Proving Properties of Accidents

C.W. Johnson,
Glasgow Accident Analysis Group,
Department of Computing Science,
University of Glasgow,
Glasgow, United Kingdom, G12 8QQ.
E-mail:johnson@dcs.glasgow.ac.uk
WWW: http://www.dcs.gla.ac.uk/~johnson

Keywords: accident analysis; formal methods; human factors; proof; temporal logic, CAE diagrams.

Accident reports are produced by regulatory and commercial authorities, such as the UK Air Accident Investigation Branch and the US National Transportation Safety Board, in response to most major accidents. These documents are intended to ensure that disasters do not recur. They, typically, contain accounts of the human and system failures that lead to major accidents. These descriptions are then used to identify the primary and secondary causes of the failure. Finally, recommendations are made so that the operators and regulators of safety-critical systems can avoid future accidents. Unfortunately, it is often difficult for readers to trace the way in which particular conclusions are drawn from the many hundreds of pages of evidence in these reports. Natural language arguments often contain implicit assumptions and ambiguous remarks that prevent readers from understanding the reasons why a particular conclusion was drawn from a particular accident. In contrast, this paper argues that mathematical proof techniques can be used to support the findings of accident investigations. These techniques enable analysts to formally demonstrate that a particular conclusion is justified given the evidence in a report. The later sections of this paper then introduce Conclusion, Analysis and Evidence diagrams. These can be used to communicate the results of a formal analysis. The intention is not to replace the natural argumentation structures that are currently used in accident reports. Rather, our aim is to increase confidence that particular conclusions are well supported by the evidence that is presented within a report.

1. Introduction

Accident reports are intended to ensure that major failures do not recur. They are produced by a wide range of national (Cullen, 1990, Fennel, 1988) and international bodies (Worley and Lewins, 1988). Typically, these documents begin by providing a brief synopsis of the events leading to an accident. The synopsis is then followed by a number of expert analyses. These identify and prioritise the failures leading to the accident. Finally, conclusions are drafted from the experts' findings. These form the basis of any actions that companies or regulatory authorities might take to prevent future failures.

1.1 Conventional Reporting Techniques

Unfortunately, it is not always easy for readers to understand the justifications that support particular conclusions (Johnson, 1994). Accident reports are often many hundreds of pages in length. The evidence that supports a particular line of analysis may be lost amongst the paragraphs of contextual detail. A further problem is that natural language can be ambiguous. For example, accident reports often refer to situations of 'high workload' and 'operator error' without explaining the precise meaning of these terms (Reason, 1988). Many accident reports are also inconsistent in the sense that the same term is used to refer to several different objects or people (Johnson, McCarthy and Wright, 1995). Later sections of this paper will argue that these problems create considerable confusion for the reader and may even lead them to doubt the accuracy of the final report.

1.2 Formal Methods and Accident Analysis

Formal proof techniques can be used to avoid the ambiguity and inconsistency of natural language (Austin and Parkin, 1993). A number of authors have also used these techniques to support the design of dynamic, interactive systems. For example, Dix (1991) has used an algebraic notation to reason about high level properties of multi-user systems. Paterno, Sciacchitano and Lowgren (1995) have used the LOTOS notation to examine interaction with complex multimedia applications. Palanque and Bastide (1995) have applied Petri Nets to examine safety and liveness properties of distributed systems. None of this work has been applied to reason about accident reports. In particular, there has been no attempt to use mathematical techniques to prove that conclusions are well-founded with respect to the analysis that is presented in an accident report.

1.3 Outline of the Paper

Section 2 describes a collision between the bulk carrier Mount Ymitos and the passenger vessel Noordam. The United States' Coast Guard report into this accident provides an appropriate example for this paper because it describes a complex combination of operator 'errors' and system 'failures'. Section 3 presents a

formalisation of the events leading to this accident. A Critical Entity Table is constructed to document the operators, tasks, roles, speech acts, physical locations and control systems that contributed to the failure. A temporal extension to first order, propositional logic is then used to model the relationships between these entities. This helps to strip away some of the unnecessary detail that prevents readers from identifying the main causes of an accident. Section 4 goes on to demonstrate that formal proof techniques can justify particular conclusions in terms of the events that are described in a report. If this relationship cannot be proven then either the analysis is incorrect or the report does not provide the reader with enough evidence about the accident. Section 5 argues that in order for this approach to be successful, non-formalists must be able to access the products of the mathematical analysis. Conclusion, Analysis and Evidence (CAE) diagrams are introduced to address this problem. Finally, Section 6 introduces areas for future research.

2. The Case Study

This paper focuses upon an accident report that was produced by the United States' Coast Guard in response to a collision between the passenger vessel Noordam and the bulk carrier Mount Ymitos (United States Coast Guard, 1993). We are interested in this case study because it typifies the many different operator errors and organisational failures that exacerbate accidents with complex, interactive systems. The remainder of this section brief outlines the course of the accident. The Noordam collided with the Mount Ymitos at 20.42 (Central Standard Time) on November 6th, 1993. The accident occurred two miles south of the Southwest Pass Entrance Light Buoy in the Gulf of Mexico. The exact location was recorded as 28 degrees, 50.0 minutes North and 89 degrees, 25.7 minutes West. Both ships were damaged in the collision but there was no loss of life.

The Mount Ymitos was outbound from the Mississippi River en route to St Petersburg, Russia. It had cleared the Southwest Pass out of the River when the Third Officer noticed an inbound passenger vessel using their binoculars. At this stage, he estimated that the vessel was approximately six miles from the Ymitos. He did not immediately report his observation as the Captain was busy with the Pilot who was preparing to leave the Mount Ymitos. The watch-standers re-established visual contact when the Noordam had closed to two miles from the Mount Ymitos. The Captain reduced their speed to dead slow and expected the Noordam to alter its heading. At this point the ARPA (Automatic Radar Plotting Aid) showed that the closest point of approach was under six hundred feet. The Captain made several attempts to alert the Noordam. At 20:40:08 the Coast Guard logged a Channel 16 VHF call: 'Passenger Vessel, Passenger Vessel, Go to South Pass'. At 20:40:50 they logged 'Passenger Vessel Going to South Pass, I Turn Hard Starboard'. The third officer then attempted to communicate the warning using an Aldis lamp. No response was received.

The Noordam was en route to New Orleans from Cozumel, Mexico. At approximately 20:00:00, Second Officer Smit called the Pilot Station and learned that two other vessels were also in-bound towards the Mississippi and could be overtaken. The Pilot did not alert the Noordam to the presence of any outward bound vessels. Quartermaster Salyo was the designated lookout He left the bridge on two separate occasions during the approach. Shortly after 20:00:00 he left, with the permission of Second Officer Smit, to make sandwiches and coffee for the bridge crew. At 20:10:00 he unlashed the anchors in preparation for entering port. He returned at 20:20:00 but did not detect the Mount Ymitos until immediately prior to the collision. A scheduled watch change took place at 20:30:00. Second Officer Smit performed navigation checks using the radar, together with Chief Officer Broekhoven, before handing over to Third Officer Veldhoen. Veldhoen, in turn, handed over to the Chief Officer at 20:36:00 when an 'end of sea voyage' was declared. This is a point of convenience determined by the watch officer and represents the point at which the Chief Officer assumes control for the manoeuvring watch prior to arrival in port. In order to complete this hand-over Veldhoen had to fix the vessel's position, complete the log and notify the engine room. As the Noordam changed course to enter the final leg of the approach, Fourth Officer Kuiper, who was on the bridge but who was not on duty, saw the lights of the Mount Ymitos and immediately issued a curse. The manoeuvre was halted while the crew determined the course and position of the vessel that they had seen, Approximately one minute before the collision, Chief Officer Broekhoven ordered left full rudder to pull away from the danger.

The Coast Guard's report argues that the principle reason for the collision was the failure by the Noordam's crew to keep an adequate watch. Unfortunately, the report does not provide a detailed explanation of why this failure occurred. The reader is left to infer the causal relations that link the observations about the accident and the conclusions that are listed at the end of the document. The following pages, therefore, show how formal techniques can be used to explicitly link the findings of an investigation to the account of an accident.

3. A Formalisation of the Accident

In order to reason about the findings of an accident report, it is first necessary to model the events leading to the failure. The first stage in this process is to identify the critical operators, tasks, roles, communications, systems and locations that helped to shape the course of the accident.

3.1 Critical Components

A limitation with natural language approaches to accident reporting is that it can be difficult to identify critical information from a mass of background detail. For example, the Coast Guard's report into the Noordam collision includes the following account:

> "Fourth Officer Daniel Kuiper, who was not on duty, was the first to notice the lights of a vessel off the starboard side of the Noordam. This was between one and two minutes before the time of collision. He saw a red light that he estimated was approximately 2 points off the NOORDAM's starboard bow - a point being 11.25 degrees of arc. First Officer Kuiper uttered a curse word that attracted the attention of others on the bridge. Third Officer Veldhoen, upon looking to starboard, also saw lights." [Paragraph 42]

Additional information, such as the conversion between points and degree of arc, is included to help the reader form a picture of the accident. Unfortunately, such details may actually obscure the underlying causes of operator 'error' and system 'failure'. Our previous work on accident analysis has, however, identified a number of categories that can be used to identify critical components in an accident:

- **operators.** It is necessary to represent the people involved in an accident so that readers can follow the way in which operator intervention affects the course of system failures;
- **roles.** It is important to distinguish particular individuals from the roles that they perform during an accident. For example, a number of individuals performed the tasks associated with the role of watch-stander during the Noordam collision;
- **tasks.** It is necessary to identify the tasks that operators were or should have been performing during accidents if readers are to understand the ways in which human intervention safeguarded the system or exacerbated any key failures;
- **speech acts.** It is vital to represent communication between the operators that are involved in an accident. Misunderstandings have a profound impact upon the safety of many applications;
- **information and control systems.** This type of information is included because the quality of information that is available to system operators is often determined by the channel that is used to support their observations. For instance, ARPA radar provides more detailed and arguably less reliable information than direct visual contact;
- **physical locations.** It is necessary to represent the place in which an accident occurs because the location of a failure can have a profound impact upon an operator's ability to respond to an accident (Johnson, 1996).

Paragraph [42], cited above, can be used to identify physical locations, such as the Noordam and the Mount Ymitos. It is also possible to identify operators such as Veldhoen and Kuiper who perform the roles of First and Fourth Officers respectively. We can identify observation channels; in this case the visual observation of the Ymitos' lights as well as critical speech acts such as Kuiper's curse. The following table shows the results that can be obtained by extending this analysis throughout the Coast Guard's report.

Physical Locations	**Roles**	**Information/Control Systems**
captain_veniamis	*lookout*	*arpa_radar*
pacific_trident	*chief_officer*	*visual*
mount_ymitos	*first_officer*	*binoculars*
noordam	*third_officer*	
	fourth_officer	
	watch_officer	
Operators	**Speech Acts**	**Tasks**
pilot_station	*inbound_pacific_trident*	*navigation_radar_check*
engine_room.	*inbound_captain_veniamis*	*collision_radar_check*
smit.	*outbound_mount_ymitos*	*correlate_radar_targets*
salyo	*curse*	*declare_end_of_sea_voyage*
broekhoven	*take_bearing_on_lights*	*fix_vessel_position*

veldhoen	*lights_moving_right*	*complete_log*
kuiper	*officer_change*	*notify_engine_room*
	end_of_sea_voyage	
	left_full_rudder	

Table 1: Critical Entity Table for the Noordam Accident

In formal terms, the elements of this table define the types that model the Noordam accident. The process of building such a table helps to strip out irrelevant detail that obscures critical properties of major accidents.

3.2 Axiom for the Accident System

The identification of operators, roles, tasks, speech acts, information systems and locations is of little benefit if analysts cannot represent and reason about the relationships that exist between these components. The following section uses a simple form of temporal logic to demonstrate how this might be done for the Noordam case study.

3.2.1 Operators and Roles

The previous sections argued that it is important to identify the critical roles that operators play in an accident. This affects the range of tasks that operators are expected to perform. For example, Broekhoven was the Noordam's Chief Officer during the incident, Smit was the First Officer:, Veldhoen was the Third Officer and Salyo was the lookout

role(chief_officer, broekhoven). (1)
role(first_officer, smit). (2)
role(third_officer, veldhoen). (3)
role(lookout, salyo). (4)

Such clauses gather together information that is, typically, scattered throughout conventional, natural language documents. The roles performed by key individuals in the Coast Guard's report are listed in paragraphs [13, 16, 25, 30, 37, 42]. Such a formalisation is also important if an individual's role changes during the course of an accident. For example, the officer in charge of the watch on the Noordam changed at 20:30 hrs:

at(role(watch_officer, smit) , 2029). (5)
at(role(watch_officer, veldhoen) , 2030). (6)

The previous clauses exploit a simple form of temporal logic in which the binary *at* operator takes a proposition and a term denoting a time such that *at(p, t)* is true if and only if *p* is true at *t.* A number of technical problems surround the general application of this simple extension to propositional logic. In particular, the philosophical issue of reification forces analysts to clearly state the relationship between particular terms and objects over time. This theoretical problem is less of an issue for our purposes because we are always refering to definite entities at specific times during an accident. We, therefore, retain this simple temporal framework rather than the more elaborate temporal languages in our previous work (Johnson, 1993, 1995a, Telford and Johnson, 1996).

3.2.2 Operators and Communications

Communications problems exacerbate many major accidents. It is, therefore, important to represent and reason about this source of 'error'. During the accident, Smit requested and received specific information about the Captain Veniamis and the Pacific Trident that were inbound towards the Mississippi:

$\exists$ *t: at(message(pilot_station, smit, inbound_captain_veniamis), t).* (7)
$\exists$ *t: at(message(pilot_station, smit, inbound_pacific_trident), t).* (8)

The existential $\exists$ quantifier (read as 'there exists') is used because the accident report does not represent the precise times associated with each of these individual communications. The following clause shows how the same approach can be adopted to represent a lack of communication. Smit did not receive information about outbound traffic from the Pilot Station:

$\forall$ *t: not at(message(pilot_station, smit, outbound_mount_ymitos), t).* (9)

The universal ∀ quantifier (read as 'for all') is used because it was never the case that Smit received information from the Pilot Station about the Mount Ymitos. Similar clauses can be used to represent more complex verbal exchanges. For example, Kuiper first observed the Ymitos' lights and issued a curse which was heard by Veldhoen and Broekhoven. Broekhoven then requested that Veldhoen take a bearing on the lights. Veldhoen responded that the lights were moving right. The following clauses represent these individual speech acts:

$$\exists t, t' : at(message(kuiper, [veldhoen, broekhoven], curse), 2040) \wedge at(message(broekhoven, veldhoen, take\_bearing\_on\_lights), t) \wedge at(message(veldhoen, broekhoven, lights\_moving\_right), t') \wedge after(2040, t) \wedge after(t, t'). \quad (10)$$

It is important to note that the preceding clauses do not represent the precise verbal components of each speech act. This information could be introduced if it were available, for instance through studying cockpit voice recordings. In the case of the Noordam there was no such record. Place holders, such as *curse*, are used to capture the recollected sense of the communication without specifying its exact form.

3.2.3 Operators and Locations

It is important to consider the physical location of system operators during major accidents. For example, the lookout left his position on the bridge at critical moments during the lead-up to the Noordam collision. Clause (11) states that *salyo* was in the galley at 20:00hrs. Similarly, clauses (12) and (13) describe Salyo's subsequent movements from the galley back to the bridge at 20:10 hrs and from the bridge down to the decks at 20:15 hrs. They do not specify when Salyo moved from each of these locations because the report does not provide accurate journey times:

$$at(position(salyo, galley(noordam)), 2000). \quad (11)$$

$$at(position(salyo, bridge(noordam)), 2010). \quad (12)$$

$$at(position(salyo, decks(noordam)), 2015). \quad (13)$$

The previous clauses do not specify the relative position of the galley, bridge or decks. Such information can be introduced by formalising a three-dimensional co-ordinate scheme (Johnson, 1996). This was not done because clauses (11,12,13) reflect the level of detail in the Coast Guard's report. This illustrates an important benefit of the formalisation. Logic provides an explicit representation of the level of abstraction that is considered appropriate for the readers of the report. They do not need to know the relative positions of the galley, bridge and decks in order to understand the events leading to the collision. Such decisions are extremely important. Too much detail and readers will be swamped amongst a mass of contextual information. Too little detail and it will be difficult for them to reconstruct the flow of events leading to disaster. Clauses, such as (11,12,13), can be used to represent and reason about appropriate levels of abstraction. This helps to avoid the ad hoc decisions that frequently seem to be made about the amount of location information that is included in accident reports (Johnson, McCarthy and Wright, 1995).

3.2.4 Operators and Tasks

The Coast Guard's report contains the following paragraph:

> "Between 2030 and 2036, Broekhoven and Veldhoen checked the radars occasionally, using the six mile scale. Broekhoven was planning the turn from 325 degrees to 000 degrees to coincide with bringing the Racon 'T' platform abeam, at 1.5 miles to port. Both Veldhoen and Broekhoven used the 10-centimetre and centimetre radars to check the distance of the domino platforms, and particularly the bearing and range of the Racon 'T'. They were not using the radars for collision avoidance and observation of moving targets, and did not attempt to correlate every fixed target contact in the radar with fixed platforms observed visually to see if any were any underway contacts rather than fixed platforms." [Paragraph 39]

From this it is possible to extract two critical observations about the operation of the Noordam. Firstly, that between 20:30, and 20:36 both Broekhoven and Veldhoen were performing navigation radar checks. Secondly, that during this interval they did not correlate radar targets with visual observations. The following clauses introduce a *during* operator such that *during(p, t)* is true if and only if the situation denoted by *p* occurs at sometime during the interval denoted by *t*. Formally, this can be given as follows:

$$\forall t : during(p, t) \Leftrightarrow \exists t' : at(p, t') \wedge before(t', end(t)) \wedge before(begin(t), t'). \quad (14)$$

This assumes that *before(t, t')* is true if *t'* occurs at some time after *t* or at the same instant as *t*. The following clauses also introduce the operator, *in*, such that *in(t, t', t'')* is true if *t* is wholly contained within

t' and *t''*. This can be formalised in a similar manner to *during*. In contrast, the following clauses formalise the observations made in paragraph [39] of the accident report:

$$\exists t : during(perform(broekhoven, navigation\_radar\_check), t) \wedge not\ during(perform(broekhoven, correlate\_radar\_targets), t) \wedge in(t, 2030, 2036). \quad (15)$$

$$\exists t : during(perform(veldhoen, navigation\_radar\_check), t) \wedge not\ during(perform(veldhoen, correlate\_radar\_targets), t) \wedge in(t, 2030, 2036). \quad (16)$$

An important benefit of the formalisation process is that clauses, such as (15) and (16), can be translated back into natural language sentences; between 20:30 hrs and 20:36 hrs Broekhoven and Veldhoen performed navigation radar checks but did not correlate radar targets. The formalisation process helps analysts to focus upon critical aspects of an accident, such as operator tasks. This benefit might be obtained using a conventional task analysis technique such as TAKD (Johnson, Diaper and Long, 1984). Later sections will, however, argue that formal reasoning techniques can be used to prove properties of accident reports. This provides the additional degree of assurance that is demanded by bodies such as NASA and the UK Ministry of Defence (Austin and Parkin, 1993).

The previous example describes a relatively simple set of observations about operator tasks. Typically, the co-ordination of group activities is more complex. For example, Veldhoen declared an 'end of sea voyage' between 20:34 and 20:38. This procedure handed over control of the watch to the First Officer Broekhoven. He was responsible for navigating the Noordam into port. This change was not, however, announced to the lookout:

$$\exists t : during(perform(veldhoen, declare\_end\_of\_sea\_voyage), t) \wedge not\ during(message(broekhoven, salyo, officer\_change), t) \wedge during(role(watch\_officer, broekhoven), t) \wedge \wedge in(t, 2034, 2038). \quad (17)$$

The failure to inform the lookout was important because the task of declaring the 'end of sea voyage' involves the watch officer in a number of sub-tasks that reduce the amount of time that they have available for navigation and collision avoidance:

$$\forall t: during(perform(veldhoen, declare\_end\_of\_sea\_voyage), t) \Leftrightarrow during(perform(veldhoen, fix\_vessel\_position), t) \wedge during(perform(veldhoen, complete\_log), t) \wedge during(message(veldhoen, engine\_room, end\_of\_sea\_voyage), t). \quad (18)$$

Such clauses illustrate how the products of hierarchical task analysis might be introduced into formal models of major accidents. The higher order task of declaring the 'end of sea voyage' is comprised of three sub-tasks: fixing the vessel's position; completing the log and notifying the engine room.

3.2.5 Operators and Observations

The entities that were identified in Table 1 are generic in the sense that operators, roles, tasks, speech acts, information systems and physical locations are central to all of the accidents reports that we have examined (Johnson, 1994, 1995, Johnson, McCarthy and Wright, 1995, Telford and Johnson, 1996). This does not mean that the list is exhaustive. A related point is that the significance of individual entities will vary from accident to accident. For example, automated control systems did not have a significant impact upon the course of the collision between the Ymitos and the Noordam. In contrast, information systems played a critical role in the observations that operators made during the accident. Veldhoen made visual observations of the ship but did not use an azimuth circle to verify his observation:

$$\exists t : at(observe(veldhoen, mount\_ymitos, visual), t). \quad (19)$$

$$\forall t : not\ at(observe(veldhoen, mount\_ymitos, azimuth), t). \quad (20)$$

As before, the existential $\exists$ quantifier is used in clause (19) because the accident report does not identify the particular interval when Veldhoen made his observation. All we know is that there exists a time at which Veldhoen made a visual observation of the Ymitos. The universal $\forall$ quantifier is used in clause (20) because Veldhoen did not use an Azimuth circle at any time in the accident. This shows how an analysts concerns can direct the formalisation process. Clause (20) represents something that the officer did not do. If it had not been formalised then readers would not have been aware of this omission. In

fact, Veldhoen's failure to verify his visual observations reinforced Broekhoven's judgement that the ships would pass starboard to starboard. He had seen a green (starboard) light shortly after the initial observation made by Kuiper:

$$\exists t : at(observe(broekhoven, green\_light(mount\_ymitos), binoculars), t). \quad (21)$$

It was only when Broekhoven saw a red light that he realised the imminent possibility of a collision with the Mount Ymitos and took evasive action:

$$at(observe(broekhoven, red\_light(mount\_ymitos), visual), 2041) \\ \wedge\ at(message(broekhoven, engine\_room, left\_full\_rudder), 2041). \quad (22)$$

This section has used temporal logic to formalise the events leading to an accident. This formalisation process helps to strip out the contextual detail that hides critical observations in the many hundreds of pages that form conventional reports. We have not, however, shown that this approach can be used to reason about the conclusions that are drawn from an accident report.

4. Reasoning About Accident Reports

This section argues that formal methods can be used to establish the relationship between the evidence presented in an accident report and the conclusions which boards of enquiry use to draft future legislation. Unless this can be done, it will be difficult for commercial organisations to understand the reasons why particular sanctions may be imposed in the aftermath of major accidents (Johnson, 1994). For example, the Coast Guard enquiry made the following observation about the collision between the Noordam and the Ymitos:

> 'The proximate cause of the casualty was the failure of Chief Officer Broekhoven, the person in charge of the watch on the NOORDAM at the time of the casualty, to maintain a vigilant watch in that he did not detect the presence of the MOUNT YMITOS visually or on radar until the MOUNT YMITOS was less than 1 mile away, less than 2 minutes before the collision.' [Conclusion 1].

Such findings create a number of problems for organisations that must prevent the recurrence of future accidents. In particular, it does not explain the reasons why Broekhoven failed to spot the Mount Ymitos. Readers are left to piece together or infer these justifications from the evidence presented in the many previous pages of analysis. This can have extremely serious consequences. Two readers might easily infer two different reasons why Broekhoven failed to keep an efficient watch. Each might, therefore, adopt quite different strategies for avoiding future failures (Reason, 1990).

Formal proof techniques can be used to demonstrate that a conclusion is valid given the evidence that is presented in an accident report. For instance, the following clause is derived from Conclusion 1 in the Coast Guard report:

$$\forall t:\ not\ \ during(vigilant(broekhoven), t) \\ \Leftrightarrow not(\ during(observe(broekhoven, mount\_ymitos, visual), t) \\ \vee\ during(observe(broekhoven, mount\_ymitos, arpa\_radar),t)) \\ \wedge\ before(t, 2040). \quad (23)$$

We can re-write this clause as follows:

$$\Leftrightarrow not\ during(observe(broekhoven, mount\_ymitos, visual), t) \\ \wedge\ not\ during(observe(broekhoven, mount\_ymitos, arpa\_radar),t) \\ \wedge\ before(t, 2040). \quad [\text{DeMorgan's Law (23)}] \quad (24)$$

$$\Leftrightarrow (not\ during(observe(broekhoven, mount\_ymitos, visual), t) \wedge before(t, 2040)) \\ \wedge\ (not\ during(observe(broekhoven, mount\_ymitos, arpa\_radar), t) \wedge before(t, 2040)). \\ [\wedge \text{ Identity (24)}] \quad (25)$$

In order to justify Conclusion 1 we must consider two different cases. The first concerns the reasons why Broekhoven failed to make visual contact with the Mount Ymitos. The second addresses the failure to detect the Ymitos using the ARPA radar. In order to establish the connection between the conclusion and the evidence presented in the body of the report it is necessary for analysts to explicitly state the reasons supporting particular findings. For example, one of the reasons why Broekhoven failed to observe the Mount Ymitos was that he used the radar for navigation and not for collision avoidance:

$\forall$ *t: not during(observe(broekhoven, mount_ymitos, arpa_radar), t)*
$\Leftarrow$ *during(perform(broekhoven, navigation_radar_check), t)*
$\wedge$ *not during(perform(broekhoven, correlate_radar_targets), t).* (26)

We can now prove that the second part of our formalisation of Conclusion 1 is satisfied by the evidence in the accident report. This can be done by applying the following inference rule to (15) and (26).

$$\forall t: P(t) \Rightarrow Q(t),\ \exists t': P(t') \ \vdash\ \exists t': Q(t') \quad (27)$$

Informally, this argument can be expressed as follows. From clause (26), we conclude that Broekhoven failed to observe the Mount Ymitos using the ARPA radar during any interval in which he was performing a navigation radar check and did not correlating radar targets. From clause (15) we know that know that Broekhoven was performing a navigation radar check and was not correlating radar targets between 20:30 and 20:36. Clause (27) tells us that if, we have clause (26) and clause (15) we can infer that Broekhoven failed to observe the Mount Ymitos using the ARPA radar during the interval between 20:30 and 20:36.

The previous proof illustrates a weakness in the accident report. Our formalisation of Conclusion 1 stated that Broekhoven did not observe the Mount Ymitos using the radar until 20:42. Our model has been used to prove that Broekhoven was pre-occupied with navigation checks between 20:30 and 20:36. This leaves at least six minutes unaccounted for. During that time, Broekhoven began turning the Noordam to the North. The accident report makes no reference to the use of the ARPA during this interval. The reader has to assume that the system was not used during this or subsequent operations prior to the collision at 20:42. Such findings are significant because they have important consequences for the recommendations that might be drawn from the report. For example, it is normal practice for officers to correlate radar targets when approaching an unfamiliar port. In the interval from 20:30 to 20:36 we can clearly see that navigation problems explain **why** Broekhoven did not perform these checks. We cannot, however, explain the omission during the final six minutes before the collision.

The second part of Conclusion 1 states that Broekhoven did not make any visual observation of the Mount Ymitos until 20:42. The justification for this finding can be found in a subsequent conclusion, rather than in the body of the accident report:

> 'The number of personnel (both watch-standing and non-watch-standing) on the bridge of the NOORDAM between 2020 and the time of the collision may have raised the complacency level and lowered the attentiveness of the bridge watch-standers with regards to maintaining a dedicated visual and radar watch.' [Conclusion 5].

IThe evidence for this conclusion can be found in paragraph [41] which states that:

> 'There were seven other persons on the bridge of the NOORDAM at this time (20:37hrs) in addition to the chief officer, who was in control of the vessel - three other licensed officers (one on duty, and two off duty), one cadet, two quartermasters and the chief officer's wife' [Paragraph 41].

This led to considerable confusion during our analysis of the report. We initially identified eight, and not seven, other individuals on the bridge in the final minutes before the collision. This confusion arose because Salyo was identified both by his name and by his role as Quartermaster In order to form this association, the reader must remember the allocation of responsibilities that was introduced in paragraph [25] when reading paragraph [41]:

$\forall$ *t: not during(observe(broekhoven, mount_ymitos, visual), t)*
$\Leftarrow$ *during(position(kuiper, bridge(noordam)), t)*
$\wedge$ *during(position(veldhoen, bridge(noordam)), t)*
$\wedge$ *during(position(helmsman, bridge(noordam)), t)*
$\wedge$ *during(position(chief_officers_wife, bridge(noordam)), t)*
$\wedge$ *during(position(quartermaster_1, bridge(noordam)), t)*
$\wedge$ *during(position(quartermaster_2, bridge(noordam)), t)*
$\wedge$ *during(position(cadet, bridge(noordam)), t)*
$\wedge$ *during(position(broekhoven, bridge(noordam)), t).* (28)

Paragraph [41] suggests that there were nine people on the bridge at 20:37:

at(position(kuiper, bridge(noordam)), 2037). (29)

at(position(veldhoen, bridge(noordam)), 2037). (30)
at(position(helmsman, bridge(noordam)), 2037). (31)
at(position(chief_officers_wife, bridge(noordam)), 2037). (32)
at(position(quartermaster_1, bridge(noordam)), 2037). (33)
at(position(quartermaster_2, bridge(noordam)), 2037). (34)
at(position(cadet, bridge(noordam)), 2037). (35)
at(position(broekhoven, bridge(noordam)), 2037). (36)

We can apply our definition of *during,* given in clause (14), to re-write each of the clauses from (29) to (36) in the following form:

∃ t: during(position(kuiper, bridge(noordam)),t)
∧ before(2037, end(t)) ∧ before(begin(t), 2037).
[Application of (14) to (29)] (37)

By repeating the application of (14) in the manner described above, we obtain the following:

∃t : during(position(kuiper, bridge(noordam)), t)
∧ during(position(veldhoen, bridge(noordam)), t)
∧ during(position(helmsman, bridge(noordam)), t)
∧ during(position(chief_officers_wife, bridge(noordam)), t)
∧ during(position(quartermaster_1, bridge(noordam)), t)
∧ during(position(quartermaster_2, bridge(noordam)), t)
∧ during(position(cadet, bridge(noordam)), t)
∧ during(position(broekhoven, bridge(noordam)), t)
∧ before(2037, end(t)) ∧ before(begin(t), 2037).
[Introduction of ∧ from application of (14) to (29..36)] (38)

Finally, by applying inference rule (27) we get the following clause which corresponds to the second condition in Conclusion 1. In other words, the derivation of the following clause formally proves that our conclusions are consistent with the information contained in the body of the report:

∃t : not during(observe(broekhoven, mount_ymitos, visual), t)
∧ before(2037, end(t)) ∧ before(begin(t), 2037).
[Application of (27) to (28) using (38)] (39)

This proof helps to identify a further problem with the Coast Guard report We have previously cited Conclusion 5 which states that the number of personnel on the bridge between 20:20hrs and the time of the collision may have lowered the attentiveness of Broekhoven with regards to maintaining a visual and radar watch. Our formal analysis reveals that the evidence for this assertion only applies to the interval from 20:37hrs until the time of the collision. This poses a number of problems. We do not know why Conclusion 5 mentions 20:20hrs rather than 20:37hrs as stated in the body of the report. It can only be speculated that a number of people arrived on the bridge at this time earlier time. Alternatively, if additional crew members gradually were arriving from some time before 20:20hrs then we do not know why this was chosen as the critical moment at which collision avoidance tasks were impaired.
□

5. Communicating the Results of Formalisation

Unfortunately, mathematical analysis provides non-formalists with an extremely poor idea of the argumentation processes that support particular conclusions. It is difficult for people without some mathematical background to understand the various proof rules that are applied during the formal derivation of particular conclusions. This section, therefore, describes how literate specification techniques can be extended from the field of software engineering to support the formal analysis of accident reports.

5.1 Literate Specification

Communicating the results of mathematical analysis is a general problem for the application of formal methods. It affects the techniques described in this paper. It also affects the development of safety -critical systems. For example, designers might use the following clause to specify that a control system automatically removes a warning at some time after a failure has occurred. This is an important requirement if users are not to be over-whelmed by obsolete error messages. Unfortunately, it is not easy for non-formalists to understand the natural language requirement from its formal statement. A related point is that the formal expression of the requirement provides no clues as to the motivation or justification

behind the requirement. In other words, it describes **what** the system should do, it does not describe **why** it should do it:

$$\forall t, \exists t': at(automatically\_remove\_warning(blow\_back\_error), t') \Leftarrow at(state(blow\_back, failed), t) \wedge at(display(blow\_back\_error\_icon), t) \wedge at(system\_cancel(blow\_back\_error\_icon), t') \wedge before(t, t'). \quad (40)$$

In previous papers, we have addressed these problems by developing literate specification techniques (Johnson, 1996a, 1996b). This approach uses the semi-formal argumentation of design rationale to support the use of formal methods during the systems development. Figure 1 illustrates this approach. Rank Xerox's Questions, Options and Criteria (QOC) notation is used to document the reasons why the previous clause might be adopted within the design of a particular system. QOC diagrams are built by identifying the key questions that must be addressed during the development of an interactive system (Buckingham Shum, 1995). The options that answer a particular question are then linked to it using the lines shown in Figure 1. Finally, options are linked to the criteria that support them, using solid lines, or weaken them, using broken lines. In Figure 1, the question of how to cancel blow-back warnings is answered by the design option that is specified by clause (40). This approach is justified by the criteria that the automatic cancellation of warnings reduces burdens on system operators. It is not supported by the criteria that this helps the operator to observe the warning. The diagram shown in Figure 1 is relatively simple in that it only shows a single option for the design question. In practice, these diagrams tend to show a number of alternative clauses each of which represents a different design option for the problem being considered. The interested reader is directed to Johnson (1996b) for more detail on the application of this approach.

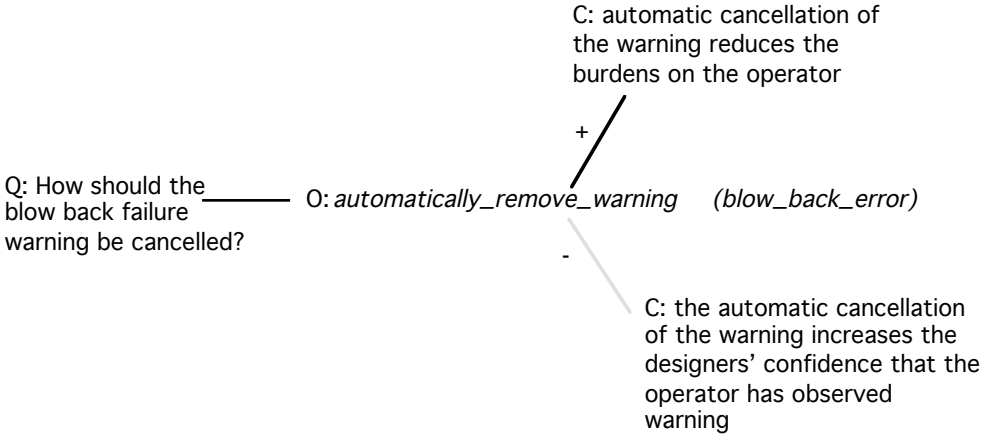

Figure 1: Literate Specification for the Warning Cancellation.

This blend of formal and semi-formal notations can also support the formal analysis of accident reports. Natural language annotations of the Questions and Criteria provide non-formalists with an entry-point into the clauses that represent particular Options. In literate specification, these annotations provide the justifications for and against formal design requirements. In accident analysis, they link source material to the clauses that describe the relationship between evidence and conclusions.

5.2 Conclusion, Analysis and Evidence (CAE) Diagrams

The Questions, Options and Criteria notation can be translated into a form that directly supports the formal analysis of accident reports. Instead of using questions to represent critical design issues, diagrams can represent the conclusions that are presented in a report. The options of a QOC diagram correspond to alternative interpretations of the events leading to a conclusion. Criteria can be compared to the evidence that supports or weakens the interpretation of an accident. Figure 2 presents a Conclusion, Analysis and Evidence (CAE) diagram for the Noordam collision. Broekhoven failed to maintain a vigilant watch. This is supported by [Conclusion 1] in the report and is formalised in clause (25). The conclusion relies upon an analysis which suggests that the number of people on the bridge prevented Broekhoven from visually detecting the Mount Ymitos. This is supported by the analysis in [Conclusion 5] of the report and is formalised in clause (28). The analysis rests upon evidence presented in [Paragraph 41] of the report. The conclusion also depends upon an analysis of the way in which Broekhoven used the radar. In

this analysis, he was preoccupied with navigation rather than collision avoidance, from [Paragraph 39] represented in clause (26). This is supported by evidence in [Paragraph 39].

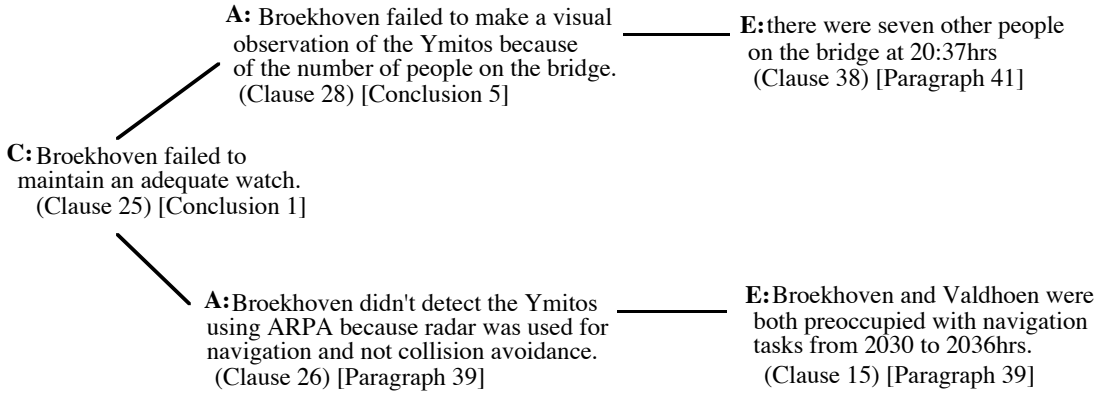

Figure 2: Conclusion, Analysis, Evidence (CAE) Diagram for the Noordam Collision

There is an important difference between Conclusion, Analysis and Evidence diagrams and the Question, Options and Criteria notation. Options represent alternative design choices in QOC. In contrast, the analysis components of a CAE diagram support a single conclusion. They are not mutually exclusive. It should also be noted that the evidence shown in Figure 2 supports the analysis. It is possible to use dotted lines and '-' signs to indicate evidence which might contradict a particular line of enquiry.

CAE diagrams are not intended to replace the formal proof techniques that are used in their construction. The vernacular labels that represent the conclusions, analysis and evidence are open to the same problems of inconsistency and mis-interpretation that weaken the use of natural language in accident reports. For instance, it is perfectly possible to link a conclusion to a line of analysis that has little or no relationship to the conclusion. The use of formal proof techniques helps to ensure that this does not happen. It should also be emphasised that none of the techniques presented in this paper are intended to replace the use of natural language in accident report. Our use of discrete mathematics is similar to that of forensic scientists who frequently use continuous mathematical models, for instance of combustion. Both sorts of model can be used to represent and reason about the events leading to failure.

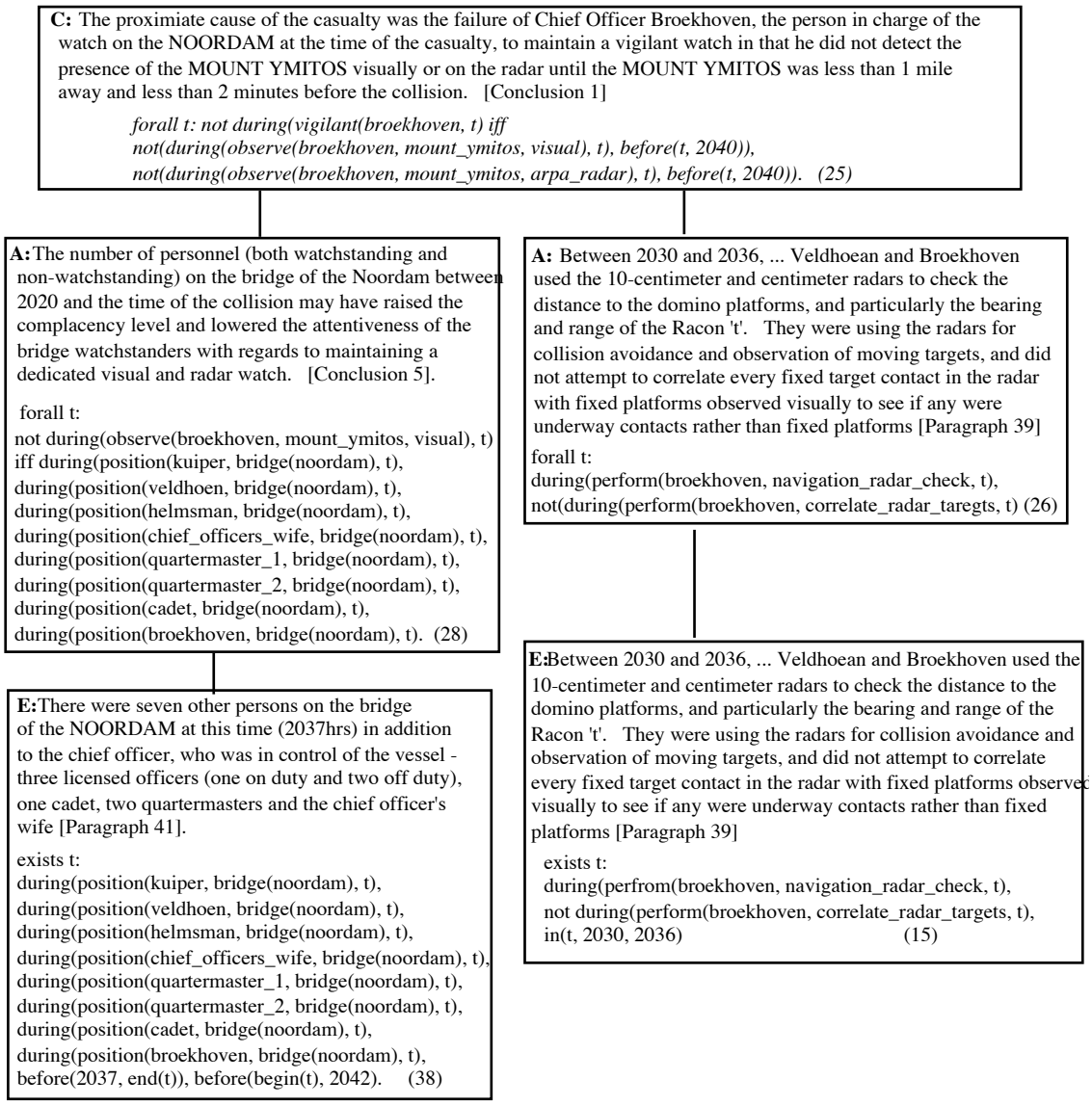

Figure 3: Conclusion, Analysis and Evidence diagram Integrating Formalisation and Informal Material

The United Kingdom Engineering and Physical Sciences Research Council has recently funded a three year investigation into the integration of formal reasoning and Conclusion, Analysis and Evidence diagrams for accident reports. We are particularly concerned to provide tool support for these techniques. For example, Figure 3 illustrates how CAE diagrams can be extended to represent the clauses that are used within the proof of a conclusion. This illustrates the mathematical relationship between the underlying evidence, at the bottom of the diagram, and the higher level conclusions. The task of constructing and maintaining such diagrams for complex accidents clearly requires some form of tool support, especially when one realises that key components of the proof, such as clause (27), are not shown. This problem could be addressed by exploiting hierarchical, graphical representations of formal proofs, such as tableaux . Hypertext display strategies might also be used to filter out the associated prose, or conversely, the mathematics at different stages during the analysis (Johnson, 1996b).

6. Conclusions and Further Work

This paper has argued that formal methods can support the use of natural language in accident reports. In particular, we are concerned to demonstrate that the recommendations of a report can be justified in terms of the events that are described in these documents.

6.1 Identifying Missing Information.

A key point in this paper has been that informal argumentation is weakened by the omission of critical information. For example, the Noordam report did not explicitly state the reasons why Broekhoven failed to perform collision checks using the ARPA radar between 20:36 and 20:42. Similarly, it did not

explain why 20:20 was cited as the critical moment when other crew members impaired operations on the bridge. Some of this detail can be inferred from other sections of the report. This is dangerous because incorrect inferences may lead readers to form inappropriate conclusions. For example, it would be wrong to assume that the number of crew members on the bridge at 20:20 should be used as a limit to the number of people allowed on the bridge of another ship (Kantowitz and Casper, 1988). Formal methods can be used to avoid such problems. We have shown how proof techniques can be used to establish that an accident report contains all of the evidence that is needed to support particular conclusions.

6.2 Structuring Critical Information.
An additional benefit from the application of formal proof techniques is that they help analysts to present supporting evidence in a coherent format. By this we mean that there is a clear distinction between the axioms that model the accident and the theorems that represent the conclusions which can be made from that model. This is critical because many accident reports mix these two different types of information. For instance, the Noordam case study presents evidence about the number of people on the bridge in the body of the report [Paragraph 41]. It also presents further evidence about this in the closing sections of the report [Conclusion 5]. This gradual presentation of information forces the reader to piece together the events leading to the accident over the hundreds of pages that, typically, form an accident report. Formal proof techniques can help with this because they require that the model is built before inferences can be drawn.

6.3 Avoiding Ambiguity.
Natural language argumentation structures frequently make effective use of ambiguity. This is useful when it is difficult or impossible to provide exact information about particular events during an accident. For instance, the Coast Guard report does not represent the particular words that were uttered by Kuiper when he first observed the lights on the Mount Ymitos. It is important to note that this form of ambiguity can be modelled through the abstraction mechanisms of formal languages. Terms such as *curse* can be used in place of the precise words uttered by an operator. However, there are times when unnecessary ambiguity can have disastrous consequences for an accident report. A detailed analysis of the Noordam case study has shown considerable problems in identifying the seven individuals who were present on the bridge of the Noordam immediately before the collision [paragraph 41]. We initially identified eight people who contributed to the events leading up to the accident. This inconsistency can be explained in terms of the ambiguity of roles, such as *quartermaster*. They are ambiguous in the sense that they cannot easily be matched against the names of the individuals involved in the accident, such as the lookout Salyo, from lengthy natural language accounts. Formal analysis helps to avoid this problem by forcing analysts to explicitly represent the relationships between the terms of Table 1.

6.4 Defining Relevance
A final benefit from our formalisation is that it helps to define a notion of relevance for the material in an accident report. Information must be included if it is necessary in explaining the conclusions that are reached in the report. This is not to say that any details which are not called upon in the conclusions ought to be omitted. Much of the detail in an accident report helps to establish the context of failure rather that just the events that led to the accident. In the Noordam, this includes detailed consideration of the 'rules of the road' for maritime navigation. In contrast, we argue that information must be included if it supports the conclusions that are drawn from an investigation. This does not just relate to factual information, such as the missing timings mentioned in Section 6.1. It also refers to the supporting inferences that help to link the factual analysis to the conclusions. For example, in order to prove Conclusion 1, we were forced to explicitly state the reasons **why** Broekhoven failed to maintain a vigilant watch, see clause (23). Unfortunately, our work has shown that readers are often expected to infer the arguments that support the conclusions in accident reports.

6.5 Future Work
The techniques that are described in this paper can be applied to represent and reason about the bias that is often embodied in accident reports. This is achieved by examining the factual information and the inferences that are presented in each account. Formal analysis can then be used to identify the impact that factual omissions have for the reader. For example, very different interpretations might have been produced if the Coast Guard's report had removed information about the number of people on the bridge of the Noordam. Such an omission not only affects the timeline of events leading to failure, it also restricts the valid inferences that can be made about an accident. For instance, readers would have been forced to find alternative explanations for Broekhoven's failure to visually observe the Mount Ymitos. Formal analysis can identify these differences because it would no longer be possible to prove theorem (23). We have already demonstrated that this approach can be used to identify 'biases' in the reporting of nuclear power accidents (Telford and Johnson, 1996). It remains to be seen whether these techniques can be applied to accident reports from other domains. An important pre-requisite for this work is the tool

support mentioned in the previous section. CAE diagrams quickly become unmanageable for the more complex proofs that are required to demonstrate the impact of bias between different accident reports.

It is important to emphasise that CAE diagrams and formal proof techniques are not intended to replace the natural language presentation of accident reports. In contrast, our intention is to provide a clear and coherent structure for the argumentation in accident reports (Reason, 1988). This additional degree of precision is required if companies are to use these documents as a means of guiding future development and investment decisions.

Acknowledgements
The research reported in this paper has been supported by UK Engineering and Physical Sciences Research Council grants GR/J07686, GR/K55042 and GR/K69148. I would like to thank the members of the Department of Computing Science, University of Glasgow for their support and encouragement in this work.

References

Air Accidents Investigations Branch, Department of Transport. *Report On The Accident To Boeing 737-400 G-OBME Near Kegworth, Leicestershire on 8th January 1989,* number 4/90, Her Majesty's Stationery Office. London, United Kingdom, 1990.

S. Austin and G.I. Parkin. Formal Methods: A Survey, Division Of Information Technology And Computing, The National Physical Laboratory, Sponsored by the United Kingdom Department of Trade and Industry, Teddington, United Kingdom, 1993.

S. Buckingham Shum, Analysing The Usability Of A Design Rationale Notation. In T.P. Moran and J.M. Carroll (eds.) Design Rationale Concepts, Techniques And Use, Lawrence Erlbaum, Hillsdale, New Jersey, United States of America, 1995.

Cullen, *Proceedings Of The Public Enquiry Into The Piper Alpha Disaster*. The Department of Energy, Her Majesty's Stationery Office, London, United Kingdom, 1990.

A.J. Dix, *Formal Methods For Interactive Systems*, Academic Press, London, United Kingdom, 1991.

D. Fennel, *Investigation Into The Kings' Cross Underground Fire*. Department of Transport, Her Majesty's Stationery Office, London, United Kingdom, 1988.

C.W. Johnson, *A Probabilistic Logic For The Development of Safety-Critical Interactive Systems*. International Journal of Man-Machine Systems, 39(2):333-351, 1993.

C.W. Johnson, *The Formal Analysis Of Human-Computer Interaction During Accident Investigations*. In G. Cockton, S.W. Draper and G.R.S. Weir, editors, People And Computers IX, 285-300. Cambridge University Press, Cambridge, 1994.

C.W. Johnson, *The Application of Petri Nets to Represent and Reason about Human Factors Problems During Accident Analyses* In P. Palanque and R. Bastide, editors, The Specification And Verification Of Interactive Systems, 93-112, Springer Verlag, Berlin, 1995.

C.W. Johnson, *Using Z to Support the Design of Interactive, Safety-Critical Systems* Software Engineering Journal, (10)2:49-60, 1995a.

C.W. Johnson, *Impact of Working Environment upon Human-Machine Dialogues: A Formal Logic for the Integrated Specification of Physical and Cognitive Ergonomic Constraints on User Interface Design.* Ergonomics (39)3:512-530, 1996.

C.W. Johnson, *Literate Specification.* To appear in the Software Engineering Journal, 1996a.

C.W. Johnson, *Literate Specification: Using Design Rationale To Support Formal Methods In The Development Of Human-Machine Interfaces.* To appear in the Human Computer Interaction Journal, 1996b.

C.W. Johnson, J.C. McCarthy and P.C. Wright, *Using A Formal Language To Support Natural Language In Accident Reports.* Ergonomics, (38)6:1265-1283, 1995.

P. Johnson, D. Diaper and J. Long, *Task, Skills And Knowledge: Task Analysis For Knowledge Based Descriptions*. In □B. Shackel (ed.) Human-Computer Interaction - INTERACT' 84, Elsevier Science Publications, North Holland, Netherlands, 23-27, 1984.

B.H. Kantowitz and P.A. Casper. *Human workload in aviation*. In E.L. Wiener and D.C. Nagel, editors, Human Factors In Aviation, 157-187. Academic Press, London, United Kingdom, 1988.

National Transportation Safety Board, Aircraft Accident Report, American Airlines Inc. DC-10 at Chicago Illinois, May 25, 1979, NTSB AAR-79-17, Washington DC.

P. Palanque and R. Bastide, Formal Specification and Verification of CSCW Using The Interactive Cooperative Object Formalism, In M.A.R. Kirby, A.J. Dix and J.E. Finlay (eds.), People and Computers X, 213-232. Cambridge University Press, Cambridge, 1995.

F. Paterno, M.S. Sciacchitano and J. Lowgren, A User Interface evaluation, Mapping Physical User Actions to Task-Driven Formal Specifications. In P. Palanque and R. Bastide (eds.), Design, Specification and Verification of Interactive Systems '95, 35-53, Springer Verlag, Berlin, 1995.

J. Reason, *Human Error*, Cambridge University Press, Cambridge, United Kingdom, 1990.

A.J. Telford and C.W. Johnson, *Extending the Application of Formal Methods to Analyse Human Error and System Failure During Accident Investigations*. To appear in the Software Engineering Journal, 1996.

United States Coast Guard, *Investigation into the Circumstances Surrounding the Collision Between the Passenger Vessel Noordam (NA) and the Freight Vessel Mount Ymitos (MT)*, United States Department of Transport, Washington DC, 1993.

N. Worley and J. Lewins (editors), *The Chernobyl Accident And Its Implications For The United Kingdom*, Report Number 19 Of The Watt Committee On Energy, Elsevier Science, North Holland, 1988.