Applying Empirical Modelling to railway management scenarios?

Chris Roe

April 5th, 2001

1 Introduction

1.1 Motivation

Railways around the world are in a period of significant change [6]. Accidents on the railways have always attracted the attention and concerns of the public and, unlike risks in other parts of industry and commerce, seemingly everyone has views on how to manage them (and indeed how to run the railway itself). Echoes of todays major issues in Britain can be found in our history and elsewhere in the world. Accidents often occur that could be preventable by more effective (and expensive) safety mechanisms. Captain Tyler (Chief Inspector of Railways, 1872) commented that :

> Stationmasters, signalmen and porters must be expected, in the course of their duties and their rough work, to make mistakes.....

1.2 An ESRC research project

"Tabletop" training exercises have recently been introduced to improve coordination. Key personnel from each of the agencies involved meet to manage a simulated emergency based around a tabletop model. The players take on the roles they would in the real emergency, and so learn how to coordinate decision-making. New developments in computer simulation and training technologies present opportunities to improve the realism of tabletop training. The analysis will make use of the emerging theory of 'distributed cognition', which describes how the intelligent behaviour of individuals is coordinated through communications and the sharing of knowledge. The study will focus on conflicts between the knowledge, assumptions and priorities of the personnal from the different agencies, and identify the coordination mechanisms operating between them, such as the mechanisms by which priorities are negotiated. Requirements for computer-based training simulators will be formulated. These will be defined by the problem of coordination (what mechanisms need to be learnt), and the good practice model of training (how coordination training is currently supported).

They will be informed by recent developments in computer-based training. A specific version of the requirements will be provided for Railtrack. The project will extend the theory to account for training processes, contributing directly to the theory of group training. Computer-based simulators have begun to appear in this area and are already in operation with the 'blue lamp' services. However, the need to focus on the particular training issue of inter-agency communication remains outstanding. This project will address that need through formulating common requirements for such simulators [7].

2 Case Study

In this section we introduce the case study that we shall use throughout this paper as our main example.

2.1 The Clayton Tunnel disaster

Situation description

Three heavy trains leave Brighton for London Victoria on a fine Sunday morning, travelling on the London, Brighton and South Coast railway. They are all scheduled to pass through the Clayton Tunnel — the first railway tunnel to be protected by a telegraph protocol designed to prevent two trains being in the tunnel at once. Elsewhere, safe operation is to be guaranteed by a time interval system, whereby consecutive trains run at least 5 miuntes apart. On this occasion, the time intervals between the three trains on their departure from Brighton are 3 and 4 minutes.

There is a signal box at each end of the tunnel. The North Box is operated by Brown (B) and South by Killick (K). K has been working for 24 hours consistently. In his cabin, he has a clock, an alarm bell, a single needle telegraph and a handwheel with which to operate a signal 350 yards down the line. He also has red (stop) and white (go) flags for use in an emergency. The telepgraph has a dial with three indications : NEUTRAL, OCCUPIED and CLEAR.

When K sends a train into the tunnel, he sends an OCCUPIED signal to B. Before he sends another train, he sends an IS LINE CLEAR? request to B, to which B can respond CLEAR when the next train has emerged from the North end of the tunnel. The dial at one end of the telegraph only displays OCCUPIED or CLEAR when the appropriate key is being pressed at the other — it otherwise displays NEUTRAL.

The distant signal is to be interpreted by a train driver either as *all clear* or as *proceed with caution*. The signal is designed to return to *proceed with caution* as a train passes it, but if this automatic mechanism fails, it rings the alarm in K's cabin.

The accident

When train 1 passed K and entered the tunnel the automatic signal failed to work. The alarm rang in K's cabin. K first sent an OCCUPIED message to B, but then found that train 2 had passed the defective signal before he managed to reset it. K picked up the red flag and displayed it to Scott, the driver of train 2, just as his engine was entering the tunnel. He again sent an OCCUPIED signal to B. K did not whether train 1 was still in the tunnel. Nor did he know whether S had seen the red falg. He sent an IS LINE CLEAR? signal to B. At that moment, B saw train 1 emerge from the tunnel, and responded CLEAR. Train 3 was now proceeding with caution towards the tunnel, and K signalled all clear to the driver with his white flag. But S had seen the red flag. He stopped in the tunnel and cautiously reversed his train to find out what was wrong from K. Train 3 ran into the rear of Train 2 after travelling 250 yards into the tunnel, propelling Train 2 forwards for 50 yards. The chimney of the engine of Train 3 hit the roof of the tunnel 24 feet above. In all 23 passengers were killed and 176 were seriously injured.

2.2 Studying the accident scenario

The Clayton Tunnel railway accident occured in 1861 [14]. It was significant as the first major accident to involve the new technology supplied by the telegraph. An investigate study of the accident raises a very wide range of concerns :

- social conventions : railway procedures and communication protocols;
- human capabilities : viability of work regimes;
- technologies : telegraph operation, train speed, reliability of signals and safety devices;
- physical context : distances, visibility, weather conditions, audibility.

The model can be used as a way of exploring the tasks demanded of the human agents, either with a view to training a human user in the appropriate protocols, or assessing the degree of skill and attentiveness needed to perform the appropriate role. Possible scenarios to be considered include:

- demonstrating normal operation, e.g by coordinating the interaction of the relevant human agents in running trains through the tunnel at realistic time intervals and speeds;
- testing the signal operator's familiarity with protocols and speed of response, e.g. through automatic generation of sequences of trains arriving at ever greater frequency;
- intorducing unreliable operation of components such as the telegraph, signal resetting treadle and alarm bell;
- changing the physical environment, e.g. by introducing fog, or ice.

The model can be interactively adapted in a way that can be interpreted as "negotiating its referent". For instance, it is possible to adapt the model so that the individual views reflect subjective misconceptions about the objective state (e.g the signal operator mistakenly thinks the signal is set to caution), fantasy scenarios (e.g the tunnel moves as the train approaches), or to embellish the model by introducing richer observables (e.g. adding a bell to the telegraph or - in principle - superimposing a 3D visualisation [15].)

3 Railway accident Modelling

Whereas the section on the Clayton Tunnel might form part of the conclusions of the crash enquiry, the independent personal accounts of the participants would have the character of evidence. Of its essence, evidence has an open-ended quality : even after an inquiry, it is still possible to admit new evidence. The findings of an enquiry are in contrast oriented towards declared judgments and incontrovertible facts. The official account of the accident omits much that is deemed irrelevant, and attempts to arbitrate or leave conflicts unresolved as appropriate. For instance, the fact that Killick had been working for 24 hours non-stop is recorded, and the time intervals between train departures from Brighton are officially declared despite conflicting evidence from independent sources.

Accident reports help to ensure that designers and engineers learn from the mistakes of the past. Unfortunately, it can be difficult for readers to trace the increasingly complex arguments that are presented in accident reports.

Conclusion, Analysis, Evidence (CAE) diagrams can be used to avoid these problems. CAE diagrams explicitly capture the relationship between evidence and lines of argument. They can also be used to capture the different viewpoints that often reflect important divisions between official accounts and eyewitness testimonies.

Formal reports focus on a single view of an accident.

Conclusion, analysis and evidence diagrams were specifically developed to provide a graphical overview of the argument that is presented in accident reports [10]. This paper (sic) uses CAE diagrams to chart the differences that exist between alternative aacounts of the same accident. This helps to identify areas of conflict between the "official" view of an accident and eyewitness testimony. Readers must trust to the skills and expertise of the investigator. CAE diagrams have also shown how these diagrams can be extended to represent the opposing arguments that are often made by eyewitnesses in the aftermath of an incident. They provide a graphical representation of the multiple viewpoints that can help a reader's understanding of an incident or accident.

Accidents do not simply 'happen'. They, typically, have complex causes that take many days, weeks or even years to develop. Engineers have developed a range of tools and techniques that can be used to represent and reason about these causes of major accidents. We argue that novel approaches also suffer from serious limitations as tools for modelling the temporal properties of human 'error' and systems 'failure'. A number of factors make it difficult to produce clear and consistent accident reports. Accident reports contain the work of many different experts. Conclusions are, typically, seperated into a number of different chapters. This has important consequences for the 'usability' of the resulting documents. It can be difficult to trace the ways in which system 'failure' and operator 'error' interact over time. There are a number of further reasons why previous approaches cannot easily be used to model the events leading to recent accidents. The first is that many techniques, including timelines and Fault Trees, provide only limited means for reasoning about concurrency. This is an important limitation; the increasing integration of both production processes and control technology make it increasingly likely that major accidents will involve simultaneous failures in many different areas of a complex system. Existing techniques, such as time lines or Fault Trees, and novel approaches, including Petri Nets and logics, provide little or no support for identifying and resolving these inconsistencies. In consequence, many accident reports contain incomplete and contradictory information about the sequencing of human error and systems failure.

Johnson [11] presents a list of requirements for the temporal modelling of accident sequences. Like Green's work on Cognitive Dimensions [9], our criteria should be thought of as heuristic. They are derived from experience in modelling a large number of complex accidents.

It is possible to identify three myths that are often cited as barriers to the practical application of human error analysis :

- Human error is inevitable. Users will eventually defeat whatever safeguards and measures are put in place to protect them and their environment.
- Human error cannot be predicted. In particular, it is difficult to anticpate the many ways in which inattention and fatigue jeopardize safety.
- Human error is too costly to guard against. In this view, market forces prevent companies from employing the analysis and prevention techniques that reduce the human contribution to major accidents [12].

Sorted First Order Action Logic (SFOAL) is a model logic introduced by Khosla [ref]. SFOAL forces analysts and investigators to explicitly consider the agents that contribute to an accident. It also provides syntactic structures that can be used to represent the actions that they perform [5]. The construction of a higher level model of an accident forces analysts to strip out such detail and focus upon the critical properties that directly led to an accident. Identifying the individuals, or agents, who contributed to, or responded to, a failure is a critical stage in any accident enquiry. SFOAL, therefore, provides an agent type, *Agt*, to represent 'non passive objects' that interact with and affect their environment. In accident analysis, computer systems and other automated mechanisms might also be viewed as agents, if they are capable of affecting the environment. Agent definitions, such as those given above, encourage some agreement over which personnel might have inteacted with the safety mechanisms (and any other systems) during major accidents. The SFOAL approach encourages the analyst to focus on the fundamental objects of interest in the behaviour of the accident: the users and their interactions with safety systems.

3.1 Time Lines

Time-lines are one of the simplest means of representing the flow of events during major accidents. Each critical incident is mapped to a point on a line which starts from the earliest incident in the accident and finishes at the last moment that is considered to be important to the analysis. The simple relationship between spatial locations on the diagram and temporal locations during an accident has already been noted. There are a number of weaknesses. There is an 'uneven' distribution of events over time. The concentration of critical events crams many different annotations into a small area of the line. This reduces the tractability of the resulting timeline.

3.2 Fault Trees

Fault trees provide means of avoiding the crowding associated with timelines. This is achieved by using two dimensions to represent the flow of events. Horizontal space is used to represent concurrency. Vertical space is used to represent sequence. Fault trees can present a clear and consistent overview of major accidents. They have a number of limitations, they cannot capture temporal properties of human and system failures. They also do not capture the difference between *necessary* and *sufficient* causes. To overcome limitations various extensions have been proposed [13]. Fault trees typically stop at the accident itself. Events after the 'undesired' event are important too. In the rooted fault tree the hazard is at the centre of the tree, the branches spread out above and below the undesired event. Temporal fault trees include a timing in the bottom left hand corner of each box. To impose relative timings, the tree orders events from left to right. Timings are annotated with the word 'approx' if the exact moment is known.

3.3 Petri Nets

Petri nets have been specifically developed to represent the complex sequencing and synchronisation constraints that cannot easily be captured by fault trees and time lines. A number of limitations complicate the application of Petri Nets to analyse accidents that involve interactive systems. In particular, they do not capture 'real' time. Places (circles) represent facts. Transitions (rectangles) represent events. Marked places (filled circles) are true. Transitions fire if all input places marked. All output places are then marked.

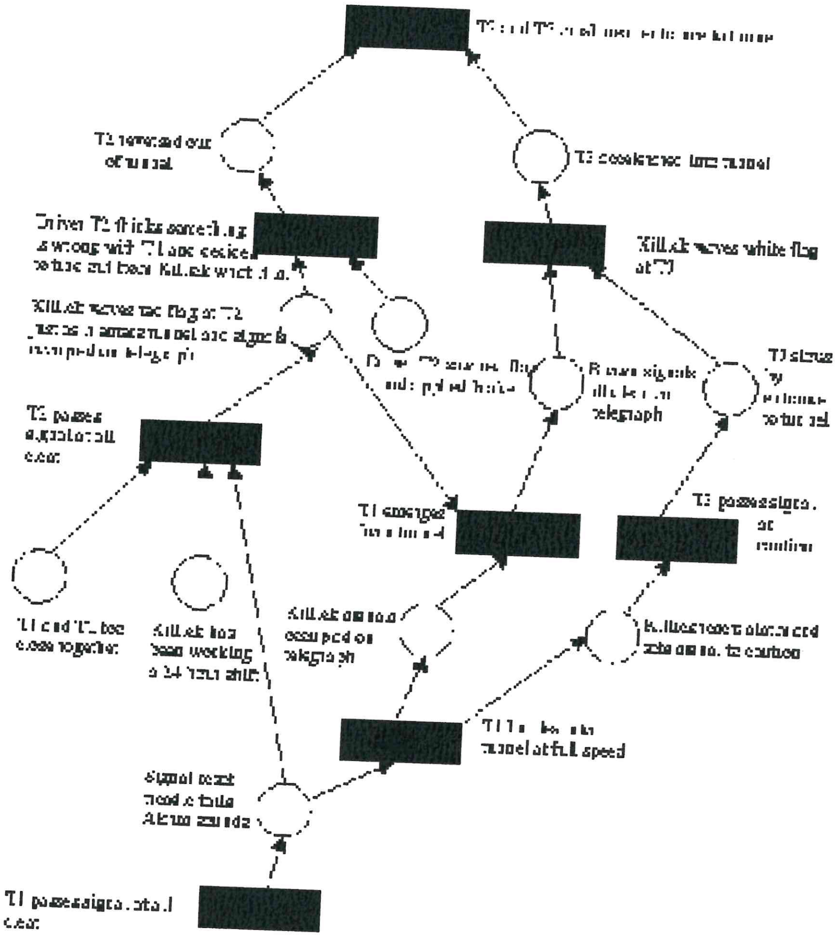

Figure 1: A petri net of the Clayton Tunnel accidentl

3.4 Logic

Textual notations provide a further means of representing and reasoning about the causes of major accidents. Unfortunately, there is no notion of time or sequence in first order logic.

3.5 Practical approaches

Narratran is an an environment for authoring case based exercises for training decision-makers. An exercise constructed with Narratran consists of a typical or critical scenario with emebedded questions and specified answers to those questions. Narratran consists of a knowledge base and a set of authoring tools. A training designer creates an exercise in Narratran by creating a scenario model, a set of decision-making questions (or considerations, more broadly), and related answers to the questions (and issues raised). The scenario describes a catastrophe and the emergency response operation 'on the ground', and is expressed in the form of discrete, structured facts. Facts are primarily textual, but can be represented in other media too, primarily graphics (e.g maps), and stills and video images. Facts are categorised within the scenario by various schemes, including semantic categories and agency roles. Role categorisation allows narratives to be systematically different for trainees with different agency affiliations. Trainees receive only explicit facts in their narratives; discerning the implicated implicit facts is a vital part of the discovery processes within the simulation exercise.

Future research priorities : (amongst others) iii) to implement the emergency management model computationally, for the purpose of investigating coordination mechanisms, and validating contingency plans, iv) to use the model for discussion-based training to develop enhanced and advanced training techniques ,such as the use of branching event trees in scenario narratives.

4 Empirical Modelling

4.1 Introduction to

From a human perspective, any technological trend prompts a whole family of questions concerning the inegrity of its intended goal, and the potential social impact and desirability of its expected outcome [3].

The Empirical Modelling (EM) approach is based on an agent-oriented analysis, where the focus is upon the observables that are construed to mediate agent response and action, and the dependencies to which these observables are subject in any change of state. The result of this analysis is a classification of observables with respect to the role they can play in interactions between agents. The process of agent-oriented analysis occurs in parallel with the construction of a computer-based artefact. In effect, the construction of the artefact is intimately linked with explaining the roles of observables, agents and dependents in its referent, and interaction with the artefact accordingly retains an open-ended experimental quality.

EM is an approach to computer-based modelling that is based on new principles for domain analysis and model construction. Computer models constructed using EM principles are not to be viewed as implementing an abstract mathematical model. Their significance is instead similar to that of an experimental scientist might build to account for a phenomena, or that an engineer constructs to prototype or test a design concept. In this respect, they are distinguished from abstract computational objects that happen to be executed on a computer : the manner in which they manifest state to the user is of the essence, as is the interaction that the user can perform upon them.

An interactive situation model (ISM) is so called because its interpretation is shaped by open-ended interaction with both the model and (at least, in principle) also with its referent. In EM, the construction of an ISM is seen as linked in a fundamental way to the activities that shape the modeller's insight into the referent.

Like a construal, an ISM implicitly represents knowledge of an evidential nature. Because of the way it is conceived and built, an ISM does more thatn simulate a particular behaviour of its referent. The knowledge of observables, dependency and agency that informs its construction is acquired through experiment. The significance of EM is that it offers principles to account for how one experience represents another : principles that can be used both to validate such a representation and to create one. The role of an ISM is not in the first instance to prescribe a pattern of activity to suit a particular function, but to track an evolving state of mind. For the ISM (god view), this is the state of mind of the external observer, who tries to imagine the interaction between the agents in the system, and their corporate effect, from an objective viewpoint. This ISM reflects the way in which the external observer construes railway operation to occur, but is not primarily expressed based on the preconceived 'significant events' in the railway protocol.

Two modes of generating state-transitions in the ISM are useful in this connection. Where appropriate, certain predictable state-changes can be implemented by automating the redefinition of observables. In typical interaction with the ISM (god view) the mechanics of the train motion is handled in this fashion. Alternatively, when it is necessary to emulate state-changes that in some respect are unpredictable, the external observer can intervene directly to simulate the redefinition of observables. The failure of the treadle to reset the signal can be modelled in this way, as can the telegraph communication between the signalmen.

4.2 Distributed Empirical Modelling

Distributed EM exploits the client-server architecture of the EDEN interpreter. In the modelling activity, each participant makes use of a different client. The way in which modellers interact is shaped by the interactive mode of communication established by the server. This gives scope for interaction between modellers either to be determined entirely at the discretion of the server, or to be interactively programmed to reflect the explicit privileges to observe and change observables of modellers. In the versatile and flexible environment for distributed interaction established in this way, it is possible :

- to give privacy and independence to individual modellers;
- to enable people to interact with each other and with their artefact *as if* in the role of an agent within the environment being modelled;
- to support higher-level intervention, such as is needed for arbitrating where there is conflict in concurrent design [1], and in simulating exceptional scenarios, such as a railway signal failure [2].

The development and application of distributed EM, though still at an early stage, raises many promising avenues for further research. Our experience of simulating railway operations with schoolchildren in the role of signalmen and drivers proved very helpful in enabling us to assess the plausibility of the assumptions that had to be made in reconstructing the accident scenario. These confirm the advantages of being able to see events from each participant's perspective.

4.3 case study bits

The idea is to analyse the events leading up to historic railway disasters with the principles of LSD specification in mind. This analysis will illustrate the subtlety of the relationship between perceptions and privileges of agents and their corporate behaviour. Issues include :

How oracles, handles and privilegs of agents are influenced by :

- locality - how are the agents distributed;
- roles - the same agent may play different roles;
- authority - one agent may delegate to another;
- knowledge - motivations for action, cultural context, acquired experience, skills.

How the effect of actions is influenced by :

- commitment - when is an agent required to act, pledged to act;
- conflict - two agents can act at cross purposes;
- synchronisation - when must actions occur at the same time;
- environment - how do environmental factors influence outcome of actions;
- modes of communication - e.g intermittent vs persistent.

The essence of our method is faithful modelling of the behaviour of objects in combination as reflected in indivisibly associated cahnges in observations. [Here 'observation' is used in a broad sense-closer to its scientific meaning, rather than its everyday meaning - to refer to anything that could conceptually be observed by experiment.] [4]. An LSD specification is intended to document the way in which the behaviour of a system depends upon the characteristics and interrelationship of its components. This information is expressed in terms of the observations of the system that define the role of each agent. In our modelling approach, the primitive abstraction is the observation rather than the object. The agent-oriented modelling process makes use of a special-purpose notation LSD in which to represent the interfaces between agents. The LSD specification can be viewed as describing the stimulus-response patterns in the application.

4.4 LSD

Informal notes on LSD..

- LSD account of an accident : "description of what happened" but NOT a specification.
- to identify *systems* in our experience.
- shape artefacts and our interactions with them, so as to make our state of mind : mode of observation coherent, identify how the environment must be constrained.
- sometimes this will lead to a stable context where agency and observation follows a general pattern. Can then talk of an LSD specification.
- such a specification is a normal operation or expectation of behaviours set in the context of potential rogue occurences.
- can't write the specification first, any more than the railway pioneers caould have specified a modern railway.

Merits of the accident analysis exercise :-

- accident = aberration caused by an unforseen turn of events.
- reveal the subtlety of character of the potential observables / interactions / agents.
- demonstrate the difficulties that surround the recognising / establishing a closed world.
- shed light on what kind of observables / scenarios have to be excluded from normal operation.

Illustrate activities that are needed when identifying a system :-

- restricting agent privileges.

- constraining environment.
- establishing conventions.
- training for teaching skills.
- enhancing oracles and handles.

The ADM was primarily developed as a tool for animation of LSD specifications. There are two principal themes behind animation with definitive representations of state :-

- the representation of conceurrent action by parallel redefinition
- the use of scripts to reflect context dependence of agent actions.

The LSD notation was first developed by Beynon in collaboration with Mark Norris of BT in 1986. An LSD specification is oriented towards understanding the interaction between agents in a system in a spirit that is closer to the concerns of the designer of a user-computer interface than to abstract formal specification. The idea is to formalise what an agent observes of a system, and how it can affect the state of the system by performing actions such as an experimenter might. Modelling and simulation associated with LSD specification is in principle intimately connected with physical experiment and observation. Most methods of computer modelling put the emphasis on trying to specify/mimic the global behaviour of a system without explicitly modelling the relationship between its component parts. LSD is concerned primarily with requirements analysis, and with the identification of system structure that precedes circumscription of its actual / intended behaviour. An important function of LSD is to raise an unusually rich set of questions concerned with requirements that would be difficult to identify without thinking about agents and their interaction. [see lecture T2 from the S4 Msc Module].

5 Applying Empirical Modelling to railway simulations

A computer model that can be useful in the context of crash investigation must allow us to manipulate parameters of all these kinds. It must also admit open-ended interaction of an exploratory "what-if?" character [2].

The privileges for observation and action through this view are comprehensive. They include the possibility of non-deterministic intervention such as is needed to simulate "Acts of God". Potential examples are : a landslide in the tunnel, train brake failure, or the incapacity of a human agent. Normal interaction with the model entails users playing the roles of the human agents concurrently. The views supplied by the computer model are intended to reflect the real world views and capabilities of these agents.

5.1 Requirements for Accident Models : Temporal Expressiveness

A principle requirement for any accident modelling notation is that it should be capable of representing both human 'error' and system 'failure'. This creates problems because the temporal properties of control systems are a very different from those of their operators.

5.2 The beginning and the end

When does an accident begin? The key point is that the starting point for an accident is often a subjective decision that reflects the analyst's view of its causes. Accident modelling notations must, therefore, represent this subjective decision.

5.3 Concurrency

If a reader wants to build up a coherent view of all of the events in an accident at a particular point in time then they are forced to cross-reference many different sections of the report. Formal and semi-formal notations can be used to represent the way in system failures and human error might combine, at critical moments, to create the circumstances for an accident.

5.4 Lack of evidence

Accident modelling notations must be capable of representing the real-time properties of human 'error' and system 'failure'. It is important, however, to emphasise that this must not force analysts into undue commitment when the exact timing for an event is unknown.

5.5 Real and relative time

Using a mix of real-time and temporal variables, it is possible to construct increasingly more complex models of the timings that are given in both eye-witness accounts and the synopses that are constructed within accident reports.

5.6 Inconsistencies

It is a frequent observation in accident reports that the evidence of one witness does not agree with that of another. Most oftern, these disagreements focus upon the sequence and timing of critical events. Analysts are forced not so much to represent uncertainty but to represent at least two different views of the events leading to an accident. It must be possible for analysts to resolve any inconsistencies that are critical to a clear and coherent understanding of an accident. However, if analysts do not explicitly represent this 'probable' version of events then it is very likely that individual readers will choose to construct different interpretations of the course of an accident.

5.7 Impact

Events can have a different impact at different times during the course of an accident. The US Department of Defence defines a negligible failure as one that will not result in injury, occupational illness or system damage. A marginal failure may cause minor injury, minor occupational illness or minor system damage. A critical failure causes severe injury, severe occupational illness or major system damage. A catastrophic fault may cause death or system loss. These have been used in weighted fault trees [13].

6 Requirements for Accident models : Usability requirements

6.1 Visual appeal and cost benefit analysis

The following are taken from [11]. 'Readability' is a significant barrier to the application of formal notations. Different notations offer different degrees of support to various stages of the learning process. For instance, graphical notations may be easier for novices to understand the textual notations.

6.2 Easy integrration of human factors and systems engineering

It might be argued that analysts should recruit different notations for modelling the different temporal characteristics of human 'error' and systems 'failure'. Johnson is unaware of any existing notation that can be used to satisfactorily integrate human factors and systems account and which provides a means of representing the evidence which justifies those observations.

6.3 Tool support

Is essential if analysts are to validate models that represent human error and systems failures. Firstly, they can implement sysntactic checks to ensure that designers have correctly constructed valid sentences from the lexical tokens in the language. Secondly, they can provide support for automated theorem proving. Thirdly, they can provide simulation environments.

The first set of problems relate to the difficulty of constructing coherent temporal models for major accidents. It is a non-trivial task to resolve the contradictory timings that often appear in human factors and systems accounts. It can also be difficult to integrate imprecise temporal information about operator behaviour with the more precise temporal schemas that are available for process components. Tool support has been identified as one means of improving the 'usability' of notations with a relatively low visual appeal. The final set of problems stem from the difficulties of managing cooperative work between heterogenous groups of experts. Rather than focusing on temporal expressiveness or visual appeal, these problems relate to aspects of control. For example, what are the consequences of allowing more than one author to simultaneously work on a formal or semi-formal description of an accident? Main argument in this paper has been that we must urgently address the lack of integration if we are to avoid the omissions, inconsistencies and errors that currently weaken most accident reports.

7 Conclusions

blurb here...

The aim of Woodforth's project [15] was to create an interactive, distributed virtual reality front-end to the Empirical Modelling tool DTkEden. The tools and virtual reality created should provide sufficient detail and realism to enhance the understanding of the underlying DTkEden model that it represents. Currently there is no perception of actually being there, of seeing what it was like when the circumstances surrounding the accident occured, no feel of what signalman Killick saw, or what it was like to be the driver of one of the trains. Because of this, only a limited amount of knowledge can be gained into the accident, but, with virtual reality, as systems progress, a closer approximation to actually being there could be created. At present you can't really get a feel for what it was like to be there because of the 2D graphics. With integrating VRML into the picture, then we can actually interact with the simulation through a virtual world. With the ability to communicate over the internet then the distributivity could be greatly broadened.

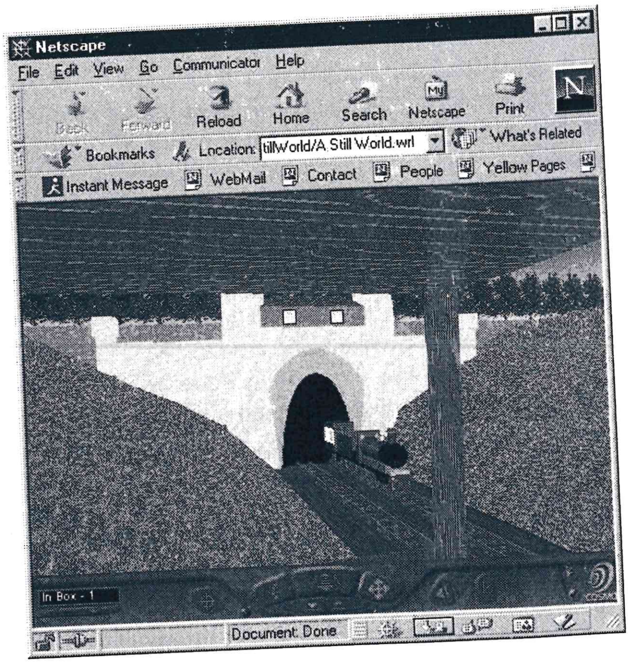

Figure 2: The view from Brown's signal box

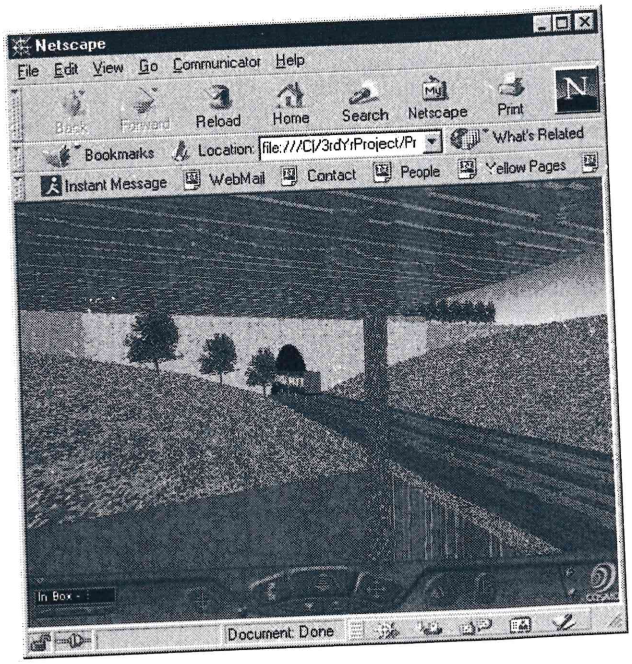

Figure 3: Killick's signal box - looking towards tunnel

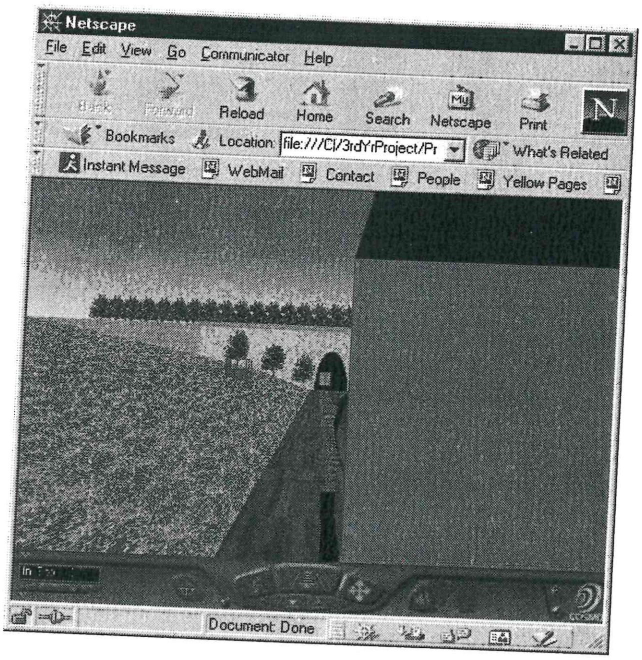

Figure 4: A train driver's view approching the tunnel

References

[1] Adzhiev, V. D., Beynon, W. M., Cartwright, A. J., & Yung, Y. P. "A computational model for multi-agent interaction in concurrent engineering". *In Proc.* CEEDA94, pp227-232, 1994.

[2] Beynon, W. M. "Empirical Modelling and the Foundations of AI", *Proceedings of CMAA'98*, Lecture Notes in AI 1562, Springer, pp322–364, 1999.

[3] Beynon, W. M., Sun, P-H. "Computer mediated communication : A distrubted EM perspective", Department of Computer Science, University of Warwick, UK, 1998.

[4] Beynon, W. M., Bridge, I., Yung, Y. P. "Agent oriented modelling for a vehicle cruise control system", CS Dept, University of Warwick.

[5] Burns, C., Johnson, C., Thomas, M., "Agents and actions : Structuring human factors accounts of major accidents", Glasgow Accident Analysis Group.

[6] Coleman, V. "Railway safety - taking stock", Lecture given by HM Chief Inspector of Railways, 19 January 1999.

[7] Dowell, J. (et al) "The design of collaborative training", ESRC Research programme in Cognitive Engineering. 1996-2000.

[8] Dowell, J. (et al) "Coordination in emergency management and the design of collaborative training", Final report of above project!

[9] Green, T. R. G. "Cognitive Dimensions of notations : A tutorial ", 1998.

[10] Johnson, C. "Using CAE diagrams to visualise the arguments in accident reports", WHERE AND WHEN.

[11] Johnson, C. "Representing the impact of time on human error and systems failure", WHERE AND WHEN.

[12] Johnson, C. "Why human error anslysis fails to help system development", Glasgow Accident Analysis Group.

[13] Johnson, C., Love, L. "Using extended fault trees in conjunction with traditional accident reports", Glasgow University.

[14] Rolt, L. T. C. "Red for Danger : A History of railway accidents and railway safety precautions", 4th edition, The Bodley Head, London, 1982.

[15] Woodforth, J. "Interactive VRML front-end to DTkEden", 3rd year project report, Dept. of Computer Science, University of Warwick, UK, 2000.