Using 'Accident 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.

Email: {love, johnson}@dcs.gla.ac.uk

ABSTRACT Accident reports help to ensure that operator 'error' and system 'failure' do not threaten other applications. Unfortunately, a number of usability problems limit the effectiveness of these documents. Each section is, typically, drafted by a different expert; forensic scientists follow metallurgists, human factors experts follow meteorologists. In consequence, it can be difficult for readers to form a coherent account of an accident. This paper argues that fault trees can be used to present a clear and concise overview of major failures. Unfortunately, fault trees have a number of limitations. For instance, they do not represent time. This is significant because temporal properties have a profound impact upon the course of human-machine interaction. Similarly, they do not represent the criticality or severity of a failure. We have, therefore, extended the fault tree notation to represent human-machine interaction during major failures. The resulting Accident Fault Tree diagrams can be used in conjunction with an official accident report to better visualise the course of an accident. The Clapham Junction railway disaster (Department of Transport, 1989) is used to illustrate our argument.

KEYWORDS accident analysis, fault trees, operator 'error', system 'failure'.

1. FAULT TREES

Fault trees are, typically, used pre hoc to analyse potential errors in a design. They have not been widely used to support post hoc accident analysis. They do, however, offer considerable benefits for this purpose. The leaves of the tree can be used to represent the initial causes of the accident (Leplat, 1987). These basic events can be used to represent the phenotypical failures that lead to an accident (Hollnagel, 1993). Intermediate events can represent the operator 'mistakes' that frequently exacerbate system failures. An undeveloped event is a fault event that is not developed further, either because it is of insufficient consequence or because information is unavailable.

There are a range of important differences that distinguish the use of Accident Fault Trees from their more conventional application. Some arise from the semantics of the gates that are used to construct the diagrams. Conventionally, the output from an AND gate is true if and only if all of its inputs are true. Accidents cannot be analysed in this way. Most accident reports do not distinguish between necessary and sufficient conditions. In Accident Fault Trees, therefore, an AND gate represents the fact that an accident report cites a number of initiating events as contributing to the output event. No inferences can be made about the outcome of an AND gate if any of the initiating events do not hold.

The output of an OR gate is true if and only if at least one of its inputs is true. An OR gate can be used in an Accident Fault Tree to represent a lack of evidence. Evidence can be removed accidentally or deliberately

from an accident scene. Alternatively, evidence may be missing because the person holding the information died in the accident. The output of an XOR (exclusive OR) gate is true if and only if exactly one of the inputs are true. They are useful in Accident Fault Trees when we know an intermediate event was caused by either of two events, but not both.

2. ACCIDENT FAULT TREES

2.1 Introducing Paragraph References

The results of an initial usability test with accident analysts indicated that the standard fault tree notation did not support cross-referencing between the tree and the original document. Events in Accident Fault Trees are annotated to include a paragraph number. This number refers to the paragraph number of the accident report that the information in the node is taken from.

2.2 Representing Post-Accident Sequences

Fault trees typically stop at the 'undesired event'. In accident reports, events after the accident are important too. These, typically, include the operator actions that are taken to mitigate the effects of system failure. For example, the Ambulance service played an important part in the Clapham railway accident. Although their actions did not cause the accident, they reduced the *consequences* of the accident. It is, therefore, important that Accident Fault Trees include post-accident events. Accident Fault Trees explicitly frame the accident. Branches spread out both above and below the accident.

The accident is at the centre of the tree. The roots below the centre represent the factors influencing the accident. The leaves above the centre specify the actions taken and the subsequent events following the accident.

2.3 Introducing Time

Temporal properties can have a profound impact upon the course of human-computer interaction. Delays in system responses can lead to frustration and error. Conversely, rapid feedback from monitoring applications can stretch an operator's ability to filter information during critical tasks (Johnson, 1996). Accident Fault Trees, therefore, include real-time. It is important to note, however, that is not always possible or desirable to associate an exact time with all of the events leading to an accident. Given limited evidence in the aftermath of an accident it is unlikely that operators will be able to recall the exact second in which they did or did not respond to a system failure.

2.4 Introducing Criticality

Many existing fault trees fail to represent the criticality of an event. This is surprising because different faults will carry different consequences for the continued operation of an interactive system. For example, keystroke errors may only have a marginal impact whilst more deep-seated mode confusion can have catastrophic consequences. Figure 1 illustrates a graphical extension to the fault tree notation that can be used to represent criticality.

Figure 1: Weighted fault tree nodes

A negligible failure leads to a loss of function that has no effect on system. A marginal failure degrades the system but will not cause the system to be unavailable. A critical failure completely degrades system performance. A catastrophic fault produces severe consequences that can involve injuries or fatalities. It should be noted that we are currently evaluating a range of alternative presentation formats for these symbols.

It is important to emphasise that the criticality categorisation is a subjective assessment. What is important is not whether the reader agrees with our particular assessment, but that the diagram makes the categorisation explicit. Too often these assessments are left as implicit judgements within the natural language of an accident report.

3. THE CLAPHAM ACCIDENT FAULT TREE

Figure 2 illustrates an application of the extensions presented in the previous section. The Clapham Accident Fault Tree includes paragraph references and

post-accident events. It also links the event nodes to the times at which they took place. Finally, the Accident Fault Tree makes explicit the level of criticality of each event.

Figure 2: Extract from a Clapham Accident Fault Tree

REFERENCES

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

E. Hollnagel, *The Phenotype Of Erroneous Actions*, International Journal Of Man-Machine Studies, 39:1-32, 1993.

C. Johnson, *Documenting The Design Of Safety-Critical User Interfaces*, Interacting With Computers, (8)3:221-239, 1996.

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.

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