Using 'Extended' Fault Trees in Conjunction With Traditional Accident Reports

Lorna Love and Chris Johnson

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

http://www.dcs.gla.ac.uk/~{love, johnson}
Email: {love, johnson}@dcs.gla.ac.uk

ABSTRACT: Existing accident reporting techniques produce lengthy, detailed documents that can be confusing to read. Different sections are contributed by forensic scientists, metallurgists, human factors experts or meteorologists. This makes it difficult for readers to form a coherent account of human factors and system failures. This paper argues that fault trees can be used to present a clear and consistent overview of major accidents. Unfortunately, fault trees have a number of limitations. For instance, they cannot capture temporal properties of human and system failures. We, therefore, present an extended fault tree notation. These diagrams can be used in conjunction with an official accident report so that the reader can better visualise the causes of an accident.

KEYWORDS: accident analysis; fault trees; operator 'error'; system 'failure'.

1. INTRODUCTION

Official accident reports are produced in response to most major accidents, where there is loss of life or loss of capital. Lessons from the accident must be learned in order to ensure that a similar incident does not recur. Unfortunately, present reporting techniques produce lengthy, detailed documents which can be confusing to read (Johnson, McCarthy and Wright, 1995). This paper argues that when a fault tree is presented alongside a traditional accident report, the reader can better visualise the relationships between the causes of operator 'error' and system 'failure'.

Section two gives a brief account of the Clapham Junction railway accident which will serve as an example throughout the paper. Section three explains why fault trees should be considered as a potential technique for reporting accidents. Section four identifies some limitations attributed to fault trees and proposes an extended fault tree notation. The extensions are introduced, and their use is illustrated with the Clapham Junction case study. Conclusions are presented, and directions for future work are suggested in Section six.

2. THE CASE STUDY

The Clapham Junction railway accident report (Department of Transport, 1989) serves as a suitable example to illustrate our argument. This was chosen for several reasons. The accident is complex. Both human and system faults were involved in the accident. Many of these problems played only a marginal role in the accident, while several others were critical.

On the morning of Monday the 12th of September, 1988, just south of Clapham Junction railway station in London, a crowded commuter train collided head-on into the rear of a stationary train. The impact of this collision forced the first train to veer to it's right and strike a third oncoming train. This tragedy resulted in five hundred people being injured, thirty-five of those fatally and sixty-nine seriously. The first two trains

were the 6.14 Poole train coming from the South Coast and the 7.18 Basingstoke train heading into Waterloo. The third train was the 8.03 Waterloo to Haslemere train which was travelling out of London on an adjoining line with no passengers. In the accident report these trains are referred to as the Poole train, the Basingstoke train and the Haslemere train respectively. At ten past eight, after passing signals in his favour, the driver of the Poole train came upon what would become the accident scene. Once the visual obstruction of a steep bank had been eliminated, he found that on the same line and immediately ahead of him was the stationary Basingstoke train. Despite emergency braking, the front coach of the Poole train collided with the rear of the Basingstoke train. The impact of the head-on collision forced the Poole train to it's off side where it struck the empty Haslemere train a glancing blow. Part of the Haslemere train was subsequently derailed, which probably kept the Poole train from moving further to its off side across the other tracks.

3. WHY USE FAULT TREES ?

3.1. Alternative approaches

A number of techniques can be recruited to support accident investigations that involve human factors and system failures. For example, Johnson, McCarthy and Wright (1995) show how a Petri net can represent the events leading up to the Kegworth aircraft accident.

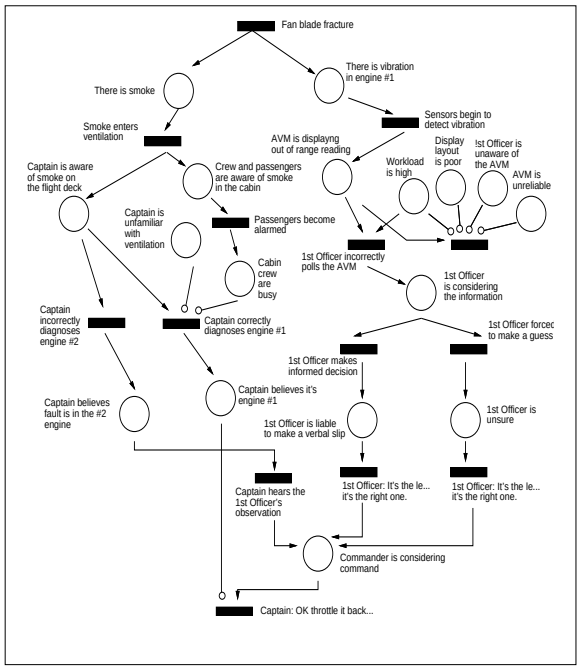

Figure 1: Petri net of the Kegworth aircraft accident

There are, however, a number of limitations with these diagrams. In particular they do not capture temporal information. Various modifications have been applied to the classic model. Levi and Agrawala (1990), use 'time augmented' Petri nets to introduce the concept of 'proving safety in the presence of time'. Unfortunately, even if someone can understand the complex firings of a 'time augmented' Petri net, they may not be able to comprehend the underlying mathematical formulae. Palanque and Bastide (1995) are addressing this problem.

Cause-Consequence Analysis was developed by Neilson in the 1970s.

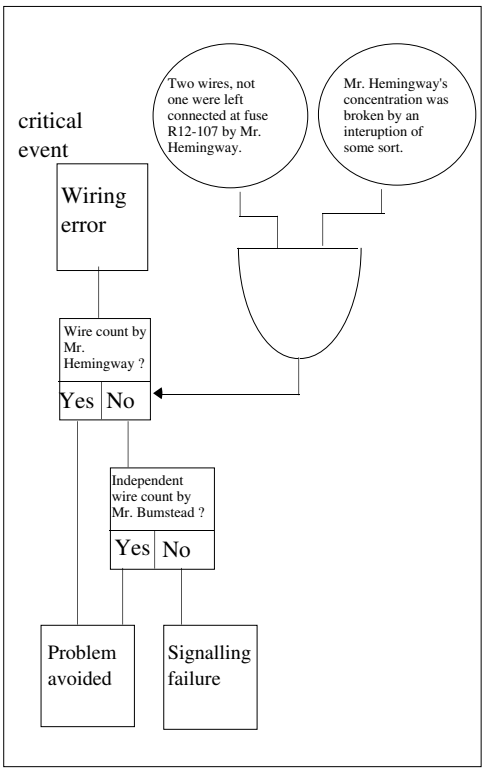

Figure 2: Cause consequence diagram of one aspect of the Clapham accident.

These diagrams explicitly represent sequences of events. They also allow the representation of time delays, alternative consequence paths, and combinations of events. Despite these advantages, cause consequence diagrams are not well suited to accident analysis. Separate diagrams are required for each initiating event. In an accident, there may be dozens of contributory factors and so several diagrams might be required. Figure 2 shows only the causes of the wiring error for the Clapham accident. Other diagrams would be required to represent the causes of bad working practices and to represent the events on the day of the accident.

3.2. Fault trees

Fault trees provide an ideal framework for representing and tracing causality through accident reports. They have an intuitive appeal and are effective in presenting conditional logic (Subramanian, Nosek, Raghunathan and Kanitkar, 1992). Trees graphically reveal the structure inherent in data or processes. This is more desirable than using linear symbolic languages (Jane and Sarson, 1979). Constructing a fault tree entails the production of a logic diagram illustrating conceivable event sequences that could result in a specified hazardous state. By focusing on the accident as the specified hazard, a fault tree can be constructed whereby the event sequences originate at the initial causes of the accident. This deductive approach, is the technique adopted by this paper and is the reverse of that used in Cause-Consequence analysis.

Although fault trees have been extensively researched in recent years (Xing, Fleming and Loh, 1996, Andrews, 1994, Ivanovic, Popovic, Stojovic and Djokic, 1994, Smith, Schwarzblat and Baker, 1994) no major work has been conducted to incorporate fault trees into official accident reports.

4. FAULT TREES IN ACCIDENT REPORTS

4.1. The fault tree notation

This paper uses a notation which is based on that presented in the U.S. Nuclear Regularity Commission's, 'The Fault Tree Handbook' (Vesely, Goldberg, Roberts and Haasl, 1981). The syntax is shown in Figure 3.

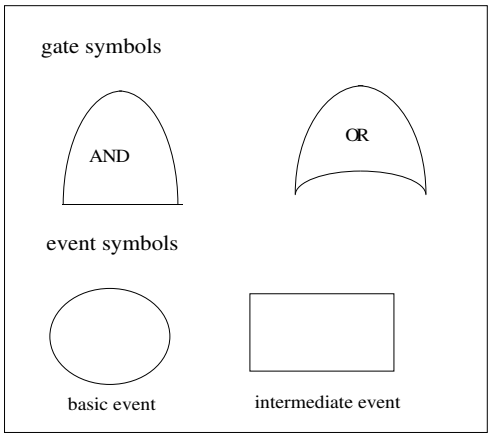

Figure 3: Fault tree symbology

A basic event is an initiating fault that requires no further analysis of it's pre-conditions. An intermediate event is a fault that occurs because of one or more antecedent causes acting through logic gates. A point to note here is the precise meaning of AND in this context. The output of an AND gate should be true if and only if all the inputs are true. Figure 4 shows a

fault tree representing the Clapham accident. At first sight the reader might conclude that the accident happened because of all four errors shown. Accidents cannot be analysed in the same way as electrical circuits. The AND gate in this context is taken to mean that the accident happened exactly as it did because of the four faults. This is not to say that the accident would not have happened if one of the intermediate events were not true. For example, the accident might still have happened if cab radios were installed in the trains.

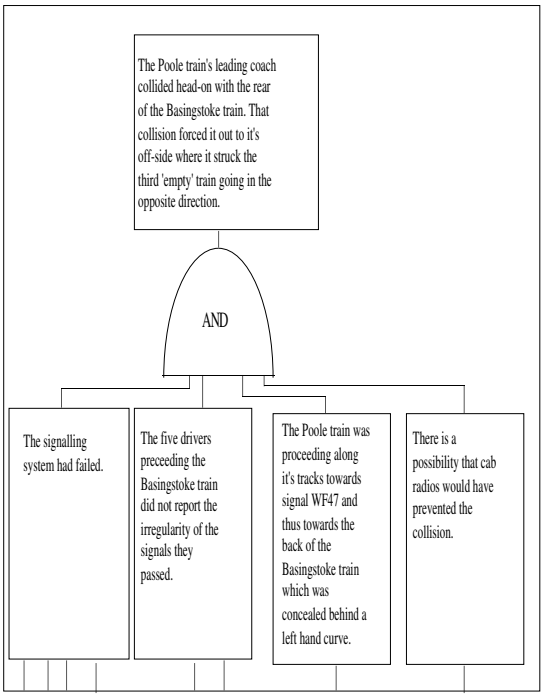

Figure 4: Extract from the Clapham fault tree

4.2. Limitations of fault trees in accident analysis

This paper builds upon the work of Leplat (1987) who first applied fault trees to analyse human error. He did not, however, apply his analysis to official reports. It is likely that a number of limitations would have been exposed if this had been attempted. For example, fault trees do not capture the distinction between *necessary* and *sufficient* causes. For example, Figure 5 shows a partial fault tree of part of the Clapham accident. This states that a wiring error was made because of Mr. Hemingway's actions. The fault tree does not show that the wiring error was also due to his supervisor, Mr. Bumstead. He should have performed an independent wire count which would have established that two wires were left connected instead of one.

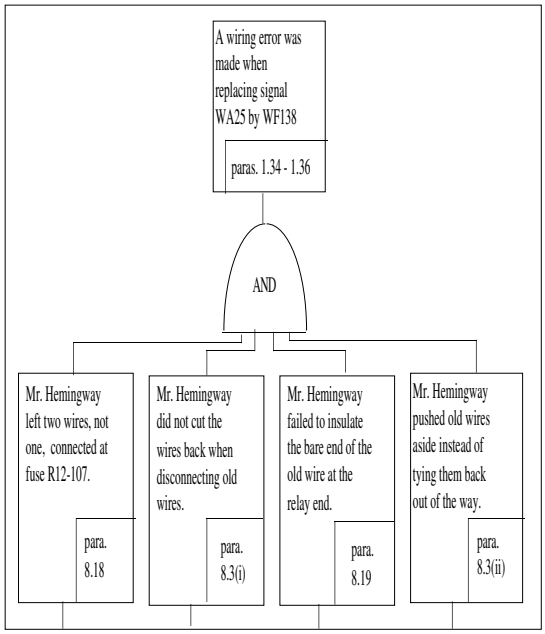

Figure 5: A 'partial' fault tree

Accident analysis requires 'total' fault trees. The constructor of the fault tree must take care to ensure that all of the known causes are included in the tree. It must be stressed here that accident analysts cannot claim to convey absolute truth. All of the contributing causes of an accident may never be known. The aim of the 'total' fault tree must be to communicate as accurately as possible all of the *known* causes of the accident.

There are further problems. Fault trees have no support, other than natural language annotations, for conveying the level of importance of an event. A further limitation is that they do not capture temporal orderings. Finally, fault trees do not describe the remedial actions that may be taken after a fault occurs.

5. EXTENDED FAULT TREES

This section describes ways in which fault trees can be extended to avoid the limitations described in the previous paragraph.

5.1. Rooted fault trees

Fault trees typically stop at the accident itself. Events after the 'undesired event' are important too. For example, the Ambulance service played an important part in the Clapham accident. Although their actions

didn't cause the accident, they contributed to the saving of lives, i.e. they reduced the consequences of the accident. Failure by the emergency services to react quickly and effectively can result in many more lives being lost, aggravating the effect of the accident.

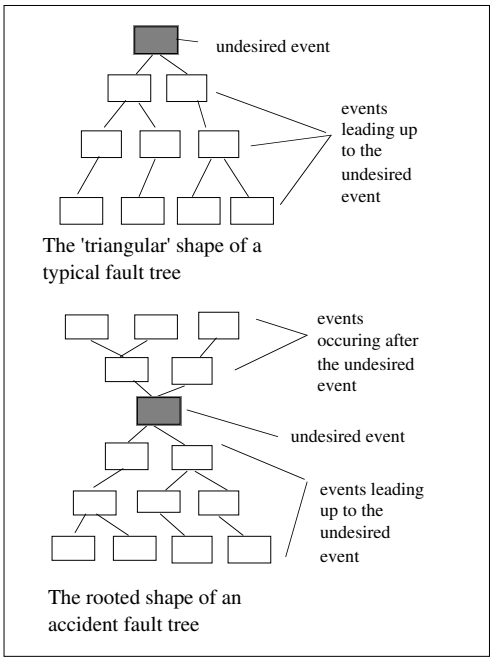

Figure 6: Comparison of triangular and rooted fault trees

Figure 6 shows the difference in 'shape' of a typical *triangular* fault tree and a *rooted* accident fault tree. In the rooted tree, the branches spread out both above and below the undesired event. The hazard is at the centre of the tree. The roots below the tree represent the causes of the hazard. The leaves above the hazard specify the actions taken and the subsequent events following the accident. Figure 8 shows part of the Clapham fault tree, illustrating after-accident events.

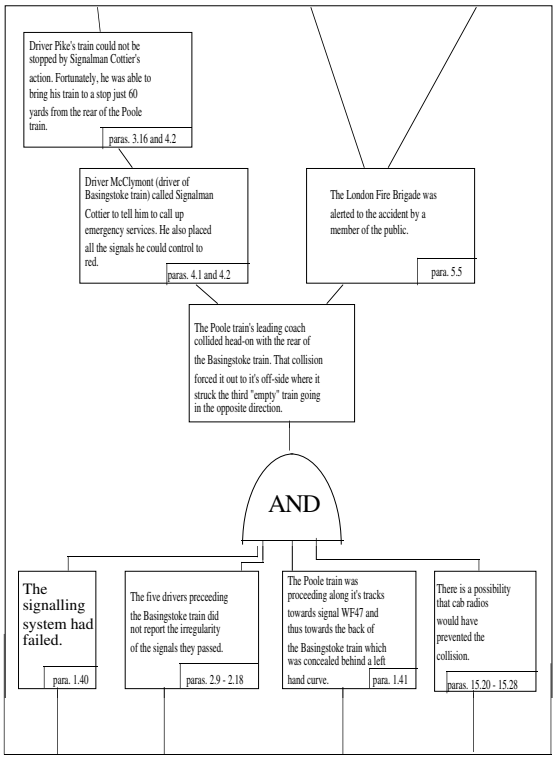

Figure 7: Extract from the Clapham fault tree showing after-accident events

5.2. Temporal fault trees

When reading lengthy natural language accounts of an accident, it can be hard to remember all of the critical points, and the order in which they occurred. This task becomes greater when, as in the Clapham report, allowance has to be made for approximate or conflicting timings. A further complication is that in accident reports two timings are often quoted for events - the time an event was scheduled to happen (for example a reference to a railway timetable) and the time it actually occurred.

Fault trees can be extended to capture this information in a number of ways. The U.S. Nuclear Regulatory Commission's 'Fault Tree Handbook' (Vesely, Goldberg, Roberts, Haasl, 1981) defines a PRIORITY-AND gate which is a special case of the AND gate. The output event occurs only if all input events occur in a specified sequence. The sequence is usually shown inside an ellipse drawn to the right of the gate. Figure 8 shows a PRIORITY-AND gate describing the order of four events. Representing the whole of the Clapham accident using 'priority-and'

gates would result in a cluttered diagram, conveying only relative temporal orderings.

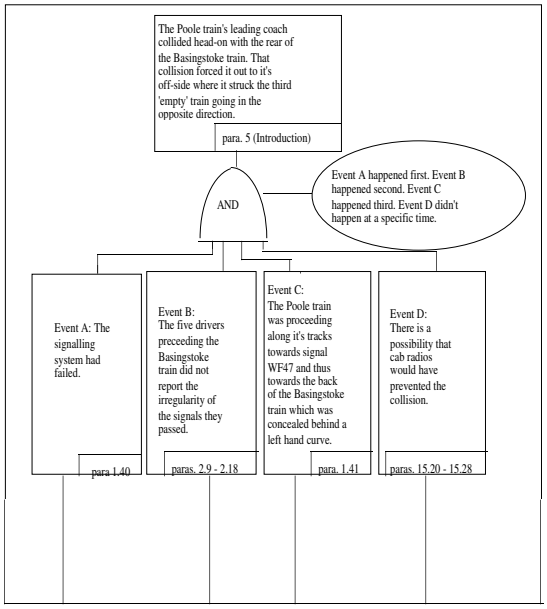

Figure 8: Illustration of PRIORITY-AND gate.

To cater for absolute time, we have extended fault tree nodes to include a timing in the bottom left hand corner. If the event took place years before the day of the accident, the exact time of day will probably not be of interest, and the date alone will suffice. If the event took place shortly before the accident, then the exact timing will be more important and should be included.

To impose relative timings, the tree orders events from left to right. Ranges of time are written with a '-' between the start and end of the interval in which the event took place. Timings are annotated with the word 'approx.' if the exact moment is known. All conflicting times appear with a brief explanation. Concurrent event nodes are placed immediately adjacent to one other. Events which occurred with a large time gap between them are placed spatially separate with an appropriate horizontal distance between them. Causes without times can be placed in the fault tree with no time subscript. To minimise confusion, they should not appear inside the timed list.

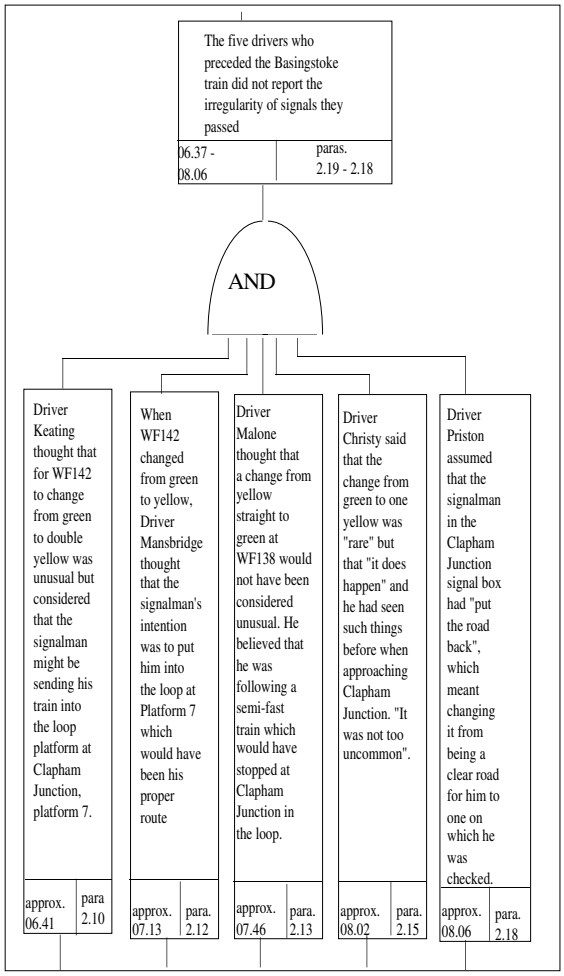

Figure 9: Extract from Clapham fault tree illustrating temporal properties

5.3. Weighted fault trees

Accident reports must discuss all the surrounding events, even if their contribution to the accident was negligible. Any omission could be interpreted as deliberate. Because of this the reader faces the demanding job of sifting through masses of detail. Minor factors can be complicated to explain. Events whose causal role is in dispute have to be examined and reasoned about. Related events which do not participate in the accident must also be discussed and their elimination explained. Critical events which are a 'matter-of-fact' and not a 'matter-of-opinion' can be written succinctly. Therefore, the amount of space dedicated to a cause is not directly related to it's importance in most accident reports.

Natural language can tell the reader how important a cause in the accident was, using words such as 'important', 'incidentally', 'primary', 'significant' and 'inconsequential'. However, the reader has to digest large chunks of text before finding all of the events which really did cause the accident.

A more subtle problem can arise when different sections of the report refer to different aspects of the accident. The importance of events may be prioritised relative to one another, and not relative to the accident as a whole. For example, human factors specialists might focus upon events that are ignored by systems engineers.

The Fault Tree Handbook (Vesely, Goldberg, Roberts, Haasl, 1981) presents the categorisation of faults as: 'negligible' - loss of function that has no effect on system; 'marginal' - this fault will degrade the system to some extent but will not cause the system to be unavailable; 'critical' - this fault will completely degrade system performance; 'catastrophic' - this fault will produce severe consequences which can involve injuries or fatalities. Figure 10 shows how this classification might be used with our extended fault tree notation.

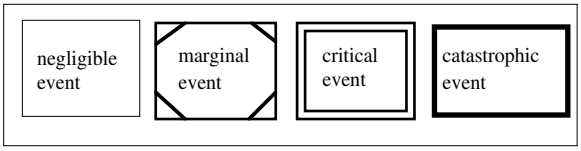

Figure 10: Weighted fault tree nodes

Our extended fault trees fault trees show post-accident events which are not actually 'causes'. For example, the event of the first ambulance arriving did not affect the collision of the trains. Events after an accident are not causes and so should be represented differently as shown in Figure 11.

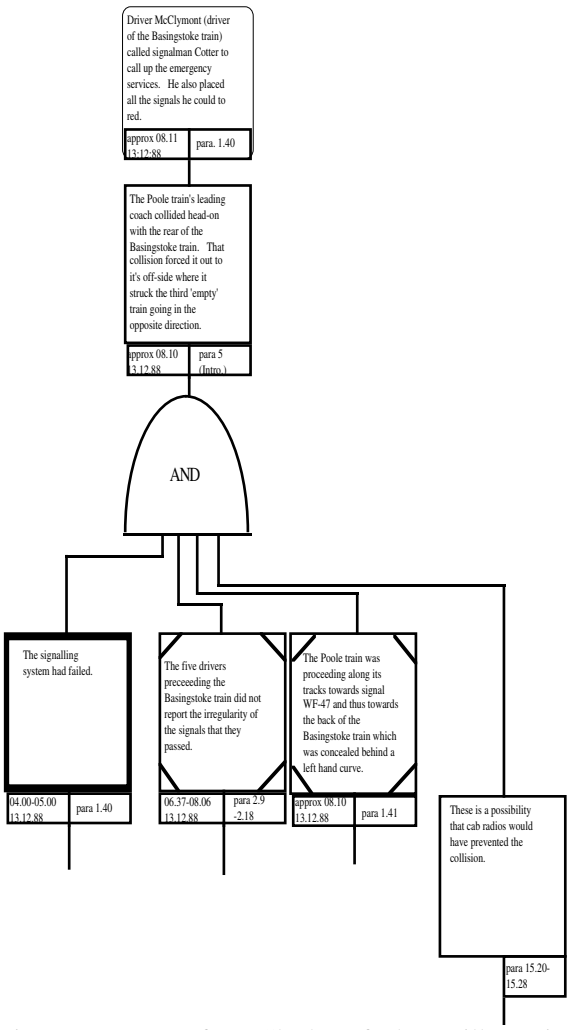

Figure 11: Extract from Clapham fault tree illustrating weighting properties

Figure 11 shows that the failure of the signalling system was a catastrophic event. Failure of the five preceding drivers to report the irregularity of the signals they passed was marginal. The accident could have happened with the first train. The location of the Poole train was negligible. The collision could have involved a different train, but the Poole train's location describes the context of the accident. The lack of cab radios is also negligible. It is unknown whether they would have prevented the collision or not. It is important to emphasise that the categorisation is a subjective assessment. What is important is not whether the reader agrees with a particular assessment, but that the diagram makes the categorisation explicit.

6. FURTHER WORK AND CONCLUSIONS

This paper has argued that fault trees can be used to support natural language accident reports. They provide an overview of the human factors 'errors' and system 'failures' that contribute to major accidents. Unfortunately, existing approaches do not capture the temporal information that can have a profound impact upon system operators. They do not capture the importance that particular failures have for the course of an accident. They only represent contributory causes and not post-accident events. We have, therefore, introduced an extended fault tree notation that avoids all of these limitations.

Work is being done at present to introduce types into our extended fault tree notation. For example passengers, drivers and emergency workers are of type person. The Poole and Basingstoke trains can be represented as lists of carriages. The idea is that the originating causes in the fault tree should be written in terms of primitive objects. This helps to avoid some of the ambiguities that can arise from natural language labels of fault trees. This approach also supports the animation of accidents. 'Types' and 'time' can be used as a basis for the data structures that would be required.

We are in the process of performing empirical studies to evaluate the effectiveness and usability of our extended fault trees. Interim results indicate the need to provide tool support during both the construction and inspection of these diagrams. Fortunately, a number of tools for standard fault-trees already exist and future work intends to extend this approach to support accident analysis.

Acknowledgements

Thanks go to members of the Glasgow Accident Analysis Group and the Glasgow Interactive Systems Group. This work is supported by UK Engineering and Physical Sciences Research Council Grant No. GR/K55042.

References

J. D. Andrews. *Optimal Safety System-Design Using Fault Tree Analysis.* In Proceedings of the Institution of Mechanical Engineering Part E - Journal of Process Mechanical Engineering, (208):E2, 123 - 131, 1994.

Department of Transport. *Investigation into the Clapham Junction Railway Accident.* Her Majesty's Stationery Office. London, United Kingdom, 1989.

G. Ivanovic, P. Popovic, M. Stojovic, M. Djokic. *Fault Tree Analysis Applied To Vehicle Design.* In International Journal of Vehicle Design, (15):3 - 5, 416 - 424, 1994.

C. Jane and T. Sarson. *Structured Systems Analysis: Tools and Techniques.* Prentice Hall, 1979.

C. W. Johnson. *The Formal Analysis of Human Computer Interaction During Accident Investigations.* In G. Cockton, S. W. Draper and G. R. B. Weis. People and Computers IX, 285 - 297, CUP, Cambridge University Press, Cambridge, 1994.

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

J. Leplat. *Accidents and Incidents Production: Methods of Analysis.* In J. Rasmussen, K. Duncan and J. Leplat (eds.), New Technology and Human Error. John Wiley and Sons Ltd, 1987.

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

S. Levi and A. Agrawala. *Real Time System Design* . McGraw-Hill International Editions, 1990.

P. Palanque and R. Bastide. Formal Specification and Verification of CSCW Using The Interactive Co-operative 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.

J. Peterson *Petri Net Theory and the Modelling of Systems.* Prentice Hall, 1981.

J. E. Smith, M. Schwarzblat, J. C. Baker. *Application of a Fault-Tree Construction Expert-System to an Actual Nuclear Generating-Station System.* In Reliability Engineering & System Safety, (44):3, 237-242, 1994.

G. H. Subramanian, J. Nosek, S. P. Raghunathan and S. S. Kanitkar. *A Comparison of the Decision Table*

and Tree. In Communications of the A.C.M. 35(1). 89 - 94, 1992.

W. E. Vesely, F. F. Goldberg, N. H. Roberts, D. F. Haasl. *Fault Tree Handbook.* U.S. Nuclear Regulatory Commission, 1981.

L. M. Xing, K. N. Fleming, W. T. Loh. *Comparison of Markov Model and Fault-Tree Approach in Detereming Initiating Event Frequency for Systems with 2 Train Configurations.* In Reliability Engineering & System Safety, (53):1, 17-29, 1996.