Reasoning about Human Error and System Failure for Accident Analysis

Chris Johnson

Glasgow Accident Analysis Group,
Department of Computer Science, University of Glasgow, Glasgow,
Scotland, G12 8QQ.

http://www.dcs.gla.ac.uk/~johnson
E-mail: johnson@dcs.gla.ac.uk

ABSTRACT: 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 describe the human and system failures that lead to major accidents. Recommendations are then 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 account. Operator error is frequently blamed for accidents that might equally have been blamed upon poor systems engineering or interface design. This paper, therefore, 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.

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

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 (Morehouse and Subamaniam, 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.

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, 1990). 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). These problems create considerable confusion for the reader and may even lead them to doubt the accuracy of the final report.

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.

2. THE CASE STUDY

The events leading to the Kegworth disaster are used to illustrate the argument that is presented in this paper. The Air Accident Investigation Branch's (1990) report concluded that the accident was caused by a complex interaction between system and human failures. The main events leading to the accident can be summarised as follows. A British Midlands Boeing 737-400 took off from Gatwick on course for Belfast. Thirteen minutes later the turbofan in the number one (left) engine fractured. This caused a series of compressor stalls in that engine. The pilots were unsure about what had happened. There were excessive vibrations throughout the airframe. Loud noises and a smell of fire could also be detected in the cockpit. There were transitory fluctuations on the primary instrument displays and a maximum reading on the airborne vibration meter (AVM) for the left engine.

The crew's initial reaction was to diagnose a fire. The commander dis-engaged the auto throttle and asked the First Officer to throttle the right engine back. This was a mistake because it was the left hand engine that was faulty. Surprisingly, when the First Officer did this all indications of trouble in the left engine went away except for a maximum reading on the AVM for the left engine. The pilots did not notice this warning. The aircraft was then diverted to East Midlands Airport. The aircraft appeared to be flying normally and there was no reason to suspect that the wrong engine had been shut down.

Approximately fifteen minutes later, as the aircraft was being manouvered for its final approach to runway twenty-seven at East Midlands Airport, there was a sudden fall in power in the left engine. Attempts to re-start the right engine failed. The commander then tried to stretch the glide of the aircraft. He failed and the aircraft crashed on the embankment of the M1 motorway two hundred yards short of the start of the runway. A total of forty-six passengers died and a further seventy-four suffered serious injury.

3. MODELLING 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, communications, systems and process components 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 Air Accident Investigation Branch's report into the Kegworth crash includes the following account:

> "During the 11 seconds that elapsed between the disengagement of the autopilot and the throttling back of the No. 2 engine, the aircraft rolled slowly to the left through 16 degrees but the commander made no corrective movement of the aileron or rudder." [Page 3]

Additional information, such as the degree of roll, is included to help the reader form a picture of the accident even though this information is not used in the subsequent analysis. 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 (Johnson, 1995, 1995a, 1996):

- **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;
- **tasks.** It is necessary to identify the tasks that operators were, or should have been, performing during accidents;
- **communications.** 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;

- **physical components.** Components failure often forms the starting point for many accidents involving interactive systems.

"During the 11 seconds that elapsed between the disengagement of the autopilot and the throttling back of the No. 2 engine, the aircraft rolled slowly to the left through 16 degrees but the commander made no corrective movement of the aileron or rudder." [Page 3]

The paragraph from the Air Accident Investigation Branch (AAIB) report, cited above, can be used to identify an operator, the Commander. It is also possible to identify information and control systems such as the autopilot. We can identify physical components including the aileron and rudder. The following table shows part of the results that were obtained by extending this analysis throughout the AAIB report.

Operators	Tasks	Messages
commander	*program_FMS*	'It's the le...it's the right one'
first_officer	*navigation*	'Shut it down'
london_ATC	*radio_ATC*	'Okay throttle it back'

Systems	Components
eis	*engine_1*
	engine_2

Table 1: Critical Entity Table for Kegworth

In formal terms, the elements of this table define the types that model the Kegworth accident.

3.2 Axiom for the Accident System

The identification of such critical entities is of little benefit if analysts cannot represent and reason about their role in an accident. For example, the following quotation describes the crew's activities prior to shutting down the working engine:

"Immediately after throttling back the number 2 engine, the first officer advised London Air Traffic Control that they had an emergency situation which looked like a fire. The commander then ordered the first officer 'SHUT IT DOWN'." [page 4]

The following clause captures the observation that the first officer issued input to throttle-back the number two engine. This formula is constructed using the critical entities which were identified in table 1:

$$input(first\_officer,\ throttle\_back(engine\_2)). \qquad (1)$$

This states that the first officer issues input to throttle back the number two engine.

The problem with such representations is that they strip out the temporal information that frequently has a critical impact upon the course of an accident. This can be introduced using a simple temporal logic. The following clause states that there exists a time at which the first officer throttled back the number two engine. Unfortunately, we cannot be more precise than this because the previous citation does not state the exact moment at which this occured:

$$\exists t : input(first\_officer,\ throttle\_back(engine\_2),\ t). \qquad (2)$$

This states that the first officer issues input to throttle back the number two engine at some time *t*.

In fact, the AAIB report does provide a precise timing for the first officer's action. This is presented in Figure 2 of Appendix 4 on page 170, well away from the previous quotation from page 4. This scattering of temporal information throughout a report can make it extremely difficult for readers to construct an accurate time-line of the events leading to major failures. The following clause illustrates how logic can be used to avoid this limitation:

$$input(first\_officer,\ throttle\_back(engine\_2),\ 20\_05\_24). \qquad (3)$$

This states that the first officer issues input to throttle back the number two engine at 20:05:24.

Given this starting point it is now possible to reconstruct the sequence of events that were described in the previous quotation. We know that the command to 'SHUT IT DOWN' occured after the input described in clause (3):

$$\exists t : message(commander,\ first\_officer,\ SHUT\_IT\_DOWN,\ t) \wedge after(20\_05\_24,\ t) \qquad (4)$$

This states that the commander told the first officer to SHUT IT DOWN at some time after 20:05:24..

It is important to note that the previous clause does not capture all of the temporal constraints in the accident report. For example, the previous paragraph stated that the commander's order was issued 'immediately after'. the engine was throttled back. Additional clauses could be introduced to specify that the order must have been issued within five, ten, fifteen seconds of the first officers input. This would only be justified, however, if analysts conducted further investigations into the cockpit interaction immediately before the accident.

4. REASONING ABOUT OPERATOR ERROR

Clauses, such as (3) and (4), provide a number of additional benefits for accident analysis. In particular, they provide a precise and concise means of reasoning about the system failures that lead to operator 'error'. For example, the AAIB report found that:

> "Throughout the period of compressor surging, the No. 2 engine showed no parameter variations but because the first officer was unable to recall what he saw on the instruments, it has not been possible to determine why he made the mistake of believing that the fault lay with the No. 2 engine. When asked which engine was at fault he half-formed the word 'left' before saying 'right'. His hesitation may have arisen from genuine difficulty in interpreting the readings on the engine instruments or it may have been that he observed the instruments only during the 6 second period of relative stability between the second and third stages." (page 97)

This quotation reveals how accident reports may not provide a single, definitive analysis of the events leading to a major failure. Either the First Officer observed the engine information systems and experienced 'genuine difficulty in interpreting the readings' or 'he observed the instruments only during the 6 second period of relative stability'. The following clauses represent the two hypothesised causes for the operator error. As before, the timings for the period of quiescence could not be obtained from the pages surrounding the quotation. These were obtained from a trace of the critical engine parameters in Appendix 4 to the main report:

$$\begin{aligned}
&\exists t, \forall t' : \\
&\quad \mathit{input(first_officer,\ throttle_back(engine_2),\ t)} \Leftarrow \\
&\qquad \mathit{not(observe(first_officer,\ pei(engine_1),\ t')} \vee \\
&\qquad \mathit{observe(first_officer,\ pei(engine_2),\ t'))} \wedge \\
&\qquad \mathit{before(t',\ t).} \qquad (5)
\end{aligned}$$

This states that the first officer throttles back the number 2 engine at some time, *t*, if they fail to observe the primary engine information systems for the number 1 or number 2 at any time before they issue the input.

$$\begin{aligned}
&\exists t, \forall t' : \\
&\quad \mathit{input(first_officer,\ throttle_back(engine_2),\ t)} \Leftarrow \\
&\qquad \mathit{observe(first_officer,\ pei(engine_1),\ t')} \vee \\
&\qquad \mathit{observe(first_officer,\ pei(engine_2),\ t'))} \wedge \\
&\qquad \mathit{before(20_05_10,\ t')} \wedge \mathit{before(t',\ 20_05_16)} \wedge \\
&\qquad \mathit{before(t',\ t)} \qquad (6)
\end{aligned}$$

This states that the first officer throttles back the number 2 engine at some time, *t*, if they observe the primary engine information systems for the number 1 or number 2 engine between 20:05:10 and 20:05:16 and the input is issued after the observation.

It is possible to use formal reasoning as a means of demonstrating that these hypotheses are supported by the description of the accident that is presented elsewhere in the report. *If such a proof cannot be constructed then either there is a mistake in the formalisation or there is an omission in the accident report itself.* For example, Finding 7 states that:

> "The flight crew did not assimilate the readings on the engine instruments before they decided to throttle back the No. 2 engine. after throttling back the No. 2 engine, they did not assimilate the maximum vibration indication apparent on the No. 1 engine before they shut down the number 2 engine 2 minutes 7 seconds after the onset of vibration, and 5nm south of EMA (East Midlands Airport). The aircraft checklist gave separate drills for high vibration and for smoke, but gave no drill for a combination of both." (Finding 7, page 142)

The following clause formalises this using the timing for throttling back the engine that was given in (3):

$$\begin{aligned}
&\forall t:\ \mathit{not(observe(first_officer,\ pei(engine_1),\ t)} \wedge \\
&\qquad \mathit{observe(first_officer,\ pei(engine_2),\ t))} \wedge \\
&\qquad \mathit{before(t,\ 20_05_24)} \qquad (7)
\end{aligned}$$

$$\begin{aligned}
&\forall t:\ \mathit{not(observe(commander,\ pei(engine_1),\ t)} \wedge \\
&\qquad \mathit{observe(commander,\ pei(engine_2),\ t))} \wedge \\
&\qquad \mathit{before(t,\ 20_05_24)} \qquad (8)
\end{aligned}$$

Clause 7 states that the first officer did not observe the primary engine information systems before 20:05:24. Clause 8 states that the commander failed to regard these instruments before 20:05:24. We assume her e that values of *t* range from the initiating event for the accident. This technical point is discussed in more detail in Johnson (1986).

In order to formally prove that the finding of page 97 is supported by the evidence given on page 142, we must apply the following inference rule to (5) and (7). This states that if at all times we can conclude Q given some fact P and at some time we know that P is true then we must know that at some time Q is also true:

$$\forall t: P(t) \Rightarrow Q(t),\ \exists t': P(t') \vdash \exists t': Q(t') \qquad (9)$$

Informally, this argument can be expressed as follows. From analysis on page 97, clause (5), we know that know that the first officer throttles back the number two engine if he fails to observe the primary engine instrument systems. From the evidence of page 142, clause (7), we know that the first officer failed to observe the primary engine instrument systems before 20:05:24. We can, therefore, infer that the first officer did indeed throttle back the number two engine:

$$\begin{array}{l} \forall t': input(first\_officer, \\ \quad throttle\_back(engine\_2), 20\_05\_24) \Leftarrow \\ \quad not(observe(first\_officer, pei(engine\_1), t') \vee \\ \quad observe(first\_officer, pei(engine\_2), t')) \wedge \\ \quad before(t', 20\_05\_24). \end{array}$$

[Instantiating 20_05_24 for t in (5) given (3)] (10)

$$input(first\_officer, throttle\_back, engine\_2, 20\_05\_24)$$

[Applying (9) to (10), given (7)] (11)

This formal analysis helps to identify an important conflict between the human factors chapter in the report and the AAIB's overall findings. The human factors account admits the possibility that the First Officer did observe the engine information systems but that he did so during the seconds of quiescence, see clause (6) and the quotation from page 97. In contrast the overall findings of the report, used in the previous proof, do not consider this possibility, see clause (7) and the quotation from page 142. The First Officer's error was explained in terms of their failure to monitor the systems rather than the failure of the systems to provide information about the engine problem throughout the failure. The report does not provide any explanation of why operator 'error' was a more likely cause of the accident than the failure of the systems to indicate a potential problem during the period of quiescence.

5. FINDING EVIDENCE FOR ANALYSIS

It is important to emphasise that there might have been a number of different reasons why the operators failed to assimilate the readings on their computerised instrumentation systems. The previous analysis stated that the crew failed to observe their displays, *not(observe(first_officer...* The human factors account also suggests that there may have been presentation problems which might have prevented an accurate diagnosis even if the crew had observed the displays:

> "Unlike the transient fluctuations that would have appeared on the primary engine instruments, the reading on the No. 1 engine vibration indicator rose to maximum and remained there for about three minutes On the EIS (Electronic Engine Information Systems) however not only is the pointer of the vibration indicator much less conspicuous than a mechanical pointer but, when at maximum deflection, it can be rendered even less conspicuous by the close proximity of the No. 1 engine oil quantity display, which is the same colour as the pointer and is the dominant symbology in that region of the display." (page 100)

This illustrates further problems with natural language argumentation structures in accident reports. The quotation documents human factors concerns about the presentation of the EIS. This issue was ignored in the overall findings of the AAIB report which focussed upon operator error. In other words, the overall findings focussed upon the crew's failure to correctly monitor their instruments rather than on the problems with the presentation of the systems themselves. Such inconsistencies between the different sections of a report might be blamed upon the problems of coordinating diverse teams of experts from many different backgrounds. Logic can, however, provide a common means of reasoning about human error, interface design and systems engineering. For example, the following clause relates the first officers command to throttle-back the functioning engine to the sampling and presentation of the oil quantity indicator on the number 1 engine:

$\exists t, \forall t'$: *input(first_officer, throttle_back(engine_2), t)* $\Leftarrow$
close(avm(engine_1), oil_quantity(engine_1), t') $\wedge$
same_colour(avm(engine_1),oil_quantity(engine_1), t') $\wedge$
before(t, t') (12)

This states that the first officer issues input to throttle back engine 2 at some time, if at all previous times the AVM display is close to the oil quantity indicator and both displays are the same colour.

It is important to emphasise, however, that the formalisation process does not ensure that the relationship is 'correct'. The link between the oil quantity indicator and the First Officer's failure must be proven by conventional accident analysis techniques. In other words, given that we know about the detailed presentation and layout of the EIS, is it safe to conclude that at some time the commander will fail to monitor the AVM? The AAIB have addressed this issue by conducting a survey:

> "The overall results, however, showed that a large majority of pilots considered that the EIS displayed engine parameters clearly and showed the rate of change of parameters clearly. Fewer that 10% of pilots reported any difficulty in converting to the EIS from the earlier hybrid instruments and only a few reported minor difficulty in alternating between the EIS and hybrid displays. 64% of pilots stated that they preferred instruments with electromechanical pointers to the EIS" (page 69).

The results of this survey are inconclusive; they do not directly support the argument presented in (12). Further evidence might be gathered through the experimental analysis of pilot performance with the AVMs. This illustrates the way in which formal analysis provides a means of explicitly linking the products of an accident investigation with the findings that are documented in a report. Surveys, such as that cited above, and other forensic investigations help to establish the validity of clauses, such as (12). Failure to confirm a hypothesis indicates the need to conduct further investigations to establish alternative clauses all to treat any consequent inferences with a degree of scepticism in the final report.

6. PRESENTING FORMAL ARGUMENTATION

Mathematical analysis provides non-formalists with an extremely poor idea of the argumentation processes that support particular conclusions. This section, therefore, argues that elements of design rationale might be recruited to communicate the formal analysis of accident reports.

6.1 Design Rationale

Semi-formal, design rationale notations avoid the communications problems of mathematical specifications. For instance, the graphical Issue Based Information System (gIBIS) uses a complex web of issues, positions and arguments to record the rhetorical events in a design meeting (Conklin and Begeman, 1989). Rank Xerox's Questions, Options and Criteria (QOC) notation identifies key concerns that must be addressed during the development of interactive systems (Buckingham Shum, 1995). For example, Figure 1 shows that automatic cancellation might be used to answer the question of how to cancel a particular warnings. This approach is justified by the criteria that it reduces the burdens on system operators. This option is not supported by the criteria that it 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 (199a) for more detail on the application of this approach.

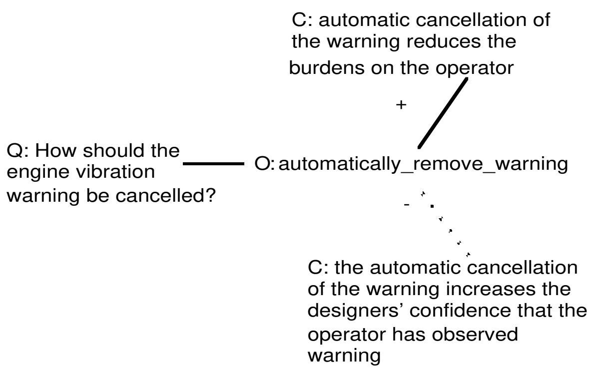

Figure 1: QOC for the Cancellation of a Warning .

Design rationale notations are appropriate for our purposes because they provide an explicit structure for many different forms of argumentation. In design rationale, they represent the reasons for and against particular development decisions. In accident analysis, they might represent the evidence for and against particular causes of an accident.

6.2 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 Kegworth Accident

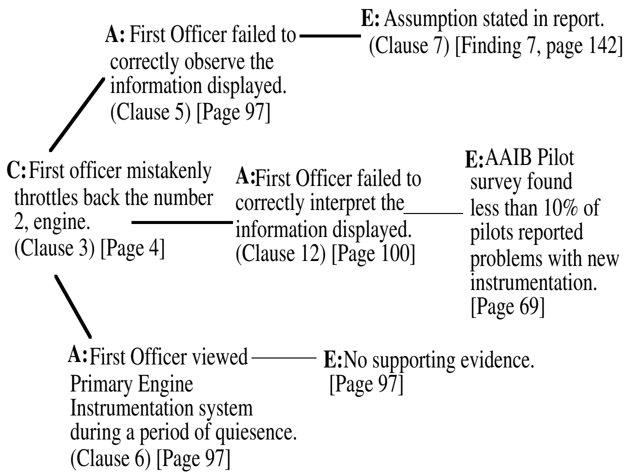

Figure 2: Conclusion, Analysis, Evidence (CAE) Diagram for the Kegworth Accident

The first officer mistakenly throttled back the number 2 engine. This conclusion is taken from page 4 of the report and is formalised by clause 3. It relies upon an analysis which suggests that the first officer failed to correctly interpret the information on their instruments. This is supported by the analysis in Page 97 of the report and is formalised in clause (5). The analysis rests upon an assumption that is presented as evidence in page 142, [Finding 7], of the report. The conclusion is also supported by an analysis which suggests that the operator failed to correctly interpret the information because of the display layout. This analysis is formalised in clause 12 and is taken from page 100 of the AAIB report. The analysis is not supported by survey evidence which suggests that less than 7% of pilots reported any problems with the displays. Finally, the conclusion is supported by an analysis that the first officer viewed the instrumentation during a period of quiescence. This is taken from page 97 and is formalised in clause 6. No supporting evidence was offered for this assertion.

7. CONCLUSION AND FURTHER WORK

This paper has argued that formal methods support the use of natural language in accident reports. They provide a precise and concise means of representing critical events during the course of major disasters. These representations effectively form a model or a time-line for the accident. Formal proof techniques can then be applied to determine whether the model actually supports the findings that are contained in an accident report. In the case of the Kegworth report, we have shown how the overall finding neglect the evidence of problems in the cockpit layout by focussing almost exclusively upon the evidence for operator error.

Further work intends to develop this approach in a number of ways. The task of maintaining CAE diagrams, such as Figure 2, clearly requires some form of tool support. One direction for further work is to exploit 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, 1996a).

The techniques that are described in this paper can also 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 of factual omissions. For example, very different interpretations might have been produced if the Kegworth report had removed information about the possible period of quiescence. 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 accept operator error as the primary cause of the accident. Formal analysis can identify these differences because it would no longer be possible to prove theorem (6). 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.

Acknowledgements

Thanks go to the members of the Glasgow Accident Analysis Group and the Glasgow Interactive Systems Group (GIST) and to the Formal Methods and Theory Group in Glasgow University. This work is supported by the UK Engineering and Physical Sciences Research Council, grants GR/JO7686, GR/K69148 and GR/K55040.

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*, 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.

J. Conklin and M.L. Begeman, *gIBIS: A Tool For All Reasons,* Journal Of The American Society For Information Science, 200-213, May, 1989.

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

Dix, A. *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, *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, *Decision Theory and Safety-Critical Interfaces*. In K. Nordby, P. Helmersen, D. Gilmore and S. Arnesen (eds.), Interact'95, 121-127, Chapman Hall, London, 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. Software Engineering Journal, (11)4:225-237, 1996a.

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.

W. Morehouse and M.A. Subamaniam, The Bhopal Tragedy. Technical Report. Council for International and Public Affairs, New York, United States of America, 1986.

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, Novermber 1996.