RISK ASSESSMENT – AN INTRODUCTION

L J Wain

East Midlands Trains, UK

INTRODUCTION

This paper introduces the concept of risk and identifies the statutory requirements for performing risk assessments. It discusses the differences between qualitative and quantitative risk assessments and their advantages and disadvantages. It looks at why we must undertake risk assessment and how this is encompassed within the Railways Safety Management System.

The term "risk" can be attached to any quantity we wish to assess and control. We can talk about several forms of risk

- Economic risk
  - How much money could we lose?
- Environmental risk
  - How much oil will we spill?
- Safety risk
  - How many fatalities could result from an accident?

Many of the techniques introduced in this paper are applicable to any of these risk measurements with a little imagination and tailoring.

For the purposes of this paper we shall consider safety assessments where risk is defined in terms of the chance of an accident occurring and the severity of the accident. We can accept more accidents if the consequences are only minor injuries, but can accept only very few accidents where several fatalities may result. The increase in risk can be seen graphically in Figure 1.

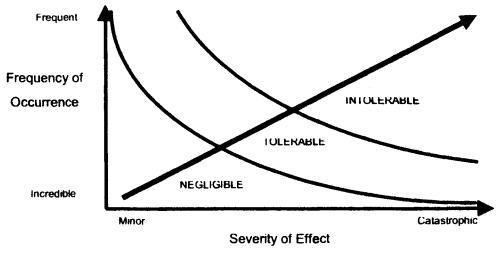

Figure 1 A Pictorial Definition of Risk

BACKGROUND

Risk assessment has been of importance in all industries for some time. Since World War 2, the defence industry has been in the forefront of reliability and risk assessment developments. It was realised by them in early days that unreliability was not only a major cost inducer, but also gave unacceptable risks to life.

The incidents listed below are those in the UK that have had a major impact on legislative requirements for safety. Many other major incidents have occurred, but these have not had the same effect even though some accidents have been more severe.

- Windscale 1957
  - 10-100 subsequent deaths
- Flixborough 1974
  - 28 deaths
- King's Cross 1987
  - 30 deaths
- Clapham Junction 1988
  - 36 deaths
- Kegworth 1989
  - 47 deaths
- Piper Alpha 1988
  - 100+ deaths
- Herald of Free Enterprise 1987
  - 200+ deaths

Public inquiries held after each of these incidents have shown that none of them ever needed to occur if more thought had been carried out prior to implementation. In each case the conclusions have been similar - a fully justified argument for the safety of the operation must be provided to and accepted by the HSE before any operation can be carried out. That is, a safety case. As part of these safety cases, a full probabilistic safety assessment (PSA) is required - another name for quantified risk assessment (QRA).

Recently there has been significant change in the legislation and governing bodies affecting railway operations. On 1st April 2006, the Office of Rail Regulation (ORR) became the health and safety regulator for the rail industry, responsibility transferred from the Health and Safety Executive (HSE). The Railways and other Guided Transport Systems (Safety Regulations) 2006 (ROGS) came into force in April 2006, superseding Railway Safety Case Regulations (RCSR) (2000), Railways and Other Transport Systems Approval of Works, Plant and Equipment) Regulations

(1994) and Safety Critical Work Regulations (1994). The ROGS Regulations implement requirements for railway operators and infrastructure managers to:

- Maintain a Safety Management System (SMS)
- Hold a safety certificate indicating the SMS has been accepted by the Safety Authority (now ORR)

ROGS replace the safety case regime in the RSCR for mainline railways and creates a proportionate system of safety verification to control risks arising from the introduction of new or altered vehicles and infrastructure. A sample of other relevant legislation is shown below. In general, legislation is moving towards the development of an integrated European railway system.

- Health and Safety at Work Act (1974)
- Transport and Works Act (1992)
- Railways Act (2005)
- Railway Safety Directive
- Interoperability Regulations (2006)

The legislation does not provide a prescriptive approach to risk assessment. The emphasis is on the employer/operator to tell the regulatory authorities what they intend to do and why it is safe to do so.

In addition to legislation, there are a number of guidance documents and standards from other relevant bodies that should be adhered to. The Railway Strategic Safety Plan (SSP) is a joint statement by the companies responsible for Britain's mainline rail network, setting out an industry agreed approach to managing safety related activities during 2006. Railway Safety and Standards Board (RSSB) have published "How Safe is Safe Enough?" which beings together an overview of good practice in making decisions that affect safety. It ensures these are:

- Taken and recorded – safety decisions should not happen by default.
- Taken at the right level – responsibility should be devolved to those with the experience and authority.
- Taken for the right reason – it is acceptable to do nothing if nothing is the correct conclusion.
- Taken using professional judgement – considering all appropriate factors.

All safety related decisions should take into account, rules and standards, good practice, quantative analysis, ethical responsibilities and commercial considerations.

HSE have produced "Reducing Risks, Protecting People", the HSE's decision making process for ensuring consistency and coherence across risk assessment and management.

Network Rail's "Engineering Safety Management", colloquially known as the "Yellow Book", applies to any change that affects or may affect the safety performance of any railway operation, system or item of equipment at any level of an organisation, or the organisational structure itself.

The Yellow Book is currently at Issue 4 (YB4), recently being up issued to include the importance of maintenance and human factors in safety management. It recommends the "7 stage process" for risk assessment which includes the following areas that are more fully detailed later in this paper;

- Hazard Identification
- Causal Analysis
- Consequence Analysis
- Loss Analysis
- Options Analysis
- Impact Analysis
- Demonstration of ALARP and Compliance with Benchmarks

QUANTIFICATION VS. QUALITATIVE ASSESSMENT

Most people prefer a quantitative argument as it is easier to assess the size of a problem in this way. Comparisons between risks are more easily made when assessments are quantified. However, it is quite feasible to provide a sound argument purely qualitatively. A qualitative argument is often useful where very novel approaches are being used and experience cannot be used to quantify the likelihood of occurrence. Even for well known systems, adequate data can be difficult to obtain to ensure accurate quantification of the risks.

The Management of health and Safety at Work Regulations require a suitable and sufficient assessment of safety risks to those exposed to hazards to be undertaken. YB4 advises that "To be suitable and sufficient, the sophistication and depth of analysis in risk assessment shall be proportionate to the level of risks being addressed. For most railway undertakings not potentially leading to major and catastrophic (multi-fatality) consequences, a qualitative approach to the demonstration of compliance with the legal and professional duties may prove adequate."

In many cases involving lower risk levels, risk assessments can be performed purely qualitatively if it is clearly evident that existing risk has been removed and no new risks created.

UNDERTAKING RISK ASSESSMENT

Prior to investigating the methods used in risk assessment, it is worth noting the definitions and sequence of the terms failure, hazard and accident.

A ***Failure*** may cause	A component, sub-system, system or design is unable to fulfil its required function, *e.g. crack in track welding*

a ***Hazard*** which can potentially cause	A condition or practice which has the potential to cause death, injury, ill health or damage, *e.g. broken rail*
an ***Accident***	An unplanned, uncontrolled event which results in death, injury, ill health or damage, *e.g. derailed train strikes infrastructure*

Some hazards, and consequently accidents, may arise without a clear failure - these hazards are called inherent hazards and are the result of a "design failure", *e.g. automatic doors have inherent risks in that passengers may become trapped between closing doors*. Platform edges are also another cause of inherent hazards. However, even these do follow the same progression shown above since each arises from some failure of a passenger or staff to act in a specific (expected) manner.

Failures are sometimes referred to as hazardous events and should not be confused with the hazards themselves. In many cases a number of failures or hazardous events may need to occur to cause a hazard.

Hazards are different at each stage of a system life cycle. The hazards encountered during manufacture and commissioning are very different to those during operation which are different again to those during de-commissioning and disposal. Risk must be assessed and controlled throughout each of these stages.

The safety plan details the safety activities, including risk assessment process, which will be undertaken to control the level of risk. It will need to be developed and updated throughout the life cycle of the system. Figure 2 shows the process that must be applied throughout the life cycle of the system. Any change in operating circumstances, whether it be in terms of the hardware involved or the procedures used to operate it, results in a design change.

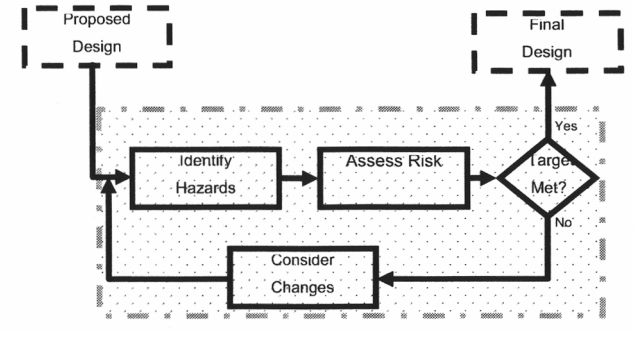

Figure 2 Risk Assessment Management Process

Note that for any design changes, it is necessary to apportion the risks for the whole system to the sub-systems involved in the changes. For major projects, this is an art in itself. Risk targets must be set for each system, sub-system and perhaps even lower levels of detail.

HAZARD IDENTIFICATION

Hazard identification is one of the most important parts of the risk assessment process. If a hazard is not identified then methods for managing the risk cannot be implemented. A properly performed analysis will identify all potential hazards and accidents that are associated with an operation. Appropriate techniques include;

- Preliminary Hazard Analysis (PHA)
- Checklists
- Failure Mode and Effects Analysis (FMEA)
- Hazard and Operability Studies (HAZOP)

It is not normally necessary to employ all these methods. However, for large and/or complex systems, it may be necessary to use all the available techniques before being confident that all potential hazards both inherent and those resulting from failures, have been identified.

PHA is a means of recording a "brainstorming" exercise. It is normally useful for an individual or small team only. It provides a quick way of identifying the major hazards associated with an operation. Normally PHA is used purely to identify areas of concern for further hazard identification.

A checklist of hazards typically associated with a particular activity or type of system should prevent the more common ones from being omitted from the hazard list. Checklists can be updated as further experience is gained and in the light of incidents and accidents to help prevent recurrence.

FMEA looks at the effects of all failures, not just the critical ones. This makes it a thorough but time consuming exercise. As it only considers single failures, it must be supplemented by other techniques in systems where redundancy and/or dependency is present. It can be conducted at any indenture level to identify system or component hazards, see Figure 3.

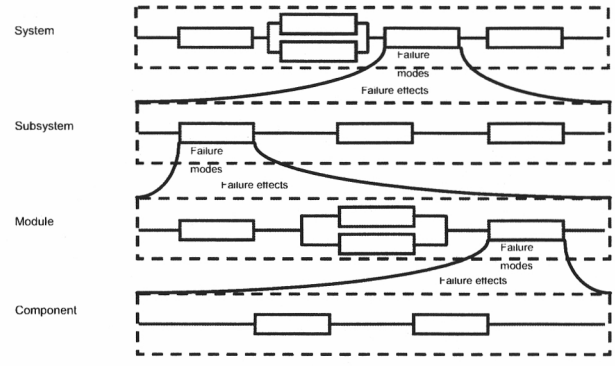

Figure 3 FMEA Levels of Indenture

HAZOP studies allow the risk assessor to ensure that the system is safe under both normal and abnormal or failure conditions. It uses the combined knowledge of a team under the guidance of a facilitator to give a full understanding of the behaviour of the system. Application of a set of deviations (*e.g. too much, too little, none*) to a group of relevant parameters (*e.g. flow, pressure,* force), result in all critical effects being identified. A HAZOP works in the opposite sense to a FMEA by identifying a relevant effect and then determining the possible causes of that effect.

In addition, a number of human factors techniques may be considered for systems with significant human interaction.

Cause and Consequence Analysis

This section discusses techniques which can be used to assess the scale of the risk once the hazards have been identified. The following standard techniques provide the assessor with a means of determining the possible effects of a hazard and the chance of them occurring;

- Fault Tree Analysis (FTA)
- Failure Mode Effects and Criticality Analysis (FMECA)
- Event Tree Analysis (ETA)
- Cause Consequence Analysis (CCA)

FTA can be used to analyse a single hazard to determine all combinations of failures (base events) that will result in the hazard (top event). Each event is decomposed into the events that must occur to produce that effect. Eventually, the decomposition will result in component failure modes where the analysis usually ends. The top event can be quantified, if required, in terms of a frequency or probability of occurrence. An example FTA is shown in Figure 4.

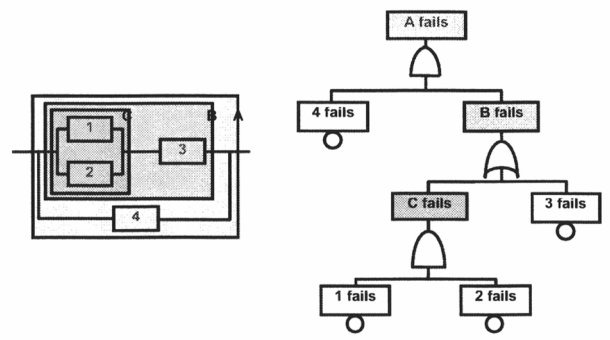

Figure 4 Example Fault Tree Analysis

It is possible to use a fault tree to develop the *probability* of a hazardous event occurring. In this case, each base event must be expressed in terms of a probability. This would be useful for protective systems or any fault tree used to model a hidden hazard such as the fire protection system case study.

FMECA is an extension of FMEA and identifies all functional failures, the relevant ones of which can be used as base events in fault trees. The criticality levels used may depend on the system being assessed and any reasonable set can be used. The total frequency of failures for a given severity
category can be obtained by adding the frequencies of all failures resulting in that severity category. An example worksheet is shown in Figure 5.

System: Traction (Class ABC EMU) Date: 15 February 2002
Analyst: J Smith Sheet: 1 of 5
Approved by: AN Other

Ref.	Item	Function	Failure Mode / Cause	Local Effect	System Effect	Sev	Detection Method	Compensating Provisions
1.1	Gearbox	Transfer rotational movement from traction motor to axle	Bearings seized	Rotational movement not transferred. Axle seizes.	Major flats. Unit stopped. Requires assistance. Extensive delays. Possible derailment.	4	Unit will not move. Motor overload relay will trip	Gearbox oil level checked every 12,000 miles. Oil changed every 50,000 miles.
2.2	Traction motors	Provide rotational movement for powering train	Brushes worn	High probability of flashover. Will result in motor overload relay tripping.	Unit will be stopped by tripped overload relay. Short term delay whilst affected motor is isolated.	2	Unit will stop. Motor overload relay will trip.	Brush length checked on exam. Motors can be isolated in pairs if flashover is a problem.

Figure 5 Example Failure Mode, Effect and Criticality Analysis

ETA is often used to take up where FTA leaves off. FTA is used to determine the frequency of a hazardous event and ETA is used to develop this into the possible accident scenarios once the hazard has developed. The event tree models the sequence of events. That is, the chronological order of events is important, unlike fault trees. Figure 6 shows an example of an ETA.

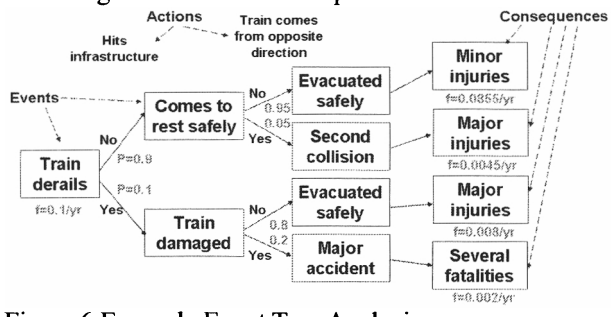

Figure 6 Example Event Tree Analysis

Frequency and consequence of failure need to be established quantitatively or qualitatively for inclusion in the risk analysis. Sources of failure frequency can include;

- In-service data for item
- In-service data for similar item
- (Adjusted) Manufacturer's data
- Generic failure data (e.g. MIL217f, NPRD)
- RSSB Profile on safety risk on UK mainline railway

Sources of accident data can include;

- Network Rail Safety Management Information System (SMIS)
- Network Rail Quarterly Safety Performance Reports
- HMRI Annual Report
- Incident Logs
- Control Logs
- Company databases
- Railway Group Safety Plan (Actual and Target)

The level of uncertainty of the data will determine the level of accuracy of the risk assessment undertaken. It may be necessary to undertake sensitivity analysis on critical areas if the data collection is not of sufficient integrity to accurately determine the risk.

RISK ACCEPTABILITY

It is clear that "safety at any cost" is not a viable option. Companies attempting to work according to this regime would soon be forced out of business. But how do we know when the risk of an accident is acceptable? The risk ALARP (As Low As Reasonably Practicable) principle is sometimes represented by the "ALARP triangle" or "carrot" shown in Figure 7, the width of the triangle representing the degree of risk.

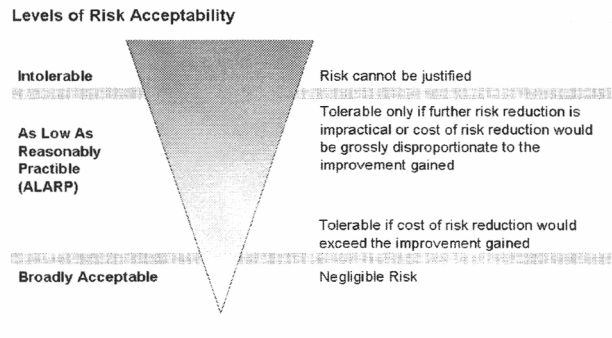

Figure 7 The ALARP Triangle

Whether an identified risk is acceptable is a question of perceptions. Society is worried more by a few multi-fatality accidents than by a much larger number of accidents in which one person is killed, even if the total number of deaths from single fatality accidents is greater. People are more willing to accept risk if they perceive a benefit which compensates for it. For example, travelling by car presents a degree of risk but the benefit of mobility outweighs this risk for most people.

The HSE have issued guidelines concerning risk tolerability. The guidelines group risk of individual fatality into the following bands:

Individual Risk of Fatality	**Acceptability**
$>10^{-4}$ /year	Intolerable
Between 10^{-4} /year and 10^{-6} /year	Tolerable only if risk is ALARP
$< 10^{-6}$ /year	Broadly Acceptable

Note that these levels apply to the **total risk** for the operation, not just single accident scenarios. The apportioned levels for a project will be derived from the overall level by considering the proportion of the total risk the project can contribute. Individual risk is the probability that an identified individual will be killed or injured by the accident scenario in a given time interval. An example table of risk tolerability is shown in Figure 8.

	Severity Category			
Probability Level	4 Catastrophic	3 Critical	2 Marginal	1 Minor
A Frequent	Intolerable	Intolerable	Intolerable	Tolerable
B Probable	Intolerable	Intolerable	Tolerable	Tolerable
C Occasional	Intolerable	Tolerable	Tolerable	Tolerable
D Remote	Tolerable	Tolerable	Tolerable	Negligible
E Improbable	Tolerable	Tolerable	Negligible	Negligible
F Incredible	Negligible	Negligible	Negligible	Negligible

Figure 8 Example Risk Tolerabilities

LOSS ANALYSIS

If the risk is acceptable no further measures need to be taken to manage the risk. If the risk is intolerable actions MUST be undertaken to reduce the risk to a tolerable level. If the risk is found to be in the tolerable region then further analysis is required to establish what is the total "cost" of the risk, what actions could be taken to reduce the risk and are the actions cost effective.

Fatalities and injuries caused as a result of the accident scenarios, arising as a result of the hazard, are converted to equivalent ISO lives. The "lives lost" are converted to a monetary value by the use of the relevant Value of Preventing a Fatality (VPF), presented as a minimum value in the Railway Group Safety Plan each year. Consequential losses include items such as penalty payments, fines, increased insurance premiums, cost of dealing with accident etc. can also be calculated. The HSE requirements require only the figures based on VPF to be met. However, best practice would include the additional costs shown above. The total loss resulting from each hazard can then be established.

OPTIONS ANALYSIS

For each hazard it is necessary to identify possible risk mitigation options. Options may include reducing the frequency of hazard occurrence or reducing the consequences of the hazard. This could include changes to design or operation. For each option identified next determine the total cost on a suitable common basis, e.g. annualised cost, net present value (NPV).

If the costs of the options are a constant annual expenditure, annualised cost would be appropriate. If the option requires initial capital expenditure followed by annual maintenance costs, NPV would be a more suitable basis and would make comparison of different options easier.

IMPACT ANALYSIS

Impact analysis consists of feeding the effects of each option in turn into the original causal and consequence analysis and then reworking the loss analysis to calculate the overall reduction in loss. The reduction in loss is then compared to the cost of achieving it.

When comparing the cost of options with safety benefits this must be done on a consistent basis, e.g. annualised total or NPV.

COMPLIANCE WITH ALARP BENCHMARKS

From the Loss, Options and Impact analyses it is possible to identify whether there is a cost effective method of reducing the risk associated with a specific hazard. Only if further risk reduction is impracticable or cost of risk reduction would be grossly disproportionate to the improvement gained can the risk be termed tolerable and ALARP.

In practice this method should be an aid to establishing that an option is reasonably practicable, not used as a simple pass-fail test. It is not sound judgement to cite the results of a risk assessment as a reason for not taking "common sense" precautions.

The use of a quantified cost benefit technique for determining "reasonableness" enables objective decisions to be made whilst reducing vulnerability to reactive and emotive decisions. It also helps prioritise schemes to enable limited resources to be used to the best effect.

The concept must not be used "in reverse", i.e. it is not acceptable to attempt to save money by making an operation less safe, even if the saving is in excess of the "value" of the additional lives lost.

SYSTEMATIC FAILURES

Systematic failures are treated in a different way to random events by defining a Safety Integrity Level (SIL) for the safety function which represents different levels of rigour in the development process. There are four safety related SIL levels, ranging from SIL 4, the most stringent to SIL 1, the least stringent. Each integrity level is associated with a target probability of failure. IEC 61508 defines the process for safety related systems incorporating electrical, electronic or programmable electronic devices. Systematic failures are of particular concern in software based systems, although hardware can exhibit systematic failures and SILs may be applicable to them as well.

CONCLUSION

So, in summary, why should we perform a risk assessment?

- Risk Assessment is the cornerstone of a safety case which in turn provides a fully justified argument regarding the safety of any operation or installation
- Legislation requires an assessment of risk to employees and public
- Risk Assessments provide evidence of risk acceptability in approval / acceptance processes for new installations and rolling stock and for modifications which could affect safety
- Railway Group policy requires a pro-active approach to safety