RAILWAY SAFETY CASES AND RAILWAY RISK ASSESSMENT IN BRITAIN

Andrew W Evans
London Transport Professor of Transport Safety
University College and Imperial College London, UK

June 1995

Summary

The privatisation of British Rail has prompted the creation of a new railway safety regime in Britain. All railway operators are required to prepare "railway safety cases", which are documents setting out their safety arrangements and their arrangements for coordinating safety management with other operators. This paper discusses the background and content of safety cases, and then goes on to discuss the principles used by Railtrack and Eurotunnel to estimate and evaluate their risks.

Acknowledgements

The author is grateful to Railtrack and Eurotunnel for copies of their safety cases.

1 INTRODUCTION

The break-up of British Rail under the Railways Act 1993 required the establishment of a new railway safety regime. An important part of the new safety regime is the statutory requirement on all operators to prepare "safety cases", which are documents setting out each operator's safety arrangements, and the operator's arrangements for managing the interfaces with other operators. Each safety case must be approved by a separate organisation from the one that prepared it: the approving body for infrastructure controllers' safety cases is the railway safety regulator, the Health and Safety Executive; the approving body for other operators is the infrastructure controller on whose infrastructure they will operate.

This paper first discusses the background, content, and role of safety cases. It then discusses railway risk assessment, as discussed in safety cases or equivalent documents, with particular reference to Railtrack and the Channel Tunnel. The paper continues as follows. Section 2 considers the background to requirement for safety cases: rail privatisation and the changes to the railway safety regime. Section 3 considers safety cases. Section 4 considers the elements of railway risk assessment, including hazard identification, risk estimation, and risk evaluation, with particular reference to Railtrack and Eurotunnel. Section 5 presents conclusions.

2. BACKGROUND

2.1 Break up of British Rail

The White Paper *New Opportunities for the Railways* (Department of Transport, 1992) started the process of breaking up British Rail (BR) into some 80 separate successor organisations. The Railways Act 1993 separated the provision of railway infrastructure from the operation of trains for the first time in Britain. The provision of track and signalling has remained with a single organisation, *Railtrack*, but there will eventually be about 30 separate train operating companies, including both passenger and freight operators. In addition, there are three rolling stock providing companies, and the intention is also to have separate operators for the thirteen main passenger stations, which are at present operated by Railtrack. It was recognised from an early stage that these changes would have important implications for the management of railway safety, because the safe operation of railways closely involves infrastructure, train operation, rolling stock and station operation. Arms' length relationships between the providers of these elements might just possibly be defensible on business or economic grounds, but they are not helpful for safety, because of the possibility of confusion between the organisations concerning their safety responsibilities.

It is useful to note that there are two other major railway operators in Britain besides the ex-BR companies: London Underground Ltd (LUL) and Eurotunnel. LUL is on many measures about 15% of the size of the former BR; Eurotunnel is about 6%. LUL is therefore larger than many of the successor companies to BR, and Eurotunnel is of the same order of size as the larger ones. Eurotunnel is both a train operator and an

infrastructure provider, with other operators' trains using its infrastructure. LUL is also both a train operator and an infrastructure provider, but it is largely self-contained, operating its own trains on its own infrastructure; some exceptions to this are a number of long-standing places where LUL trains run on ex-BR tracks, and ex-BR trains run on LUL tracks. There are no proposals at present to separate train operation and infrastructure provision on LUL.

2.2 British railway safety regulation

The primary responsibility for safety in any mode of transport rests with the transport operators, but all the non-private modes are also subject to safety regulation by public regulators. In the case of the railways in Britain, the long-standing safety regulator is HM Railway Inspectorate (HMRI), which was established in 1840. For many years HMRI was a semi-independent arm of the Department of Transport, but in December 1990 it was transferred to the Health and Safety Executive (HSE), which is the national safety regulating body for industrial and occupational safety. In addition to its general field force, the HSE has safety policy sections, and several specialist inspectorates such as the Nuclear Installations Inspectorate; HMRI forms one further such inspectorate. The transfer of HMRI to the HSE has led to, or at least has coincided with, a profound change in railway safety policy, which has brought it very much into line with HSE's approach to industrial safety. Several ideas from industrial safety have come to be applied in railways, one of which is the idea of Railway Safety Cases (RSC) discussed in this paper.

Railways are at present the only mode of transport for which the HSE is the safety regulator. Aspects of road transport are regulated by various divisions and agencies of the Department of Transport. Civil aviation and merchant shipping are regulated by the Civil Aviation Authority and the Marine Safety Agency respectively, which are both semi-independent agencies of the Department of Transport. None of these have HSE-type safety regimes.

2.3 "Ensuring Safety on Britain's Railways"

Given the important safety implications of the privatisation of BR, and given that HSE was the safety regulator at the time of the privatisation proposals in July 1992, it was not surprising that the government should ask the HSE to carry out a detailed study of safety, and make recommendations for a new safety regime to apply after the break up of BR (Department of Transport. 1992, p.17). The study was published by the Health and Safety Commission (1993) with the title *Ensuring safety on Britain's Railways*. All the HSE's recommendations were accepted by the government, and these formed the basis of subsequent safety legislation and the current safety regime.

The guiding and derived principles adopted by the HSE in recommending a safety regime included the following.

> (a) Any system adopted must not lead to a diminution of current safety standards; it should, as far as possible, facilitate any necessary improvement of

those standards.

(b) Duties and responsibilities must be adequately defined.

(c) The prime responsibility for ensuring safety must rest with the party which has control.

(d) Within the limits of their control, the infrastructure controllers will bear primary responsibility for the coordination of measures to control the risk on the railway.

(e) There must be effective coordination and cooperation between all parties and individuals.

(f) Any arrangements should be demonstrably fair to all parties involved.

(g) All legislation concerning railway safety should be administered by the HSE.

2.4 The new safety regime

The new British railway safety regime is based on these principles. The regime was given legal effect by a single section of primary legislation, s117 of the Railways Act 1993, which makes all existing railway legislation subsidiary to the general Health and Safety at Work Act 1974, enforced by the HSE. An exception is the legislation concerning the Channel Tunnel, which has special arrangements, mentioned below. In addition, a number of new regulations have been enacted under the Health and Safety at Work Act, including the Railway (Safety Case) Regulations 1994, which are of most relevance to this paper. The key features of the current regime are, first, the role of the "infrastructure controller", and, secondly, the introduction of so-called "Railway Safety Cases". We consider each of these in turn.

An infrastructure controller is an organisation which controls day to day access and movement on railway infrastructure. There are two main infrastructure controllers in Britain subject to the new regime: Railtrack, for the ex-BR system, and LUL. Under the new safety regime, the infrastructure controller has the prime responsibility for railway safety: it must ensure the safety of its own operations, and it must ensure the safety of all the activities of those who operate on the infrastructure in so far as they interact with its own operations or with those of other operators. Because there is only one principal infrastructure controller for the ex-BR lines, the regime has ensured that there is a single "directing mind" for safety, notwithstanding the multiplicity of new railway organisations.

The second key feature of the new safety regime is that infrastructure controllers, and all railway operators, are required to produce so-called Railway Safety Cases (RSCs). A safety case is a document, or series of documents, setting out the safety arrangements of the undertaking. It includes (a) the undertaking's safety policy; (b) an assessment of the risks which the undertaking's activities give rise to; and (c) a description of the

safety management system. Each operator's RSC must be accepted by an independent body. In the case of infrastructure controllers, this body is the HM Railway Inspectorate; in the case of all other railway operators, the accepting body is the infrastructure controller of the system on which they will operate. The RSCs of infrastructure controllers must include a discussion of the criteria by which they will accept operators' RSCs.

2.5 The Channel Tunnel

Eurotunnel is an infrastructure controller, but it is subject to a different safety regime from other railways in Britain. The general regulator for all matters concerning the construction and operation of the Tunnel is a French/British Intergovernmental Commission (IGC) set up for the purpose; safety matters are dealt with by the Channel Tunnel Safety Authority (CTSA), which advises the IGC. The CTSA required Eurotunnel to prepare a safety case, but this was not produced under the same statutory requirements as those of other operators. Nevertheless, it was apparently accepted by the HSE (Short, 1994), presumably in fulfilment of a requirement by the CTSA.

3. SAFETY CASES

3.1 Origins

The source of this phrase is the view that if an organisation wishes to carry out a hazardous activity, then it must make a case that it will do so safely. The first general application of safety cases was to industrial installations which present major hazards to employees, or to the public, or to the environment. The impetus for safety cases for major industrial hazards came in Britain from the chemical explosion at Flixborough in 1974, which caused 28 deaths, and in Europe from the release of chemicals at Seveso in Italy in 1977, which caused no immediate human loss of life, but much chemical damage and injury. The requirement for industrial safety cases in Britain was enacted in the Control of Industrial Major Accident Hazards Regulations (CIMAH) 1984. This was followed by similar requirements for the offshore oil industry, following the destruction by fire of the Piper Alpha platform with 167 fatalities in 1988.

Although a safety case regime for major hazardous industrial plants has been in place for ten years, and although safety cases are widely supported both by industry and regulators, there appears to be no evidence that they have actually improved safety (Wilson, 1995). This does not mean that they have *not* improved safety; it just means that relevant evidence is difficult to obtain. One reason for this is that industrial safety cases are concerned only with major hazards, and major industrial accidents are very rare: there have been none in Britain since Flixborough, apart from Piper Alpha, which was then not covered by a safety case regime. More recent safety case regimes - for the offshore industry and railways - cover *all* hazards, and not just major ones. The wider scope may provide more evidence of their effects; on the other hand, it will still be difficult to disentangle the effects of safety cases from the other simultaneous changes.

3.2 Railway Safety Case Regulations

The safety case model was taken up for railways when a new safety regime was needed at privatisation. The requirement for railway safety cases was enacted in the Railway (Safety Case) Regulations 1994, made under the Health and Safety at Work Act, which came into force on 28 February 1994. These regulations provide that:

> "a person in control of any railway infrastructure shall not use or permit it to be used for the operation of trains or stations unless...he has prepared a safety case...[and] the [Health and Safety] Executive has accepted that safety case" (regulation 3).

Also:

> "a person shall not operate a train in relation to any railway infrastructure unless he has prepared a safety case...and the safety case has been accepted by the relevant infrastructure controller at least 28 days before the operation commences" (regulation 4).

There is a similar requirement for station operators. A consequence of these regulations is that not only are the newly privatised railway operators required to prepare safety cases, but so also are other existing operators, notably London Underground.

There is a transitional provision for existing operators: provided that they were operating on 28 February 1994, and do not change their legal identity, they have until 28 February 1996 to prepare their safety cases and have them accepted. Therefore Railtrack, which was a new company on 1 April 1994, had to have its safety case accepted by that date. It duly did, though it is very difficult to believe that the national rail system would have been closed down for want of an accepted safety case. In addition, those minor parts of the rail network whose status changed on the same date, such as the Waterloo and City tube line, which was transferred from British Rail to London Underground, also required safety cases. On the other hand, the train operating units do not require accepted safety cases before 28 February 1996, unless they are privatised before that date, and London Underground does not require a safety case before that date. At the time of writing, London Underground and many train operating companies are preparing their safety cases.

3.3 Contents of railway safety cases

The regulations provide lists of topics which must be included in safety cases. One list covers all operators, that is infrastructure controllers, train operators, and station operators; a second list gives additional requirements for infrastructure operators only. The list for all operators is the following (the item numbers in this list correspond to the paragraph numbers of the schedule to the Safety Case Regulations in which the items are listed):

(1) The name and address of the operator;
(2) a description of the operation;
(3) a description of the premises or plant which is intended to be used;
(4) particulars of any technical specifications, and of operating and maintenance procedures;
(5) a statement of the operator's general health and safety policy;
(6) a statement of the significant findings of the operator's risk assessment;
(7) particulars of the operator's safety management system;
(8) particulars to demonstrate that the operator has adequate arrangements for implementing his safety policy, and for ensuring the competence of staff;
(9) arrangements for disseminating safety information both within the organisation and to other affected organisations;
(10) arrangements for consultation with employees on health and safety;
(11) arrangements for investigating accidents, if necessary in cooperation with other operators;
(12) arrangements for ensuring the safety of work done by contractors;
(13) arrangements for dealing with accidents and emergencies;
(14) for station operators, arrangements for dealing with overcrowding, and for emergency evacuation;
(15) particulars of safety procedures in the design and procurement of premises and plant;
(16) arrangements for safety audit;
(17) arrangements for cooperation on safety matters with other operators.

The additional topics to be covered by infrastructure controllers concern the arrangements for scrutinising the safety cases of those operators who will operate on the infrastructure, and for ensuring that they will meet the controller's safety requirements.

As mentioned above, these requirements do not apply statutorily to the Channel Tunnel, but the CTSA required Eurotunnel to produce a safety case.

3.4 Level of detail

The regulations do not specify at what level of detail the topics above are to be discussed in safety cases, and obviously different levels of detail are possible. One of the aims of purposes of safety cases is

> "to provide a comprehensive working document against which management, and also the acceptor and HSE, can check that the accepted risk control measures and safety systems have been properly put into place and continue to operate in the way in which they are intended." (HSE, 1994, p.2.)

This would seem to require a rather detailed safety case. Moreover, another part of the HSE guidance on RSCs suggests that

> "where provided, plans or diagrams should be drawn to a scale suitable for easy

identification of the key features of the undertaking, especially those which have a bearing on safe operation (eg location and details of major rail junctions, level crossings, stations, track gradients, etc)." (HSE, 1994, p.33).

This is also rather detailed, and it is clear that for some purposes that level of detail is required. However, it is obviously not possible to provide that kind of detail in a manageable document for an undertaking the size of Railtrack. Therefore it is not clear what details ought to be in the statutory safety case, and what should be in subsidiary operational documents.

3.5 Publication of safety cases

In addition to the purpose mentioned above, the other main purpose of safety cases is

> "to give confidence that the operator has the ability, commitment and resources to properly assess and effectively control risks to the health and safety of staff and the general public" (HSE, 1994, p.2).

There is some conflict between this purpose of safety cases and the preceding one. This is because "comprehensive working documents" are not suitable for publication, but generating public confidence that risks are properly controlled *does* require a public document.

In fact, there is no requirement that safety cases should be published, even though they are statutory documents. To the author's knowledge, the only published railway safety case so far is that for the Channel Tunnel (Eurotunnel, 1994). Railtrack's safety case is *not* in the public domain; in fact, it is labelled "confidential", even though it has to be widely distributed to all train and station operators or would-be operators, and Railtrack has been kind enough to provide a copy to the author. However, Railtrack does publish a non-statutory *Railway Group Safety Plan* (Railtrack, 1995), which contains much of the safety policy information in the safety case, though it contains little on the safety management system.

For the purpose of generating public confidence, it seems desirable that safety cases should be in the public domain, even if not actually published. Admittedly, they would not have a wide distribution even if they were in the public domain; however, it would be their availability as much as their contents that generated confidence, and no doubt they would be referred to in public on critical occasions. There is a parallel with accident inquiry reports: those are also not widely read by the public, but their public availability is essential in giving confidence that accidents have been properly investigated.

4. RAILWAY RISK ASSESSMENT

From the point of view of railway policy, the most interesting parts of the content of safety cases are items (5) and (6) from the list above, that is safety policy and risk

assessment. These together cover:

(a) identification of all the principal hazards of the operation

(b) risk estimation, that is the estimation of the size of the risks stemming from each hazard; and

(c) risk evaluation, that is establishing criteria for deciding what, if anything, should be done to reduce the risks.

The effect of the introduction of safety cases is to place a statutory requirement on operators to consider these matters systematically, and to write down their conclusions. As mentioned above, Railtrack's safety case is not in the public domain, but fortunately much of Railtrack's consideration of these matters is published in a different document, the *Railway Group Safety Plan* (Railtrack, 1995); there is also a *British Rail Safety Plan* (British Railways Board, 1995), covering the companies remaining with BR. Eurotunnel's (1994) safety case *is* published. In what follows, we discuss hazard identification, risk estimation, and risk evaluation, using these documents.

4.1 Hazard identification

There are broadly two approaches to hazard identification: one is from the experience of accidents; the other is by "thinking the unthinkable", and considering in advance all the things that might go wrong with a system. In industry, systematic methods for considering what might go wrong have been developed, notably so-called "hazard and operability" studies (Kletz, 1986), but thinking what might go wrong is easier for an installation which is fixed, and to which access is controlled, than for an extensive transport system open to the public.

Both approaches have advantages and disadvantages. The obvious disadvantage of the first approach is that it is "learning the hard way", by bitter experience of those very events that one wants to avoid; on the other hand, experience provides conclusive evidence of the presence of a hazard, and it is possible to learn from "near misses" as well as accidents. The disadvantage of the second approach is that it is difficult to validate one's conclusions. Both approaches, and indeed safety cases as a whole, are vulnerable to what Reason *et al* (1995, p.18) have labelled, using Ashby's (1956) phrase, "the problem of requisite variety". This problem is that the variety of ways in which things *could* go wrong will always be greater that the variety of ways in which things *have* gone wrong; therefore, experience of accidents can never generate defences against all possible accidents. Similarly, the variety of ways in which things could go wrong will always be greater than the variety that can be foreseen in advance in methods such as hazard and operability studies. Therefore, no approach can lead to the identification of all possible hazards.

Having said that, hazard identification is obviously a useful, indeed essential, process. The choice between experienced-based and study-based approaches turns very much on the availability of relevant experience or accident data. If an industry has a long

history, or if accidents are relatively frequent, then there will be considerable data; on the other hand, if an industry has a short history, or if accidents are infrequent, then there will be little data. Hazardous industry usually adopts the study-based approach, because major accidents, with which most industrial studies are concerned, are rare.

The approaches to hazard identification by Railtrack and Eurotunnel reflect this distinction. Main line surface railways have a long history, with a substantial number of accidents of various kinds: therefore Railtrack's hazard identification is based mainly on experience. On the other hand, the Channel Tunnel has almost no operational history at all, certain unique hazards, and - so far - no fatal accidents in operation: therefore Eurotunnel's hazard identification is based on study of the ways in which the various safety systems could fail. A further point is that Eurotunnel's system is both physically much smaller, and operationally much simpler, than Railtrack's, thus lending itself more to industrial-style hazard identification. Thus, for example, many of the hazards common to ordinary surface railways, such as level crossings, stations, access for trespassers, and passenger-operated doors, are non-existent in the Channel Tunnel.

4.2 Risk estimation

Having identified risks, they must be quantified. Again, there are two approaches: (1) direct estimation from past accident data, and (2) the development and use of a quantified risk model. There is no sharp divide between these approaches, since any use of data requires some model, if only an implicit one, and any model requires data. However, the extremes of the spectrum are clear. Again, Railtrack generally adopts a data-based approach, because there exist enough data on the most important types of accidents for a data-based approach to be feasible. On the other hand, Eurotunnel does not have past data, and has therefore estimated the main risks from a quantified risk model.

The author has elsewhere (Evans, 1995) expressed the view that if relevant data on past accidents exist, they will almost certainly provide a better estimate of risks than risk models. It is sometimes said that one should not expect to estimate risks more precisely than to within a factor of 10 using risk models, and there have been experiments where the same risks have been estimated independently using different models, with results differing by at least that amount. Saccomanno *et al* (1993) provide an example involving the transport of hazardous goods. By contrast, the statistical variation, even in very small samples of data, is usually less than a factor of 10. As an illustration of this point, British Rail (1994) recently made an estimate of the frequency of fatal accidents that would be preventable by the installation of Automatic Train Protection, which automatically stops any train that exceeds a safe speed as a result of driver error. BR's estimate of this frequency was based on the fact that 24 such accidents occurred in the 26 years 1968-1993, giving an estimated frequency of 0.92 per year. Although that estimate is clearly subject to considerable statistical uncertainty, it is almost certainly more reliable than any estimate that could be obtained by modelling the multifarious ways in which train driver errors could lead to fatal accidents. The conclusion is that Railtrack are almost certainly sensible to base their estimates of the various risks on past accident data.

Eurotunnel did not have that option, and has therefore used a quantified risk model. The major sources of risk of multiple-fatality accidents in the Channel Tunnel are identified as being collisions, derailments, and fire. (We should note in passing that unwanted events due to breaches of security, as distinct from accidents, are not covered in the safety case, rightly in this author's view.) According to Eurotunnel's risk model, the expected total number of accidental fatalities from all causes in the Channel Tunnel system is less than 6% of that on an equivalent sized part of BR or the French railways, which implies a fatality rate of about 0.25 deaths per year, or 1 in 4 years. The frequency of accidents with two or more fatalities due to collisions, derailments and fire is only about 1 in 400 years (Eurotunnel, 1994, p.172). It is extremely difficult to judge how reliable are these estimates, but one should not expect too much from such a model.

4.3 Risk evaluation: principles

In a previous paper (Evans, 1994), the author classified the practical approaches to risk evaluation into three groups, labelled *cost benefit analysis*, *industrial risk assessment*, and the *elimination of avoidable accidents*; industrial risk assessment was subdivided into two parts, labelled *individual risk* and *societal risk*. In this paper, we adopt the we adopt a similar scheme to discuss risk evaluation criteria, labelled as follows:

(1) cost benefit analysis
(2) industrial risk evaluation:
    (2a) individual risk criteria
    (2b).criteria based on frequencies of accidents (formerly labelled *societal risk*)
(3) elimination of avoidable accidents.

We now briefly describe each of these evaluation criteria in turn. For further discussion, see Evans (1994).

(1) *Cost benefit analysis* (CBA) starts with given safety measures, and compares their benefits and costs in monetary terms. The decision criterion is that a safety measure should be adopted if and only if the benefits exceed the costs. The benefits of safety measures include reductions in (a) the numbers of fatalities and injuries; (b) physical damage; and (c) disruption and loss of business. For CBA, all these must be valued. The difficult item. which is often the most important, is the valuation of reductions in the risks of death and injury. The increasingly accepted principle for valuing such reductions is the so-called "willingness-to-pay" principle, under which the value of a statistical life is taken to be the aggregate amount that a large group of people would be willing to pay for a safety measure that will on average save one fatality among them. The best-researched context in which such values have been estimated is road safety (see Jones-Lee. 1990, for a survey; and Elvik, 1995, for international comparisons). The valuations of statistical life emerging from willingness to pay studies have a fairly wide range: in British currency anything between about £0.7 and £2 million at 1993 prices can be defended, but this is not too wide to be useful. The 1993 British valuation for a road fatality was £0.74 million, at the low end of the

defensible range (Department of Transport, 1994). Corresponding valuations have been estimated for non-fatal road injuries (see O'Reilly and McMahon, 1993). A final important point about CBA is that in general the analysis is not concerned with *absolute* levels of risk, or with the distribution of risk among individuals, but only with the *changes* in risk brought about by specified safety measures.

(2a) By contrast industrial risk evaluation is concerned with absolute levels of risk. *Individual risk* is usually defined as the probability of death per year to a representative individual or member of a group, as a result of some activity, though it may also be defined more generally. The concept has a fairly long history in industrial and occupational risk: it was used in the Health and Safety Executive's work on the risks of the Canvey Island industrial complex (HSE, 1978 and 1981), and it is now the key risk variable in the HSE's so-called "tolerability of risk" framework (HSE, 1992), which guides the evaluation of industrial risk in Britain. In this framework the range of individual risks is divided into three regions by two boundary points, called the *intolerable risk* and the *acceptable risk*; the former is greater than the latter. Individual risks greater than the intolerable risk are declared intolerable; they must be reduced without regard to cost, or the activity must cease. Individual risks lower than the acceptable risk are so low that they merge into the background risks of life, and they require no action. Individual risks between these levels must be made "as low as reasonably practicable" (ALARP), and this region is therefore often called the *ALARP Region*. The informal day-to-day interpretation of what is reasonably practicable is the adoption of good practice in health and safety for the activity concerned. When a more formal analysis is required, cost benefit analysis is increasingly being used: risk reduction is defined to be practicable if and only if it is possible to find cost-beneficial risk reduction measures. If ALARP is interpreted in this way, then the main contribution that the concept of tolerability of risk adds to CBA is to require that if individual risks exceed the intolerable level they must be reduced without regard to cost. The general justification for having such a limit is to ensure equity in the distribution of risk, and that no individual or small group carries a disproportionate share of risk. The most-canvassed values for the intolerable risk of death are 1 in 1,000 per year for employees and 1 in 10,000 per year for third parties (HSE, 1992). The first figure is approximately the highest risk encountered at work in practice by large groups of individuals, though a few small groups carry higher risks.

(2b) *Criteria based on frequencies of accidents* are again part of industrial risk evaluation. They are often labelled *societal risk criteria*. The term *societal risk* usually refers to the frequency of multi-fatality accidents, but it can be generalised to refer to the frequency of accidents with any specified type of far-reaching effect. Societal risk criteria then refer to the tolerable frequency of such accidents. For example, as we discuss below, Eurotunnel has criteria based on the frequency of multiple-fatality accidents: the just-tolerable frequency of accidents with 2 or more fatalities is about 0.07 per year (Eurotunnel, 1994, p.141). The idea of such criteria stemmed from the appreciation by industrial risk assessors that individual risk criteria were insufficient on their own; some safety measures might be worthwhile, even though no individual was at high risk. That is correct. However, such accident frequency criteria were developed before CBA began to be applied in industrial risk evaluation, and once CBA

is brought in, it is much less obvious that accident frequency criteria have a useful job to do. A closely related issue is whether fatalities in multiple-fatality accidents should be valued more highly than those in smaller accidents; this question is unresolved (though none of the arguments for valuing such fatalities more highly seem convincing to this author).

Before leaving industrial risk evaluation, it is useful to distinguish between an intolerable level of risk and a *target* level of risk. Many organisations have target levels of individual risk that are lower (ie better) than the intolerable level. For example, as discussed below, the Railway Group Safety Plan (Railtrack, 1995) aims to ensure that "working on Railtrack controlled infrastructure does not pose a risk of fatality greater than 1 in 10,000 per annum", which is a factor of 10 better than HSE's intolerable level for employees. This should be interpreted as Railtrack's view of what can be achieved by reasonably practicable safety measures for that activity. If it did not prove reasonably practicable, or if it proved practicable to achieve an even lower level of risk, then the target for that activity could be adjusted. By contrast, the intolerable level of risk must be achieved whether it is reasonably practicable or not. The same distinction between targets and intolerable risks also applies to criteria based on frequencies of accidents.

(3) The *elimination of avoidable accidents* has the longest history of all as a criterion for prescribing safety measures. The classic examples are the recommendations made in accident inquiry reports. In these cases, an accident has happened; the sequence of events leading to it is understood; one or more measures to prevent such accidents are identified; and the measures are recommended. The same idea may be used to propose preventative measures *before* accidents occur. The strength - and the weakness - of this type of prescription is that no quantification of risk is necessary. The fact that an accident has happened - or perhaps demonstrably *could* happen - is proof that the risk is not zero, and that therefore there is some benefit from the proposed safety measure. For many practical safety measures this is the most sensible way to proceed. In many situations, the quantification of risk is not necessary, especially where the cost of a safety measure is zero or small, as many costs are. In other situations, quantification of risk may not be possible, but safety measures are still obviously sensible. However, the absence of quantification of risk is also a weakness, because it is possible unwittingly to recommend safety measures that have small benefits in relation to their costs.

4.4 Risk evaluation in railway safety cases: Railtrack

The traditional approach to the evaluation of railway risks was criterion (3) above, the elimination of avoidable accidents. That is still important for day-to-day safety measures, but for the reasons given above quantification of risk has been adopted for major decisions. Coincidental with assumption by the HSE of the role of safety regulator for the railways, both Railtrack and Eurotunnel have adopted industrial-style risk evaluation for evaluating railway risk. However, Railtrack and Eurotunnel have interpreted this in somewhat different ways.

Railtrack's primary evaluation criterion is HSE's tolerability of risk framework applied to individual risks, with reasonable practicability defined using cost benefit analysis (Railtrack, 1995, p.5-6). In other words, it is a combination of criteria (1) and (2a) above. Railtrack have adopted HSE's general values for the intolerable levels of risk, namely a probability of death of 1 in 1,000 per year for employees, and 1 in 10,000 for passengers and third parties. In practice these limits do not bind, because no identifiable groups of individuals are subject to risks as high as those, so the effective criterion for safety measures on Railtrack-controlled infrastructure is CBA. In its Safety Plan Railtrack has adopted the same valuation of statistical life as the Department of Transport uses for road accidents - currently £0.74 million - for the evaluation of general railway risks, but Railtrack allows consideration of higher figures of up to £2 million per life where individual risks are near the limit of tolerability, or where there are reasons to believe that willingness to pay to reduce risks might be higher. The only empirical work specifically concerned with the willingness to pay to reduce rail risk is that by Jones-Lee and Loomes (1994) for London Underground. They found that people's willingness to pay to reduce the risk of an Underground fatality was about 50% higher than for a road fatality, mainly because of the context in which such fatalities might occur, that is outside the control of the victims, and possibly underground. This provides some justification for adopting a higher valuation of statistical life when risks are outside the victim's control. However, Jones-Lee and Loomes found no evidence that people were willing to pay more to avoid a fatality in a multiple-fatality accident than in a smaller accident.

Railtrack also has numerical targets for individual risk. The same targets have been adopted by British Rail (British Rail, 1995) as the main rail operator. There are separate targets for the workforce, passengers, and third parties; all are lower than HSE's intolerable risks. Currently the targets for the risk of fatalities are the following.

> Passengers: 1 in 50 million passenger journeys
> Members of the public: 1 in 1 million per year
> Road vehicle occupants at level crossings: 1 in 100,000 per year
> Trackside staff: 1 in 10,000 per year.

As mentioned previously, these are to be interpreted as a view of what is reasonably practicable in the context concerned. If for some reason they turned out to be unachievable for one reason or another, presumably they would be adjusted. These targets have the advantage that they can be applied not only to Railtrack but also reasonably easily to all railway operators. Presumably Railtrack will expect all railway operators either to adopt the same targets in their safety cases, or else explain why different targets - either higher or lower - should apply. In practice, these targets are approximately being met for the Railtrack and BR network as a whole, though doubtless there are variations between areas and train operating units.

Railtrack have no numerical targets or tolerability criteria based on the frequency of multiple-fatality accidents, or other specified types of accident, that is criteria of type (2b) above. This author agrees that they are unnecessary in the presence of the other criteria.

4.5 Risk evaluation in railway safety cases: Eurotunnel

Eurotunnel (1994) has adopted the same framework for risk evaluation as is typical of hazardous industrial installations, which is somewhat different from that of Railtrack. In particular, the main criteria used are those traditionally used in industrial risk evaluation, namely the tolerability of individual risk, that is (2a) above, and the tolerable frequency of multiple-fatality accidents, that is (2b) above. However, cost benefit analysis is not a major criterion, and there is no explicit valuation of fatalities. The closest Eurotunnel's safety case gets to CBA is in discussion of the ALARP principle, where it is stated that

> "if the risk level is close to the intolerable level, and the implied cost of avoiding loss of a life is less than, for example some few millions of pounds sterling, the [safety] measure should be implemented..." (p.129).

There is no commitment here to any particular value of statistical life, and there is no statement concerning safety measures where the risk level is *not* close to the intolerable level, which is usually the case.

The main individual and societal risk evaluation criteria used by Eurotunnel are derived from the requirement set by the Channel Tunnel safety Authority that

> "a passenger travelling from London to Paris should be in the part of the journey through the tunnel at least as safe as in the equivalent length of the journey (ie 50km) from either Waterloo to Folkestone or from Sangatte to Paris" (Eurotunnel, 1994, p.125).

Eurotunnel has interpreted this requirement to mean that the *average* passenger safety performance of BR over the last few years is to be taken as the upper limit of tolerability for the Channel Tunnel. Eurotunnel has also interpreted this requirement to apply both to individual passenger risk and to the frequency of multiple-fatality accidents. These are extremely stringent requirements, which by definition about half of BR would not meet, since about half of BR's operations must be worse than the average. However, for staff Eurotunnel has adopted the HSE's general limit for the risk of death of 1 in 1,000 per year, which is less stringent. In the case of non-Eurotunnel staff (the train crews of through trains operated by other railways), this limit has been converted into a risk per tunnel transit. The resulting intolerable levels of risk of death are the following (Eurotunnel, 1994, p.139)

> Car-carrying train passengers: 5.6 per 100 million transits;
> Through train passengers: 4.7 per 100 million transits;
> Through train crew: 26 per 100 million transits;
> Freight train crew: 31 per 100 million transits:
> Eurotunnel staff: 1 in 1,000 per year.

On the basis of their risk model, Eurotunnel estimate that these limits are easily met: the actual risk for most categories of person at risk is at most about 5% of the intolerable limit.

As mentioned above, Eurotunnel also has limits for the frequency of multiple-fatality accidents, derived from BR's performance over in the period 1971-1989. BR's actual frequency of accidents with two or more fatalities was about 1.2 per year; Eurotunnel is about one eighteenth of the size of BR, measured by passenger-kilometres; therefore the just-tolerable frequency of Channel Tunnel accidents with two or more fatalities per year is taken to be 1.2/18, or 0.067 per year, equivalent to 1 in 15 years. As mentioned above, Eurotunnel's model-based estimate of the actual frequency of such accidents is 1 in 400 years, which is more than twenty times better than the limit. There are corresponding estimated frequencies and limits for accidents with higher numbers of fatalities.

While the apparent high level of safety in the Channel Tunnel is in some ways a matter for congratulation, the obvious criticism of the safety case is the absence of a rationale for the particular levels of safety chosen. The limits for the tolerability of individual staff risk do have a rationale, equity in the distribution of risk, as discussed under (2a) of section 4.3 above. However, those for individual passenger risk and for the frequency of multiple-fatality accidents do not have this rationale. Moreover, Eurotunnel has chosen, or been forced, to adopt safety levels that are some twenty times better than these limits. This means that the risks are well into the "ALARP region", in which fresh safety measures are justified only if they are "reasonably practicable". The absence of any discussion of the costs of safety measures makes it impossible to know whether the adopted safety measures were cost beneficial or not. From comments elsewhere, one may guess that some were not. Thus, for example, Sir Alastair Morton, co-Chairman of Eurotunnel, in discussing the interaction of Eurotunnel and the Safety Authority, has said that in the absence of clear objectives for safety

> "...you end up piling up a lot of requirements, one on top of another, Pelion upon Ossa[1] - and grief all the way for the client - who pays. You aggregate, rather than optimise: you create, as we have, a tunnel system designed and built to a standard of safety provision so high that it would exclude the equipment long in use in tunnels everywhere else with an excellent safety record" (Morton, 1995, p.9).

It may be noted that, quite apart from any requirements of the Safety Authority, Eurotunnel has a strong commercial incentive to safety, comparable perhaps with the airlines, since a major accident in the first few years of operation would almost

---

[1] The author confesses that he had to look this up in the *Oxford Companion to English Literature*. In Greek mythology, the Giants heaped the mountain Ossa upon the mountain Pelion in an attempt to reach heaven. The metaphor seems remarkably appropriate. However, Sir Alastair Morton has transposed the mountains: Pelion was the one underneath and Ossa on top.

certainly lead to a substantial reduction in demand. The quotation above suggests that Eurotunnel has been required to go further than it judges to be commercially desirable.

5. CONCLUSIONS

Railway safety management in Britain has been transformed in the last few years, from being somewhat reactive and prescriptive to being more proactive, quantitative and evaluative. This process was occurring well before the rail privatisation proposals, having been triggered particularly by the major accidents in the late 1980s at Kings Cross and Clapham Junction, and the subsequent accident reports (Department of Transport, 1988 and 1989). However, rail privatisation and the introduction of Railway Safety Cases have made the process more systematic. Moreover, the requirement for safety cases has led to the involvement in safety assessment of senior managers who would not otherwise have been involved. Whether safety cases actually improve safety outcomes is something that may never be known.

The appropriate use and level of detail of safety cases remains open, and perhaps should vary between one safety case and another. At one end of the scale, safety cases could be rather detailed operational documents, to be referred to in day-to-day management of safety, and to be used by safety auditors and the HSE in monitoring. At the other end of the scale, safety cases could be high-level documents, expressing general principles and arrangements on the required topics. Of necessity, both the Railtrack and Eurotunnel safety cases are of the latter kind, but there is much supporting material outside the safety cases, and presumably the safety cases of some train and station operators may well be more detailed.

If safety cases are detailed operational documents, it would be inappropriate for them to be published. However, if they are not published, it seems important for generating public confidence, which is one of their purposes, that they should be in the public domain.

In this author's view, Railtrack's current framework for risk assessment, as expressed in the *Railway Group Safety Plan*, is broadly right. Railtrack adopted the established industrial risk assessment framework as a starting point, and developed it by introducing a much more explicit cost-benefit interpretation of what safety measures are "reasonably practicable" than is common in industrial risk assessment. In other words, they have interpreted the ALARP principle as cost benefit analysis, with explicit valuations of statistical life. They were able to do this partly by drawing on experience of road safety evaluation. Presumably the acceptance of Railtrack's safety case by the HSE implies that the HSE accepts this framework. Eurotunnel has been less successful in securing the agreement of its Safety Authority on a framework for evaluating safety measures. The result is apparently a very safe system, but at a high cost, which has presumably added to Eurotunnel's debt.

REFERENCES

Ashby, W R (1956). An Introduction to Cybernetics. Chapman and Hall, London.

British Railways Board (1994). Automatic train protection: report from British Railways Board to Secretary of State for Transport. BRB.

British Railways Board (1995). British Rail Safety Plan 1995. BRB.

Department of Transport (1988). Investigation into the Kings Cross Underground Fire (the Fennell Report). Cm 499, HMSO, London.

Department of Transport (1989). Investigation into the Clapham Junction Railway Accident (the Hidden Report). Cm 820, HMSO, London.

Department of Transport (1992). New Opportunities for the Railways. Cm 2012, HMSO.

Department of Transport (1994). Highways Economics Note No 1: 1993 Valuation of Road Accidents. Department of Transport, London.

Elvik, R (1995). An analysis of official economic valuations of traffic accident fatalities in 20 motorized countries. *Accident Analysis and Prevention* 27(2), 237-247.

Eurotunnel (1994). The Channel Tunnel: a Safety Case. Eurotunnel, Folkestone.

Evans, A W (1994). Evaluating public transport and road safety measures. *Accident Analysis and Prevention*, 26(4), 411-428.

Evans, A W (1995). Risk assessment by transport organisations. Paper presented at a conference on *Risk in Organisational Settings* organised by the Economic and Social Research Council in London on 16-17 May 1995.

Health and Safety Executive (1978). An investigation of potential hazards from operations in the Canvey Island/Thurrock area. HMSO, London.

Health and Safety Executive (1981). Canvey: a second report. HMSO, London.

Health and Safety Executive (1992). The tolerability of Risks from Nuclear Power Stations, 2nd edition. HMSO, London.

Health and Safety Commission (1993). Ensuring Safety on Britain's Railways. Department of Transport, London

Health and Safety Executive (1994). Railway Safety Cases: Guidance on Regulations. HSE Books, Sudbury, Suffolk.

Jones-Lee, M W (1990). The Value of Transport Safety. *Oxford Review of Economic Policy*, 6, 39-60.

Jones-Lee, M W and G Loomes (1994). Towards a Willingness to pay based value of Underground Safety. *Journal of Transport Economics and Policy*, 28(1), 83-98.

Kletz, T A (1986). Hazop and Hazan: notes on the identification and assessment of hazards, 2nd ed. Institution of Chemical Engineers, Rugby.

Morton, Sir A (1995). Eliminating risks for the travelling public. Paper presented to the Royal Academy of Engineering, London, on 20 March 1995.

O'Reilly, D and nine others (1994). The value of road safety: UK research on the value of preventing non-fatal road injuries. Journal of Transport Economics and Policy, 28(1), 45-59.

Railtrack (1995). Railway Group Safety Plan 1995/96. Railtrack, London.

Reason, J, D Parker, R Lawton and C Pollock (1995). Organisational controls and the varieties of rule-related behaviour. Paper presented at a conference on *Risk in Organisational Settings* organised by the Economic and Social Research Council in London on 16-17 May 1995.

Saccomanno, F F, D Leeming and A Stewart (1993). Comparative assessment of risk model estimates for the transport of dangerous goods by road and rail. Institute for Risk Research, University of Waterloo, Canada, and the Health and Safety Executive, Sheffield.

Short, R (1994). Railway safety cases in action. Paper presented at a conference on *Managing Safety through the Change Process* organised by IBC Technical Services Ltd in London on 16 June 1994.

Wilson, D J (1995). The effectiveness of safety cases: a major contractor's view. Paper presented at a conference on *Safety Cases* organised by IBC Technical Services Ltd in London on 23 February 1995.