of impact) and distance past the threshold (overrun likelihood).

The resulting values from this statistical test (Multivariate test for Intercept and Scenario both showed Sig. = .000) show that there is a statistically significant effect on all dependent variables when considered as a group ($p < 0.05$) by the instruction to avoid heavy landings. This improves upon the data analysis from above and makes it clear that the instruction (barrier) is central to the differences.

Looking further than this it is possible to see whether the changes in the data values ‘distance past threshold’ and ‘normal acceleration of impact’ are related. Due to the nature of the results a simple one-way ANOVA is not sufficient to reveal the true extent of significant differences or relationships between values. As such a doubly multivariate repeated measures design was adopted (nested ANOVA type approach) and a summary of the results is given in table 6-8.

Effect	**Significance (p value)**
Instruction	0.000
Scenario	0.006
Instruction*Scenario	0.706

Table 6-8 - Sample of results of ANOVA analysis between scenarios

What the results in table 6-8 tell us is that when looking at normal acceleration (heavy landings) and distance from threshold (overrun) the effect of the instruction and the effect of the scenario are significant upon the results when looked at independently ($p < 0.05$). However, with a p value of 0.706 there is little evidence to suggest that the interaction between the instruction and scenario have a significant effect on the outcome. In other words, there is little evidence to suggest the effect of each scenario is dependent upon the instruction. This is not in itself a bad result since it has already been shown the effect of each on the results is significant and it is preferable that the effect on the results of the scenario is not changed by the instruction so that alone may be tested. However, it does not provide immediate information about any relationship between the two variables. Figures 6-8 and 6-9 plot the estimated means used in this statistical test for the instruction and the scenario respectively. They show many similarities and that is what is investigated in the next part of this section.

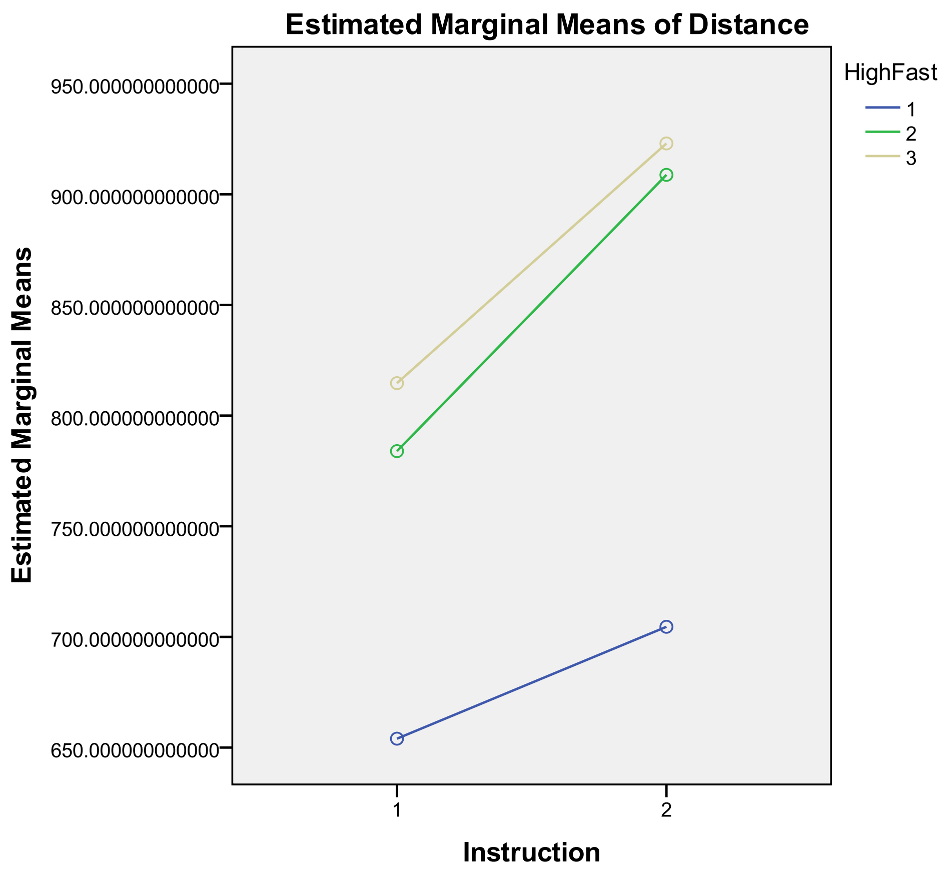


Figure 6-8 – The effect of the instruction on the estimated means of distance past threshold

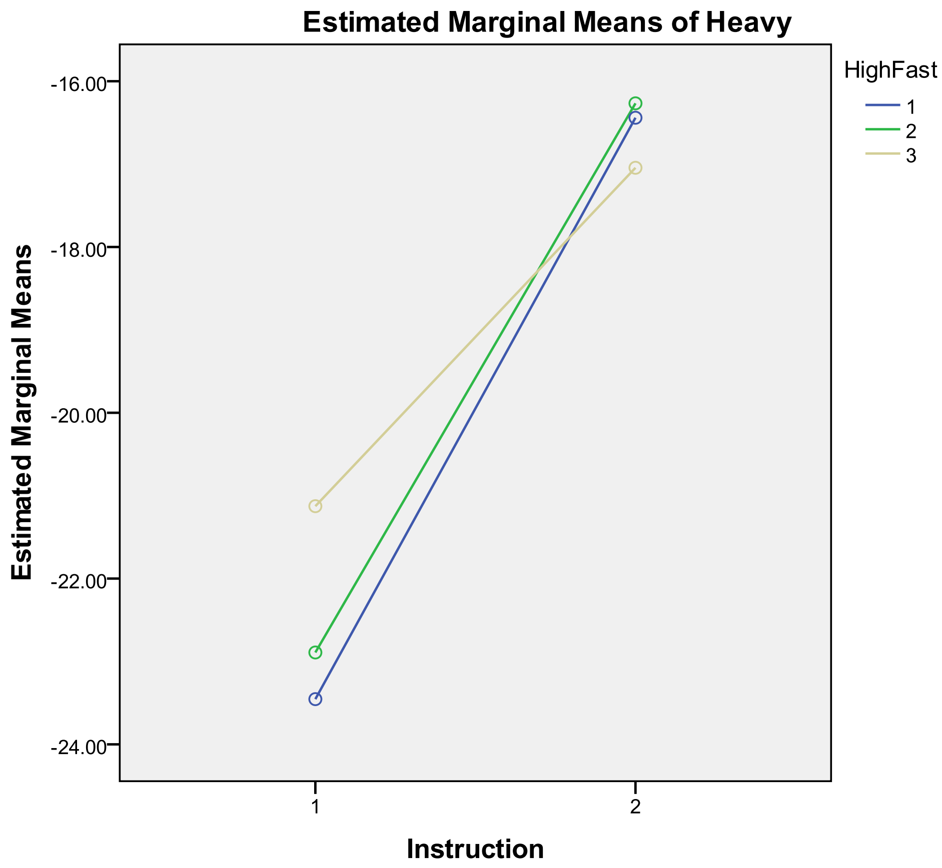


Figure 6-9 - The effect of the instruction on the estimated means of normal acceleration

These data would now appear to suggest that there are indeed statistically significant effects on the overall event outcome by the instruction mid-experiment. However, despite there being some real similarities between the plots for each scenario above there may be no overriding relationship (statistically significant enough to be used) between distance past threshold and force of impact in this dataset. To test this assumption the data were subjected to tests for correlation; or the presence of a relationship between variables.

	Normal Acceleration	Sig. (2-tailed)
Distance past T/hold (m)	.096	.263

Table 6-9 - Results from a Pearson's Correlation Test

Pearson's correlation divides the covariance of the two variables, distance and force, by the product of their respective standard deviations. The correlation value is +1 in a perfect positive linear relationship and -1 in a perfect negative linear relationship. Since the value given between distance and force is 0.096 it can be seen that there is no relationship visible at this level of analysis. The following scatter plot illustrates visually the lack of a simple relationship.

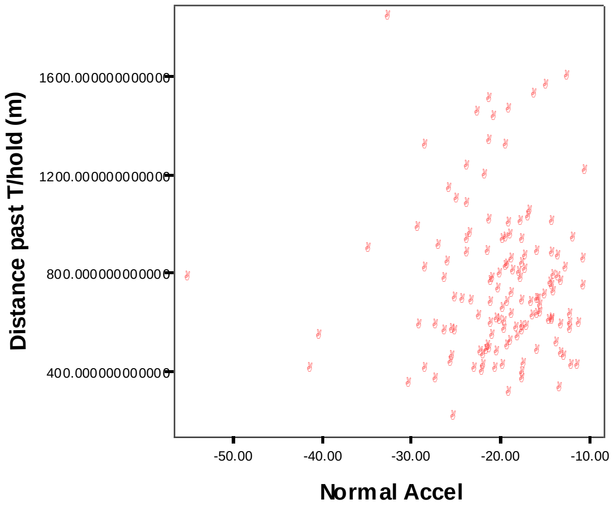


Figure 6-10 – Scatter plot of the relationship between distance from threshold and force of impact

The statistical analysis could be taken further to investigate regression curves, non-linear regression curves or regrouping data as discussed earlier in the chapter in an attempt to create a relationship. However, it would appear futile given the top-line statistics not revealing a relationship, therefore the assumptions not being met, to dig until one is found.

Despite the lack of a clear statistical relationship between the factors, the data certainly indicate links and differences between sets of scenarios as described above and also summarised here:

In total there are 62 sets of scenarios (e.g., 1 and 4, 2 and 5, 3 and 6) that can be compared after removing any that have a go-around situation within. Of these 62 sets, 47 comparisons show that scenarios 1, 2 and 3 resulted in a full-stop with less distance past the threshold than scenarios 4, 5 and 6; a majority at 75.8%.

Additionally, 60 out of the 62 comparable sets of scenarios showed a harder landing in terms of normal acceleration from scenarios 1, 2 and 3 when compared to their counterpart scenario 4, 5 or 6. This equates to 96.8%.

These figures simply illustrate that the instruction to avoid heavy landings had a significant effect on the study pilots and that as the heaviness reduced so the length of runway required increased.

6.3.5 **Bayesian Application**

Referring back to the Bayesian information networks of chapter 5, we now have the raw data that can be used to attempt to validate the predictive nature of probability (or error) migration. The occurrence of heavy landings reduced from 0.6714 to 0.1765 after the instruction (barrier) which is a reduction factor of 0.2628. In the context of the MATLab code, DF is multiplied by 0.2628 to get the new df and then the program executed. The resultant probability of nosewheel collapse is reduced from the AAIB data probability of 0.2627 to 0.0738 (a reduction factor of 0.2809).

From the simulator study data there were 13 cases considered to result in a nosewheel collapse (normal acceleration exceeded -2.75g). This results in a probability of nosewheel collapse pre-instruction (heavy-landing reducing barrier) of 0.17143 (12 out of 70 successful landings within scenarios 1 to 3).

Post-instruction there was only one case of a nosewheel collapse (normal acceleration > -2.75g on impact). This results in a probability of occurrence of 0.014706 (1 out of 68 successful landings within scenarios 4 to 6).

Binomial Test

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (1-tailed)
NWC	Group 1	1	1	.0147	.0738	.035[a,b]
	Group 2	0	67	.9853		
	Total		68	1.0000		

a. Alternative hypothesis states that the proportion of cases in the first group < .0738.

b. Based on Z Approximation.

Table 6-10 - Binomial Test of Significance for scenarios 4 to 6

Table 6-10 displays the results of a binomial test for the significance of any deviation from a predicted outcome (null hypothesis). The test shows that there is a significant difference between the nosewheel collapse probability in the Bayesian network and the flight simulator study (at $p < 0.05$) based on the predicted probability of nosewheel collapse from the Bayesian network (populated by AAIB data); 0.0738.

Binomial Test

		Category	N	Observed Prop.	Test Prop.	Asymp. Sig. (1-tailed)
NWC	Group 1	1	11	.157143	.262700	.026[a,b]
	Group 2	0	59	.842857		

Total			70	1.000000		

a. Alternative hypothesis states that the proportion of cases in the first group < .262700.

b. Based on Z Approximation.

Table 6-11 - Binomial Test of significance for scenarios 1 to 3

Based on the AAIB historical data, the proportion of nosewheel collapses for scenarios one to three was predicted as 0.2627. This binomial test shows that there is a statistically significant difference (at $p < 0.05$) between that prediction and the proportion of nosewheel collapses observed in the flight simulator experiment.

Although these binomial tests show that there are significant differences between the datasets (AAIB versus flight simulator study) it is the relationship between them that is more important. Figure 6-11 illustrates the difference in expected and observed values as used in the binomial test.

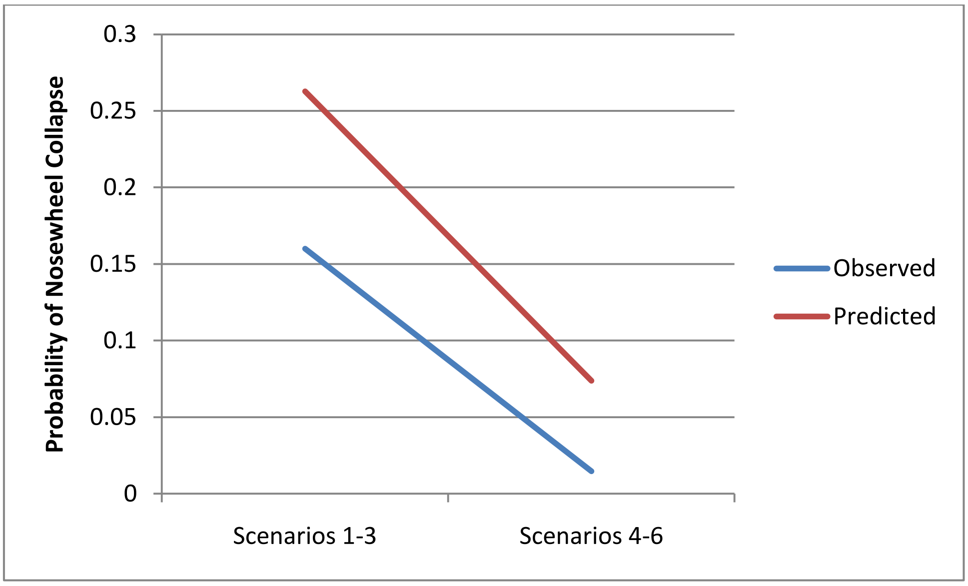


Figure 6-11- Lineplot of predicted versus observed Nosewheel collapse values

Despite the different significant differences of proportion in absolute terms, a visual inspection of the data illustrates a relatively similar change in probability pre and post barrier. Thus there appears to be some validity in the model with regards to predicting relative effects of barriers rather than absolute values. Further work could be carried out on attempting to normalise or calibrate the relationships for the data. This would involve increasing the sample size of the flight simulator participants to more reflect the AAIB data pool. These, and other limitations of using a flight simulator to validate these data, are expanded upon in section 6.5.

6.4 Other Results of Interest

Throughout the experiments comments were taken from the subjects outside the bounds of the experiments themselves in order to gain a deeper understanding of the study. A number of different types of pilots could be informally identified including those who were more nervous of committing a mistake and those who, possibly with behaviour modified by the fact it was a safe simulator environment, made riskier choices.

Those pilots who had a lot of time in very basic GA aircraft and flying into farm strips and small airfields reported finding it a very difficult exercise as their “seat of the pants” sensing had been removed in the artificial environment. Additional factors that weren’t present including a windsock and no realistic air noise that a few (although very few in comparison to the number of participants) said they found it hard to land without. It would be an interesting further study to continue these experiments and compare the data amongst gender and number of hours flown rather than on the purely objective levels that are of most importance to this chapter. Finally, some landings would be considered unacceptable regardless of the data collected. Certain pilots stalled the aircraft from a considerable height onto the ground, others were extremely eratic on the controls near the ground and a large number used flap well above the flap limiting speed shown on the air speed indicator. These are not issues that affect the crux of the study but are points that would make for interesting further study in the future.

Of all the interesting comments made the most significant were that the aircraft did not feel “real” in terms of handling and that it was very difficult to gauge height due to the graphics-limited visual cues. These are limits that can not be avoided on current GA simulators and as discussed above overall they have very little effect on the data collected.

6.5 Discussion

This validation study has done two things. It has shown that historical data can, to a certain extent, be used to predict future events. However, this is in approaching the event in a new way which looks at highlighting the barriers, links and nodes that will be affected by change, or are currently failing, rather than attempting to predict what the accident may ultimately present itself as. Previously all studies using Bayesian networks have used classification and eventual outcome taxonomies resulting in methods that attempt to investigate scenarios (Luxhøj and Kauffeld, 2003). In contrast, this new method is a study of the pathology of the system rather than the surface. This is the first time that Bayesian mathematics and information networks have been merged and used to attempt to identify the effect of barrier insertion and possible migration of information within a network not just towards a linear chain.

Secondly, a method has been introduced which may allow an approach similar to cost-benefit analysis in terms of predicting error migration through a network following manipulation of the links and barriers. This predictive method using bayesian mathematics can itself be manipulated by SMEs and other factors in order to elicit the most likely migration routes of information or error. This is further discussed in chapter 8.

Simulators have been used in aviation training and even in recreating aspects of aviation accident investigation. However, to the author's knowledge they have never been used to validate a method such as that described in this chapter and chapter 5. It is hoped that running such simulations may enable effective predictions to improve aviation safety and limit damaging effects of error migration. This provides a much more objective method of identifying issues related to barrier insertion within a system than methods such as SHA and ISHA (FAA, 2000) and the high-level assessments discussed earlier as part of MIL-STD-882E (US DoD, 2005). It appears that this method, not only through the Bayesian mathematics and iterative process discussed later in chapter 8, but also in the simple clarity of the illustrated network design may allow an investigator to identify relationships that are not apparent on a high level analysis or one that is dominated by linear chains as in those presented by the FAA (FAA, 2000).

What the results of this study have shown, with statistical significance, is that a strong verbal instruction does indeed work as inserting a barrier into the network. This would appear to be initial evidence then consider that all other 'barriers' discussed in e.g., MIL-STD-882E (US DoD, 2005) could be tested in a similar method. The landing network used in this study has been limited to a too high/too fast approach with limited outcomes and nodes in order to be able to manually work the mathematics. In the future this could be expanded to much more complex networks and relationships. However, even at this stage, evidence has been gathered that shows inserting a barrier has a significant effect on the presence (or activation) or other nodes within the network, i.e., when a barrier restricting the node "heavy landing" was inserted, the node "overrun" was much more readily activated. This can be extrapolated in larger networks to identify all possible migration routes of information given insertion of a barrier.

Due to the limited number of suitably qualified subjects the data could not be used to fully elicit a relationship between nodes and links. It is not overly surprising there is not a linear regression/correlation between the data given that the system being portrayed and investigated is itself a non-linear complex one. However, the statistics confirm that there are statistically significant relationships both within the data but more importantly possible relationships between the experimental data and the predicted AAIB data. Additionally it was seen in the introduction to this study that Bayesian networks can utilise distributions of values to model a relationship (Ale *et al.*, 2007) and this may account for the differences in exact values whilst a relationship may still exist. This gives the foundation required for a great deal of interesting future work to establish relationships and using an iterative process, eluded to in chapter 8, attempt to fully predict outcomes.

The node "Overrun" was identified in chapter 5 as having a subsequent nosewheel collapse probability of 0 in the AAIB data. However, this in itself would seem unlikely and is probably limited by the number of accidents studied. If the data is taken at face value, it can be seen that the ideal in this event is to migrate error towards that node. This results in the largest reduction of nosewheel collapse. In order to back up claims like this though the networks need to be expanded and the validation exercise continued.

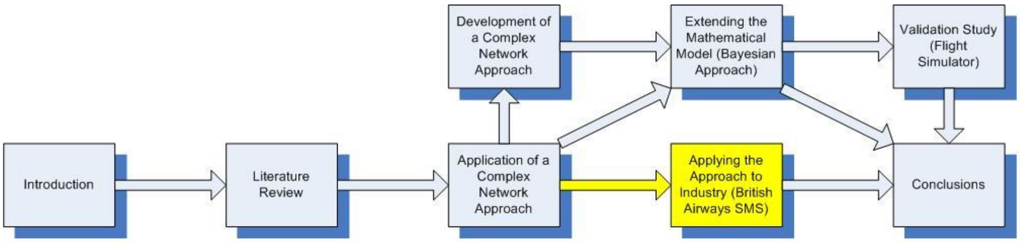
It is indeed a major limitation of this project that the landing scenario studied has been artificially isolated from the flight system. There needs to be this step back at the initial stages due to the fact that the programming and computation required to test would be unwieldy. It is the basic premise that the Bayesian information networks can help to predict error migration, albeit possibly only at a relative and not exact quantitative level, that is being tested not a fully developed model of flight.

This expansion would eventually look to include positive data and complete 3D networks for a particular phase of flight or even a series of 3D networks that are linked for the entire flight system. The next step though would be to take a few parallel scenarios that are linked in the information networks to predict the strength of barriers and the potential gains of predicting the probability, or error, migration. This future work would require a larger number of participants, improved simulator facilities and a larger database of GA accidents studied to populate the networks.

6.6 Summary

Through chapters 5 and 6 a theoretical and experimental extension of information networks has been developed. This has show real potential in merging the functions of information networks and Bayesian mathematics to produce a model which moves towards prediction and greater understanding of the wider system. Chapter 7 looks at industrial application and extension of the model which is a central tenet to the research of this thesis.

7 Incidents versus Accidents; an Industrial Study



Chapters 5 and 6 investigated the increased usability and function of the information network method as an accident investigation and mitigation technique with the use of Bayesian mathematics. Central themes of this research addressed in chapters thus far have included the comparison and use of both commercial and GA aviation and the need to address dominant linear models. The final tenet of this research is that it remains firmly rooted in applicability and usability to improve real-life industry.

Incidents, or “near-misses”, can be defined as ranging from partial penetration of defences to situations in which all the available safeguards were defeated but no actual losses were sustained. As such they cover a whole multitude of sins and would hopefully therefore promulgate a multitude of information for safety development. This chapter sets out to develop the way in which industry is currently working with accidents. Incidents, in relation to accidents and their potential use in accident investigation, were discussed during the review of literature for the thesis (chapter 2). Of particular interest to this research project, is a concept of taking such incidents and visualising their outcome if the corrective actions hadn’t stopped the chain of events. Thomas (1994) had a vision of “safety imagination” whereby he suggested one was forced to visualise the development of “near-miss” events into accidents. This reflects a method whereby the possible outcome of incidents was related to actual outcomes of accidents. Thus, the causal pathways compared, one for the common cause hypothesis investigation, but in future terms as a tool for accident prevention.

This chapter centralises that goal, takes the arguments outlined in earlier chapters of this thesis, and in work closely centred on real-industry, attempting to improve on the current use of incidents and near-misses. The author was approached by the safety management team manager at British Airways (BA); a legacy carrier and one of the world's largest airlines. British Airways were interested in the work being carried out in accident investigation and were looking for novel applications to drive forward a new generation of incident reporting and risk rating tools. The majority of this chapter addresses the key elements of this work and then draws out the issues central to this thesis in the concluding sections.

The structure of this work with BA is outlined here for clarity:

Introduction: Section 7.1 introduces Safety Management Systems (SMS) before looking at the development of British Airways' SMS in particular. Subsection 7.1.2 addresses the main limitations of the current methods and models being used. This draws support from relevant literature, subject matter experts and those working within the safety management team at BA themselves.

Section 7.2 continues the introduction by reviewing best practice from across industry in order to establish the dominant models in use today and learn any lessons that are available. This section ends with a summary of the dominant models and methods in use across complex risk industries.

Finally, section 7.3 concludes the introduction by addressing the true value of risk with particular reference to its value to British Airways and the wider aviation community. This includes breaking free from the constraints of Risk = Severity x Frequency.

Method and Results: This part of the project looks at developing alternative models. Section 7.4.1 introduces a novel model of risk rating and incident investigation for use within BA. 7.4.2 takes this further and provides the reader with a walkthrough style guide of the model's use in its current guise. Finally within this section, 7.4.3 looks at the validation and implementation of the new method. Annexe 5 contains a letter of appreciation from BA's manager of operational risk.

Conclusions: Section 7.5 then returns to the place of this work within the bigger picture that is the thesis. Benefits and limitations of working with industry are addressed and the further work required to continue taking forward the model discussed.

It may be helpful for the reader, and reflects the current status of this study, to think of this as a three-stage process. This is displayed in figure 7-1 and not only illustrates the three-stage process but also reflects the three-part chapter. The first part is dictated by the practices and safety system in place at BA before the work discussed in this thesis. The middle section reflects the work of this study and the position BA are now in; this is an interim stage. The final section of the study and chapter reflect the future for the method, model and BA.

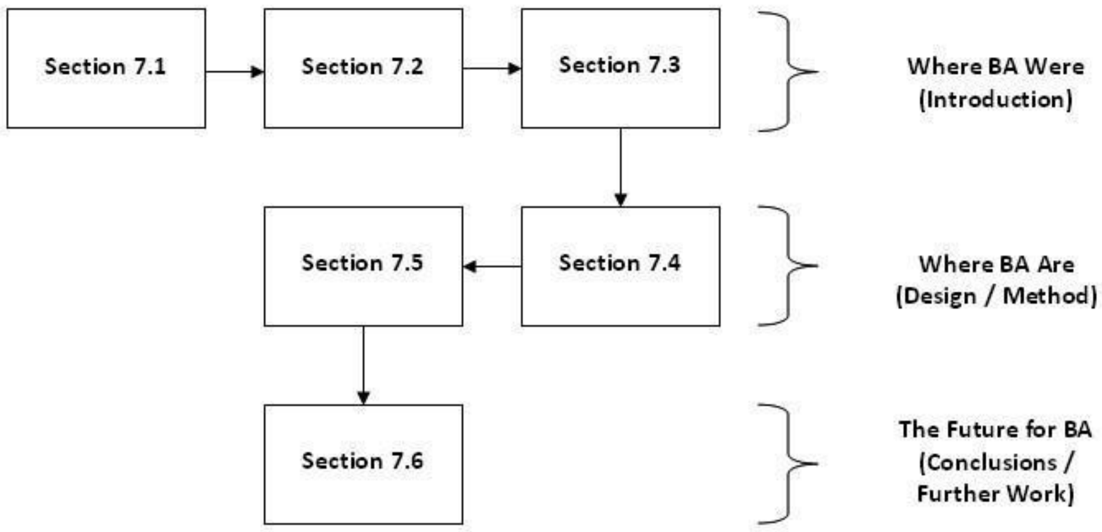


Figure 7-1 – The three-stage process of the BA project

7.1 Safety Management Systems within Industry

The International Civil Aviation Organisation (ICAO) mandates, in annexe 6 (2009), that aircraft operators, such as BA, must establish a Safety Management System beyond that required as a state safety system. The International Air Transport Association (IATA) defines a SMS as "…a systematic approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures." (IATA Website, July 2009). IATA goes on to state that a SMS should be capable of identifying safety hazards, managing remedial action when necessary, providing a method of monitoring and assessing safety, and to continuously improve safety levels within an organisation.

ICAO have amended paragraph 3.2 in annex 6 and produced a Safety Management Manual (Document 9859) to detail the requirements. Further than this, BA are required to abide by national, or in BA's case European, regulators. The European Aviation Safety Agency (EASA; the successor to the Joint Aviation Authority (JAA)) have produced a document (EU-OPS paragraph OPS 1.037) which details the ways in which EASA and EASA state operators must comply with ICAO. The exact wording of these documents can be found through the EASA website but for the purposes of this chapter the requirements and aims of any such SMS are as set out in the paragraph above.

7.1.1 **The development of BASIS to date**

In this introductory section the design and method of use of the current SMS within BA, BASIS, are reviewed. This lays the foundation to discuss the limitations and problems encountered in its current guise in section 7.1.2.

In 2009 IATA is including SMS reviews in its IATA Operational Safety Audit (IOSA). This follows well with the ever increasing commitment to safety and management of risk that airlines are showing. However, even back in the late 1990s, BA had been honing a Safety Management system for a couple of decades. It was during this time that the British Airways Safety Information System (BASIS) gained popular usage, both within and outside of BA to coincide with the popularity of organisational safety models such as those propagated by Reason (1997) and Turner and Pidgeon (1997). The pivotal three streams from which BASIS was populated were Air Safety Reporting (ASR; see Annexe 1 for copy), Operational Quality Monitoring (FDR; AKA Flight Data Recording), and Human Factors Reporting (HFR). BA have stipulated tougher inclusion criteria for the requirement of submitting an ASR (with approximately 8000 raised per year) than is compulsory by the Civil Aviation Authority's (CAA) Mandatory Occurrence Reporting Programme (MORs). The ASR programme is primarily concerned with establishing *what* happened and is an excellent tool for identifying the day to day safety problems. FDR is an automatic monitoring system of certain flight parameters such as speeds, configurations and handling characteristics. FDR was born out of its predecessor named SESMA; Safety Event Search and Master Analysis (O'Leary et al., 2002). Any non-standard (or outside allowed normal limits) events are automatically recorded and the data can be investigated. There is an expectation within the airline that an ASR is submitted voluntarily by a pilot to coincide with them receiving the FDR data; thus showing a level of integrity and honesty that is paramount. Finally, any ASR that is submitted initially had a voluntary HFR questionnaire sent to those involved. This system is completely confidential (unlike the previous two mentioned) and aims to elicit more information on the *why* and *how* of an event rather than the *what*. It is in this area of HFR working with the ASR that most potential for proactive safety management is found and that is central to the aims of this thesis. These three elements are core to the Incident

Reporting Programme (and thus the BA SMS) for BA. An Incident Reporting Programme is well described by Van der Schaaf's seven step framework (1995):

1. Detection (usually through reporting)
2. Selection for further analysis
3. Detailed description and investigation
4. Classification of the causes
5. Recognition and computation of patterns and priorities
6. Interpretation of results of investigation for recommendations
7. Evaluation and monitoring

In the early 2000s the BA ASR program had been adopted by well over 100 airlines world-wide and demonstrates the pedigree of the format (O'Leary et al., 2002). Indeed, O'Leary et al. (2002) state that in a few short years the ASRs and BASIS were key to an overall improved safety culture of reporting and managing risk. Following on from the original winBASIS (the name for the software behind the British Airways SMS at the time) being sold off in the early 2000s, BA set about developing a new generation of BASIS known as eBASIS. It is this generation of the SMS program that is still in use today.

As a central part of this risk assessment and prioritisation procedure, "analysis and assessment of reports is principally reliant on trained investigators' professional judgement" (Macrae *et al.*, 2002). So how are the received data currently analysed within BASIS?

Once an ASR is raised, it is converted into an electronic format and entered onto eBASIS. Professional judgement of the operator determines the salient features of each incident including likely causal factors, risk to flight safety and operational integrity.

There are four generalised steps to the task of analysis as follows:

1. The text is input and technical details are reviewed. A summary is then written identifying salient points and important elements of each incident such as those that characterise their relationships. A causal structure is then inferred. 2. In order to allow classification of an event, suitable keywords are applied. This step is intended to allow for trend analysis of the full incident database. Keywords are applied to causes, effects,

influencing factors at different levels according to the event that took place e.g. operational effects, technical causes and filtering down to the specifics of that particular incident.

3. A risk category is assigned to each incident so that historical trend analysis and the prioritisation of response to incident reports can be carried out. Implicitly though, this step embodies the consideration of each incident's potential impact on flight safety and BA's business as a whole. In the initial version of eBASIS, an assessment of risk category is made according to a 3 x 3 risk-matrix comprising severity vs probability of recurrence (a standardised risk-matrix across industries). Later this was replaced with a 5 x 5 risk matrix again based on standard theories of risk categorisation but with the aim of allowing more detailed analysis and trending. This risk categorisation process results in an ordinal 5 point scale of risk: A-E.

Severity	**Occurrence**					
		Minimal	Low	Medium	High	V. High
	V. High	100 (A)				
	High	71 (B)	86 (B)	100 (A)		
	Medium	35 (C)	43 (C)	55 (C)	71 (B)	
	Low	15 (D)	19 (D)	25 (D)	35 (C)	
	Minimal	1 (E)	3 (E)	6 (E)	10 (E)	15 (D)

Table 7-1 - BA Flight Safety Risk Rating Matrix with Letter Value

Risk	Response
A	AAIB/State Investigation
B	Company/BASI 4 Investigation
C	Departmental Action Required

D	Monitoring Required Only
E	Statistical Data Only

Table 7-2 - BA Flight Safety Risk Rating Guidance

The ordinal value given to an event is reliant upon the company's response to that event and "…allocation relies on the expert judgement of safety officers and investigators." (Macrae *et al.*, 2002)

4. Some events require further action such as further investigation or a callback to the staff involved in the incident. These actions are assigned within eBASIS dependent on their letter rating (Table7-2) and can be monitored by safety data personnel. Finally, an incident can be considered closed when all required steps have been fulfilled and no further action remains.

Further information about the intended use of ASR, FDR and HFR data and how it was originally analysed can be found in e.g., O'Leary et al. (2002), and O'Leary (2002a).

7.1.2 **Limitations of use and requirement for further development**

The aim of the rest of this chapter is to highlight and tackle some of the issues that BA is facing in the current use of its eBASIS tools. BA safety managers have expressed concerns with certain limitations of the current system and were looking for an original and novel method to develop and take the SMS forward in a unified way. BA were very interested in the models being developed within this thesis and requested that I work to apply them to the SMS. As such, a significant length of time was spent working within the BA safety management team. In line with this, it was hoped that the network-based approach to system investigation may elicit a more useful and proactive method of safety management.

As outlined above there are a number of streams for the supply of safety data and information. However, key to developing safety models and methodology is to improve the cohesion and unification of how safety data are gathered, and more importantly how they are actioned. This is particularly true within an organisation such as British Airways where demands on safety data are increasing alongside expansion of services and equipment. In discussion with BA's Safety Management Services team a number of issues were highlighted as concerns in the current system and areas that could lead to potential improvements.

The rest of this section will highlight the eight key issues that arose as areas of concern for the current eBASIS SMS system during discussions and research. Following on from this, the issues will be expanded upon and then two mini case-studies will represent the main issues before then looking at ways of improving the situation with reference to best practice and literature.

1. Frequency Skew:

The primary concern raised by BA with the current risk rating method is that using current matrices, obviously less important events are being reported as having a serious effect on operations. With the use of matrices, probability and severity are given equal values in terms of the effect they have on the overall scoring of an event so if an event has an unusually high frequency, despite a low severity, it can be reported that such an event has an undue risk. The issue within the current system is that if an event is given the risk rating of 1 and it occurs once its value is 1. However, should its frequency increase to, e.g., 10 occurrences, suddenly each event would be valued as 10 (i.e. risk 1 x frequency 10) and the ten occurrences amount to a risk of 100 to the company. This logarithmic rise distorts corporate risk data.

2. Lack of Theoretical Models and Cohesion:

Michael O'Leary and the team that set up winBASIS in the 1990s predominantly relied upon subject matter experts and the knowledge and judgement of those people applying a risk rating methodology. This has its intrinsic issues in terms of items 5, 6 and 7 below but also in that without a solid scientific model as a basis it may be that development and progression may be stunted.

3. Granularity of D and E rated events:

As would be expected within an airline, most events recorded and reported are low severity and therefore fit into what BA classifies as a D or E event. Since the majority of incidents are reported at this level and there is only a 0-100 risk rating point variation within them, it is often very difficult to gain the granularity that may allow for separation and further study of specific events and incidents or separate out those which are more, or less, serious.

4. Five Different Risk-Rating Matrices:

Without a solid scientific foundation at the centre of the current system, each department has developed its own interpretation of events and with that their own classifications, rating requirements and even rating matrices. There was a shift from 3x3 matrices to 5x5 (Table 7-1) but this didn't result in the enhanced granularity that was expected. This is obviously not conducive to the cohesive safety management method reflecting a system as a whole. For this reason, BA were looking to take steps towards a common incident management system.

5. **Retention of Knowledge:**

BA is currently very aware of the knowledge levels they have fostered and developed after the past ten or twenty years. However, the current methodology leaves very little real chance of converting individual knowledge into system knowledge. As such, learning and retention of knowledge is a concern of the team at present should individuals leave or new safety specialists join. To date, training and knowledge sharing has taken on the approach similar to that of an apprenticeship and working closely with a suitably experienced safety specialist.

6. **Subjectivity of Ratings:**

Without clear guidelines for applying ratings to events, it is often the case that certain events are considered key or important at a particular time and these often receive more attention than some other events. Due to the nature of the risk rating on an individual specialist's basis, subjectivity of ratings is an issue that may affect the resultant risk based decisions.

7. **Replicability of Ratings:**

Again, as with subjectivity and individual knowledge and experience versus objectivity and system, or collective knowledge, there are issues with the replicability of ratings especially between individual risk raters.

8. **Operational vs Occupational Risk:**

These have developed to be two very distinct areas of risk for BA's current risk rating methodology and again a method will be sought that helps to draw together all aspects of safety or at least be capable of integrating them.

"The problem to those with a high level responsibility for ensuring aviation safety is to identify the highest priorities to ensure that they are using resources effectively" (Rose, 2008, p.1381). It is therefore an essential requirement for a risk rating method or SMS that the highest priorities produced from any such process are indeed reflecting the most serious and relevant safety issues to the system. The eight issues above illustrate that this is not always the case for the current iteration of eBASIS. The Safety Management Services Team Manager has to present regular risk-based safety reports to the BA board and to identify key areas or issues that the company could make best use of resources in terms of time and money in order to improve safety. The BA management team reported that during these management meetings the statistics were being skewed overwhelmingly by the issues outlined above leaving high severity, low frequency events in particular in the shadows. This is key to the argument for a new and very different method of risk rating and safety management. Frequency currently skews the identification of central issues and therefore effort and resources are being wasted in the wrong areas; this would suggest that "risk" as a value is not sufficient in traditional terms of frequency and severity, and this is examined in more detail in section 7.4.

Whilst interviewing and observing winBASIS specialists in action, Macrae (2002) reported that all of "the analysis and risk assessment of flight safety incident reports within BASIS relies on the expert judgement of trained investigators". There is a danger, in this being the sole method, of not retaining knowledge and information, but this also highlights the issues of subjectivity and lack of solid foundation principles and objective limitations through which to work. Macrae (2002) goes on to say that "…experts may possess different tacit models of accident and human error". Lucas (1990) spoke of three general models which may be held at the expense of all others by an individual. Those that focus on the individual (issues such as Health & Safety or coercion), models based on what is seen as the more traditional risk management focus (i.e. engineering and HMI), and finally, systems safety approaches incorporating organisational safety. This appears to have happened within BA and given rise to the different risk matrices with slightly different agendas for each department.

Again, the issue of subjectivity is brought to the forefront due to the reliance on specialist knowledge and individuals (although it must be reiterated that these individuals do have a lot of knowledge and often do a great job) as we see "the assessors' evaluation of the risk of individual incidents or their underlying factors appeared to be heavily weighted by the recency and frequency of similar events, or current topics of interest each analyst was keeping in mind" (Macrae 2002). This form of bias is a possible way for important and underlying issues to be missed in my opinion. Therefore, it would make sense to have a more objective structure to the process to be followed regardless of "hot topics" (a BA term in safety reports and discussions). We know by now that recent events (as implicated by recency or "hot topic" biases) do not always predict future incidents but recurring safety lapses (i.e. barrier breaches) may do so. This refers back to the literature covered in chapters 2, 5 and 6 in terms of maximising the usefulness of incidents in understanding the system's safety issues as a whole (e.g., Dekker and Hollnagel (1999)).

Macrae's take on BA's ASR "analysis and assessment of reports is principally reliant on trained investigators' professional judgement". Key therefore to moving forward and progressing the SMS is to look at removing subjectivity and increase objectivity as well as improving knowledge retention, reducing frequency bias and addressing as many of the other eight issues as possible.

Next, two examples summarising polarised yet equally important issues are introduced which formed central discussion points with BA as they address many of the flaws and issues currently facing eBASIS and the BA SMS.

- Example One: Bag falling from overhead locker

With the large number of flights BA operate per year and therefore the high number of bags and passengers transported there are occasions when a bag falls from an overhead locker before, during or after flight. These events are therefore considered to be high frequency but owing to the fact that often no injury or damage occurs and threat to life is minimal they are classified as low severity events. However, the overwhelming effect of the high frequency is to skew BA's safety data to suggest that this is one of the greatest dangers in safety terms that BA must face. The Safety Data Team obviously apply caveats to such data when reporting to the board but this is symptomatic of a larger problem where frequency appears to have too much power in determining unsafe events.

- Example Two: The crash of Air France Flight 4590 (Concorde), 25 July 2000

This event is truly at the opposite end of the spectrum to the bag case above. The crash was extremely complex in nature, as are most accidents, and gladly a very low frequency type event. What is important to BA though is whether, should this accident occur with them, the event could be termed preventable. This is not necessarily from a legal standpoint or a moral one but more specifically is there a way of recognising the information and possible issues surrounding such an event before it happens. If there is found to be a way, does BA's SMS draw these issues out and highlight real risks effectively. Alternatively, does the current SMS maintain the possibility that important information is being lost or hidden by relatively unimportant safety matters.

As a result of the work set out in this section with BA's safety management team a summary of aims could be made. In order to do this effectively, it is best to refer back to Van der Schaaf's (1995) seven-step framework:

Detection (reporting) needs to be driven by the needs of the model and method in use and therefore it will be paramount that this research is conducted without the limitations imposed by current reporting practices. Intrinsic to the model must be a method for selecting those incidents that require further investigation and so a reporting grade or rating is required. There needs to be more understanding of each incident so a method that encourages the risk-rater to fully-examine each incident including the background and outcomes is essential. Potential for prioritising and centralising important issues is also required for the method to be effective. Importantly, a pathway for feedback and evaluation of the method would be advantageous.

7.2 "They've Rebadged it you fool!"[8]; A Review of best practice in aviation and beyond

The final part of this study's introduction (sections 7.2 and 7.3) looks into wider aviation and other complex risk industry practices. This identifies the gaps in the industry that can be used together with the gaps identified within BA's own processes to underpin the development of a new approach in section 7.4. The major industries within the literature of complex systems and risk include aviation, rail and petrochemical processing. These areas directed a review of current practice in order to ascertain what models were already being applied in risk management. It was found that although there was a plethora of accident investigation techniques both within and outside aviation, such as the Human Factors Analysis and Classification (HFACS) System (Shappell and Wiegmann, 2000), actual risk rating and safety management methodologies were centred on matrices. A Hazard and Operability (HAZOP) study (Kletz, 1983) is well used within these complex industries yet they often become unwieldy and time-consuming therefore making them unpractical for application to the large number of incidents BA has reported each year. The vast majority of techniques studying accidents and incidents, and to a certain extent the current format of eBASIS, are essentially classification methods. As the title, somewhat tongue in cheek suggests, there is a danger in these methods that incidents or events are merely grouped together and relabelled. This may help to understand the current state of safety and trend analysis but does very little in the

[8] © BBC, "I'm Alan Partridge", Steve Coogan 1997.

way of truly gaining any further insight into what is going on underneath; the pathology of a system. That is not to say, however, that the use of other analyses is precluded when an incident is deemed to require it or is of sufficient importance. Rather, as an everyday occurrence, suitability to BA's requirements were not found.

There is limited use of accident investigation methodologies to actually rate within a system and they are often used alongside, or even because of, risk-rating methods applying an important enough severity to an event. There has been much work in the petrochemical industry in particular though to investigate and study more advanced methods which move away from rigid matrix standards. The following paragraphs summarise the main methods which are presently the industry standard and highlight areas of improvement but also where the methods fall short of what BA require.

Risk ranking matrices based upon the edict "Risk = Frequency x Severity (R=FS)" are still by far the most common basis to risk ranking methodologies used in safety-critical industries. A comprehensive review of the literature and working documents from across the rail, petrochemical, health, marine and aviation industries did not reveal any safety model which was not based on a R=FS structure. Particularly in the aviation industry, this comes as no surprise since eBASIS is based upon the most successful implementation of risk ranking in aviation thus far (i.e., winBASIS).

Even within risk matrices there are variations depending upon intended output. Tables 7-3 to 7-5 (Railtrack, 2000) illustrate some of these variations. In all matrices, the higher the rating, the more priority should be assigned to the hazard. What we see with these, however, are biases and skews to risk ranking figures which reflect what the company is most concerned with.

Table 7-3 is the most simple and most commonly used type of matrix weighting method with figures based on severity and frequency. Here, the figures in the table are derived as a multiplicative model, i.e., frequency x severity. Table 7-4 is preferred by some practitioners as it assigns the same rank to risks which are associated with a similar number of equivalent fatalities per year due to the fact that it is additive in nature, i.e., frequency + severity. Table 7-5, on the other hand, assigns similar ranks to risks which are associated with a similar number of equivalent fatalities per year, but is biased to assign higher ranks to risks with more severe consequences; i.e., it is a weighted model based on increased severity yielding increased rating scores.

Severity of Potential Harm/Loss

	5	**4**	**3**	**2**	**1**
Frequency	Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly	25	20	15	10	5
4= Monthly to yearly	20	16	12	8	4
3=yearly to 10-yearly	15	12	9	6	3
2=10-yearly to 100-yearly	10	8	6	4	2
1= Less often than 100-yearly	5	4	3	2	1

Table 7-3 - Example hazard ranking matrix

	Severity of Potential Harm/Loss				
	5	**4**	**3**	**2**	**1**
Frequency	Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly	10	9	8	7	6
4= Monthly to yearly	9	8	7	6	5
3=yearly to 10-yearly	8	7	6	5	4
2=10-yearly to 100-yearly	7	6	5	4	3
1= Less often than 100-yearly	6	5	4	3	2

Table 7-4 - Example skewed hazard ranking matrix

	Severity of Potential Harm/Loss				
	5	**4**	**3**	**2**	**1**
Frequency	Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly	25	23	20	16	11
4= Monthly to yearly	24	21	17	12	7
3=yearly to 10-yearly	22	18	13	8	4
2=10-yearly to 100-yearly	19	14	9	5	2
1= Less often than 100-yearly	15	10	6	3	1

Table 7-5 - Example biased hazard ranking matrix

Despite the ability of these risk matrix models to be manipulated by the user to magnify the importance of certain types of incident, they are very limited by the type and quality of data that can be input. In order to develop the current risk rating system employed by BA the natural starting point is to look at updating, or developing the current sets of matrices. The matrices currently in use are relatively simple and a search of the literature, and in particular risk documents for large public and private organisations, yield a number of developments to these methods. By adding additional broad-term groupings such as those represented in figure 7-2, it is possible to extend the scope of these matrices. Doing so would allow for greater cross-departmental integration of matrices and reduce the number of different models in use. This would be advantageous to the overall risk methodology and safety system in that it would help to validate and support cross-departmental, and hence organisation wide, analyses of risk (e.g., in reports to the board). Additional groupings (e.g., for engineering or cabin crew reports) could lead to several descriptors from different areas, thus providing similar risk rankings based on a company-wide implementation.

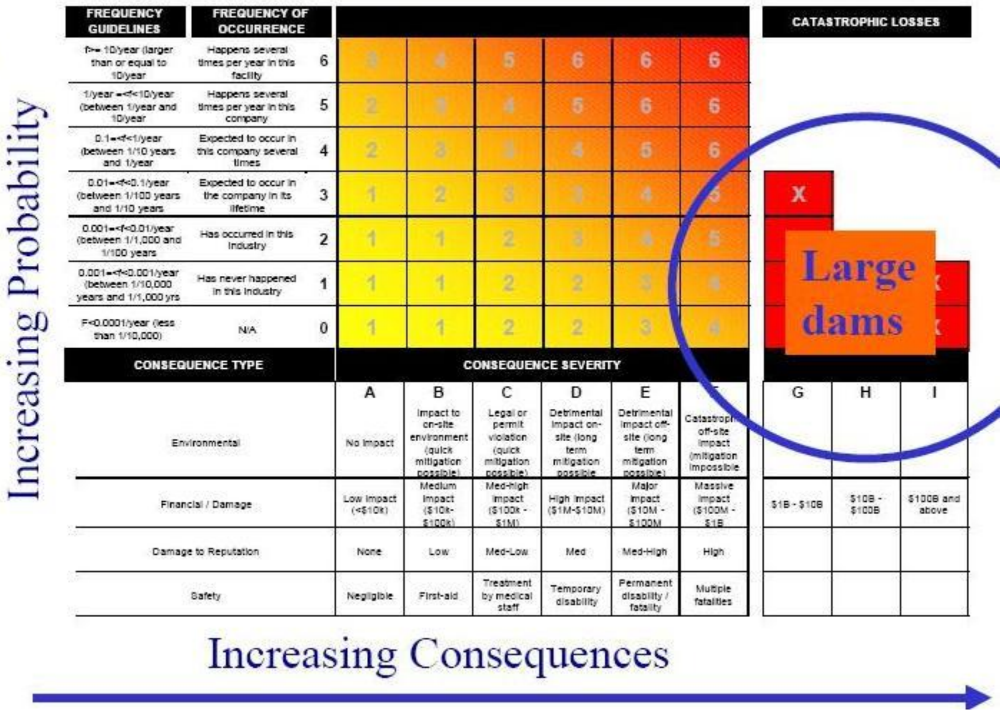


Figure 7-2 - Illustrating possible additional levels to a risk matrix (FEMA, 2002)

Nevertheless, since these matrices are still based upon a rigid R=FS structure, none of them will overcome the issues in eBASIS which restrict the effectiveness of frequency in eliciting the required information. The need to remove this skew leads us to eliminate risk matrices based on severity and frequency alone as possible methods to take forward.

To move away from the skewed effect of frequency on incidents, literature for non-frequency based risk methodologies was reviewed in order to develop a novel risk ranking method. Methods based on non-frequency models, propagated and in actual use within organisations, are few and far between. Fault-trees are often used within 'hard' engineering tasks where probability of failure data is commonplace. However, there were very few examples of potentially non-linear methods that could also incorporate Human Factors issues. One such example that appeared to have potential to extend beyond the linear and incorporate Human Factors issues is Layers of Protection Analysis (LoPA).

LoPA (Figure 7-3) was developed by the Center for Chemical Process Safety (CCPS) in 2001. LoPA is a semi-quantitative risk assessment method for evaluating scenario risk, whether existing safeguards are adequate, or whether the addition of supplemental safeguards, or barriers, is necessary. In this way it encapsulates the theoretical background required to develop a risk ranking structure not based solely on frequency.

LoPA is used as a method for evaluating the risks identified in a qualitative safety measurement tool such as a Process Hazard Analysis (PHA). These identify possible sources of failure and then attempt to identify the barriers present, or required, through the LoPA strategy.

For use as a method within eBASIS LoPA must be changed to focus more interest on the link between number of safety barriers remaining following an incident and severity of that incident. In relation to the incident reports that populate eBASIS, the initiating event can be seen as the descriptors used in the database. At present there is no requirement to formally identify what type of event the descriptor identified in a report was leading to, but this analysis of descriptors and identification of the possible event outcomes would need to be carried out for LoPA to work.

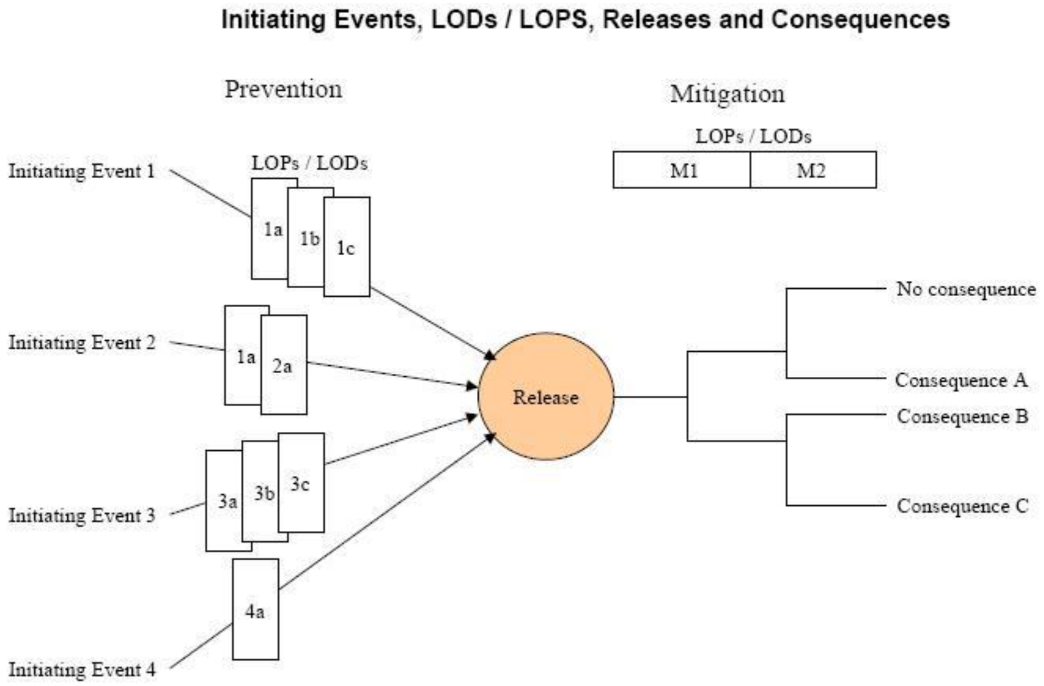


Figure 7-3 - Generic LoPA diagram depicting basis of model (CCPS, 2001)

Prior to rolling out the method across eBASIS, a number of core incidents would have to be studied and worked on to provide groupings of descriptors that lead to particular immediate events (e.g., GPWS warning, incorrect configuration etc.) as well as identifying possible event outcomes (e.g., CFIT, runway excursion etc.). Pathways, or networks, would be formed for these incidents and safety barriers identified at all stages from any descriptor event occurring to any potential outcome associated with that descriptor.

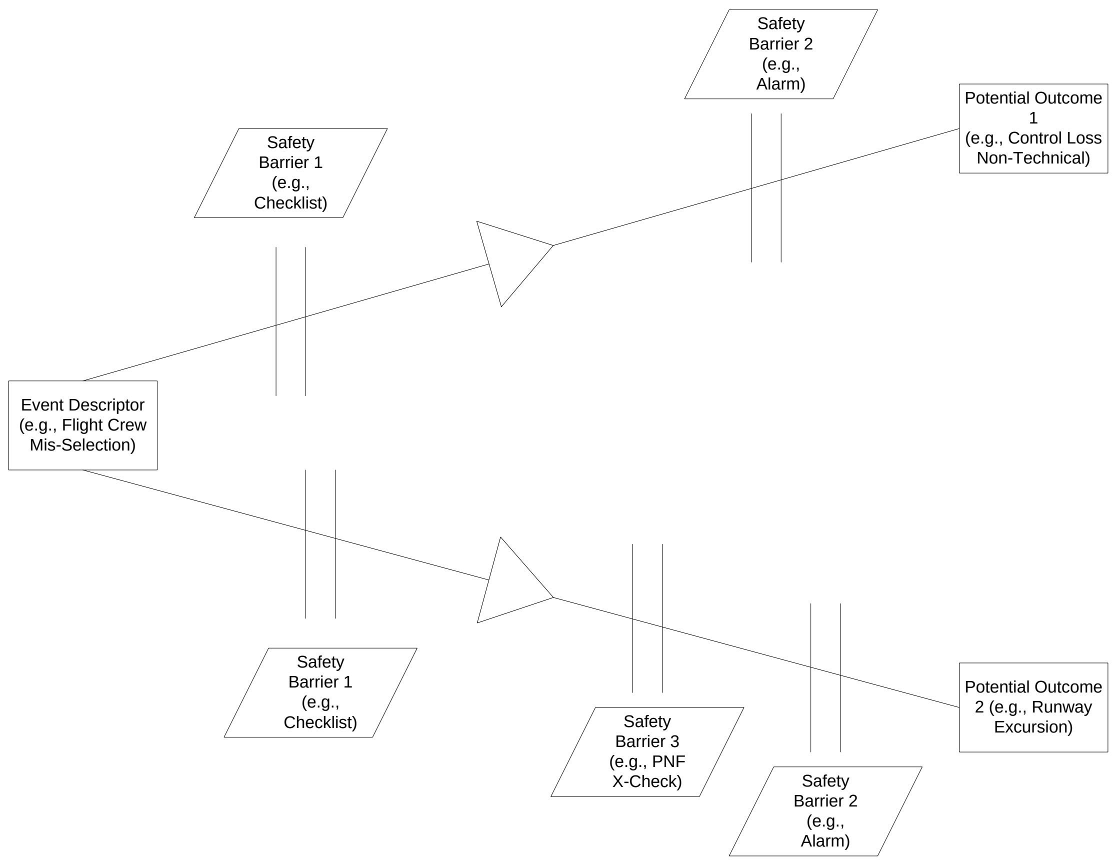


Figure 7-4 - Illustration of how an event descriptor links (via safety barriers) to several possible potential outcomes

In figure 7-4, the mitigation stages of the LoPA diagram have been removed so as to concentrate on the pre-event stages which are most important in an eBASIS investigation. As illustrated, there may be a different number of safety barriers from a single descriptor towards each potential outcome related to that event. The relative risk of such an event descriptor occurring (i.e., being reported) is therefore associated with the number of safety barriers present between it and the potential outcome, and the number of safety barriers which have been breached before the event was averted.

Prior to rolling out the method across eBASIS, a number of core incidents would have to be studied and worked on to provide groupings of descriptors that lead to particular immediate events (e.g., GPWS warning, incorrect configuration etc.) as well as identifying possible event outcomes (e.g., CFIT, runway excursion etc.). Pathways, or networks, would be formed for these incidents and safety barriers identified at all stages from any descriptor event occurring to any potential outcome associated with that descriptor.

In its original formulation within chemical process safety, LoPA utilised “Independent Protection Layers” (IPLs), whose failure was defined as being independent of any other failure in the scenario. These IPLs exclude Human Factors issues on the basis that the method was not designed to cover areas already analysed in a PHA. There is, however, "…no inherent reason these issues cannot be considered by LoPA." (Baybutt, 2002) IPLs are defined by their Probability of Failure upon Demand (PFD), which is simpler for mechanical barriers than it is for Human Factors issues. This is therefore an area that requires further review and more detailed data validation before it could be applied to a system such as BA's operations.

Each barrier (IPL) is given a value, originally in terms of a PFD, but this can be modified to reflect the potency of the safety feature (e.g., alarm < override feature but alarm > PNF X-check). It is envisaged that the "pathway" from descriptor event to potential outcome will be quantified against data and specialist knowledge. Safety barriers can then also be assigned safety values given the descriptor and potential outcome pairing. Although Human Factors values are not included in an original LoPA analysis, in the current project we proposed to modify and utilise the tool in a very different way. Notwithstanding these modifications, the method will still be based on its solid theoretical foundations. It can be agreed as good practice to separate the hard safety barriers from the more Human Factors types and to limit the effectiveness of the latter on the model outcome (Waller, 2004).

LoPA in its own right has been found to be too restrictive when attempts are made to apply it to an incident or event. The time required to develop a LoPA case for each event would also be prohibitive in a commercial organisation such as British Airways where the number of events per year is high (as in all aviation companies). In addition, the theory works well at a level where mechanical barriers (i.e. barriers which can have probabilities applied to them post-destructive testing) are the primary concern but lacks the fluidity required to identify the less quantifiable human-factors issues within a complex system. Although these probabilities of failure do have an important place in investigation, we believe it is more appropriate to develop a method that can be based on historical data as indicators of current and future risk rather than attempting to develop LoPA style p-values.

Barrier theory is, as its name suggests, a group of theories and foundations upon which ideas can formulate and thus makes an ideal candidate for incorporation in a risk rating methodology. Barriers, or levels of removal from a potential outcome, do not require exact "probabilities" or "distances" but instead create a relative safety system. Each event is considered relative not only to all other events (as in standard risk matrix type systems) but also relative to an eventual, or possible, outcome. This gives a truer audit of system safety in relation to negative events.

As already has been seen throughout this thesis there are numerous uses of barriers in theories and for illustrating safety models. System safety practices such as MIL-STD-882E (US DoD, 2005) refer to the implementation of mishap mitigation measures which envelop a wide variety of barrier types including at design strategies, physical barriers and additional training. Outside of the military barriers too are inextricably linked to the safety practices legislated by aviation authorities (e.g., FAA, 2000). At an academic level safety specialists such as Ale (2007) have used barriers within fault trees to illustrate the ability to prevent accident 'pathways'. Luxhøj (2002) applies barrier theory to complex Bayesian networks of complex systems stating that "according to the algorithms of Bayesian Belief Networks, that if the state of the defense system is known, and is working properly, then the relationship between the sequence of errors and the accident is blocked". This association of a variety of barriers with models and techniques sets precedence for using barriers within safety but to the author's knowledge barriers have never been actively linked to risk rating events or a system at the level of information elements. Neither has the model underpinning the introduction of barriers had information networks at its centre. Ale *et al.* (2005 & 2007) when looking at attempting to model the aviation system in order to utilise barrier theory and understand aviation accidents used event sequence diagrams as their initial basis and introduced some Bayesian theory into this. BA had looked at using ESDs in 1999 under O'Leary so there was some evidence that these would work. What was of more interest to the study was to analyse a deeper level than ESDs tend to.

With this centralisation of safety barriers and potential outcome risk we remove the bias and skew of frequency in the analysis. Through the process of deriving a safety barrier pathway, a risk value is produced based on the potential outcome risk minus any safety barriers that remained intact to prevent the scenario. This risk value can then be factored to fit into the eBASIS risk rating system organisation-wide.

As Figure 7-5 shows, the concept of centralising the potential outcome of an event and the use of barriers, or defences, has been introduced by British Airways (albeit in matrix format) and show the recommendations of this thesis are consistent with BA practice. Our literature reviews and methodology critiques have validated this as a scientifically solid foundation on which to build a risk rating methodology.

Potential Consequences V	OPERATIONAL RISK MATRIX				
Major Accident with significant loss of life	D	C	B	A	A
Limited accident scenario with some loss of life	D	C	B	A	A
Minor accident with some injuries and damage	E	D	C	B	B
Degradation of safety margins with little direct consequences	E	E	E	D	D
Defences --->>	Normal human intervention was why it didn't happen	Reliable hard defences was why it didn't happen	Abnormal human intervention was why it didn't happen	Providence was only reason this was not an accident	No defences left this was an accident

Potential Consequences V	OCCUPATIONAL INJURY RISK MATRIX				
Fatality	D	C	B	A	A
Major Injury resulting in permanent disability	D	C	B	A	A
Significant Injury but usually recoverable	E	D	C	B	B
Minor injury	E	E	E	D	D
Defences --->>	Normal human intervention was why it didn't happen	Reliable hard defences was why it didn't happen	Abnormal human intervention was why it didn't happen	Providence was only reason this was not an accident	No defences left this was an accident

Figure 7-5 - Risk Matrices reproduced from British Airways working document

Table 7-6 summarises the main methodologies used in the primary complex-system industries to date. The biggest issue facing a company such as BA when comparing with these other industries is that more than ever, there is little to separate Human Factors from hard factors such as engineering issues. In some industries it is easier to use hard-barriers to prevent negative events and to limit the input of humans to some extent. Some industries, despite still being complex, also have a more limited variety of possible outcomes. Due to these reasons it appears that no single method discussed and in current use will suffice so the rest of this chapter looks at developing a new model as the basis of a risk rating and safety management system; i.e., one based on information networks.

General Area of Use	**Base Methodology**	**Advantages**	**Disadvantages**
Aviation in general	Risk Matrices (including extended/ complex matrices)	- Simple implementation - Only requires severity and frequency - Able to extend across departments with labels	- Unable to unify cross-departmentally - Limited by use of R=SF - No real scope for further improvement
Other Transport (e.g. railways)	QRA Type (e.g. LUL, RSSB)	- Based on Fault-Tree methods - Extremely in-depth studies	- Inhenrent inflexibility of method - Too detailed for purpose - Very time consuming
Nuclear/ Petrochemical	Process Hazard Analysis (PHA)	- Includes (limited) human factors - Thorough analysis of scenarios	- Purely qualitative - Subjective methodology - Very time consuming
Chemical	LoPA (safety barrier) based methodology	- Semi-quantitative method - Centralises safety barriers - Can incorporate human factors - Removes frequency skew	- Protection layers are deemed to be independent - Quantifying of PFDs required.

Table 7-6 - Summary of current methodologies in use across complex industries

Chapters 3, 4 and 5 of this thesis illustrate the variety of possible uses that information networks have. So how would network models fit with the requirements of BA?

7.3 Is Risk Really = Severity x Frequency?

7.3.1 Does frequency necessarily dictate risk?

Network models of accidents and incidents throughout this thesis have allowed us to illustrate and understand more clearly the information space in which decisions are made and interactions between agents (human and non-human) take place. The methodology allows clear identification of the causal factors central to an event and centralises the totality of a system space, providing an holistic approach to investigation. Information networks allow us to build an image that can be used to further understand and identify the relationships between different facets of that complex system. Networks can be built up from the information that is present within a system during a particular event or more generally.

Networks allow us to picture links between events, barriers and outcomes, and allows us to look at potential outcomes; all valuable and required facets of any comprehensive investigation method. Andrew Rose (2008, p.1381), a previous employee of BA in the Safety Management team, also points out that “where [safety related data sources] are used to make risk decisions it is generally in an individual and isolated way and without a clear understanding of their relative importance.” Here, again, is a key point in introducing a comprehensive method that embraces a network approach to safety as an attempt to bring cohesion to the SMS. Since barriers draw together all incidents that are linked not just by outcome but by causes and effects they are not simply reclassifying the same old thing but actively looking to improve the data sources through more thorough and focussed analysis.

Key to the success of a new model is addressing the eight limitations of the current methods highlighted earlier in the chapter. One of the key concerns with the current application of eBASIS is that using frequency as a rating factor is not representative of potential risk, and can distort the overall risk ratings. If risk is simply the potential outcome of an event, then alternative risk matrices and metrics should be explored. Reason (e.g., 1997) and others conceive of barriers in the system line of defence to avoid accidents and adverse events. One option is to remove frequency from the risk rating matrices and replace it with a factor relating to the success (or otherwise) of these barriers and their proximity to the event. More than this though, the importance of understanding an event in terms of the system it occurred in is of particular importance and any method must reflect this. Rasmussen understood that to isolate actions and decisions from the context in which it took place and attempt to model this decomposition was an ineffective way of learning about the system. (Rasmussen, 1997)

Macrae *et al.* (2002, p.104) state in their paper that "…the risk of safety incidents should not be directly tied to their severity". However, Rose (2008, p.1384) counters this argument in saying that "individual events can be rated for their own individual risk contribution". This slight deviation from the standard allows us to forego risk matrices and concentrate on severity and risk of particular events and yet any SMS which collects data can still intrinsically report frequency based statistics as required for trend analysis etc.

Consistent with the development of this thesis and the issues Rose and the BA staff had, Macrae points out that "...we are concerned here with issues of flight safety. That is, major organisational accidents in well defended systems. By definition, the most relevant incidents to managing these risks will always be towards the high severity, low probability end of the scale. However, quantitative analysis of such small probabilities is often very difficult", and often of very limited productive use in the opinion of the author. "As such, extreme event analysis may require extensions to current risk assessment methodologies." (Macrae *et al.*, 2002, p.101). This allows for novel application and original thinking in terms of foregoing frequency and formulating safety methods centralising severity and barriers which appear to be more useful and applicable across a complex system thus far. Macrae *et al.* (2002, p.102) continue, "what is more, there still remain considerable modelling challenges to be met in capturing the actions embedded in organisational context. These include…the means by which latent organisational and management factors shape outcomes at the 'sharp-end' of operations (e.g. Reason 1997)." This last point can be addressed through the application of networks to events such as in Chapter 3 of this thesis; information networks have shown a degree of modelling and pliability that other methods cannot replicate.

The next issue that this novel method would seek to address is again an over-emphasis by current models on frequent but less significant events on an organisational level – such as bags falling and injuring staff. By quantifying safety barriers, it can be determined whether there is a need for additional safety barriers – and more importantly, whether these would represent a real safety improvement for British Airways. These networks allow for manipulation of barriers whilst identifying any other areas that may be potentially affected (whether in a positive or negative sense) by any changes in the area surrounding the barrier. Industry-wide, the accepted method for assessing safety standards in this way is through the principle of As Low As Reasonably Practicable (ALARP).

It is expected that implementation of this new safety barrier-centric model will allow for clearer representation of which risks need to be concentrated upon, and as such make the decision process for valuable resources simpler for BA Safety Services. All event descriptors with their associated potential outcomes will lead to a certain risk factor dependent upon the penetration of existing barriers. Although these risk factors will be consistent across the organisation and across the reporting structures, applying the ALARP principle will allow for certain threshold levels to be introduced for particular events that do not deserve as much attention as others despite a relatively high risk factor ranking.

Equivalent fatalities is a concept used across the rail industry whereby a major injury is considered to be 0.1 fatalities, and a minor injury 0.01 fatalities. (London Underground Limited Quantified Risk Assessments, 2001) This allows for simpler comparison of risk in terms of fatalities across all incidents including those with non-fatal outcomes. Equivalent fatalities may therefore be a suitable basis for the decision making process associated with ALARP and will require testing against data for suitability in the context of British Airways' operations.

"Risk prediction today is often at the level of looking at trends of safety information and assuming those trends will continue. This however does not recognise the many variables that affect safety performance and does not enable effective prediction of the affects of changes to the system". (Macrae *et al.*, 2002) These network models, it is hoped, can reflect changes because changes to SOPs, company activities, aircraft fleets, airports used etc. may affect safety due to networked links and the networks can highlight the barriers that may be affected. Macrae *et al.* (2002) go on to say that "accident theories make clear that much of the real worth of incident reporting comes from the interpretation and understanding of the organisational processes underlying unsafe events." Therefore with the networks encapsulating the defences left, and the defences (or barriers) broken, it is not purely historical quantities that are being investigated.

Another issue Macrae *et al.* (2002) had with improving winBASIS was addressing "how can risk assessment actively support the flexibility of process needed to deal with ill-structure, dynamic and ambiguous safety information?" He also examined how "in the management of ill-structured, complex problems the creative process of risk assessment often provides as much benefit as the final output. Questions of *how* such beneficial processes could be integrated into incident report management systems remain largely unresolved". It is argued that the network process addresses these issues by the risk-rater having to address each barrier in the system, and therefore being required to understand fully and acknowledge the complex problems of the situation in doing the risk assessment process.

Further than this though, a large limitation of the current eBASIS methods is that "in practice...it's often hard to distinguish [new ways a system may fail or is weak] as many incidents are unique, either in their causal factors, failure mode or combination of occurrence." (Macrae *et al.*, 2002) However, with this network barrier theory, the barriers are a common linking factor as they are part of the system that is purposefully there. Therefore, there is more chance of highlighting and trend-analysing barriers than incident-classifiers. This again harks back to section 7.2.2.

So, in answer to the question 'Does frequency necessarily dictate risk?', it would be more conducive to discuss the idea of a severity rating rather than a risk rating if this then eliminates the necessity to rely on biasing frequency. There is no doubt that the Royal Society (and it appears most complex industries) adhere to the idea that risk is based on probabilistic measures of occurrence of events combined with measures of the severity of those events' consequences. It is argued, however, that due to the nature of aviation and complex industries and the significance of low frequency events, that severity is in fact key in distinguishing the priority of investigation and study. An interesting final point made by BA's safety team is that "risk" is BA's fundamental safety metric, i.e., BA does not rely on individual events materialising to say if the organisation is safe or not but risk itself and therefore there needs to be a way of incorporating potential risk that simply is not there at present. This too is built into the network approach to risk rating and safety management outlined below.

7.4 The Distance from Disaster Model

7.4.1 A network-based approach to modelling safety information: An Overview of the Method

Section 7.4.1 presents a brief overview of the purpose of the model before section 7.4.2 takes a step by step look at the method. In its original form, the process of risk rating with the new methodology requires the risk-rater to formulate a diagram similar to that in figure 7-5 in order to ascertain the accident pathway that the event took place on. These diagrams will build up over time so it will not always be necessary to create them from scratch, but they may be modified from existing British Airways Standard Incident diagrams.

If the worst potential outcome (furthermost event) given the scenario has occurred then the event is classified as an “A” rated event. Should one barrier be identified preventing the potential outcome from occurring then the event is rated as a “B”. Given two barriers a “C”, three barriers rates an incident as a “D” and four or more barriers means that event would be rated “E”. As can be seen in the footnotes to figure 7-6 there are situations where an event occurs which could have led to a more serious potential outcome and a reason why it hasn’t cannot be identified; in these circumstances that event is also classified as “A” (see *1 in figure 7-5 below). At this point in the model there is potential for identifying the ‘strength’ of a barrier and incorporating that into the rating of an event. The risk, or severity, score could be increased if the barrier is identified as a ‘weak’ barrier or decreased if a particularly ‘strong’ and proven barrier. This idea of ‘strength’ of barriers is something which will come into its own once the model has been used for some time and it has been fully populated with a lot of data on which to base the ‘strength’ or otherwise of a barrier.

The usefulness of this technique of rating is that isolated from any other influences, each event is rated on the basis of its distance from a disaster. This in turn reflects on the positive aspects in identifying what stalled the event from becoming an actual disaster and solidifies the importance of barriers as the best method of rating safety within a system. This particular method also “walks” the risk-rater through the entire process innately and therefore does not need complicated instruction nor wholly subjective assertion which is common practice in many risk rating schemes to date. The objectivity and structure this method can bring risk-raters is an underlying feature of strong methods and should be strived for when reviewing current or future practices.

The model behind the new risk rating system is illustrated in its most simple form in Figure 7-7. It is essentially broken into three parts and each part can be represented as a network, which, in the final version is of course joined to the next in a comprehensive systemic picture of airline events.

The middle section is the first to be identified as this information is gained from the incident report from crew and any digital data recorded by the airline. This gives information on the actual event that has occurred including, for example, persons affected, the amount of deviation from normal or the extent of injury/damage.

It is then the job of the investigator to populate the first section of the diagram by studying what can be considered precursors and most importantly identifying barriers that failed to stop the event.

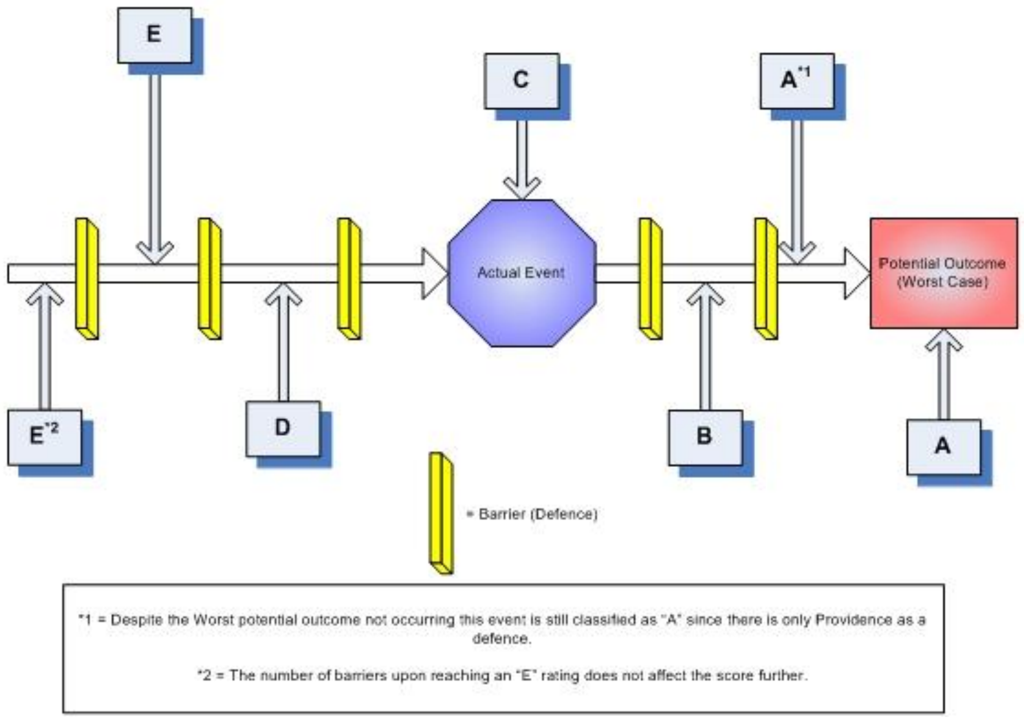


Figure 7-6 – A single strand of the "Distance from Disaster" Methodology illustrated with ratings applied at 7 locations (or events)

Finally, the model aims to encourage investigation into possible outcomes from the reported event. This would require identification of any positive-actions on the part of crew or non-human agents together with any defences or barriers that have remained intact and hold responsibility for preventing further/potentially worse outcomes; a positive slant on the picture.

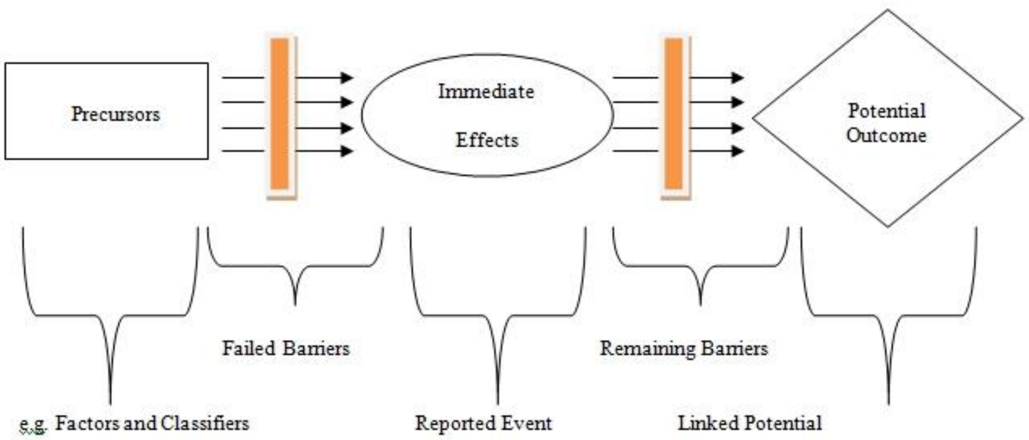


Figure 7-7 - Distance from Disaster Simplified Model

7.4.2 **The “Distance from Disaster” methodology**

In order to produce a workable rating method it was decided that the practice of risk rating has, of itself, an intrinsic “flowchart” style procedure. By this it is meant that not only is it the aim of this work to introduce a new risk rating scale but also to make that scale representative of the methodology required to carry out the action. Developing a new method must have usability at its core and as such the model above is the basis for this new risk rating system but the method itself differs in order to improve usability and reduce complication at the outset whilst retaining the ability to improve and develop over time. In other words, central to this study is that the model underpins the method. However, in order to move forward in manageable steps for the company a usable method that has attributes similar to those in current use needs to be formed as an intermediary step. This section outlines the development of the method and its usability.

Having discussed the issues involved and the requirements of the project, a number of “standard incidents” analysed by BA over time were studied together with the safety manager, a pilot specialist, an incident investigator and a subject matter expert. At this stage, the actual eBASIS files were not used so as not to limit the scope of the model (it is important that the method is not to be restricted by current shortcomings of the eBASIS system or directed to be too similar). This also meant that the eBASIS files would serve better in the validation stage later in this chapter and the results of any such validation would hold more weight.

The “standard incidents” covered significant aircraft accidents that BA felt had real potential to jeopardise the operation. These included incidents such as Runway Incursion (most notably illustrated by the catastrophic accident at Las Palmas in Tenerife), mid-air collision, Controlled flight into terrain (CFIT) and fire/smoke in the cockpit. These issues were highlighted by safety and technical professionals within British Airways. Once identified a number of causal occurrence types were identified. These, for example, would include contributory factors such as, for a runway incursion; disorientation, incorrect radio instruction, incorrect runway use etc. These incidents of note were then the basis for the safety plan within the company and spurred training modules, feedback/newsletter articles, investigation into “hot topics” and formed a safety related goal. This was at a level that was pseudo-aspirational and by this I mean there was no single formal method in place to address such an issue hence the desire for this work with the safety management team.

The main "standard incidents" had to be deconstructed in order to create network diagrams as the basis for depicting the system. The team outlined earlier sat down with each of the incidents in turn and looked to identify influences on the flight crew in particular. At this stage of the development all of the reports that are entered into BASIS are flight crew reports. This necessitates the tying together of the method and the data it is attempting to analyse. These influences, similar to any risk work, can be organisational, environmental, personal and in particular informational. Table 7-7 (on the next page) contains the human factors that were considered when creating a network style diagram for each "standard incident".

The network was originally created by working through each line of table 7-7 and inserting a node relating to any of them that were relevant to the "standard incident". The basis for this was the specialist knowledge of the team. In the future the allocation of nodes/factors/barriers etc. could be cross-checked against other specialists but more importantly through the aggregation of information from each incident outlined above the nodes would become self-perpetuating.

If the incident referred to in figure 7-9 is used as an example the relation to table 7-7 can be seen. Table 7-8 highlights some examples from where the nodes (or barriers/factors etc.) were identified. These are not an exhaustive or necessarily highly accurate group from which to ascertain the full systemic network of aviation but they worked to direct group discussion and formulation of the early networks which could then be developed further.

As already mentioned no ASR data was used at this stage but in the future it is expected that the model can aggregate any new factors, barriers and informational elements that are reported by crew/investigators so that it is a continually building and adapting database. This and the aggregation of probability data for each element ties this method into work from earlier chapters of this thesis (Chapters 5 and 6).

Table of Human Factors

Crew Actions	**Influences**	
Team Skills	**Environmental**	**Personal**
Assertiveness	Airport Facilities	Auto - Complacency
Briefing	ATC Communications	Boredom
Crew Communications	ATC Services	Currency
Crew Self Feedback	Environmental Factor	Distraction
Cross Checking	Ergonomics	Environment Awareness
Decision Process	Met Conditions	Environmental Stress
Group Climate	Operational Problem	Knowledge
Preparation / Planning	Other Aircraft	Medical - Crew
Role Conformity	Passengers	Mode Awareness
Vigilance	Technical Failure	Morale
Workload Management		Operational Stress
		Personal Stress
Errors		Post Incident Stress
Action Slip		System Awareness
Memory Lapse		Tiredness
Mis-recognition		
Mistake		
Misunderstanding		
Proc - Fail to Follow	**Organisational**	**Informational**
	Commercial Pressure	Electronic Checklists
Aircraft Handling	Company Communication	Manuals
Handling	Engineering Quality	Nav Charts
Handling - automatic	Ground Handling	Notices
Handling - manual	Ground Services	QRH
System Handling	Group Violation	SOP's
	Maintenance	
	Technical Support	
	Training	

Table 7-7 – Table used by the team to develop networks for "standard incidents"

Node Inserted	Item from Table 7-7	Type of Influence
Wig Wags available/in use	Airport Facilities	Environmental
Use of one language	ATC Communications	Environmental
LAHS/SIRO in operation	Group Violation	Organisational
Lights on entering runway	Checklists/Cross Checking	Informational/Team Skills
Low Speed RTO	Handling/Briefing	Handling/Team Skills
Incorrect readback of clearance	Misunderstanding/Mistake	Errors

Table 7-8 – Items relating Table 7-7 to Figure 7-9

From here it was necessary to apply severity scores to all outcomes (e.g., runway incursion), barriers (e.g., No ground radar being used) and factors (e.g., Low visibility). The aforementioned team gathered on many occasions to discuss the severity scale. Originally BA was using a 100 point risk rating system but it was deemed necessary to increase this to 1000 points in order to gain some granularity particularly amongst the low and mid-end risks (this is discussed further in section 7.4.3 below). This 1000 point scale set the starting point for allocating severity and the team, based on their vast knowledge of safety, aviation and BA incidents in particular, allocated a range of severity to each "standard incident" (as an aside this relates nicely to the use of ranges of values in Bayesian mathematics as described in chapter 6). Each incident was then looked at individually and moving out from the node that described the incident deemed to have been reported (e.g., runway incursion) each subsequent node that was linked had a value applied to it that resulted in an acceptable overall severity score once each permutation was completed. This was an iterative process and one which was largely subjective. This is argued to be acceptable at this stage because of the make-up of the team and the potential for feedback from future incidents, system developments and rating scores to affect the networks continuously.

The result of these discussions was a number of network diagrams where each node had applied to it a severity score so that these may represent an event or occurrence. Additionally all other nodes could represent either a positive or negative factor or barrier and as such has a score related to it. This has important implications in terms of the concept that any node is capable of having a severity score applied to it. This is discussed further in the conclusions to this chapter. The crux of the method then, is that the investigator will start at a node with a set severity rating and then look at all nodes that are linked and those that are considered active in light of the pilot report would then affect the severity score by the value of each node.

Returning to the three-stage nature of the process of developing a new method for BA, this middle stage had to be an improvement on the matrices that were in use. It was important that certain features were retained that made it relatable to the staff that would be using it and usable with the level of data received (the ASR program could be developed in the future to get more of the correct information required for a more complex methodology but that was not feasible at this stage; the model and method, however, do hold the potential for all these options in the future). For this reason the networks were modified from the information networks seen in earlier chapters of the thesis to a simplified version similar in style to figure 7-8 and in turn reduced to a flowchart style such as figure 7-9 and table 7-9. BA had a preference for this first iteration of the method to use a flowchart to direct the work of the investigator and that is from where the worksheet (table 7-9) was formed. Here the underlying principle is based on the nodes created for an information network but each node, assigned to be either a factor or a barrier, is now replaced by a series of tables and worksheets. This retains the core of the model whilst simplifying the exterior look of the method.

By means of summarising the results of this developmental method the following shows the steps required within the current iteration of this “distance from disaster” methodology:

Phase 1:

Draw networks of “incident” to identify barriers and factors for that incident. This is based on investigating the event as per the model including potential outcomes and links with other incidents. Initially this will take the form of network diagrams, similar to earlier chapters and simplified to be more akin to figure 7-8 in time. All network barriers and factors affecting that network are identified and comprehensive networks produced.

Phase 2:

These networks will then be broken down and modified to produce a flowchart style network akin to figure 7-7 and illustrated in steps similar to the developmental stages of the method in figure 7-9 and table 7-9. The barriers can thus be identified and potential outcomes or causes clearly displayed. Subject Matter Experts check the assigned values to the barriers and factors for each network, store the network diagram for future use and publish a simple to use risk-rating worksheet as shown in Table 7-9.

(These two steps are carried out by SMEs any time there is an incident that does not fit into one of the already published networks/worksheets.)

Phase 3:

Now a member of the Safety Data staff, no longer needing specialist training, can use a worksheet to score an incident that has been reported without needing to refer directly to the model itself. The score starts with the original incident rating, in the example of Table 7-9 that is 250 points. Next, each of the barriers breached boxes are checked and any that hold true for that incident incur that number of risk points to be either added, or subtracted where the figure is preceded with a minus sign (there are no negative values in the example given in Table 7-9). Next, the risk-rater also checks any factors boxes which are relevant to the incident which again alter the score resulting in an incident total. Some factors ask the risk-rater to refer to another worksheet illustrating the linkages that will develop between worksheets and thus in the incident investigation for BA.

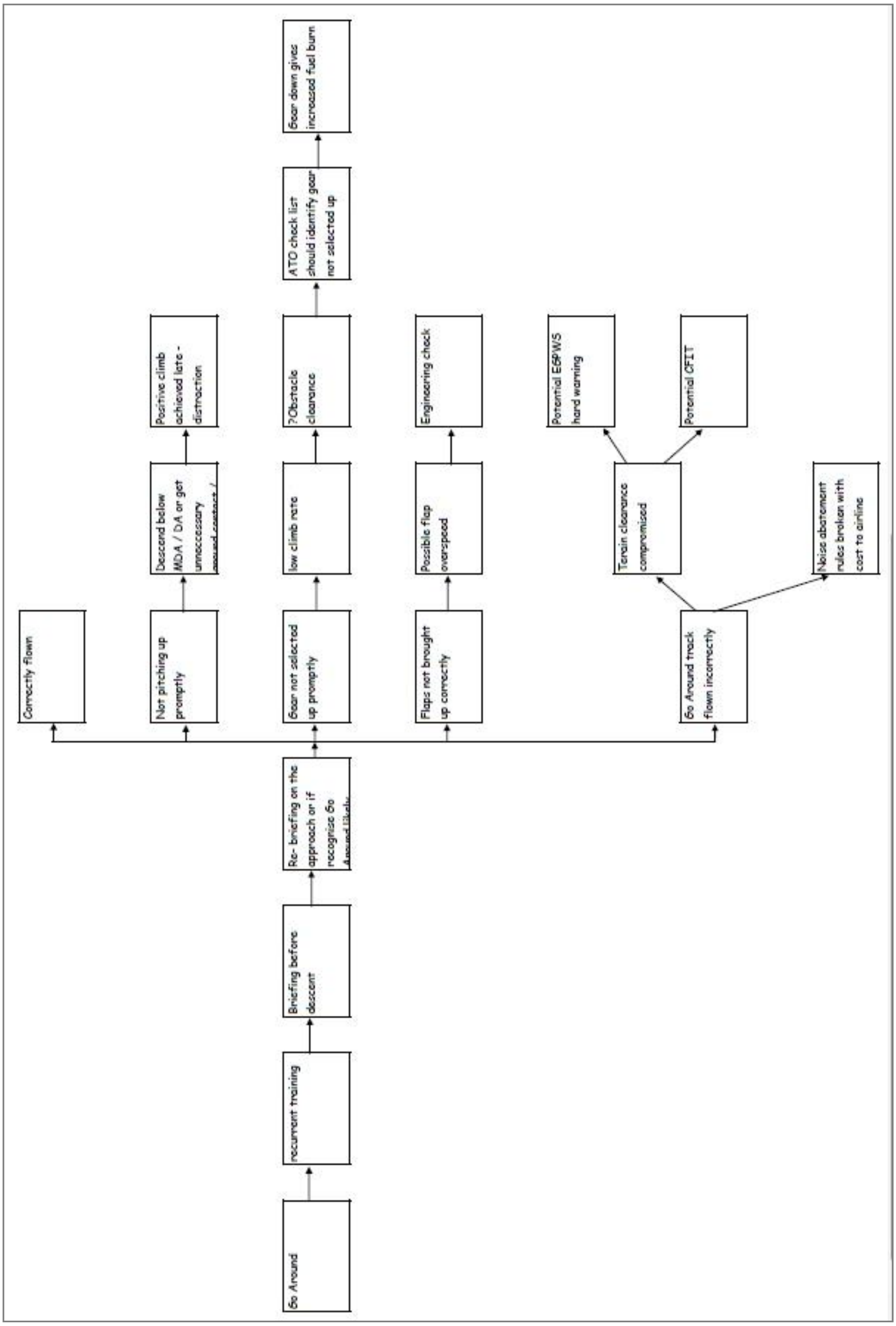
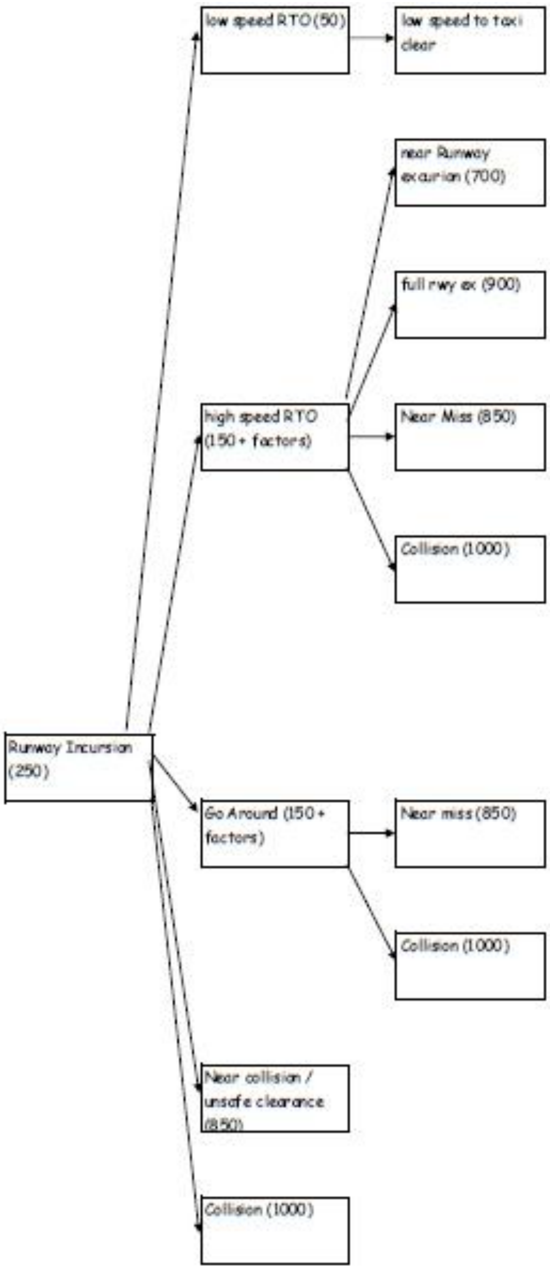


Figure 7-8 - Example simplified network for Go-Around Standard Incident

Barrier	Rating
Airport Facilities and Maintenance	
Green taxi way lights available / in use	20
Stop Bars available / in use.	20
Wig Wags available / in use	10
Clear signs and ground markings	20
ATC	
Use of ground radar	5
Not using conditional clearances	15
Use of one language (English)	25
Flight Crew SOPs and airmanship	
Briefing of appropriate holding points, esp in low vis and at unfamiliar airfields	5
In low vis discussion of taxi route and holding points before taxiing.	5
Visual check / use of TCAS before lining up or crossing a runway.	15
Read back (and writing down) of clearances. Confirming clearances where there is any lack of clarity	20
Putting all lights on when entering an active runway.	5
Total	(-)



Factors	
above decision ht with clearance to land	25
below decision ht	100
Not other operator error	50
land and hold short LAHS / SIRO in operation	200
Weather Low Vis	100
Total	(+)

Figure 7-9 - Example interim network step for Runway Incursion Standard Incident

Incident total	
Incident	**Rating**
Runway Incursion	250

Overall Risk Rating	

Barriers Breached Total	
Barriers	Rating
Airport Facilities and Maintenance	
Green taxi way lights not available / in use	10
Stop Bars not available / in use.	20
Wig Wags not available / in use	10
Signs and ground markings unclear	25
ATC	
No ground radar being used.	5
Conditional clearances being used.	20
More than one language being used	25
Flight Crew SOPs and airmanship	
No brief or discussion about taxi routes before moving at unfamiliar airfields or in low visibility.	5
No Visual check made / use of TCAS before lining up or crossing a runway.	15
Clearances not confirmed.	15
Lights not put on when entering an active runway.	5

Factors Total	
Factors	Rating
Phase of flight	
Above decision ht with clearance to land	50
Below decision ht	150
Airport Environment	
Land and hold short LAHS / SIRO in operation	200
Weather	
Low Visibility	100
Flight Crew Actions	
RTO performed	see RTO
Go Around performed	see go around
Unable to take avoiding action with no collision	200
Unable to take avoiding action with near collision	750
Unable to take avoiding action with collision	1000

Table 7-9 - A working example of the method's "worksheet" for an incident reported as "Runway Incursion"

Phase 4:

Finally, the event can be classified according to BA's Operational Safety Scoring Categorisation (Table 7-10; further discussed in the section 7.4.3) and any company/departmental action taken as appropriate to that level of incident.

Grade	Risk/Severity
A	800-1000
B	600-800
C	400-600
D	150-400
E	0-150

Table 7-10 - BA's New Operational Safety Scoring System

7.4.3 Validation and Implementation

Following development of this method for rating the severity of incidents, 637 BA Air Safety Reports (ASRs) were scored between myself and an SME pilot and the data reproduced in Table 7-12 below. To reiterate for clarity, no ASRs were referred to during the building of the networks and flowchart style worksheets so that as best a test as possible could be made of validating the severity scoring from the developmental stage. The ASRs for validation were selected from November 2009 and working back in date order until 50 of each type were tested. This was not possible with certain event-types due to their rarity. For each of the "standard incident" types detailed in table 7-12 there was a worksheet similar to that shown as table 7-9.

Screen captures of the ASR database on eBASIS are included as Figures 7-10 to 7-14 to illustrate the spread of information available from pilot reports and used to validate our method (and more generally to rate events by the safety team). These will now briefly be described so as to illustrate the method of validation used. Figure 7-9 shows mainly administrative information relating the flight details to the investigator including date, location, aircraft type and whether a formal report is required by law. At the bottom of figure 7-9 (and repeated in figure 7-10) is the incident summary. This provides an overview of the situation. The lower half of figure 7-10 show that this particular incident was rated as D by eBASIS prior to the new method and classifies what type of incident it is (in this case a take off performance issue). Figure 7-11 explains who raised the incident (e.g., was it an ATC report or a flight crew report) and further details of the flight. Figures 7-12 and 7-13 are where the majority of the information to use the worksheets is gleaned. The validation would begin at a node reflected by the "summary" box of figure 7-12 and then any barriers or factors that could be identified using the "event and cause", "action and results" and "other information" boxes would be marked on the worksheet. The starting rating would then be affected by any factors and barriers marked as active in the event and the resulting severity rating recorded. It is these scores that are recorded in table 7-12.

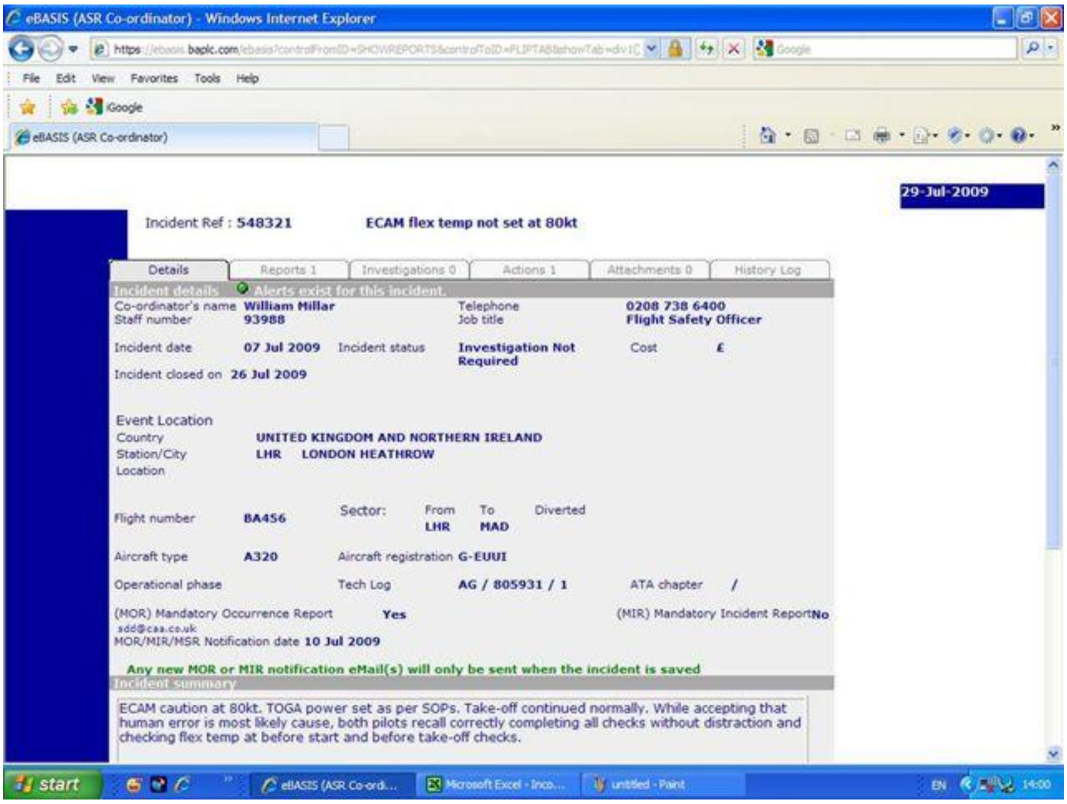


Figure 7-10 - Basic details available on an ASR include investigation details, date,
location, fleet, flight details, MOR filing and a brief incident summary.

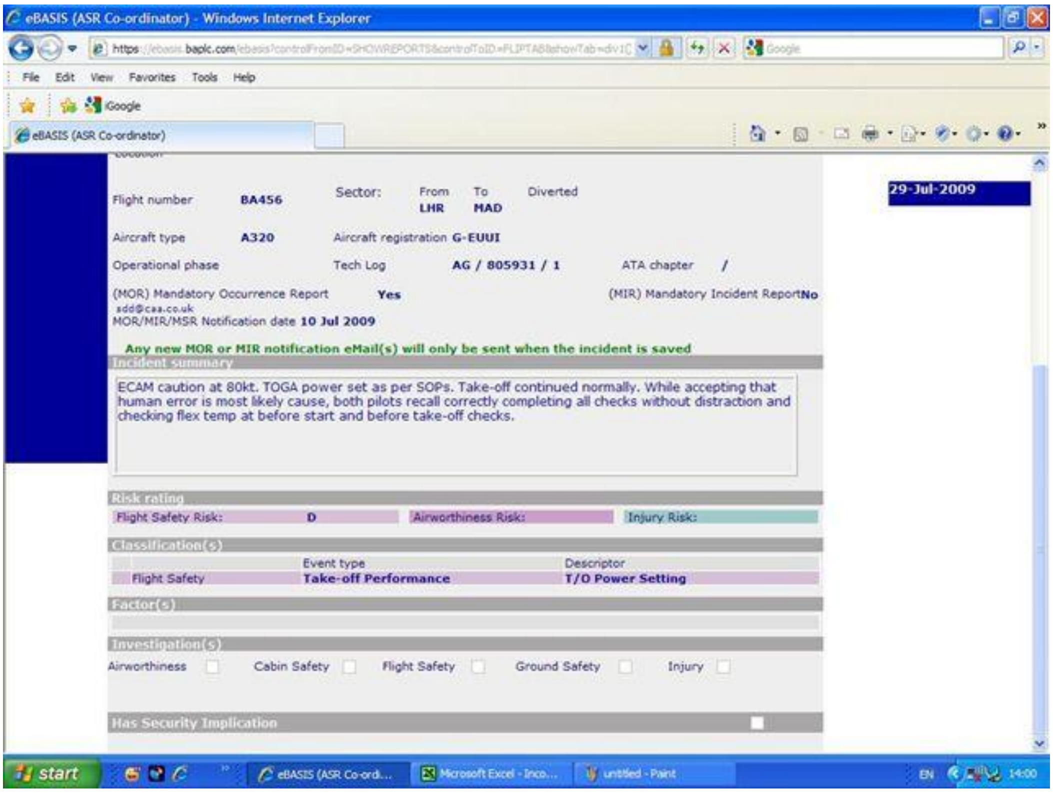


Figure 7-11 - Risk rating (A-E) and classification labels including event type and descriptor added to illustrate inferred causal structure.

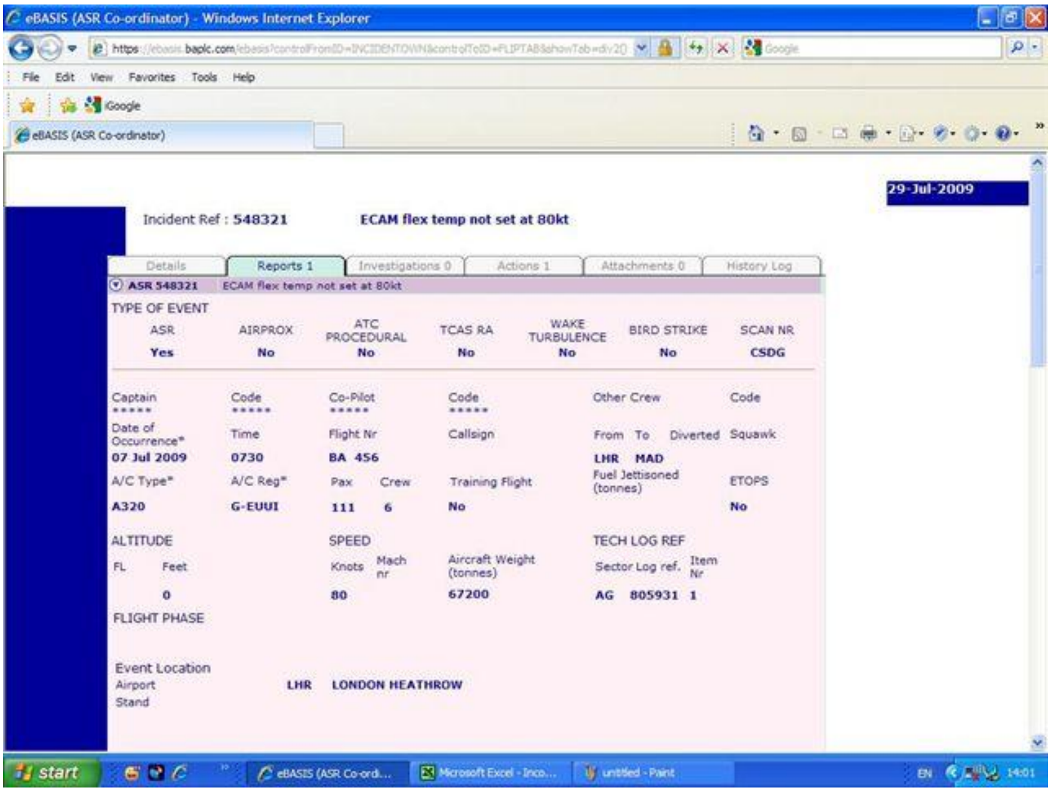


Figure 7-12 - Raw technical data is also included in the report

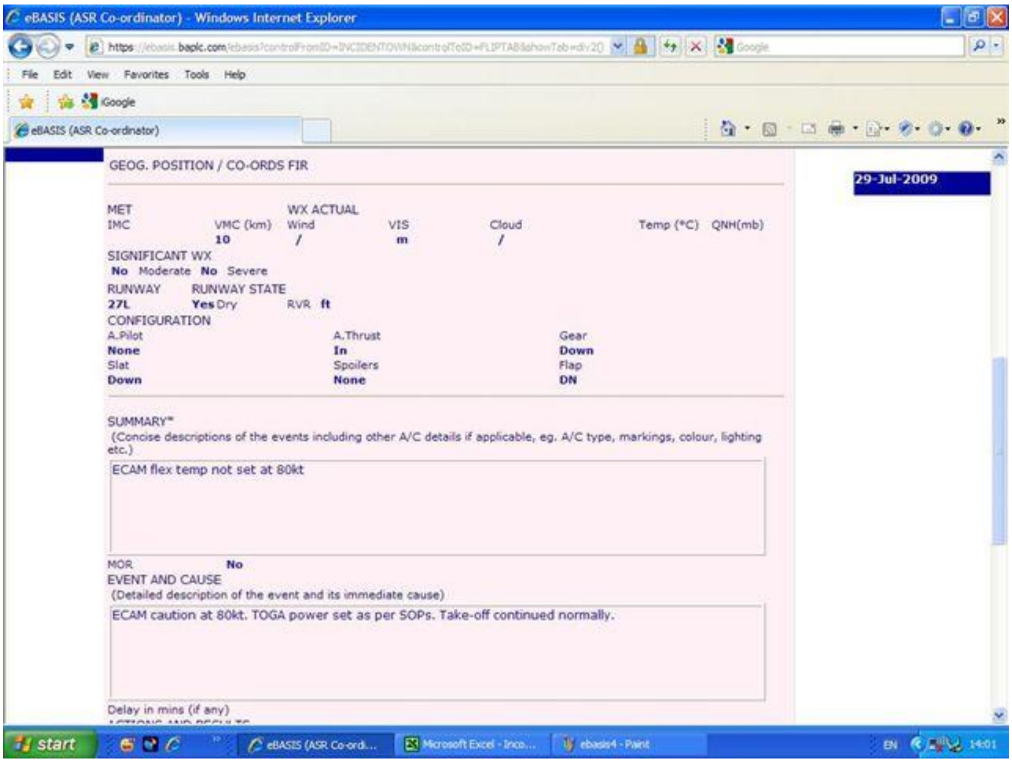


Figure 7-13 - Reports from the flight crew in terms of *what* happened are included in the report and any relevant weather or operational details

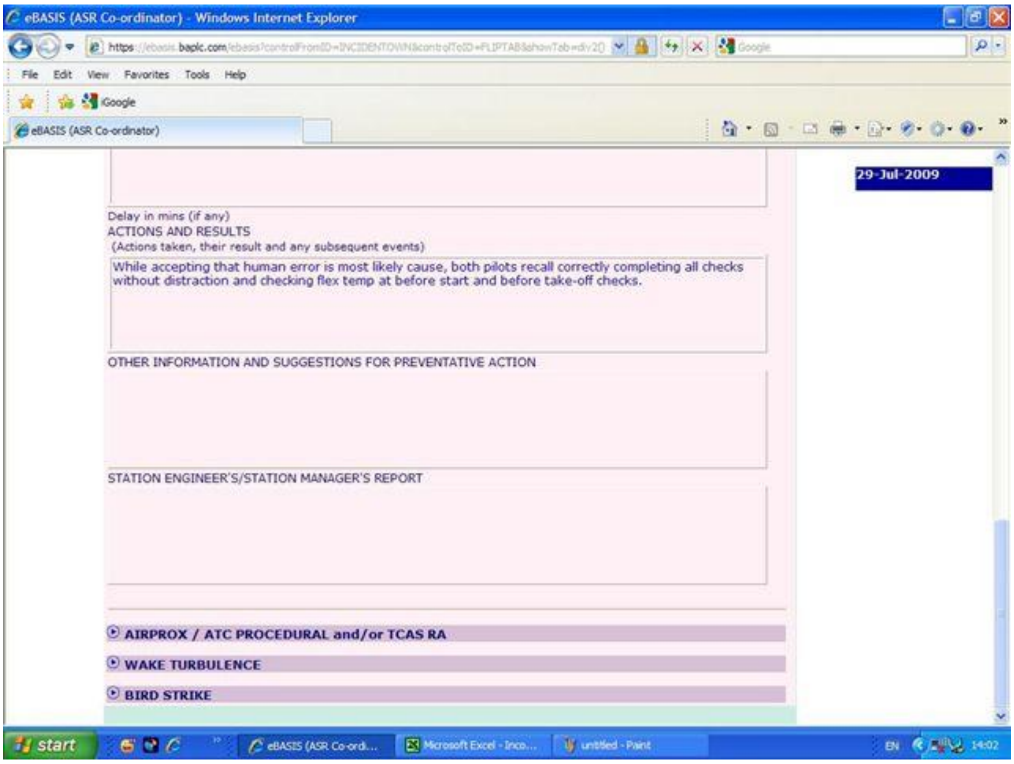


Figure 7-14 - Actions and results are entered as the incident is "closed" or further requirements are entered and the incident kept "open" for further investigation

The data have been studied against what are considered suitable severity scores for a particular type of incident together with suitable severity scores for the potential an incident shows. The highlighted cells in the table indicate the main spread of severity scoring for that type of standard incident. These scores (the 5 columns on the right of table 7-12) were compared against the values raised by the previous eBASIS risk ratings (column 3 in the table). The results can be seen to be comparable and more importantly three further subject matter experts were given the results of the new method and a selection of the ASRs and without exception there was a positive agreement. In the future a more comprehensive cross-rater test could be carried out and further validation would continue.

This validation against BA's own data is important because of the need to report on safety and risk within the company relative to the history (a method that rendered historical data useless would not be acceptable). The fact that the method maintains a relatively similar area of severity scoring to previous methods alleviates any need to reanalyse historical data and allows for comparisons to continue.

The final issue to be validated was that of whether or not to use an alphabetised scoring system to group incidents of similar severity and risk. It is important to get not only the best reflection of severity in terms of the grouped score but also the best spread of risk points in the areas most needed by the company. The use of a score from A to E has been used by BA for some time and appears to have served the company well in terms of distinguishing those incidents and accidents that require, for instance, company or regulatory investigations. This way of reflecting the severity of an incident allows the company to report and concentrate on those incidents causing the most serious problems. As a point of note though, this does not predicate against accidents scored as C, D and E being important since these can often occur in higher numbers and still, as shown in this method, elicit important facts about the system safety and where extra barriers or investigation is required.

There are two arguments surrounding the retention of the use of an A-E system. The first would dictate that since those incidents at the higher end of the scale, rated high in severity, have a wider range of outcomes in terms of levels of damage or injury and death (and all of these components in small or large amounts would cause an incident to be scored highly) then the widest range of severity points should be in those incidents described as A or B events.

The second would be to relate the range of severity points to the A-E system on the basis of volume of incidents, i.e., since there are many more D and E events than A, B and C events so the range of severity points within each of those ratings should reflect that.

Since the aim of this method is to improve incident investigation and rating and with no alternative precedent set in the literature, it is recommended that the ratings be spread as shown in table 7-10. This allows for greater granularity amongst the lower band incidents which are most prolific, which was an additional aim of this project. Since the issue of A to E rating is purely an internal method of discussing safety there is no critical issue in either approach outlined above. The arbitrary decision that is required at the outset can be modified as data is collected and levels can be manipulated depending on variations of the safety levels and approach within the company.

Incident Classification	Old System	Range of Values	New Method	Range of Values
A	100	n/a	801-1000	200
B	71-86	15	601-800	200
C	35-55	20	401-600	200
D	15-25	10	151-400	250
E	1-15	15	0-150	150

Table 7-11 - Classification Grades from A-E for incidents (The old system is not based on a continuous measurement of risk)

Incident	Starting Values	End values from eBasis	0-150	151-400	401-600	601-800	801-1000	Total tested
Birdstrike	50	50-255	47	3	0	0	0	50
Medical Emergency	50-200	50-250	42	8	0	0	0	50
Go around	75-150	125-450	8	40	2	0	0	50
Lightning strike	100	100-320	27	23	0	0	0	50
Pushback Incursion	100	175-325	0	32	0	0	0	32
Taxiway Incursion	125	175-325	0	20	0	0	0	20
TCAS RA	150	75-525	23	23	4	0	0	50
Hold Point Incursion	150	275-415	0	5	1	0	0	6
Low speed RTO	150	100-200	20	5	0	0	0	25
Taxy without flaps set / mis selected	200	200-275	0	30	0	0	0	30
Flap Mis-selection for take off	200	250-575	0	2	13	0	0	15
Altitude Deviation	250	175-400	0	50	0	0	0	50
Runway Incursion	250	275-650	0	6	14	1	0	21
Fire smoke Fumes in Cabin	225-300	225-475	0	48	2	0	0	50
Fire smoke fumes on flight deck	250-350	225-575	0	45	5	0	0	50
High speed RTO	300	250-600	0	15	5	0	0	20
Pilot incapacitation	300	100-500	2	40	5	0	0	47
Incorrect performance figures used.	300	250-650	0	19	1	1	0	21
								637

Table 7-12 - Results of the validation of methodology against BA ASRs

KEY for Table 7-11:

Column 1: Incident Title, Column 2: Incident Starting Value in the new methodology, Column 3: Resulting severity scoring range for all incidents of that type, Columns 4-10: Number of incidents from study group that scored in given severity range, Column 11: Total number of incidents in that study group tested

7.5 Discussion of the benefits and limitations of working within industry

Merging academia and industrial application is a central tenet of this research. Being able to work with industrial partners and develop a model that is not just integrated, but the basis for a new Safety Management System within a legacy airline is of great benefit to this work. However, there are issues surrounding working in real industry which can lead to limitations in methodology. A fine balance has to be struck between the ideal “Distance from Disaster” model utilising advanced network techniques and the practical application of a method to actually be used fully by BA. As such, the methodology has taken a slightly more linear approach than the networks appear to be capable of. However, this opens the door for masses of further work in the future given the correct time, finances and software development. It must be stated that this chapter does not reflect a finished application of the information network model. Indeed the letter of appreciation from BA (annexe 5) includes the continuance of work to implement and improve the interim methodology. The key to this, and previous chapters within the thesis, is that the central ideas and models are tested to an extent. This becomes the basis for future development and continuing work for many years to come.

BA required a specific and workable risk-rating and safety management model and method which has been produced in this chapter. Any limitations imposed for the needs of simplicity of use are far outweighed by the benefit of using real industry data, specialists and situations. Industrial work must take the form of a step-by-step process (figure 7-15) and BA are now at a stage much more developed than previously and on a long road that has thus far taken them from reactive to proactive and now has true potential to adopt a predictive approach with networks.

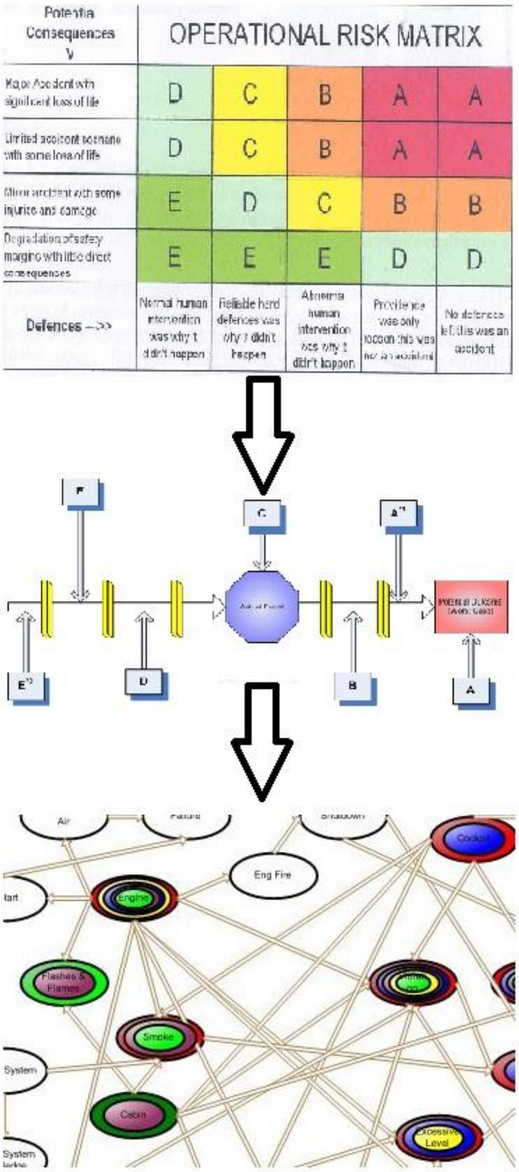


Figure 7-15 – The past, present and future of BA’s risk rating model (the three-stage process referred to throughout the chapter)

Macrae (2002) affirms that “…it is of considerable importance that any assessment process is practicable. Not only does a process need to address the assessment problem, but it must meet time and resource constraints; it must be simple enough to be implemented and understood….” There are many methods which are accused of being far too unwieldy and time consuming for real-world application and this is one stigma that cannot be appended to this work and that is a coup for academia/industry work in the thesis especially given the solid foundations and extensive development that can continue.

7.6 Conclusions and Further Work

7.6.1 The future for eBASIS?

As discussed in the previous section there is much scope to develop the current fault-tree style standard incident bank into complex networks that centralise barriers as the reporting classifier and not the incident. Ultimately, it is hoped that BA will adopt a more complex network approach to the underlying models of standard incidents; one where figures 7-6 and 7-7 are extrapolated into 3D networks interlocking with many others and sharing nodes across many, to the ‘naked’ eye, unrelated incidents using classification of outcomes. It has always been the intention throughout this project to develop the models and methods so that they can extend into the application of information networks. BA require time to implement this novel procedure and explore the potential that it has to offer. After this period the next phase of the upgrade to network based models supporting the SMS can begin. The chances of applying historical data to the networks together with SME values for barriers could lead to more predictive levels of safety management. The strength of barriers concept discussed in section 7.4, and adopted within methods discussed earlier such as MIL-STD-882E (US DoD, 2005) and Luxhøj (2002), can really come into its own it future iterations of the method. Feedback, itself a perquisite of Van der Schaaf’s framework and many positive practices within a safe organisation, can feed the very model that underlies the method. As reports, or the system itself, changes so barrier strength may fluctuate in terms of their effect on safety. If, for example, a barrier is reported as being active within a large number of incidents and stopping worse outcomes yet never has been broken so the strength may be typified as high. Conversely if a barrier is found to be weak, and often active within incidents whereby a worse severity score is issued so that barrier would be highlighted as a potential issue. What this does is centralise the barriers and nodes not the classification technique. Ideally, in time, this process could be totally automated so that a barrier that is perceived to become stronger could allow nodes around it to reduce in severity rating. This automation would also extend to updating of probabilities of occurrence of nodes and this ties in well with the work covered in chapters 5 and 6.

On the shorter term, the method requires regular checking of data trends in order to ensure barriers and factors are appropriately scored. Any changes to fleet/SOPs/training can also be reflected in the models. As briefly alluded to, there needs to be a discussion on the applicability of ALARP or equivalent fatalities to the model in order to begin a Cost Benefit Analysis (CBA) aspect to the method. BA have to make some hitherto undisclosed decisions about what is considered to cost BA; is it hull-losses, passenger injuries/fatalities, or, brand image.

7.6.2 **Conclusions**

The crux of the work in this chapter is to have produced an incident auditing method that centralises barriers and not events themselves. A barrier could be involved in more than one event, or type of events, and as such this method would allow for the barrier to be implicated and investigated the correct number of times. This is something that may be overlooked when concentrating purely on the event itself; it is the barriers that ultimately create (or destroy) a safe system.

The method designed and tested in this chapter is based on treating events on the basis of their individual risk contribution as discussed by Rose (2008). By analysing an event almost in isolation and not relying on risk = frequency x severity (thereby allowing frequency to skew the resulting risk score) the issue discussed in the introduction where logarithmic increases in frequency skew results is avoided. Yet at the same time the method is capable, through the centralisation of barriers within a large model, of allowing a more systemic approach to safety with arguably less emphasis on particular individual events (unless that is warranted as explained above) in isolation. This is in contrast to a prevalent type of safety system that aims predominantly to reclassify incidents alone. In this way the method moves away from an auditing safety method to a proactive one and it is argued has a better balance of individual event and system safety than previous methods and models.

Further than this though, the use of potential outcomes and accident pathway diagrams allows the visualisation of what could have happened and therefore highlights the importance of protecting the company in terms of responsibility in the future which was key to the Concorde example earlier in the chapter, e.g., if an incident recurs but in the future has a different outcome, if that incident was only investigated in isolation the possible outcomes may not have been addressed. However, if possible outcomes are addressed, even if a different eventual outcome occurs, there is much to say that a safe attitude and proactive attitude has been held by the company. This centralisation of potential is key to a proactive safety management system. Further than this though, the method develops the safety management system in introducing predictive elements. Macrae *et al.* (2002) and Ale *et al.* (2005) both argue that analysing an accident is not enough to understand systemic problems and can not enable effective prediction. Through the monitoring and further understanding of the barriers within the British Airways network, we have seen how potentially weak or over-strained barriers can be identified prior to a catastrophic event. This is where the method improves upon current methods of risk rating. It appears there is more potential from using the information networks as the underlying model than the use of event sequence diagrams (ESDs; e.g., Macrae 2002 and Ale *et al.* 2005) as there is a deeper level of the system being investigated with more scope for detail and highlighting or discovering nodes of interest. In using ESDs as the foundation for their investigations Macrae and Ale have to assign outcomes and classify events in order to fit the design. As is discussed throughout this section, information nodes may transcend the higher level analyses by being present in very different outcome situations or other classifications. This responds to the difficulties discussed in the introduction that Macrae *et al.* (2002) found in overcoming the uniqueness of many incidents and their causal factors an extremely limiting and important issue. It is more likely that by analysing and modelling barriers, and reducing outcome to almost a by-product in the system, that patterns can be identified and safety issues highlighted.

We have seen in the model (section 7.4.1) that the incident itself becomes the key element in any rating. By that, we mean that frequency has been removed from a central position. Intrinsically there is a value for frequency in the system, especially in how often a barrier is “attacked” and survives etc., but the severity score isn’t dominated by that value in the way risk rating to date has been. This also relates back to the classification of barriers as ‘strong’ or ‘weak’ discussed earlier (e.g., MIL-STD-882E (US DoD, 2005) and Luxhøj (2002)). If a barrier survives many attacks then it could be argued that it is a good or ‘strong’ barrier. Alternatively, it can also be argued that that barrier needs further investigation and possible funding to retain its strength and ability to defend. Indeed, there is the potential for an alerting system based on the frequency of “attack” of a barrier regardless of whether there was a positive or negative outcome. This could be a simple colour-coding to the barrier within a network diagram to highlight those areas of particular interest and potential risk. This would require increases in the amount of positive-outcome data recorded. However, the potential of an incident replaces frequency as a central facet of the method as discussed in the previous two paragraphs. In comparison with where BA were at the start of this project, using a series of 5x5 matrices, the improvement in terms of introducing system analysis to understand system safety is immense (and this will continue with the third stage of the process). The movement away from risk matrices draws accident investigation models into the centre of risk rating techniques. This is in sharp contrast to using a secondary model at a higher level with less detail in order to ‘fit incidents into boxes’ for statistical evaluation. This method has introduced to BA’s safety methods a representation of safety within the entire complex system.

The method itself has used a solid model at its core and yet has been simplified enough to be practically useful within a large organisation such as BA without restrictive amounts of user-training. The central bank of standard incidents can be built upon and, as in the flight-crew orientated incidents tested thus far, specialists from the relevant departments can be drawn upon to populate network style models that feed the worksheet approach.

The key to the proactive view of potential within the model is with the factors. Factors, alongside barriers in the worksheet, influence the severity score on the basis of potential, i.e., “no heavy crew on duty”, or, “it happened in bad weather” even though these were not causes or barriers necessarily broken.

The International Civil Aviation Organisation (ICAO), in their 2002 document introducing LOSA (Line Operations Safety Audit), discuss how incident analysis does not provide good enough information on barriers (i.e. positive actions etc.) that occur during the build up to events. Through the recreation of not only the event but the possible furthering of that event into an ultimate event outcome (including factors), risk raters are encouraged to understand more fully the scenario and look beyond the negative aspects. It has been important throughout this project not to limit thinking to the limitations of current reporting practice and data received but more to drive the reporting style and data that is required by a solid model and method; hence the future requirement for positive-outcome reporting. A significant benefit of these network models (and Bayesian style networks that could be added to the mix during the third stage) is nodes can have specific significance (e.g., be marked as an outcome or incident/accident node) as all of those things are just the manifestation of information in different ways. At the same time a node may act as any other nodes with probabilities and links to other nodes potentially in all directions. Therefore, this chapter has introduced an actual risk rating method different to those seen in the literature and more similar to an accident or system investigation tool. There is no place for stating the ‘end point’ and then looking ‘how we got there’ as the nodes are simply active or not and the interest is in what nodes are linked and also active that may have prevented a worse situation or had a part to play in the manifestation of this one. Theoretically there is no ‘end of the line’ as it is not a linear model and for BA at the end of stage two, i.e., where we are now, what this means is the networks developed in this chapter and the worksheets that are produced from them can be joined with each other. This often occurs in several places such as a common factor, barrier or outcome/potential outcome since all are merely informational nodes within the greater system. This conceptualises a truly non-linear system and maintains a natural approach to investigation and attribution or risk. As the nodes and links multiply a fully integrated view of barriers, nodes and information is formed. No longer is there a need to specify an ‘overrun event’ and allocate that to a particular bracket. Instead, all events are simply events where certain nodes/factors/information were activated in the situation by their interaction with barriers and their strengths or weaknesses.

Through testing of the method with genuine ASR data the validity of the ratings that are being produced have been shown to be useful and accurate. Further than replicating a satisfactory level of rating though, the new method has allowed for greater granularity in rating an event. Through the new spread of A to E events in terms of severity score (see Table 7-10) we can see that granularity is increased as much as 25 times greater levels for D incidents and 10 times more for E incidents. This is important since these levels of incident, as mentioned above, are the most prolific for the Safety team. Any increase in granularity allows for enhanced separation of events even within alphabetised ranges and therefore greater chance to readily use the data to understand the systemic picture of safety. The use of ASR data and the good result of the validation test means historical data (of which BA have tens of thousands of records) can still be applied to the method and is not lost. The positive validation at this stage allows for each ASR feeding back into the scores, the links, the nodes and the model as a whole to keep growing and improving.

This method allows for a standard system of rating throughout the company. The matter of standardisation is not a simple one and not one that will occur overnight. However, with its emphasis on the airline as a whole and the operational *and* occupational elements of an incident the method could eventually be adopted throughout the company. Departmental and company responses to different incidents regardless of ultimate rating, may vary depending on company aims and issues of importance at the time. Departments have the ability to draw up their own addition to the method which requires further investigation within their specialist field of particular events; especially those flagged as having barriers that are constantly under attack or barriers that frequently fail.

In terms of addressing the aims of this study (section 7.1.2), it is felt that this method:

- Is formed on the basis and ***foundation of solid theory*** and exceeds current best-practice found through literature review.

- ***Removes a large amount of the subjectivity*** that is required of risk-raters by “walking” the rater through an incident. This does not prevent an incident being referred for further in-depth investigation should it be warranted; it is merely a way of dealing with a large number of similar safety events and of highlighting the smaller number of novel or significant events.

- ***Standardises the application of risk rating company*** *wide* whilst still allowing for departmental responses to be as flexible as they need to be. This standardisation also allows for non-experts to be brought into the team (or work sent outside of the team e.g. for pilots to rate incidents themselves using this method) and therefore addresses a concern that any new member of the Safety Services team would not hold the experiential knowledge of a previous member.

- ***Removes the frequency bias*** that limits the usefulness of current data whilst also improving the communicability of the data to the board by using company-wide safety metrics. Frequency remains an intrinsic part of this method though since details are kept of the number of that type of incident that occur. However, what is removed is the logarithmic skewing effect that frequency was having on 'minor' events during matrix use. In addition to this BA would benefit from keeping track of the number of times each barrier is highlighted as important in an incident whether in a negative or positive sense.

- Building on this point, all knowledge is basically built into the pathway models for incidents as they are developed and modified over time. This combats the issues of ***knowledge retention*** highlighted.

- ***Increases the granularity*** of incidents in the most common severity brackets (i.e., D and E) whilst not detracting from the significance of more severe incidents.

- Will continue to build upon itself and develop so that the more analyses are carried out so the more comprehensive the pathways and rating becomes. The networks (and worksheets developed from them) are not static; they can be updated and manipulated as the system changes or with developments in barriers/factors and staff knowledge.

The important feature of the method is not in gaining new severity scores necessarily but in the way in which those scores are gained subjectively, with an emphasis on potential and without the skewed effects of frequency taking over. Coupled with the movement towards truly predictive safety management that this model brings gives the method real potential.

The challenge ahead is to now implement this new methodology. A central core of standard incidents from the operational perspective have been drawn up and tested for this project and it would now be sensible to draw on SMEs from other areas such as Engineering, Ground Ops and Cabin Crew to do the same. Testing can be done against historical data and SME knowledge.

7.6.3 **Summary**

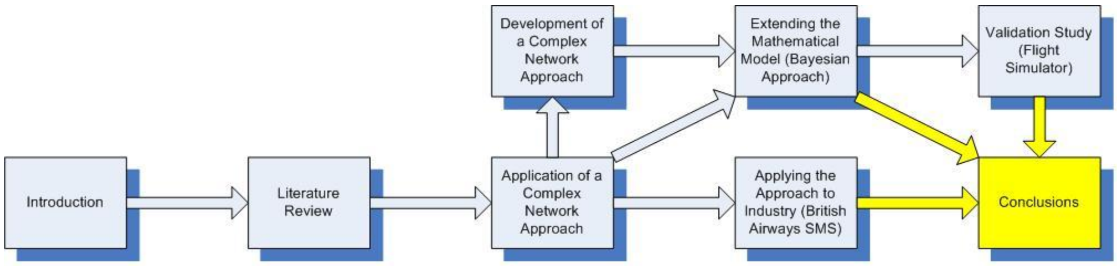
The beauty of the model presented in this chapter, for both academic and industrial partners, is that there is tremendous scope for development. As more investigation is carried out into network models and the metrics associated with those there is the great potential. Computer processes and algorithms can be integrated to analyse and test barriers, centralised due to this work, within the system. This may offer the chance to study error migration within a system and predict effects on the network as a whole should proposed changes to barriers (i.e. operational procedures and equipment etc.) be made.

Further than this is the work required to investigate and define a common value of risk. There is much scope for research and development into building a unified approach to risk management aiming to draw on the experience and specialised knowledge of operators, manufacturers, regulators and academia. Areas such as the A to E labelling of incidents and company responses to events, in order to become less arbitrary, require further modelling and identification of company priorities. This would involve defining a value of risk based upon, e.g., a cost of life (and from this a cost of injury based upon equivalent fatalities as used in the railway industry) or the cost of brand image etc.

Central to the continuing development of the work, and drawing the issues back towards the themes of this thesis, is the need to move towards complex non-linear models. The steps taken away from risk matrices are significant despite not yet being able to arrive at fully non-linear methods. Through this mini-study, the opportunity to work with the airline and maintain firm roots within industry adds extra dimensions to the thesis. It achieves real focus on the potential application of the thesis model in the future and the benefits that a non-linear method can bring to safety management.

The ultimate aim of this work and of the safety team at British Airways has to be a common direction for all industries dealing with complex systems and risk. Despite the need for BA-centric methods, the models and knowledge behind those has to be merged from aviation partners and non-aviation industries alike. This is the next big challenge in order to fully recognise the potential in network diagrams and predictive modelling of risk.

8 Conclusions



8.1 Thesis Contribution

8.1.1 Overarching Thesis Themes

This thesis has developed the notion of complex systems requiring complex models to fully understand them. The current literature has shown that for a considerable time, models used within aviation accident investigation have been dominated by linear chain models and this is addressed. EAST is initially identified as a suitable toolkit approach that moves closer towards this ultimate dynamic and complex model. The fundamental strength identified within EAST is the use of information networks and these are developed in a novel way to integrate conscious ownership and transfer of information. This centralises a continuing theme of the thesis - communication.

Information networks alone improve the understanding of the system in which events take place. They also allow positive, neutral and negative outcome events all to be integrated and studied. A common concern within accident investigation models however is the level of subjectivity and the artificial fitting of events to a method. This thesis evaluates a new quantitative method of accident investigation. This Bayesian method develops the information networks and addresses complex issues such as error migration.

The application of information networks to an industry safety management system have led to the adoption of this information network based approach. The complexity of the methodology cannot be underestimated and it will take time for the comprehensive elements of the model are working holistically in one model. However, this industrial setting allows continued testing of the usefulness and usability of the approach.

This thesis has set out to improve the model and method of aviation accident investigation currently being used as the industry standard.

8.1.2 **Contributions Summarised**

8.1.2.1 Information Networks as an Accident Investigation Method

Firstly, the thesis embarks on a journey that moves away from the linear models that currently dominate aviation accident investigation. The real world is a complex system and this is clearly identified in chapter 7 working with an airline. This thesis has developed a **novel application of information networks to aviation accidents**. Further than this though, it has **developed this method to integrate ownership of information** thereby achieving more detail within a single network.

Through this work the theme of information flow, or, **communication has been centralised** as a key aspect of understanding the state of the system. This approach gives a greater insight into not just the ‘what’ but the ‘how’ and ‘why’ of events.

8.1.2.2 Integration of Bayesian Mathematics

The thesis also sets out, in chapter 5 and 6, a new model which **incorporates the elements of information networks and those from Bayesian mathematics** in order to improve objectivity and being to address the issues of error migration and potential barrier failure. This new approach utilises historical data to highlight often used nodes and pathways and from this strong, weak, unused or overused nodes can be identified. In addition, the extra dimension that Bayesian mathematics adds to the networks is the movement towards modelling and **understanding error migration and the effects of barrier manipulation**.

8.1.2.3 Centralisation of Barriers not Accidents

General Aviation is an area that, despite some literature, is largely unstudied in terms of accidents. There is no doubt that the world of GA is very different to that of Commercial transport. However, the novel use of information networks overcomes the limitations of so many more linear methods so that it **can be applied to both GA and Commercial environments**. Through the **centralisation of understanding the system rather than the event** this new method can be used to understand both flying environments equally. This thesis contends that information transfer is key to understanding a complex system and the basis for events regardless of the levels at which this transfer is taking place. The new approach considers **barriers as fundamental** to understanding the passage of information throughout a system network. The study of both negative and positive impact barriers (or factors) reveals more than a surface level approach limited by event types.

This same thinking allows the **method to be used to address both accidents and incidents** as each can be modelled through information networks. This novel development removes the classification of events as a particular type or level and instead looks at the system holistically and regardless of whether an event has occurred or not.

8.1.2.4 Novel Safety Management System

Incidents are the basis for the integration of the method into an airline's SMS. They work well to populate the information networks and key to their use is to **identify the potential outcomes** and reasons for more **positive outcomes** than an accident. A continuous stream of incidents like these can be integrated into the network model to provide an up to date analysis of the system safety. Rather than terming these events as incidents, though, it would be more proper and in keeping with the thesis to term it as a potential-accident that has been prevented.

This thesis has introduced the **first SMS model that does not adhere to the edict that Risk = Frequency x Severity**. It was identified that such a dogmatic view is preventing airline safety staff from effectively communicating risk in the system. Instead, through the centralisation of a potential accident's severity and the barriers that were broken, or remain, on the path to that outcome, a truer value of risk to the organisation is sought. The **positive factors preventing an accident are central to this new methodology** and the approach of risk rating staff is, for the first time, encouraged to look beyond any actual event to potential and successful positive features.

Further than the aims set out originally, this thesis has progressed beyond simply a piece of academic work. The work with a legacy airline and the integration of the network approach, even at an initially developmental level, into the SMS is a coup for the usefulness of the new approach set out in this thesis.

8.2 Tying Together Several Aspects of the Thesis

The aims of the thesis are set out in chapter 1 and are three-fold. The first was to develop and test a new method that departs from the current dominating linear models. The second aim of the thesis was to make any method or model applicable to General Aviation and that is covered in section 8.2.3. Section 8.2.3 also addresses the issue of accidents versus incidents. Although no comprehensive effort has been made in this effort to support, or counter, the common cause hypothesis, the methods and model used allow that argument to be put to the side and instead concentrate on the holistic system not a singular event.

Through several varied studies found in chapters 3 to 7 of this thesis these aims have been at the centre of the work. The following example of work that can be carried out on the basis of the developments from this thesis aims to show how all the aims, studies and conclusions can work together to improve aviation safety methods.

8.2.1 Developing the Predictive Nature of the Bayesian Network

Chapters 3 and 4 look at validating information networks with respect to aviation accident investigation. Further than this the potential for quantitative metrics was identified and tested. Chapter 5 integrated a level of Bayesian mathematics into information networks and MATLab was used with a Bayesian toolkit for a general aviation scenario. This was tested in chapter 6 against a flight simulation study to validate the use of historical data within the Bayesian information networks. This can be extended though and has potential for use in a system similar to that described and developed in chapter 7 with British Airways. Therefore, the type of process explored below has the potential of bringing all of the chapters' work together and providing a comprehensive qualitative and quantitative network approach to predicting error migration and safety risks. This is not intended to form part of the studies proper for this thesis but give an indication of forward motion of the work in this thesis and a platform for indicating the relationships between chapters, studies and the methods contained within the thesis.

With slight tweaks to the program code developed in chapter 5 (figure 8-2) it is possible to develop iterative processes based on the historical data and nature of relationships of the nodes. The code has been modified in order to take into account any changes that may be made, through the introduction of a barrier, prior to the node Heavy Landing. As discussed the nature of this barrier, so long as it is shown to be effective is not important and for the purposes of this study takes the form of a verbal instruction. It is predicted that this instruction reduces the probability of occurrence of the node Heavy Landing and as such the new iterative process predicts the magnitude of effect on the network outcome; Nosewheel Collapse in this instance.

The main changes to the code are summarised here for completeness and reference back to chapter 5 is recommended to identify the changes. Lines 36 and 37 tell the program to spread the probability removed from the node Heavy Landing (by manipulating the pre-node barrier) as per the ratio of probability spread of the historical data (see figure 8-1).

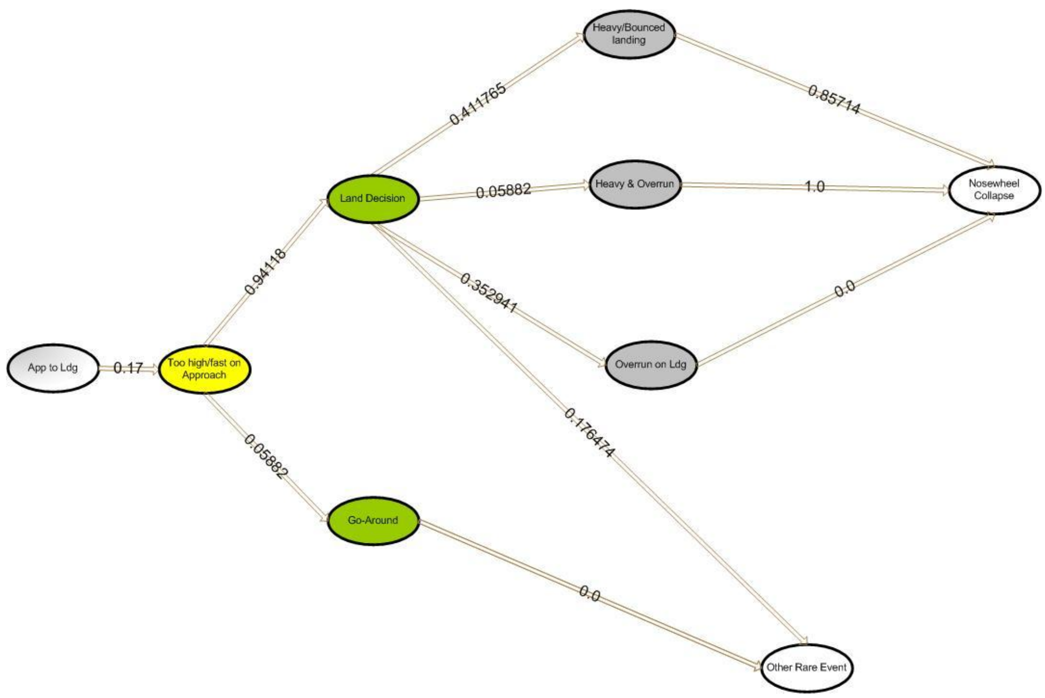


Figure 8-1 - Information network with non-conditional probabilities applied

Line 32 then tells the program to step-by-step increase the proportion of this removed probability that is going to the nodes “Overrun” and “Other Rare-Event” (therefore reducing the ratio that is received by the node “Heavy and Overrun”). This method looks at two different ways the error may migrate, therefore introduces the possibility of tracking error migration. As more data is collected and more relationships understood (and thus programmed into the network) so error migration itself may be modelled and predictions of exact migration pathways investigated. In addition this introduces a level of cost-benefit analysis since with the introduction of a barrier a best-result outcome may be observed if the error is equally split or divided based upon the probability of each node prior to intervention. This may allow for the concept of barriers being required further back in the network in order to control the migration of error and information flow in the newly manipulated network; this is an improved method above attempting to control outcomes since it is working at a deeper level.

Since the probability of a nose wheel collapse is zero from the data used if an aircraft simply overruns the program can then predict the best outcome from the limited situation. Line 33 then tells the program to iterate the process of changing the probability of the node “Heavy Landing” occurring from 0 to 1 with 0.05 intervals. This then gives the program all possible outcomes of manipulating the pre-node barrier.

Editor - E:\MATLAB\FullBNT-1.0.4\work\TooHighTooFastPlotProbabilityConditional_Ba_loops.m*

```
countDF = 1;
for ratio = 0:0.05:1 %moves probability mass on to just overrun and rare-event
    for df = 0:0.05:1 %iterate over probablility of heavy landing

           diff = 1-df - DA - DB - DE;
           da = DA + (diff*(DA/((DA+DB)+DE)))*(1-ratio);
           db = DB + (diff*(DB/((DA+DB)+DE)))+ (diff*(DA/((DA+DB)+DE)))*ratio;
           de = DE + diff*(DE/((DA+DB)+DE));

           if abs(1-(df+da+db+de))>0.00001
               keyboard
           end

           noseWheelCollapse.CPD{1} = tabular_CPD(noseWheelCollapse, 1, [1-0.94118 0.94118]);
           noseWheelCollapse.CPD{2} = tabular_CPD(noseWheelCollapse, 2, [1 1-da 0 da]);
           noseWheelCollapse.CPD{3} = tabular_CPD(noseWheelCollapse, 3, [1 1-db 0 db]);
           noseWheelCollapse.CPD{4} = tabular_CPD(noseWheelCollapse, 4, [1 1-de  0 de]);
           noseWheelCollapse.CPD{5} = tabular_CPD(noseWheelCollapse, 5, [1 1-df 0 df]);
           noseWheelCollapse.CPD{6} = tabular_CPD(noseWheelCollapse, 6, [1 1 1 0 0 0 0 0 1-0.85714 0 0 0 0 0 0 0 0 0

           evidence = cell(1,numNodes);
           evidence{1} = 2; %evidence that 'Decision to Land' is true

           engine = jtree_inf_engine(noseWheelCollapse);
           [engine, loglik] = enter_evidence(engine, evidence);

           marg = marginal_nodes(engine, 6);
           marg.T;

           pC(countR,countDF) = marg.T(2);
           countDF=countDF+1;
    end
    countR = countR+1;
    countDF = 1;
end

surf(pC);
hold on
```

script Ln 2 Col 1 OVR

Figure 8-2 - Screencapture of the modified MATLab code incorporating iterative loops

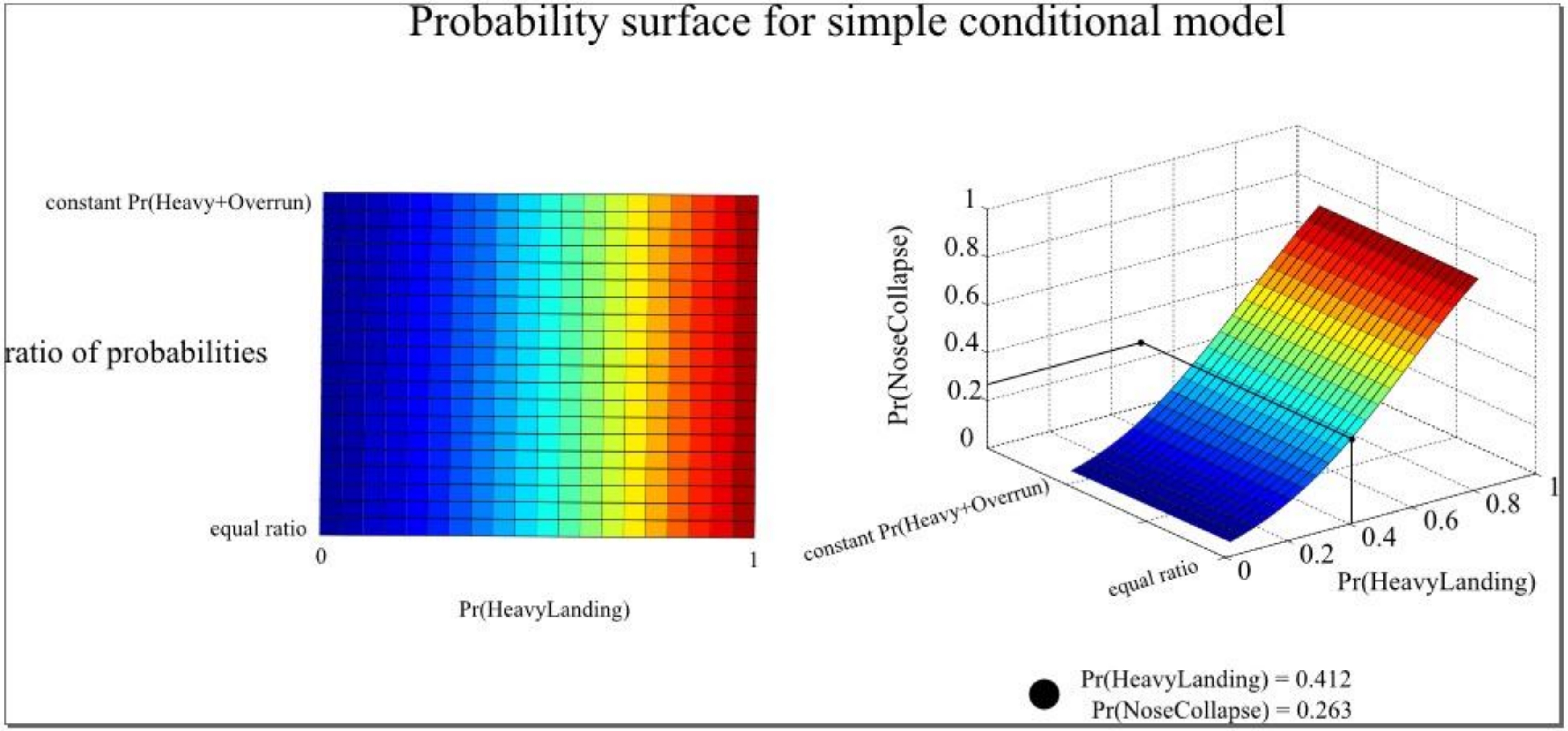


Figure 8-3 - Resultant probability surface for Bayesian iteration

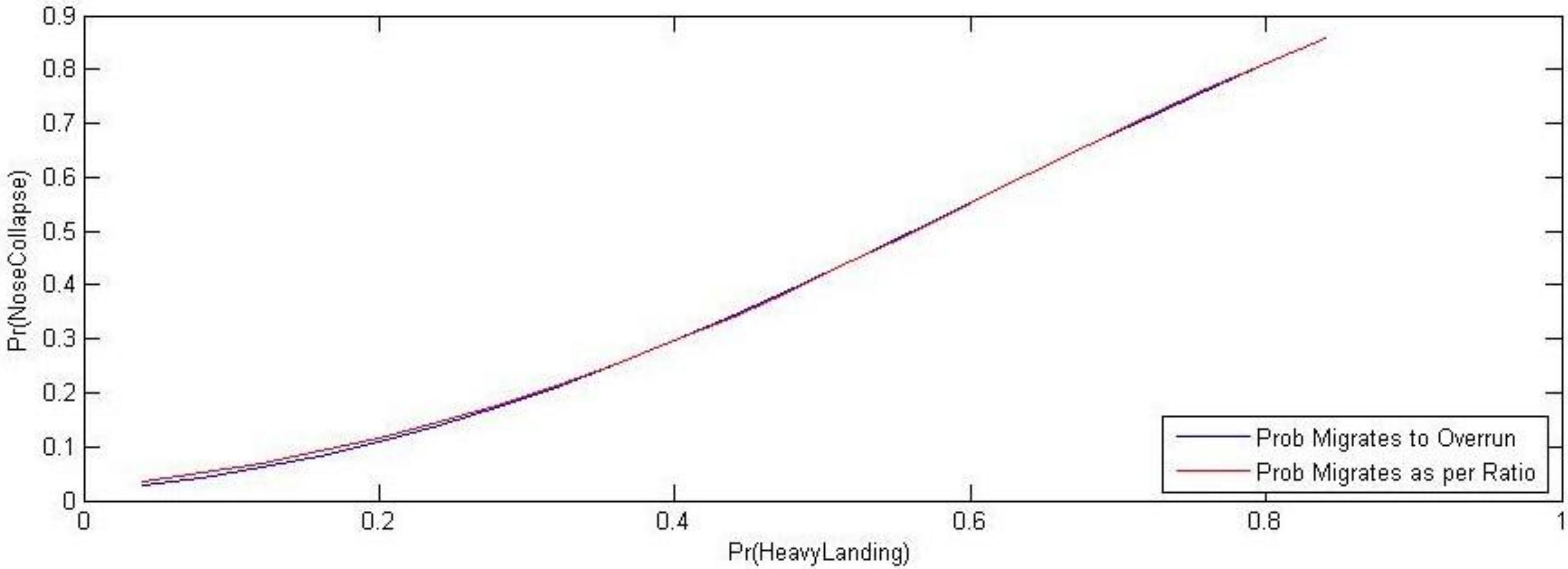


Figure 8-4 - Line graph illustrates slight reduction of Pr(NoseCollapse) with iterative process

Line 67 then executes the drawing of a surface plot (figure 8-3). This surface plot illustrates the changes in the probability of the nodes “Heavy Landing” (x-axis) and “Nose Wheel Collapse” (y-axis) through the range of iterative spread of the probability removed at the pre-heavy landing barrier (z-axis).

The surface is not uniform although the differences in this example are small. The slight distortion of colour of the flattened spread (on the left of figure 8-3) is due to slight deviations of probability reflecting a non-linear increase at different iterative stages. The black dot (on the right of figure 8-3) represents the actual AAIB data and the prediction of nose wheel collapse from that data in this network. Figure 8-4 displays the two ends of the flat surface as a line graph to illustrate the subtle differences present.

The red line in the graph is the standard result of removing probability (from 0 to 1) from the node “Heavy Landing” and spreading it as per the ratio defined in the historical data. The blue line spreads the removed probability via an increasing share to the nodes “Overrun” and “Other Rare Event”. It can be seen that this second process is slightly more favourable (probably due to the nature of the probability of Nose Wheel Collapse post-overrun only events being zero in this data sample) as the graph begins lower on the y-axis and also the line ceases much earlier up the y-axis than the blue.

The key potential of these graphs is that if the direction of probability (error) migration can be controlled (and for this reference back to the nodes within the network highlighted as being of importance (or related) is necessary) then instead of the error migrating as per the normal population of data it could be directed to gain the best net result for the whole network and not simply one event or node or barrier within the system. This removes any localised manipulation of barriers without due attention being drawn to the effects farther afield.

The ultimate aim of this method would be to have highlighted an area of concern and then look at all possible outcomes of manipulating a particular barrier (in this case the pre-heavy landing node barrier). All possible pathways of probability (or error) migration are then identified and then additional manipulations can be carried out on additional barriers in an attempt to direct and control the spread of this migration towards the most positive outcomes identified on the surface plot drawn.

Extracting this concept to larger more complex networks then, firstly it would be possible to identify links that will be affected by any planned change (or for that matter any changes noted in the recorded events’ historical data) that would not otherwise be immediately obvious. Secondly, this can be taken further to attempt to identify whether manipulating a barrier may in fact have an overall negative effect or too much of a negative effect elsewhere that the reduction it would give in one place is not enough to warrant the change. This overcomes the still current issue in industry of sticking-plaster remedies within complex systems. It is not a large step then also to develop the cost-benefit analysis side of such a networking model.

8.2.2 Further application

The potential of this novel method as a way of not only understanding the system in which accidents are occurring but also of potentially beginning to control it is clear. Using the methods above the surface plot highlights the most positive possible outcome and then the information networks behind the plot highlight the nodes and links/barriers associated with such an outcome. Together these can be manipulated to reinforce the barriers preceding negative nodes and reduce the barriers preceding perceived positive nodes in order to gain an overall increase in positive outcomes. From the thesis as a whole it can be seen how, despite being based on General aviation, this applied to the type of method developed in chapter 7 for an airline could provide real cost-benefit application from a non-linear foundation and using incidents and accidents together as one source of data (the three thesis aims drawn together).

There are, however, a number of obstacles (some of which are highlighted above) and further potential that can be identified as areas for a lot of further work in the future.

It is possible to model non-mutually exclusive events within networks and also to include feedback loops and multi-layered networks but all of this requires much more data. The aim is to arrive at a comprehensive network that could show every possible result of changing a barrier (resulting in changing a probability) and then looking to expand the usability of such a network.

Further studies are required therefore where the amount of data building and populating the information networks is increased. The number of CPTs required to populate the Bayesian information networks grows exponentially with the number of nodes included so this is not a small task. Traditionally, probabilities and changes to them are often control by subject matter experts (SMEs). As the field of Bayesian networks continues to grow there are also more opportunities to utilise advanced programming and mathematical methods to aid an information network model. Das (2004) has studied the application of algorithms to Bayesian networks (only in fault-trees which is the current standard) and this has huge potential for this work. If there were adequately populated databases that recorded trends and historical data (such as those available in aviation) then Das (2004) argues that batch learning can be used. In batch learning, the formation of CPTs is automated by advanced programs so this would overcome some of the issues of sheer size encountered by applying this approach on a larger scale. It is also possible to incorporate system learning into any large scale models. With further development, data from accident and incident reporting schemes can constantly update the probabilities and relationships of all the nodes present (Trucco *et al*., 2007).

Even at this stage though, despite the results not necessarily being exact quantitatively, the information networks allow “relative” predictions. That is to say, whether manipulation at one point is likely to cause a related node to change a lot or a little and also in which direction. This is especially true once the networks model interacting relationships rather than solely mutually exclusive ones. The more data that can be used to populate these networks using the methods above so the more potential there is to predict accurately and usefully not just in terms of quantitative data predictions of node occurrence but also relationship data between links and nodes and barriers.

For the initial analysis of the nose wheel collapse scenario the probability removed from the node “Heavy Landing” was redistributed as per the ratio of historical data. There is plenty of scope for further work in understanding whether this is a suitable assumption. Chapter 6 takes these data and attempts to validate the potential use of such Bayesian information networks using a flight simulator study.

Once a comprehensive network is arrived at that is not the end of the potential with this method. One of the major benefits of using Bayesian mathematics as a basis for this model is that it was born of merging both quantitative data and also SME knowledge. As such there are several avenues of utilising the strengths of each in order to produce the most effective and comprehensive network methodology.

Specialists can apply weightings to the Bayesian information networks in order to model known relationships that aren’t identified purely with the historical data. This can complement the iterative approach outlined in chapter 5. SMEs can also begin weighting the strength of links (and intrinsically the barriers on those links) therefore giving the network the knowledge to show migration through weaker barriers’ links. Finally, SMEs can begin to weight barriers and nodes in terms of cost, whether that be financial, to life or to brand image and publicity. In doing so, manipulating barriers within the network before the real world may elicit useful information as to the overall effect for the company/individual/operator and allow an informed decision to be made.

The approach at present is illustrated in a relatively linear fashion. However, the information network approach is far from linear and expansion of the topics discussed within this chapter to a full information network would overcome this initial limitation. The ultimate aim is to develop a 3D model which reflects more fully the real world accident system information space that is so often being misrepresented in current models. **This addresses the first thesis aim; to improve upon the linear models dominating aviation safety with a non-linear alternative.**

The potential for use of these networks does not stop at GA though. Commercial aviation holds great repositories and databases of abnormal operation information and accident/incident data that could be used to populate information networks in order to learn about salient information and communication issues. An information network model using probabilities in this way, it is anticipated, would combine very well with current safety management systems in use through aviation today. By exploiting the ability of the networks to give some insight into possible migration effects post-barrier implementation, it may be possible to provide cost-benefit analysis of future changes to an aviation system. **This addresses the second and third thesis aims; to develop a method that can transcend general and commercial aviation operations and to fully utilise incidents (or near-misses) in a way similar to accidents.**

8.3 Developments and directions for future work

As stated in the thesis, and in this chapter, there is much scope for continuing work to develop the models and ideas that have been set out. The thesis has concentrated on several aspects of a whole new approach to understanding aviation accidents and the recombination of these, although central to thinking throughout, will be the continuing goal of this work. The ultimate aim of this work is to move towards a 3-dimensional multi-network approach to illustrating and understanding the system in which events are taking place. Through the work of this thesis, this goal is much nearer and yet there is a need to identify some complex work ahead.

The synergies that exist between the chapters have been loosely highlighted in the chapter signposting and a key central thread to the thesis. Figure 8-5 illustrates aspects of the ultimate reintegration of all the facets set out.

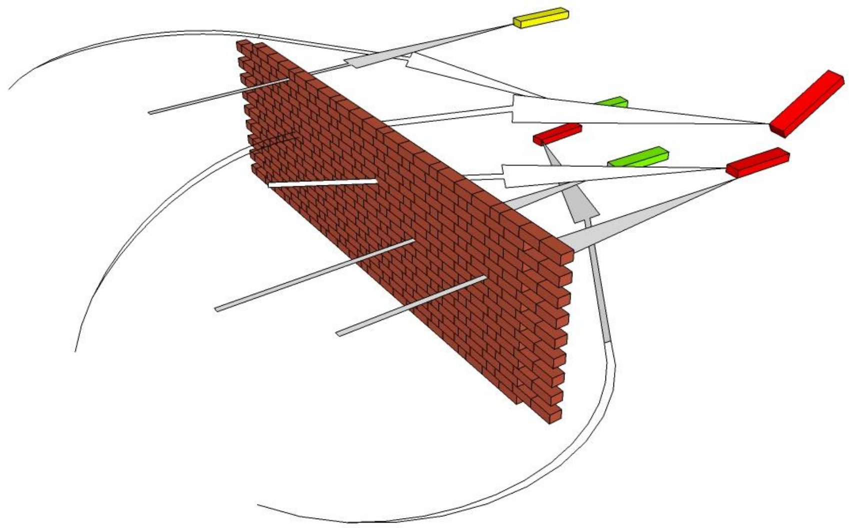


Figure 8-5 - 3D depiction of a portion of the information network and a single barrier

There is no escaping the complex nature of the world in which aviation accidents take place. Therefore, any method attempting to understand and investigate these must by its very nature be complex. A number of information networks as used throughout this thesis can be linked together so that they stack on top of each other. Links would therefore exist both intra- (grey arrows in figure 8-5), and, inter-network (white arrows in figure 8-5). These links may have barriers, and/or positive factors, associated with them (brick wall in figure 8-5). Due to the nature of the networks, more than one link may lead to the same node but via very different pathways often being affected by different barriers and factors (depicted by some links passing through, whilst others pass around the particular barrier pictured). In addition, each node may have many links emanating from it.

The work through this thesis has centralised barriers affecting the flow of information around the system. By focussing on these barriers many of the limitations of non-linear models can be overcome. Significantly, by concentrating on the barriers, the event itself becomes secondary and the issues of classification (or even whether the event has a positive or negative outcome) are avoided. This strengthens the network approaches ability to understand a system comprehensively and reap the benefits of incident and positive reporting for the future. Within the approach, a single barrier could be identified as having links from several networks with very different predecessor and successor nodes. This model makes clear that any changes to that barrier may have a far reaching effect on nodes (or even networks) not originally intended to be manipulated. A comprehensive network will draw this information out and through iterative processes and quantification, predictions can be made. In this way a complete, holistic and comprehensive analysis of barriers can be effected. Only then can the strength and importance of a particular barrier be fully understood and any action taken to modify or reinforce it. This is the basis for full a cost-benefit analysis type approach. Methods such as Bayesian mathematics allow for some prediction of the nodes and barriers that will affect each other and which of these is critical.

Ultimately this method can be developed to identify the severity or likeliness of a node occurring (or barrier failing). Nodes can be colour-coded as incident data is continually entered into the model to reflect the current true state of safety and risks to the system. Through highlighting the bottlenecks and potential failures of information flow, the network model can alert safety managers of impending issues. Further than this, the same method, when applied to specific accidents, incidents or positive outcome events, can elicit specific details about the flow of information and communication state of particular areas of the system. Together with the ability to apply metrics highlighting key information processing nodes, such as sociometric status these attributes mean that the information network model has the potential to be used in almost all aspects of system safety.

In addition to these future developments it is a continuing aim from this thesis work to ensure the successful integration of a non-linear model to the airline's SMS. As identified in chapter 7 the current stage is just one in a long line ahead. Working with industry has its benefits and restrictions so it is important to be realistic in short timescale improvements. However, the movement towards the common goal is significant and work will continue in partnership.

8.4 Closing remarks

Setting out on the journey that this thesis represents there was such a large subject area to be explored and understood. Focussing ideas to a central theme and set of aims or objectives took time and a sense of realisation that the issue of aviation accidents will not be solved in one attack. However, it is hoped this thesis at least demonstrates the passion that is felt for further understanding of the complex system as a whole and the movement away from artificially isolated and restrictive approaches. There is no doubt that the more complex a method the more often it can be passed-over by industry in particular. The fact that a developmental stage towards a comprehensive complex method has been achieved in an airline and their enthusiasm for the model underlying it shows that industry is keen to move on also.

This thesis represents several years work towards what can almost be described as an infinite goal; the improvement of aviation safety. I feel certain that this thesis has moved the theory and application of complex methods forward. As such methods are further developed and applied to more situations and across more domains so the real benefits of a data-harvesting, self-populating 3-dimensional system safety model will increase.

9 References

Adams, E. (1976). Accident Causation and the Management Systems. *Professional Safety,* (Oct), pp. 26-29.

Adelstein, A.M. (1952). Accident proneness: A criticism of the concept based on an analysis of shunter's accidents. *Journal of the Royal Statistical Society,* 115, 354-410.

Air Accident Investigation Branch, (1990). *Aircraft Accident Report (EW/C1095).* 4/90. Farnborough: AAIB.

Ale, B.J.M., Bellamy, L.J., Cooke, R.M., Goossens, L.H.J., Hale, A.R., Kurowicka, D., Roelen, A.L.C. and Smith, E. (2005) Development of a causal model for air transport safety. *Advances in Safety and Reliability ed. Kolowrocki.* London: Taylor & Francis. pp 37-44

Ale, B.J.M., Bellamy, L.J., Van der Boom, R., Cooper, J., Cooke, R.M., Goossens, L.H.J., Hale, A.R., Kurowicka, D., Morales, O., Roelen, A.L.C. and Spouge, J. (2007) Further development of a causal model for air transport safety (CATS); building the mathematical heart. *Risk, Reliability and Societal Safety – Aven & Vinnem eds.* London: Taylor & Francis. pp 37-44

Allen, T.J., (1984). Managing the Flow of Technology: Technology Transfer and the Dissemination of Technological Information Within the R&D Organization. Cambridge, MA, USA: MIT Press.

Australian Transport Safety Bureau (ATSB), (2001). Investigation Report on the accident of Boeing 747-438, VH-OJH, Bangkok, Thailand, 23 September 1999. *Accident Report No. 199904538*. ATSB, Australia.

Australian Transport Safety Bureau (ATSB), (2007) Human factors analysis of Australian aviation accidents and comparison with the United States. *Aviation Research Paper No. B2004/0321.* Canberra: ATSB.

Ayeko, M. (2002). *Integrated Safety Investigation Methodology (ISIM).* GIST Technical Report G2002-2.

Bandener, N. (2005). The Management Oversight and Risk Tree. *Paper for the Seminar: User interfaces of Safety-Critical Systems.*

Baybutt, P.(2002). Layers of Protection Analysis for Human Factors (LOPA-HF). *Process Safety Progress,* 21 (2), pp. 119 – 129.

Bayes, T. (1763). An Essay towards solving a Problem in the Doctrine of Chances. *Philosophical Transactions of the Royal Society,* 53, pp 370-418.

Beaty, D. (1995). The Naked Pilot: The Human Factor in Aircraft Accidents. England: Airlife Publishing Ltd.

Bedny, G. and Meister, D., (1999) Theory of activiy and situation awareness. *International Journal of Cognitive Ergonomics*, 3(1), pp 63-72.

Benner, L. (1975). Accident Investigation: Multilinear Events Squencing Methods. *Journal of Safety Research,* 7(2), pp. 67-73.

Bennett, S. A. (2004) The 1st July 2002 Mid-air Collision over Oberlingen, Germany: A Holistic Analysis. *Risk Management,* 6, pp 31-49.

Benta, I.M. (2003). Agna.

Besnard, D., Greathead, D. & Baxter, G. (2004) When Mental Models Go Wrong. Co-occurrences in Dynamic, Critical Systems. *International Journal of Human-Computer Studies.* Vol. 60 pp 117-128.

Bird, F.E. (1966). Damage Control. Philadelphia, USA: Insurance Company of North America.

Bird, F.E. & Davies, R.J. (1996). Safety and the Bottom Line. Loganville, GA: Institute Publishing.

Bird, F.E. & Loftus, R.G. (1976). Loss Control Management. Loganville, GA.: Institute Press.

Boeing Airplane Safety Engineering. (1996). *Statistical Summary of Commercial Jet Aircraft Accidents: Worldwide Commercial Jet Fleet 1959-1995.* Seattle, USA: Boeing Commercial Airplane Group.

Bortkiewicz, L.V. (1898). Das Gesetz der kleinen Zahlen. Leipzig: B. G. Teubner.

Braithwaite, G.R. (2001). Attitude or Latitude? : Australian Aviation Safety. UK: Ashgate Publishing Limited.

Brusberg, A., Solodilova, I., Hourizi, R. & Johnson, P. (2002). A Framework for Re-examining Accident Reports to Support Interaction Design Processes, C.W. JOHNSON, ed. In: *Proceedings of the Workshop on Investigation and Reporting of Accidents (IRIA).* GIST Technical Report G2002-2, 2002, Glasgow University.

Busby, J.S. & Hibberd, R.E. (2002). Mutual Misconceptions Between Designers and Operators of Hazardous Systems. *Research in Engineering Design,* 13(3), 132.

Carroll, J.M., Kellogg, W.A. & Rosson, M.B. (1991). The task-artifact cycle. In: J.M. CARROLL, ed, *Designing interaction: Psychology at the human-computer interface.* Cambridge, UK: Cambridge University Press, pp. 74-74-102.

Carvalho, P.V.R., Vidal, M.C. & Carvalho, E.F. (2007) Nuclear Power Plant Communications in Normative and Actual Practice: A Field Study of Control

Room Operators' Communications. *Human Factors in Ergonomics and Manufacturing,* 17(1), pp 43-78.

Carvalho, P.V.R., Gomes, J.O., Huber, G.J. & Vidal, M.C. (2009) Normal People Working in Normal Organizations with Normal Equipment: System Safety and Cognition in a Mid-Air Collision. *Applied Ergonomics,* 40, pp 325-340.

Center for Chemical Process Safety (CCPS), (2001). Layer of Protection Analysis: Simplified process risk assessment. New York, NY: CCPS.

Chappell, S.L. (1994). Using voluntary incident reports for human factors evaluations. *Aviation Psychology in Practice,* pp. 149-172.

Collins, A.M. & Loftus, E.F. (1975). A spreading-activation theory of semantic processing. *Psychological Review,* 82(6), pp. 407-428.

Connell, L. (1995). Pilot and Controller Communication Issues, B.G. KANKI and O.V. PRINZO, eds. In: *Proceedings of the Methods & Metrics of Voice Communication Workshop. Final Report No. DOT/FAA/AM-96/10,* 1995, FAA.

Cox, S.J. & Tait, N.R.S. (1991). Reliability, Safety and Risk Management. Oxford: Butterworth-Heinemann.

Cresswell, W.L. & Froggatt, P. (1963). The causation of bus driver accidents; an epidemiological study. London, UK: Oxford University Press.

Dahlstom, N., Dekker, S., Van Winsen, R. & Nyce, J. (2009). Fidelity and validty of simulator training. *Theoretical Issues in Ergonomic Science,* 10(4), pp. 305-314.

Davies, J.B., Wright, L., Courtney, E. & Reid, H. (2000). Confidential Incident Reporting on the UK Railways: The 'CIRAS' System. *Cognition, Technology and Work,* 2(3), pp. 117--125.

Das, B. (2004) *Generating Conditional Probabilities for Bayesian Networks: Easing the Knowledge Acquisition Problem.* Research Report DSTO in Journal CoRR cs.AI/0411034, Australia.

Deerwester, S., Dumais, S.T., Furnas, G.W., Landauer, T.K. & Harshman, R. (1990). Indexing by Latent Semantic Analysis. *Journal of the American Society for Information Science,* 41(6), pp. 391-407.

Dekker, S. (2006). The Field Guide to Understanding Human Error. Aldershot, UK: Ashgate Publishing Ltd.

Dekker, S. (2002). The Field Guide to Human Error Investigations. Aldershot, UK: Ashgate.

Dekker, S. W. A. (2005). Ten Questions about Human Error. New Jersey, USA: Lawrence Erlbaum Associates.

Dekker, S. & Hollnagel, E. (1999). Coping with Computers in the Cockpit. England: Ashgate Publishing Ltd.

Ebbatson, M., Harris, D., Huddlestone, J. & Sears, R. (2010). The relationship between manual handling performance and recent flying experience in air transport pilots. *Ergonomics,* 53(2), pp. 268--277.

Edwards, M. (1981). The design of an accident investigation procedure. *Applied Ergonomics,* 12, pp. 111-115.

Embrey, D.E. (1986). SHERPA: A systematic human error reduction and prediction approach, *International Meeting on Advances in Nuclear Power Systems,* 1986.

Federal Aviation Authority; FAA. (2000). System Safety Handbook. Available: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook

Farmer, E. & Chambers, E.G. (1929). *A Study of Personal Qualities in Accident Proneness and Deficiency.* 55. London, UK: Industrial Fatigue Research Board.

Farmer, E. and Chambers, E.G. (1926). *A Psychological Study of Individual Differences in Accident Rates.* 38. London, UK: Industrial Fatigue Research Board.

Fischhoff, B. (1975). Hingsight does not equal foresight: The effect of outcome knowledge on judgement under uncertainty. *Journal of Experimental Psychology: Human Performance & Perception,* (1), pp. 288-299.

General Aviation Safety Council (GASCo), (2010) A Study of Fatal Stall or Spin Accidents to UK Registered Light Aeroplanes 1980 to 2008, GASCo Publication.

Gibson, W.H., Megaw, E.D., Young, M.S. & Lowe, E. (2006). A Taxonomy of Human Communication Errors and Application to Railway Track Maintenance. *Cognition, Technology and Work,* 8(1), p. 1435.

Green, D.M. & Swets, J.A. (1966). Signal Detection Theory and Psychophysics. New York: Wiley.

Greenwood, M. & Woods, H.M. (1919). A Report on the Incidence of Industrial Accidents Upon Individuals With Special Reference to Multiple Accidents.

Gregoriades, A. & Sutcliffe, A.G. (2006). Automated Assistance for Human Factors Analysis in Complex Systems. *Ergonomics,* 49, p. 1265.

Griffin, T.G.C., Young, M.S. & Stanton, N.A. (2007). A Complex Network Approach to Aviation Accident Analysis, P. BUST, ed. In: Contemporary Ergonomics 2007, Aldershot: Ashgate Publishing.

Groeneweg, J. & Roggeveen, V. (1998). Tripod: Controlling the human error components in accidents, LYDERSEN, HANSEN and SANDTORV, eds. In:

Safety and Reliability; Proceedings of the ESREL 2003 Conference, 1998, Swets and Zeitlinger, pp809--816.

Guastelo, S., J, (1993). Do we really know how well our occupational accident preventio programs work? *Safety Science,* 16, 445-463.

Habberley, J.S., Shaddick, C.A. & Taylor, D.H. (1986). *A Behavioural Study of the Collision Avoidance Task in Bridge Watchkeeping.* Technical Report. Warsash, Hampshire: College of Maritime Studies.

Haddon, W. (1961). *Research with Respect to Fatal Accident Causes: Implications for Vehicle Design.* 336A. New York, USA: Society of Automotive Engineers.

Harris, D. (2009). A Design and Training Agenda for the Next Generation of Commercial Aircraft Flight Deck, D. HARRIS, ed. In: *Engineering Psychology and Cognitive Ergonomics,* 2009, Springer, pp 529--536.

Harris, D. (2008). Cockpit Design and Cross-Cultural Issues Underlying Failures in Crew Resource Management. *Aviation, Space, and Environmental Medicine,* 79(5), pp. 537--538.

Harris, D. (2007). A human-centred design agenda for the development of single crew operated commercial aircraft. *Aircraft Engineering and Aerospace Technology,* 79(5), pp. 518--526.

Harris, D. (2006). The influence of human factors on operational efficiency. *Aircraft Engineering and Aerospace Technology,* 78(1), pp. 20--25.

Harris, D. (2003). The human factors of fully automatic flight. *Measurement and Control,* 36(6), pp. 184-187.

Hartel, C.E., Smith, K. & Prince, C. (1991). Defining aircrew coordination: Searching mishaps for meaning, *Proceedings of the Sixth International Symposium on Aviation Psychology,* April 1991.

Haworth, N. (2003) How valid are motorcycle safety data? In Proceedings of the Road Safety Research, Education and Policing Conference. Sydney, Australia.

Heinrich, H.W. (1931). Industrial Accident Prevention. New York, USA: McGraw Hill.

Helm, L. (1996). The future of software may lie in the obscure theories of an 18th century cleric named Thomas Bayes; an interview with Eric Horvitz. *LA Times.*

Hendrick, K. & Benner, L. (1987). Investigating accidents with Sequentially Timed and Events Plotting (STEP). New York, USA: Marcel Decker.

Hignett, S. & Wilson, J. R. (2004) The role for qualitative methodology in ergonomics: a case study to explore theoretical issues. Theoretical Issues in Ergonomics Science, 5 (6), pp. 473 - 493

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

Hollnagel, E. & Embrey, D.E. (1994). Human Reliability Assessment in Safety Assessments: Addressing Cognitive and Action Errors. Parbold, Lancs: HRA Ltd.

Hollnagel, E., Woods, D.D. & Leveson, N. (2006). Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd, UK.

Horvitz, E., Ruan, Y., Gomes, C., Kautz, H., Selman, B. & Chickering, D.M. (2001). A Bayesian Approach to Tackling Hard Computational Problems, August 2001.

Houghton, R.J., Baber, C., Cowton, M., Stanton, N.A. & Walker, G.H. (2008). WESTT (Workload, Error, Situational Awareness, Time and Teamwork): An Analytical Prototyping System for Command and Control. *Cognition, Technology and Work,* 10(3), pp. 199--207.

INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). (2009). *ICAO Annexe 6.*

INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). (2009) ICAO Annexe 13 (9th Edition).

Jarvis, S. & Harris, D. (2009) Development of a bespoke human factors taxonomy for gliding accident analysis and its revelations about highly inexperienced UK glider pilots. *Ergonomics*, 52(8), pp. 1009-1018.

Johnson, C.W. (1999). Why Human Error Analysis Fails to Support Systems Development. *Interacting with Computers,* 11(5), pp. 517-524.

Johnson, H.M. (1946). The detection and treatment of accident prone drivers. *Psychological Bulletin,* 43(6), pp. 489-532.

Johnson, J.H. (2006). Can Complexity Help us Better Understand Risk? *Risk Management,* 8(4),p. 227.

Johnson, W.G. (1975). MORT: The management oversight and risk tree. *Journal of Safety Research,* 7(1), pp. 4-15.

Johnson, C.W., McCarthy, J.C. & Wright, P.C. (1995) Using A Formal Language To Support Natural Language in Accident Reports. *Ergonomics.* 38(6), pp 1264-1283.

Johnson, C.W. (1997) The Epistemics of Accidents. *International Journal of Human-Computer Studies.* 47, pp 659-688.

Johnston, A.N. (1996). Blame, punishment and risk management. In: C. Hood and D.K.C. Jones, eds, *Accident and Design: Contemporary Debates on Risk Management.* London: University College London Press, pp. 72-72-83.

Jordan, M.I., ed, (1998). *Learning in Graphical Models.* MIT Press.

Kerr, C. (1957). Wage Relationships - The Comparative Impact of Market and Power Forces. In: J.T. DUNLOP, ed, *The Theory of Wage Determination.* New York, USA: Norton.

Kerr, C. (1950). Labor Markets: Their Character and Consequences. *American Economic Review,* 40(2), pp. 278291.

Kirwan, B. (1998). Human error identification techniques for risk assessment of high risk systems - Part 1: Review and Evaluation of techniques. *Applied Ergonomics,* 29(3), pp. 157-177.

Kjellen, U. (1982). An evaluation of safety information systems at six medium-sized and large firms. *Journal of Occupational Accidents,* **3**, 273-288.

Kletz, T. (1974). HAZOP and HAZAN - Notes on the Identification and Assessment of Hazards. Rugby: Institute of Chemical Engineers.

Landauer, T.K. & Dumais, S.T. (1997). A solution to Plato's problem: The Latent Semanctic Analysis theory of the acquisition, induction, and representation of knowledge. *Psychological Review,* 104, pp. 211-240.

Landauer, T.K., Foltz, P.W. & Laham, D. (1998). Introduction to Latent Semantic Analysis. *Discourse Processes,* 25, pp. 259-284.

Latour, B. (1987) *Science in Action: How to Follow Scientists and Engineers Through Society.* Milton Keynes: Open University Press.

Latour, B. (1991) Technology is Society made Durable. In Law, J. (Ed.) *A Sociology of Monsters: Essays on power, technology and domination.* p 129. London: Routledge.

Learmount, D. (2010) Global airline accident review of 2009. Available: http://www.flightglobal.com/articles/2010/01/11/336920/global-airline-accident-review-of-2009.html [January, 2010].

Lenne, M. G. & Ashby, K. (2006) Characteristics of non-fatal general aviation crashes in Australia: insights from insurance data. Human Factors and Aerospace Safety, 6(4), pp. 395 - 407

Lenne, M. G., Ashby, K. & Fitzharris, M. (2008) Analysis of General Aviation Crashes in Australia Using the Human Factors Analysis and Classification System. The International Journal of Aviation Psychology, 18(4), pp. 340 – 352.

Leveson, N. G. (2002). A New Approach to System Safety Engineering. Unfinished Work edn. http://sunnyday.mit.edu/book2.html: Massachusetts Institute of Technology.

Leveson, N. G. (2004) A new accident model for Engineering Safer Systems. *Safety Science.* 42, pp. 237-70.

Li, G., Baker, S. P., Grabowski, J. G. & Rebok, G. W. (2001) Factors associated with pilot error in aviation crashes. Aviation, Space and Environmental Medicine, 72, 52-58.

Li, W. C. & Harris, D. (2006) Pilot error and its relationship with higher organizational levels: HFACS analysis of 523 accidents. Aviation, Space and Environmental Medicine, 77, 1056-1061.

Li, W.C., Harris, D., Hsu, Y.L. & Li, L.W. (2009). The Application of Human Error Template (HET) for Redesigning Standard Operational Procedures in Aviation Operations, D. HARRIS, ed. In: *Engineering Psychology and Cognitive Ergonomics, HCII 2009*, pp547--553.

Li, W.C., Harris, D. & Yu, C.S. (2008). Routes to failure: Analysis of 41 civil aviation accidents from the Republic of China using the human factors analysis and classification system. *Accident Analysis and Prevention,* 40, pp. 426--434.

Lucas, D.A. (1990). Wise Men Learn by Others Harm, Fools by Their Own: Organisational Barriers to Learning the Lessons From Major Accidents. In: M.H. WALTER and R.F. COX, eds, *Safety and Reliability in the 90s: Will Past Experience of Prediction Meet Our Needs?* London, UK: Elsevier.

Luxhøj, J.T., Choopavang, A. & Arendt, D.N. (2001) Risk Assessment of Organizational Factors in Aviation Systems. *Air Traffic Control Quarterly,* 9(3) pp. 135-174.

Luxhøj, J.T. (2002) Risk Analysis of Human Performance in Aviation Maintenance. *16th Human Factors in Aviation Maintenance Symposium.*

Luxhøj, J.T. & Coit, D. W. (2006) Modeling low probability/high consequence events: An aviation safety risk model. *Reliability and Maintainability Symposium, 2006.* pp 215-221.

Luxhøj, J.T. & Kauffeld, K. (2003) Evaluating the Effect of Technology Insertion into the National Airspace System [Homepage of Rutgers Scholar], [Online]. Available: http://rutgersscholar.rutgers.edu/volume05/Luxhøj-kauffeld/Luxhøj-kauffeld.htm [August 2005, 2005].

Macrae, C., Pidgeon, N. & O'Leary, M. (2002). Assessing the Risk of Flight Safety Incident Reports. In: C.W. JOHNSON, ed, *Workshop on the Investigation and Reporting of Incidents and Accidents (IRIA 2002).* UK: University of Glasgow, pp. 99-106.

Male, C. (1997). Gaining the Safety Advantage. *Aerospace International,* 10, pp. 24-25.

Marx, D. A. & Westphal, J. E. (2008) Socio-Technical Probabilistic Risk Assessment: Its Application to Aviation Maintenance. The International Journal of Aviation Psychology. 18 (1),pp. 51-60.

Mohr, D.L. & Clemmer, D.I. (1988). Accident Prone Worker: An example from Heavy Industry. *Accident Analysis and Prevention,* 20(2), pp. 123-127.

Morris, C.H. and Leung, Y.K. (2006) Pilot mental workload: How well do pilots really perform? *Ergonomics.* Vol. 49, No. 15, pp. 1581-1596.

Murphy, K. (1998). A Brief Introduction to Graphical Models and Bayesian Networks. [Online] Available: http://people.cs.ubc.ca/~murphyk/Bayes/bnintro.html

National Transportation Safety Board (NTSB), (1982) *Aircraft Accident Report AAR-82/08.* NTSB: Washington DC.

National Transportation Safety Board (NTSB), (2006) US General Aviation, Calendar Year 2003. Annual Review of Aircraft Accident Data. Report NTSB/ARG-07/01. NTSB: Washington DC.

Norman, D. A. (1990) The 'problem' with automation: inappropriate feedback and interaction, not 'over-automation'. *Philosophical transactions of the Royal Society of London. Series B: Biological sciences,* **327**(1241), 585-593.

Obradovich, J.H. & Woods, D.D. (1994) Users as designers: how people cope with poor HCI design in computer-based medical devices. *Proceedings of the Human Factors and Ergonomics Society,* 2, pp. 710-714.

Ogden, G.C. (1987) Concept, knowledge and though. *Annual Review of Psychology,* 38, pp. 203--227.

O'Leary, M., Macrae, C. & Pidgeon, N. (2002) Safety Data Collection in British Airways Flight Operations. In: C.W. JOHNSON, ed, *Workshop on the Investigation and Reporting of Incidents and Accidents (IRIA 2002).* UK: University of Glasgow, pp. 89-98.

O'Leary, M. (2002) The British Airways human factors reporting programme. *Reliability Engineering and System Safety,* 75(2), pp. 245-255.

O'Leary, M. & Chappell, S.L. (1996) Confidential incident reporting systems create vital awareness of safety problems. *ICAO journal,* 51(8), pp. 11-13.

O'Leary, M. & PIDGEON, N. (1995) Too bad we have to have confidential reporting programmes. *Flight Deck,* 16, pp. 11-16.

Orasanu, J. & Connolly, T. (1993) The reinvention of decision making. In: G.A. Klein, J. Orasanu, R. Calderwood and C. Zsambok, eds, *Decision making in action: Models and methods.* Norwood, CT: Ablex, pp. 3-20.

Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies. New Jersey, USA: Princeton University Press.

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

Pidgeon, N. & O'Leary, M. (2000). Man-made disasters: Why technology and organisations (sometimes) fail. *Safety Science,* 34, pp. 15-30.

Pidgeon, N. (1997). The limits to safety? Culture, politics, learning and man-made disasters. *Journal of Contingencies and Crisis Management,* 5(1), pp. 1-14.

Pidgeon, N. & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science,* 34(1-3), pp. 15-30.

Pidgeon, N. & O'Leary, M. (1994). Organizational safety culture: Implications for aviation practice. *Aviation Psychology in Practice,* pp. 21-43.

Pierce, J.R. (1980). An Introduction to Information Theory. Symbols, Signals and Noise Second Revised Edition edn. New York: Dover Publications.

Pritchett, A.R., Nix, D.C. & Ockerman, J.J. (2001). Empirical evaluations of pilot planning behavior in emergency situations. *Proceedings of the Human Factors and Ergonomics Society,* pp. 6-10.

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

Rasmussen, J. (1988). *Interdisciplinary workshops to develop a multi-disciplinary research programme based on a holistic system approach to safety and management of risk in large-scale technological operations.* Washington DC: World Bank.

Reason, J. (2003). Error management: achievements and challenges, 15 October 2003, RAes.

Reason, J. (2000). Human error: models and management. *British Medical Journal,* 320, pp. 768-770.

Reason, J. (1997). Managing the Risks of Organizational Accidents. UK: Ashgate Publishing Limited.

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

Reason, J.T. (2008). The Human Contribution: Unsafe acts, accidents and heroic recoveries. Farnham, UK: Ashgate Publishing Ltd.

Rose, A. (2008). Understanding Aviation Risk, *Proceedings of the 11th International Conference on Information Fusion,* June 30 - July 03 2008, pp. 1381--1387.

Rose, A. (2006). Measuring operational safety in aviation . *Aircraft Engineering and Aerospace,* **78**(1), 26--31.

Salas, E., Bowers, C.A. & Rhodenizer, L. (1998). It is not how much you have but how you use it: Toward a rational use of simulation to support aviation training. *The International Journal of Aviation Psychology,* 8(3), pp. 197-208.

Salminen, S., Saari, J., Leena, K. & Rasanen, T. (1992). Fatal and non-fatal occupational accidents: Identical versus differential causation. *Safety Science,* 15(2), pp. 109-118.

Salmon, P., Stanton, N.A., Young, M.S., Harris, D., Demagalski, J., Marshall, A., Waldman, T. & Dekker, S. (2002). Using Existing HEI Techniques to Predict Pilot Error: A Comparison of SHERPA, HAZOP and HEIST, *Proceedings of the 2002 British Computer Society Conference on Human-Computer Interaction, BCS-HCI 2002,* 2002, Springer.

Salmon, P.M., Stanton, N.A, Walker, G.H., Jenkins, D.P., Baber, C. and McMaster, R. (2008) Representing situation awareness in collaborative systems: A case study in the energy distribution domain. *Ergonomics*. Vol. 51, No. 3, pp367-384.

Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D.P., McMaster, R. (2008a) What really is going on? Review of Situation Awareness Models for Individuals and Teams. *Theoretical Issues in Ergonomics Science.* Vol. 9, No. 4, pp 297-323.

Sarter, N.B., Woods, D.D. & BILLINGS, C.E. (1997). Automation Surprises. In: G. SALVENDY, ed, *Handbook of Human Factors & Ergonomics.* Second edn. New York, NY: Wiley, pp. 1926-1943.

Sarter, N.B. (2000). The need for multisensory interfaces in support of effective attention allocation in highly dynamic event-driven domains: The case of cockpit automation. *International Journal of Aviation Psychology,* 10(3), pp. 231-245.

Shappell, S.A. & Wiegmann, D.A. (2001). Applying Reason: The human factors analysis and classification system (HFACS). *Human Factors and Aerospace Safety,* 1(1), pp. 59-86.

Shattuck, L.G. & Woods, D.D. (1994). Critical incident technique: 40 years later. *Proceedings of the Human Factors and Ergonomics Society,* 2, pp. 1080-1084.

Shorrock, S.T. & Chung, A.Z.Q. (2010) Mind the Gap: Research and Practice in Ergonomics and Human Factors, M. ANDERSON, ed. In: *Contemporary Ergonmics and Human Factors 2010,* 2010, Taylor and Francis.

Shorrock, S.T. & Kirwan, B. (2002) Development and application of a human error identification tool for air traffic control. *Applied Ergonomics,* 33, pp. 319-336.

Stanton, N.A., Harris, D., Salmon, P.M., Demagalski, J.M., Marshall, A., Young, M.S., Dekker, S.W.A. & Waldmann, T. (2006a) Predicting design induced pilot error using HET (human error template) - A new formal human error identification method for flight decks. *Aeronautical Journal,* 110(1104), pp. 107-115.

Stanton, N.A., Salmon, P.M., Harris, D., Marshall, A., Demagalski, J., Young, M.S., Waldmann, T.& Dekker, S.W.A. (2009) Predicting pilot error: Testing a new methodology and a multi-methods and analysts approach. *Applied Ergonomics,* 40(3), pp. 464--471.

Stanton, N.A., Salmon, P.M., Walker, G.H., Baber, C. & Jenkins, D.P. (2008) Modelling Command and Control. Aldershot, UK: Ashgate Publishing Ltd.

Stanton, N.A., Salmon, P.M., Walker, G.H., Baber, C. & Jenkins, D.P. (2005) Human Factors Methods: A Practical Guide for Engineering and Design. First Edition. Aldershot: Ashgate Publishing.

Stanton, N.A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., Salmon, P., Hoyle, G., Walker, G., Young, M.S., Linsell, M., Dymott, R. & Green, D. (2006b) Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. *Ergonomics,* 49(12-13), pp. 1288-1311.

Stanton, N.A., Salmon, P.M., Walker, G.H. and Jenkins, D.P. (2009) Genotype and Phenotype Schema and their role in Distributed Situation Awareness in Collaborative Systems. *Theoretical Issues in Ergonomics Science.* Vol. 10, No. 1, pp 43-68.

Swain, A.D. & Guttmann, H.E. (1983). *A handbook of human reliability analysis with emphasis on nuclear power plant applications.* Nureg/CR-1278. Washington D.C.: USNRC.

The International Air Transport Association (IATA) (2009) Safety Management Systems. Available: https://www.iata.org/whatwedo/safety_security/safety/Pages/safety_management_systems.aspx

Thomas, D. (1994). Prescribed Fire Safety: Preventing Accidents and Disasters Part II. Marana, Arizona: National Advanced Resource Technology Center.

Trucco, P., Cagno, E., Ruggeri, F. And Grande, O. (2007) A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation. Reliability Engineering and System Safety, 93, pp. 823-834.

Turner, B.A. & Pidgeon, N. F. (1997) Man-Made Disasters. Oxford: Butterworth-Heinemann.

Turner, B.A. (1995). Safety culture and its context. *Proceedings of the International Topical Meeting on Safety Culture in Nuclear Installations*, pp. 321-329.

Uttal, B., 1983. The Corporate Culture Vultures. *Fortune.*

US Department of Defense; US DoD. (2005). MIL-STD-882E Standard Practice for System Safety. Available online:
*www.system-safety.org/Documents/**MIL-STD-882**E-Feb05.doc*

Van Der Schaaf, T. W. (1995). Human recovery of errors in man-machine systems, *Proceedings of the 6th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Man - Machine Systems,* 27-29 June 1995, MIT Press.

Vaughan, D. (1997). The Challenger Launch Decision: risky technology, culture, and deviance at NASA. University of Chicago Press.

Vicente, K.J. & Christoffersen, K. (2006). The Walkerton *E.Coli* outbreak: A test of Rasmussen's Framework for risk management in a dynamic society. *Theoretical Issues in Ergonomics Science,* 7(2), pp. 93-112.

Vincoli, J.W. (1994). Basic Guide to Accident Investigation and Loss Control. New York, USA: John Wiley & Sons Inc.

Waldock, W.D. (1992) Measuring Aviation Safety or The More Things Change, The More They Stay the Same, *ISASI Forum,* March 1992 1992, International Society of Air Safety Investigators (ISASI).

Walker, G.H., Gibson, H., Stanton, N.A., Baber, C., Salmon, P. and Green, D. (2006) Event Analysis of Systemic Teamwork (EAST): A Novel Integration of Ergonomics Methods to Analyse C4i Activity. *Ergonomics.* Vol. 49, pp 1345-1369.

Weaver, D. (1971) Symptoms of Operational Error. *Professional Safety,* (104(2) Oct), pp. 39-42.

Westrum, R. (1992) Cultures with requiste imagination. In: J. WISE, D. HOPKIN and P. STAGER, eds, *Verification and Validation of Complex Systems: Human factors issues.* Berlin: Springer-Verlag, pp. 401-416.

Wickens, C.D. & Hollands, J.G. (2000) Engineering Psychology and Human Performance 3rd Edition.

Wickens, C., Gordon, S.E. & Liu, Y. (2004). An introduction to human factors engineering.

Wiegmann, D.& Shappell, S. (2003). A human error approach to aviation accident analysis: The human factors analysis and classification system. Aldershot, UK: Ashgate Publishing Ltd.

Williams, J.C. (1986). HEART - a proposed method for assessing and reducing human error, *9th Advances in Reliability Technology Symposium,* 1986.

Wood, S. (2004). *Flight crew reliance on automation.* CAA Paper 2004/10. UK: Civil Aviation Authority.

Woods, D.D. (2003). Creating foresight: How resilience engineering can transform NASA's approach to risky decision making.

Woods, D.D. (1984) Some results on operator performance in emergency events, D. WHITFIELD, ed. In: *Institute of Chemical Engineering Symposium Series 90,* 1984.

Woods, D.D. & Dekker, S.W.A. (2000) Anticipating the Effects of Technological Change: A New Era of Dynamics for Human Factors. *Theoretical Issues in Ergonomic Science,* 1(3), pp. 272-282.

Woods, D.D., Johannesen, L., Cook, R.I. & Sarter, N.B. (1994) Behind Human Error: Cognitive Systems, Computers and Hindsight.

Wright, L. & Van Der Schaaf, T. W. (2004). Accident Versus Near-Miss Causation: A Critical Review of the Literature, and Empirical Test in the UK Railway Domain, and their Implications for other sectors. *Journal of Hazardous Materials,* **111**(Special Issue), 105-105-110.

Young, M.S., Shorrock, S.T., Faulkner, J.P.E. & Braithwaite, G.R. (2004). Who moved my (Swiss) cheese? The (r)evolution of human factors in transport safety investigation. *Human Factors in Investigation,* 28(3), pp. 10 - 13.