Halcrow Group Limited

Risk assessment techniques and a new human reliability analysis technique, the Event Window specific to the behavior characteristics at Active and Passive railway grade crossings, how this can assist risk assessment and save peoples lives

December 2004

Transport Research Forum - The George Washington University, Washington D.C., USA

Halcrow Group Limited

Risk assessment techniques and a new human reliability analysis technique, the Event Window specific to the behavior characteristics at Active and Passive railway grade crossings, how this can assist risk assessment and save peoples lives

December 2004

Transport Research Forum - The George Washington University, Washington D.C., USA

Transport Research Forum - The George Washington University, Washington D.C., USA

Risk assessment techniques and a new human reliability analysis technique, the Event Window specific to the behavior characteristics at Active and Passive railway grade crossings, how this can assist risk assessment and save peoples lives

Contents Amendment Record

This paper has been issued and amended as follows:

Issue	Revision	Description	Date	Signed
1.0	1.0	First Version	15,12,20 04	TH

Contents

HYPOTHESIS

Current accepted tools in risk assessment include techniques such as Fault and Event Tree analysis to predict the level of safety risk. To date, use of these tools at Grade Crossings has been limited and analysis has reverted to safety performance statistics to correlate results. There has been a missing link in modeling to be able to provide meaningful estimates of safety risk. Until now practitioners have been unable to use factors such as sighting, conspicuity, train speed, and human behavior characteristics within their numerical techniques.

Working for Network Rail, the Railway operation company in the United Kingdom (UK) Halcrow has been using theoretical techniques to quantify safety risk at grade crossings. During this work we have applied a new tool in modeling safety risk, the Event Window. Using this concept, we have been able to relate variables such as sighting, user perception and predict human error against a timeline. The nearer a moving train to a grade crossing the less likely a user will cross in error. The advantage of this technique is that it takes into account the one common factor in past accidents, how users incorrectly judge train speed.

In this paper we shall address the following questions:

- What is the benefit of quantifying the safety risk at a grade crossing?

- How do these risk assessments help organizations responsible for risk at grade crossings discharge their duties?

- What is the quality or usefulness of different types of evidence in building up these models?

- How can we improve on existing risk assessment techniques to make more informed and location specific decisions on grade crossing safety?

- How does the Event Window assist us in predicting safety risk?

Tim Hess, AIMechE, Halcrow Group Ltd

Jim Haile BSc CEng MIMechE, Halcrow Group Ltd

1   INTRODUCTION

1.1   *History of Grade Crossings Safety*

Within the UK, grade crossings have always been the subject of relatively strict regulation by government agencies. However, it is likely that collisions between trains and road vehicles at vehicular grade crossings now represents the most significant risk to the safety of the UK railway, and has the potential to be a cause of a catastrophic incident. This has been recently been highlighted with three accidents in late 2004 where twelve people lost their lives both in the road vehicles and in the subsequent derailment of one of the trains.

The UK, however, has one of the best grade crossing safety records in the world, despite having one of the highest average train speeds, with on average 6 fatalities per year associated with over 8,000 crossings. By comparison, in Canada every year there are 450-500 accidents resulting in over 50 deaths annually, in the United States there are approximately 4000 occurrences per year that a train and a highway vehicle collide at one of the approximately 250,000 public and private grade crossings, resulting in over 400 deaths per year.

In the UK legislation surrounding grade crossings is probably best described as an amalgam of highway and railway legislation and there is wide ranging and highly complex legislation in force that impacts on grade crossings including; railway, highway, planning, rights of way and disability legislation. Because of the interface between road and rail legislature the ownership of the safety risk associated with vehicle incursions into rail property is often clouded.

The acceptance of a large amount of footpath, bridleway and user-worked crossings, such as farm crossings has become an ambiguity within a modernized high-speed railway. Footpaths are allowed across tracks at speeds up to 125 mph whereas automatic half barriers have a 100 mph limit. The reasons for this are not necessarily risk based, they are related more to the lengthy legal process for closing down individuals' 'rights of way' and the spiraling costs associated with installing mobility impaired footbridges or underpasses.

1.2   Cost Benefit and Making Investment Decisions

1.2.1   *Safety Cost Benefit*

The underlying driving responsibility for improving the safety of the UK railways belongs to the Rail Safety Directorate, presently an independent organization who in conjunction with all stakeholders prepares a yearly railway group safety plan. This plan is underpinned by the concept of there being a tolerable safety risk to people associated with the operating railway, i.e. one that is acceptable to the user and society in general. This concept requires an assessment of the risk associated with the operation of the railway and a cost to be put on the value of preventing a fatality, to enable a balance to be made between the level of risk and further investment needed to reduce that level. This concept has been used successfully by most UK high risk industries and is verified in case law.

Though safety 'leadership' is through Rail Safety the law states that the owners/operators of the infrastructure and trains are responsible for the health and safety of people, and that safety risk must be reduced so far as is reasonably practicable. In the railway industry this is accepted now as the concept of ALARP (as low as is reasonably practicable), which means that assessments of risk must be undertaken for all operations that could result in injury to people, and that all practical options for risk reduction must be considered for implementation. Those not selected must be shown, with justification (i.e. safety benefit), as not being reasonably practicable. This places a responsibility on the railway operators to risk assess all operational changes, and look for safety improvements only discarding those that are not cost beneficial.

Safety benefit analysis is not new and is interpreted, for example in the USA by the Federal Aviation Administration as an approach to predicting the safety benefits expected to accrue form a proposed project. The US approach to safety is similar to other European countries, with efforts being made to ensue that changes will not worsen safety. The concept of a tolerable level is not used. Whether using tolerability or deciding policy through safety benefit, an unambiguous understanding of the levels of safety risk is required, both for showing a legal duty of care and adding support to investment decisions.

1.2.2   *Challenges Faced when Risk Assessing Grade Crossings*

Risk management is by no means a mature discipline, or can it ever be; for risk is in the future and we manage in the present those issues that are palpable and manageable. However public understanding of risk in the UK is improving as a result of well-

documented rail accidents in the media. It is recognized that no transport undertaking can have zero risk and that as performance is managed towards the goal of zero accidents, the cost one must pay becomes unreasonable. However, one is forced to accept that in hindsight, most accidents are not formed from complex causal chains, and should be preventable, certainly those that are initiated by failures of engineering systems. It is clear, to us, that in safety terms we actually manage hazards and not risks. We can examine the past and manage the present. But only predict the future, through modeling our processes, their environments and underpinning system behaviors.

We must also recognize that surveying and subjective assessment can be inconsistent due to the large number of footpath and user-worked crossings. These inspections by a variety of rail operating staff make it difficult to ensure that an accurate view of the safety risk and indeed relative safety risk of each crossing is obtained.

In risk modeling we are concerned with making correct decisions using the. To do this we required:

- Identification of information that is pertinent to the anticipated decision

- A systematic model for the acquisition of pertinent information.

- A rational assessment of analysis of the data acquired.

- A decision based clear unambiguous representation with consideration of sensitivities within the model.

This can be represented in the following diagram (figure 1).
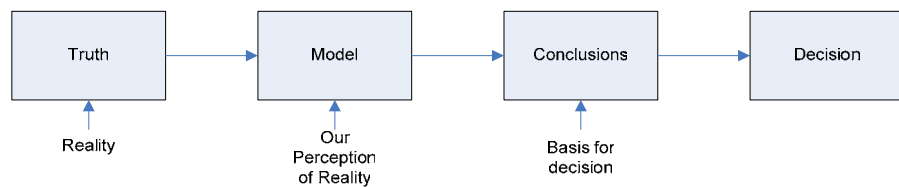

Figure 1. Relationship between system model and decision process.

There are a number of pitfalls in quantifying risk and each type of risk assessment carries its own problems. Qualitative decisions require unbiased and objective judgments on levels of risk, this doesn't necessarily mean that by coming to a consensus within a workshop to what the risk is, that the correct result will unfold. Even with the most competent and experienced people, their judgments may bear no relation to reality.

It must be recognized that the assessment of risk brings an inevitable uncertainty, which can take complex forms especially in the context of grade crossings:

- Omissions of possible cause of risk due to, incomplete analysis of the components of risk, or not quantifying of all the modes of failure associated with human error.

- Carrying out a generic risk assessment when a site specific risk assessment is needed.

2 RISK ASSESSMENT TECHNIQUES

2.1 Criteria for Decision Making

When choosing to carry out a risk assessment, decision makers often consider issues of practicability over the potential quality of the risk outputs. These issues of practicability cover cost, timescale for carrying out the work, quantity of data required etc... The basis for choosing which risk assessment process to use, needs to be based upon the required quality of the risk assessment outputs. What is the purpose of the risk assessment? How good should the risk assessment be?

As described earlier, economic limitations require that the tolerability of risk at a crossing is assessed and the safety benefit of removing the risk is ascertained. In some cases there are obvious solutions to problems and the lengthy process of analysis can be avoided. Primarily, the objective is to assess the significance of a safety risk and decide how to act to mitigate it. In order to influence stakeholders the integrity of these conclusions needs to be backed up by other considerations as described in figure 2.
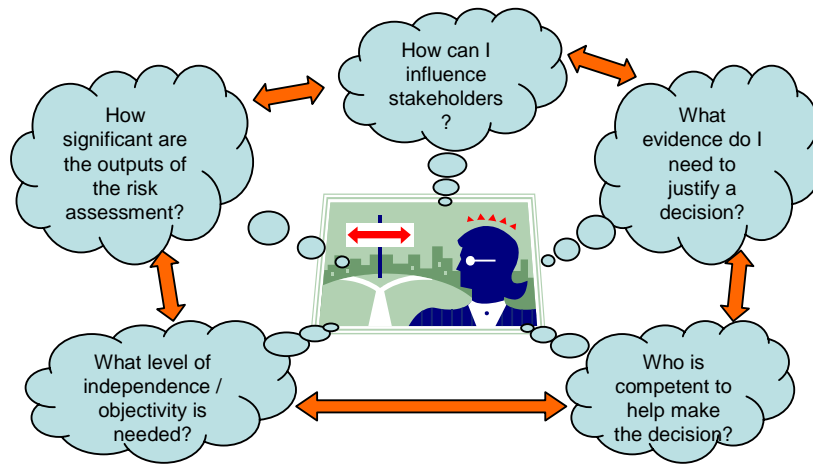
Figure 2. Considerations for safety decisions.

There are no standard rules by which these considerations can assist decision making, however it is clear, the greater the significance of the risk assessment outputs the greater the burden of proof that needs to be provided. This significance is a combination of two criteria the level of safety risk and the cost of proposed safety improvements.

Table 1 describes different levels of rigor in the risk assessment processes.

Need behind risk assessment.	Type of risk Assessment	Basis for investment decisions
No need to compare one risk to another	Hazard assessment	Intuition / 'gut feel' based on evidence.
Need to assess the significance of risk factors.	Qualitative risk assessment	Objective judgment by scoring likelihood and consequence of risks, based upon a panel of experts including people independent of the organization.
Need to demonstrate that the level of investment is proportional to the level of risk.	Quantitative risk assessment	Independent assessment using clear quantitative data / evidence and assumptions made clear.

Table 1 – Levels of analysis in risk assessment.

2.2　　　　*Risk Assessment through Compliance Checks*

Historically, risk has been managed reactively, meaning that new ways of working have usually been developed as a result of an incident culminating in either monetary or human loss. Thus standards and procedures become more onerous and, one would hope, safer. The dis-benefit of this is that the standard can become too onerous and not cost effective. As a result recently developed industrial standards generally have become 'risk-based', though by their nature are more goal orientated and often not very useful, usually citing 'that a risk assessment is required'.

Whereas conformance to standards and regular compliance audits are the basis of engineering and operational excellence, the management of risk requires more understanding. There is a need to understand the context of the operation, its interfaces and the immediate environment to identify any new potential accident causal chains. In some cases, there may be a requirement for more onerous controls, in other cases the dispensation standards may introduce a more hazards.

2.3　　　　*Risk Assessment through Hazard Assessment*

Systematic identification of hazards involves two phases; an empirical phase and a creative phase. The empirical phase relies largely upon knowledge and experience of the past to identify potential hazards. This may be, for example, through application of an appropriate checklist. Whilst empirical identification of hazards is sometimes sufficient for straightforward undertakings, more complex processes, and in particular those with several boundary interfaces and human interaction, will generally also require a more creative form of hazard identification.

Accidents happen through a causal chain of unwanted events; sometimes these chains are long and complex, sometimes very short. The identification and the mitigation of these potential causal chains is key aspect in managing safety. A result of hazard identification is that likely unwanted events that could occur can be identified and mitigated without the need for calculation. The benefits of this process is its simplicity. In additional as well as removing hazards / causal events, this process can be used to identify key performance indicators, about which a safety monitoring regime can be designed. This gives management sufficient information to make the correct risk based decisions on the need for additional control measures.

2.4   *Risk Assessment through Quantified Risk Analysis*

The need to improve reliability analysis and risk quantification was highlighted following the Three Mile Island incident on March 28, 1979. The disaster was initiated when a steam turbine failed and the reactor shutdown process started, triggering a chain reaction of events where over 2000 alarms sounded. In the overload of alarm information , operators failed to notice an open valve on the pressurized water circuit and shut down the make up water pump causing a reactor meltdown. Following this event, many new techniques were developed to understand the implications of human error in engineering systems. In particular how engineering systems can be designed to aid human control and reduce risk.

Every accident involves an element of human error, be it at the stage of design or like the Three Mile Island accident where direct human intervention caused an accident. The most widely used tool in modeling systems failures is fault and event trees.

Fault trees - describe the precursor events that may lead to the realization of risk, described as a top event. The technique uses Boolean algebra, to represent the combination of these precursor events. Using And and Or gates and working 'top down' the relationship between precursor events can be quantified.

Event trees - describe the potential outcomes that can occur once a top event is realized. In our application, would a collision between a user and a train result in a train derailment, a near miss, or a fatality?

These tools allow relationships between causal factors to be analyzed and lead to a numerical expression of risk. These resultant risk outputs assist decision makers in relating financial investment, as numbers can be easier to correlate. However, it is very easy to grasp numerical outputs and consider them to be fact. The outputs of models should be used as a guide, recognizing that they originate from a simulacrum (an imperfect model of reality). The results of risk assessment are not hard and fast figures such as one would find on a balance sheet. They are useful guides to decision making but their limitations must be clear to the decision maker.

The downside is that Quantitative Risk Assessment relies on a number of assumptions. As the uncertainties in data are multiplied together the resulting model outputs may be highly subjective. In addition, to evaluate risk at grade crossing there is a heavy reliance on human reliability data. Reliability data for machines and components are better known, and can be repeatedly tested.

2.4.1 *Human Reliability Assessment*

Why do grade crossing users fail to respond to rules? Why do normal or average human beings get hit by moving trains? Indeed, are they average? If not, how 'un-average' are they? Can we model this performance? Will it help us to deliver judgment on the safety of a particular grade crossing?

The concerns over quantified Human Reliability Assessment (HRA) are similar to those within Fault and Event Tree analysis and include the applicability and accuracy of data and the sensitivities associated with probability theory and Boolean algebra. Human error probabilities derived from HRA techniques involve considerable of expert judgment and caution needs to be exercised in using absolute human error probabilities in safety decisions.

Overall the HRA analyst must make sure that the risk assessor does not underestimate, nor, on the other hand significantly overestimate, the impact of human error on system risk. Techniques developed by Human Factor specialists within the last twenty years, such as HEART (Human Error Assessment and Reduction Technique) have gone a long way in trying to quantify human error. Each use 'standard' human reliability data tables to decide whether an operation is likely to fail. These standard values are then altered to gain a more accurate representation of the situation. Like most quantitative analysis the rigorous nature of the process creates benefits other than absolute numerical values and a well structured HRA provides a systematic consideration of the ways human error can affect safety, and may provide insights into the means by which human error can be reduced.

2.4.2 *Populating the Quantified Risk Assessment Using Probabilistic Data*

Populating fault and event trees using probability data requires a considerable amount of evidence. In addition, models need to reflect the system in question. If one were to use safety performance data to populate models, it would be possible to skip some of the mechanisms of faults and events and correlate the outputs, or factor down the data to fit known outcomes.

Quantified Risk Analysis using probabilistic data is considered bottom up and un-biased as the risk assessor (assuming he is independent) is assessing the variables of risk in without any knowledge of significance of the outcomes.

Is it possible to predict risk at grade crossings using probabilistic methods alone? Can all of the mechanisms of human error and culminating events be related through theory alone? This is a critical proposition which is considered in section 3, 'The Event Window'.

The act of a user crossing the railway at grade crossings has a number of scenarios where failure may result in increased risk of a collision with a passing train. This system considers the following known data;

- the physical parameters of the crossing,

- the speed of trains,

- the frequency of trains and users,

- the warning systems for oncoming trains,

- the state of mind of users on their approach,

- and, the purpose of the crossing.

3   The Event Window

When models become complex, or evidence to determine probabilities is scarce, there is a need to use performance statistics to assist in the formulation of conclusions. Validation of models should be carried out where possible using performance statistics. In application to grade crossings, safety performance statistics are only valuable when there is statistically sufficient information for validation of modeling outputs.

Using statistics to compare outputs is useful. Can statistics be used to build models? Analysis of statistics shows us at what types of crossings accidents occur, to which users and in which environmental conditions. Some risk assessment tools use this data to allow decision makers to compare the attribute of the grade crossing to the wealth of accident data. This in its self is a valuable exercise. These models use this data with cause trees to relate systems of failure. The answer for a particular outcome is modeled and the data within event trees are factored to represent risk. Judgments can be made on causal factors to represent risk. With this method QRA models become more representative of safety performance.

Though valuable to a decision maker use of performance statistics reflects risk from past performance. The risk event that has not yet occurred, which may be more catastrophic than any before, may not have been modeled.

Risk assessment at grade crossings has needed to rely partially upon safety performance data as no probabilistic tool has been available to model the mechanisms of risk when a user is on the track when there is an oncoming train.

Using Fault and Event trees one assumes that the act of crossing is a static environment where, human error is fixed however near or far away the train is. Other techniques exist for modeling dynamic systems such as using Minimal Cut Sequences for Dynamic Fault Trees[i] which considers data flow and dependency in modeling. Until the development of the Event Window there have not been any techniques available that relate human error to real time systems where the interaction of a number of events can be predicted.

3.1 Event Window Modeling

The term Event Window is new, a concept[ii]. It enables time dependant variables to be introduced to modeling and in particular to grade crossings, how human error relates to time. To explore its creation lets consider the system where a pedestrian approaches a grade crossing and consider how to estimate the risk of a user being hit by a train. In a simple system the risk could be seen as:

Likelihood user is hit by train per crossing event	=	Likelihood user crosses at error into path of train	×	Likelihood train arrives when the users decides to cross

We now have a measure of probability but how can we calculate the likelihood the user and train will be at the crossing at the same time? We can find the frequency of trains, we can also find the frequency of users. Does this tell us whether the user will be in the path of the train at danger? How long is the period of time where if the user were to cross, he/she would be in danger of being hit by the train? One thing that may help us is the crossing time.

If we assume that the period of time for analysis should be the crossing, which is on average for a 2 track grade crossing is 10 seconds. The risk is:

Likelihood user is hit by train per crossing event	=	Likelihood user crosses at error	×	Crossing time	×	Likelihood train arrives within the crossing time

To follow this logic the calculation might be

| Likelihood user is hit by train per crossing event | = | 0.0001 (general omission error) | × | 10 | × | 0.001 events/second | = | 0.000001 per crossing event |

Assuming that there are 10,000 crossing events per year then this would be a likelihood of 1 event every 100 years.

In this method of calculation we are analyzing risk within a window of opportunity. This period of time we describe as the Event Window.

The definition of an Event Window is: *a period of time, which starts from the first initiating event, where two or more precursor events may combine to cause a top event.*

This is all logical, but we know that this is a simplistic view. Users of grade crossings may sense oncoming trains. There is usually a noise well before the train arrives and also the user has sight of the train. This simplistic representation assumes that the likelihood a user crosses at error is the same however far away the train is. We are assuming that all elements within the calculation are independent or mutually exclusive.

We need consider the mechanics of user train interaction to be modeled using time sensitive variables within an Event Window.

0
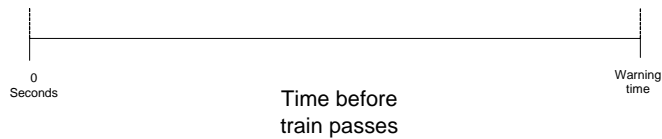Seconds

Warning time

Time before train passes

Figure 3 X-axis of Event Window

Having introduced the concept of the Event Window is introduced let us consider the time sensitive variables. The Event Window is defined on the x-axis as the time before a train passes (Figure 3). At time 0 a user arrives at the crossing at the instant the train passes. The maximum time value in this representation is the warning time. Users enter the Event Window at any arbitrary time between these points, i.e. users who arrive before the warning time will cross safely and are not modeled. If a user arrives at the crossing between the time the lights change (or with crossing without lights an arbitrary time i.e. 20 seconds) and the time the train passes, and he/she proceeds at error despite warning lights or signs then he/she will enter in to the Event Window and is at risk of interacting with the train.
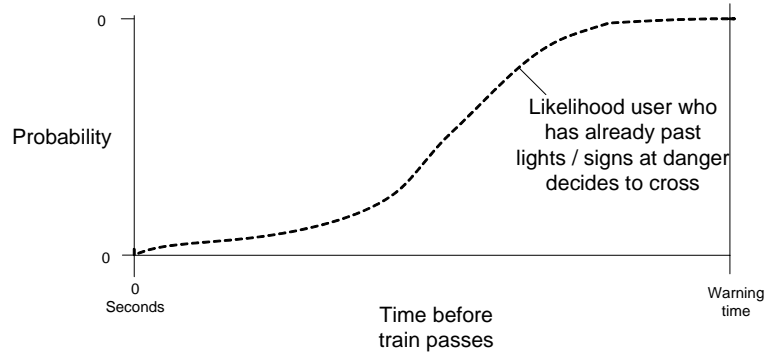
Figure 4 Event Window incorporating likelihood of crossing at danger.

Using human reliability analysis we introduce a new axis, probability, and in this case, one key part of this model, the probability a user will cross given his/her perception of an oncoming train (Figure 4). At time zero, the instant the train passes, the user is considered to have a very low probability of deciding to step into the train's path.

Introducing another variable, sighting time. After the user sees the train come into sight the probability he /she will cross decreases significantly.

Then there is a need to assess whether a user will collide with the train now that he/she has proceeded at error onto the track in front of an oncoming train (Figure 5). This is modeled by considering the likelihood of being hit given that he has decided to cross. It is assumed that at time 0 he will collide with the train. At the average crossing time there is a 50% likelihood he will collide with the train. Using a cumulative normal curve, the average crossing time and variance in crossing time for different users can be represented.
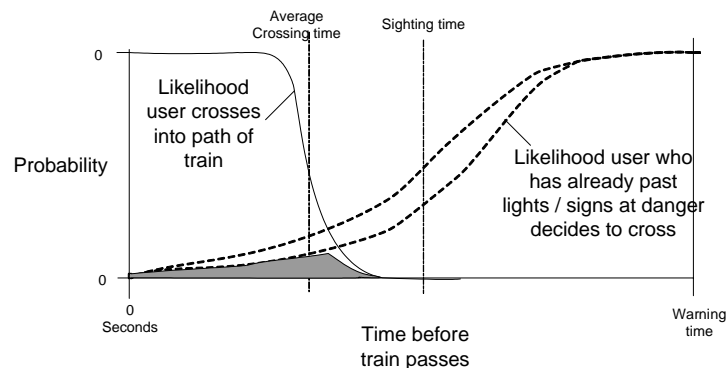

Figure 5 - Event Window likelihood user crossing at danger collides with train

The product of these curves gives a distribution for the likelihood a user will collide with the train given he/she has ventured on the railway at error within the Event Window. In actuality this is a slightly simplified view as the two curves are not mutually exclusive. In addition each user has a different propensity to cross.

This allows train speed effects to be modeled, if the warning time is low relative to the crossing time the risk goes up. If there is poor sighting time relative to the crossing time the risk goes up.

This model is similar to the Reich model, which has been developed in aircraft control to predict collision risk. The model determines the risk exposed to aircraft that are on parallel flight paths of descending or veering into each other. In this representation, aircraft are considered as moving adjacent blocks with separate attributes. This methodology was used to derive a safe separation standard for aircraft on adjacent flight paths. The similarity with the grade crossing Event Window model is the analysis of the effects of time on awareness of risk and human error.

4   Conclusions

Each risk assessment tools has its own merit depending on the environment in which it is modeling. Hazard assessment is useful to decision maker as it can be carried out by operatives employing standard 'tick lists'. Risk assessment using compliance checks has limited benefits for predicting risk. It is however a means of demonstrating compliance. Hazard assessment can be biased by the subjective views of the large amount of inspection staff required.

Quantified risk assessment enables decision makers to objectively invest resources to address grade crossings found to have a greater level of risk. Where these resources are limited, decisions can be made to priorities investment effectively and differentiate between grade crossings.

The Event Window is a new tool to the evaluation of risk at grade crossings and models dynamic systems. The tool allows human error to be evaluated over a period of time and enables probabilistic methods to be used from first principles to evaluate risk. Fault & Event Trees by their nature represent a particular point in time.

To date the benefits of its application have been demonstrated as it has aided investment in recent risk assessments in the UK, where speed increases on the railway have occurred.

Comparison of probabilistic risk outputs against limited performance data is promising. It is hoped that this tool is not limited to the evaluation of risk at grade crossings but can be used for probabilistic analysis of other systems where perception of risk and collision incidents, or dynamic systems can be modeled to greater effect.

5   References

Minimal Cut Set/Sequence Generation for Dynamic Fault Trees - Zhihua Tang & Joanne Bechta, University of West Virginia which allow time dependant variables to be placed within Fault Trees

Safety and Passive Grade Crossings - National Transportation Safety Board, Washington DC.

How did that happen? Engineering Safety and Reliability – W Wong

Engineering Safety Management, Issue 3 – Network Rail.

Doing it differently systems Rethinking Construction – David Blockly, Patrick Godfrey

Quantified Risk Assessment in Railway System Design and Operation – J Haile

Modeling User Erropr at Level Crossings – 8th International Level crossing Symposium Sheffield April 2004 – T Hess, J Haile

---

[i] Minimal Cut Sequence Generation for Dynamic Fault Trees, developed by Zhihua Tang & Joanne Bechta, University of West Virginia which allow time dependant variables to be placed within Fault Trees

[ii] Developed by Tim Hess & Jim Haile, Halcrow Group Ltd