RAIL TUNNEL FIRE SAFETY SYSTEM DESIGN IN A SFAIRP CONTEXT

Tim Procter¹, Lachlan Henderson²

¹Director, R2A, Melbourne, AUSTRALIA
²Senior Fire Engineer, Arup, Melbourne, AUSTRALIA

Corresponding Author: tim.procter@r2a.com.au

SUMMARY

Australian rail and workplace safety legislation places specific duties on rail system designers, including the requirement to eliminate or (failing that) reduce safety risks so far as is reasonably practicable (SFAIRP). This obligation places significant importance on designers’ decisions, especially given those measures which are considered ‘reasonably practicable’ are only ever determined in a court of law after an incident. The people making this legal determination are generally from a non-technical background, and are rarely engineers. It thus behoves us as engineering designers to consider how this determination would be made in relation to our designs, should an incident or failure occur, and to structure our safety-related decision-making processes and language accordingly.

This paper presents issues we have identified with the current approaches to safety decision-making in addressing SFAIRP requirements in rail tunnel fire safety system design. We discuss the context within which these approaches sit, including legislation and design standards, and how current approaches address (or fail to address) critical aspects of SFAIRP requirements.

We then present an alternative approach that allows for straightforward decision-making to address designers’ SFAIRP requirements and how they would be assessed after an incident. We present an example of how our approach and associated techniques allow for more efficient rail tunnel fire safety system and general sound design practice, while promoting innovation within an appropriate decision-making framework.

Finally, we note some challenges facing the move to more diligent rail safety design approaches, including information gaps, leadership and communication issues.

1 INTRODUCTION

Recent changes to Australian work health and safety legislation have thrown into sharp relief a number of issues with rail tunnel designers’ approaches to meeting requirements for fire safety systems.

The model work health and safety (WHS) legislation [1] first put forward by Australia and now adopted in most Australian jurisdictions takes an unusual approach. In aiming to ensure duty holders comply with the established principle of eliminating or (failing that) reducing risk so far as is reasonably practicable (SFAIRP), legislators have codified and mandated the common law principle of ‘due diligence’ for duty holders in an effort to ensure SFAIRP duties are met.

This has led to concern over how duty holders may “exercise [ie demonstrate] due diligence” [1] in engineering design safety decisions in a legal context. It seems that the due diligence principle is well understood by lawyers but less so by design engineers. Accordingly, a range of engineering design approaches are in use across industries, each addressing some aspects of SFAIRP and due diligence, but few, to our knowledge, adequately meeting all of them, and none in a clear and efficient manner.

This paper discusses these current approaches in the context of rail tunnel fire safety systems design. We look at the contexts in which these approaches arose and are used, and the wider context of legislation in which they now sit. We examine how they address (or fail to address) the specific requirements of safety legislation invoking the SFAIRP principle, and the difficulties that may arise as a result.

We then present a new approach specifically structured to meet the requirements of duties under the SFAIRP principle. We show how this is achieved by adopting an approach designed to demonstrate due diligence in safety-related engineering design decisions. We support this with an example application of the proposed approach.

In this manner we highlight issues presented by current approaches to rail tunnel fire safety system design in an Australian legal context, and demonstrate an approach that addresses these problems in an efficient and transparent manner.
2 THE RAIL TUNNEL FIRE SAFETY SYSTEM DECISION-MAKING CONTEXT

A number of key factors influence rail tunnel fire safety system design approaches adopted in Australia, including mandatory requirements (i.e., legislation), recognised good practice (e.g., Australian and international standards), common law duties of care, and independent post-event investigation and findings. These are described below.

Australia has a range of mandatory requirements with which persons and organisations in the rail industry must comply to address safety issues. Chief amongst these is legislation setting out requirements for health and safety. This includes:

- General work health and safety legislation, such as the 2012 Federal Model Work Health and Safety Act [1] implemented in most Australian states and territories.
- Industry-based legislation addressing specific domains, such as the 2012 Rail Safety National Act [2].
- The Office of the National Rail Safety Regulator, which mandates preparation and maintenance of a safety case for rail industry operators.

Within these legislated requirements are a range of requirements, including strict and prescriptive requirements, as well as performance-based requirements and duties to demonstrate that safety risk has been eliminated or reduced 'so far as is reasonably practicable'. These requirements supersede all others, and must be complied with.

In addition to legislation, the rail operations and maintenance are addressed under Australian and international standards, codes of practice and other similar documents. Provided these are not called up into legislation these represent recognised good practice. That is, they describe measures that have been developed and accepted through industry practices to an extent where they are generally accepted as an appropriate way to go about particular tasks. Other good practice is less formalised, and may be present in, for example, common work practices.

Good practice sets a baseline by demonstrating measures that are widely considered reasonable in particular situations. This presents a strong case for the same good practice being reasonable in similar scenarios.

In practice, a range of Australian and international standards are often referenced in rail tunnel fire safety system design as a means of demonstrating compliance with the mandatory approaches listed above.

Tunnel fire engineering approaches adopted for major rail tunnel projects in Australia are often based on those within AS4825:2011 – Tunnel Fire Safety [3]. However, a range of international standards and guidance are also implemented in various aspects of rail tunnel fire safety system design such as rolling stock design, ventilation regimes, emergency egress walkway provisions, cross tunnel passage spacing etc. Prominent amongst these standards are:

- Guidance from the European Union’s Technical Specifications for Interoperability, such as those listed as References [4], [5] and [6], and
- The USA National Fire Protection Association (NFPA) standards, in particular NFPA 130 – Standard for Fixed Guideway Transit and Passenger Systems [7].

The approaches in these standards are supplemented with guidance from sources such as the Australian Office of the National Rail Safety Regulator (ONRSR), in particular the ONRSR guideline on ‘Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable’ [8].

Safety issues are also addressed through litigation, in which courts make determinations as to negligence and penalties in relation to specific incidents that have occurred.

Finally, safety issues are investigated through inquiries by coroners and Government-directed enquiries such as Royal Commissions. While these do not generally have direct consequences for those investigated, prosecution or litigation may arise based on inquiry findings.

These requirements each aim to ensure that or determine if all reasonably practicable precautions are or were in place to address safety issues.

Key aspects of the four prominent standards and guidelines are provided in Sections 3-6.

3 AS 4825:2011 – TUNNEL FIRE SAFETY

AS 4825 [3] is a performance based standard that uses a risk management approach to tunnel fire safety design. Whilst performance based, the standard also provides non-prescriptive guidance as to what design measures are typically required in various types of tunnels, as well as providing guidance as to what design measures are only sometimes required and which are not typically required or not recommended.

This guidance is provided for ‘trial concept designs’ of rail tunnels separated into ‘metro passenger’ tunnels, ‘short regional passenger rail tunnels’, ‘long regional passenger tunnels’, ‘short freight rail tunnels’, and ‘long freight rail tunnels’ (where short tunnels are between 80 and 250 metres in length.
and ‘long tunnels’ are greater than 250 metres in length). Metro rail tunnels are defined as those in urban environments characterised by underground stations and frequent traffic that may be required to be held in the tunnel.

### 4 NFPA 130

The National Fire Protection Association’s standard for fixed guideway transit and passenger system, NFPA 130 [7], defines fire safety requirements for entire rail systems. It defines requirements for stations, tunnels, and rolling stock. NFPA 130 is used extensively internationally for rail infrastructure design. Outside of North America it typically finds application to rail systems where there are no explicit local legislative requirements.

NFPA 130 applies to passenger rail systems with a focus on those utilising electrical traction supply (up until its 2014 release it provided no guidance for the case of diesel powered rolling stock).

Also, in contrast to other standards, NFPA 130 does not alter its requirement sets for tunnel length, except for the provision of mechanical ventilation (which is not required for tunnels of length less than 61 metres, required for all tunnels of length greater than 305 metres, and should be the subject of an engineering assessment for tunnels of length between 61 and 305 metres).

Another interesting trend that the authors have observed with the application of NFPA 130 outside of North America, is that the rolling stock fire safety provisions of the standard are often not used. For example, rolling stock of a given rail system may be designed to European standards but the rail tunnels (and stations) are designed to NFPA 130.

NFPA 130’s rolling stock fire safety solution differs to that of standards such as BS6853 [9] and AS7529.3 [10] notably in areas such as planes of fire resistance [11], material fire performance, and running capability in the event of fire [12].

### 5 EUROPEAN TECHNICAL SPECIFICATIONS FOR INTEROPERABILITY

In Europe, legislative requirements for the fire safety design provisions for rail tunnels are defined within the Safety in Railway Tunnels Technical Specification for Interoperability (SRT TSI) [4, 5, 6]. Unlike NFPA 130, these do not define fire safety requirements for underground stations (in the TSI context, fire safety of stations are addressed using the applicable building fire safety practices), but they do give minimum requirements for rolling stock which are defined in the locomotive and passenger TSI [5].

It is also worthy of note that the TSIs do not apply to all rail European systems – only those which are geographically and functionally required to be ‘interoperable’. Whilst ‘urban rail systems’ are, as per the recast ‘top level’ TSI [4], excluded from the scope of TSIs, this is due to the fact that such systems are functionally separate and therefore not required to facilitate ‘interoperability’ rather than in a limitation of the requirement set themselves.

Also worthy of note is that the SRT TSI is written with an expectation that rolling stock operating through applicable tunnels could consist of electrically or diesel powered freight rolling stock, passenger rolling stock, and on-track machines. The SRT TSI also mandates many of its fire safety measures with reference to tunnel length.

### 6 ONRSR GUIDELINES

The Office of the National Rail Safety Regulator provides a guideline to ‘Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable’ [8], aspects of which are supplemented by ONRSR’s Major Projects Guideline [13]. These guidelines refer, inter alia, to the risk management process set out in AS31000:2009 – ‘Risk Management’ [14], the international standard which built on and superseded AS4360:2004 [15], the previous Australian risk management standard.

A key aspect of the AS31000 risk management process is the selection of risk criteria, below which risk levels are considered “tolerable” or “broadly acceptable”. Generally in the first instance these criteria are qualitative in nature.

The ONRSR guidelines also each encourage and, for major rail projects such as tunnels, require the quantification of risk associated with identified hazards, and the selection and use of quantified risk criteria for this comparison.

### 7 CURRENT APPROACHES TO RAIL TUNNEL FIRE SAFETY SYSTEM DESIGN

Rail tunnel fire safety system designers generally base safety decisions on at least one of three key approaches; compliance with legislation, compliance with standards, and hazard-based risk management. A number of issues arise with the current approach to each of these. The approaches and their associated issues are discussed in Sections 8-10.

### 8 COMPLIANCE WITH LEGISLATION

Firstly, decisions are made to comply with safety-related legislation. For prescriptive requirements this is generally straightforward.

However, Australian safety legislation, including all of the key Acts mentioned above, has increasingly moved away from prescriptive requirements in favour of imposing duties for those best able to
manage risks to implement all ‘reasonably practicable’ measures.

This shift has moved the responsibility for judging what is reasonably practicable onto rail tunnel fire safety system owners, operators and designers, and requires a sound decision-making process rather than simple compliance with legislated prescriptive requirements.

9 COMPLIANCE WITH STANDARDS

Secondly, decisions are made to comply with standards. As outlined above, there is a range of standards that could apply to various aspects of any specific rail tunnel fire safety system design.

Issues arise with this, as implicit assumptions in the standards lead to different specifications for the same design parameters. For example, Table 1 shows a comparison of the emergency egress requirements for rail tunnels for the three standards mentioned above.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Emergency tunnel egress requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFPA 130 [7]</td>
<td>Emergency egress required to the surface every 762 m, or, cross passageways required every 244 m.</td>
</tr>
<tr>
<td>SRT TSI [4, 5, 6]</td>
<td>Exits to surface every 1000 m, or cross passages to adjacent tunnel every 500 m</td>
</tr>
</tbody>
</table>

Table 1. Example comparison of requirements of design standards for rail tunnel fire safety systems.

AS4825 adapts some guidance from NFPA 130, leading to the similarity in cross passageway separation distance requirements. However there is a large difference between these requirements and the SRT TSI guidance.

The differences are due to a number of assumptions. Some of these are obvious, such as the associated tunnel ventilation design. However some are subtler. The NFPA 130 assumptions around rolling stock characteristics and fire fuel loads are considerably more conservative than those in the SRT TSI.

This leads to a significant difference in the potential tunnel fire scenarios, and a flow-on effect to conditions evacuees may face in such a scenario, and hence the much smaller cross tunnel passageway separation distances in NFPA 130 compared to the SRT TSI guidance.

These discrepancies between standards’ requirements arise in a number of areas. Selection, interpretation and application of these standards thus requires a thorough understanding of the assumptions underpinning in the approaches presented in the standards, and how these relate to the specific issues at hand.

While this has the potential to lead to inadequate safety measures being in place in rail tunnel fire safety system design, in practice it more often results in design inefficiencies, with the most conservative aspects of each standard being selected for application to a single design, without taking into account the mitigating assumptions underlying each standard.

It ought to be noted that compliance with a standard or other good practice does not guarantee compliance with the law, only that the baseline has been achieved. It is possible and indeed likely that further practicable and reasonable measures are available for any particular rail tunnel fire safety design issue.

In these situations a sound decision-making process is needed to judge the intent of the standards, to determine how best to meet the baseline requirements set by the standards as recognised good practice, and to determine if any further measures are considered reasonable under legislated requirements.

10 HAZARD-BASED RISK MANAGEMENT

As described throughout Sections 2-6, almost all of Australian rail tunnel fire safety system design legislative, good practice and regulatory requirements and guidance involves the use of risk management processes. As detailed in the ONRSR guidelines [8, 13], the recommended approach for this is the hazard-based risk management approach described in AS31000 [14].

This approach follows the following basic steps (after Francis, Robinson, Procter et al (2015) [16]):

1 Establish the context: What are we looking at? What is included in our assessment? What is to be excluded?
2 Risk assessment (hazard focused):
   a. (Hazard) risk identification: What are the risks within our context?
   b. (Hazard) risk analysis: How might these risks occur? What are their likelihoods and consequences?
   c. (Hazard) risk evaluation: Are the risks and their likelihoods and consequences tolerable or acceptable?
3 Risk treatment: What measures should be implemented to bring the likelihoods and consequences below the designated tolerable or acceptable limits?

This approach provides a clear and documented decision-making process that may be used to address safety issues.

However, problems become evident when the hazard-based risk management approach is considered in the safety decision-making context described above.

Risk management processes provide formal methods of exercising judgement. Ideally, whatever risk management process one adopts aids and demonstrates one’s good judgement in managing risks. Put another way, good risk management facilitates diligent decision-making. In the Model WHS Act’s phrasing, it helps decision-makers “exercise due diligence” [1]. But what is due diligence?

As due diligence is demonstrated through making good decisions, it follows that whoever determines if good decisions were made also determines if due diligence is demonstrated. In an Australian context, safety decisions are tested in court following an event. The court’s finding is the determination of whether the decision(s) considered were good (that is, reasonable) in relation to the event in question.

So, how do the courts go about making this determination? The process, while detailed, essentially involves finding answers to two key questions. These are:

1. Was it considered that this particular event was a credible issue? (And if not, why not?)
2. Was there anything else which ought to have been done to prevent it?

Providing convincing answers to these questions before any event occurs is the foundation of good risk management.

However, the answers provided by the hazard-based risk management process can be less than convincing.

Following its first step of establishing the context, the hazard-based risk management process’ Step 2a directs that hazards and their associated risks be identified. This essentially addresses the court’s first question by asking: “What could go wrong?”

Guidance for risk identification often discusses brainstorming and guideword-based processes that look at system elements to identify what could go wrong with each of them. The ONRSR guidelines noted above do not provide specific reference to providing confidence that all credible critical risks have been identified.

The results of this process are what will form the answer to the first question in any post-event investigation.

If, following this, an event occurs that was identified in the risk assessment, the first question is fairly simple to answer by presenting the risk assessment documentation. If, however, the event was not identified, providing a convincing answer becomes difficult. The lack of an overarching check that no critical hazards were overlooked means that there is often no documented process showing why it was believed that all hazards were identified at the time of the assessment.

After identifying risks, the hazard-based risk management process Steps 2b, 2c and 3 involve determining if and how specific hazards’ risk can be brought below thresholds deemed ‘acceptable’ or ‘tolerable’, as set by risk criteria such as those required in the ONRSR guidelines [8]. This addresses the court’s second question by essentially asking: “What can we do to lower the risk for the identified hazards?”

In this process measures are suggested and applied to individual hazards until risk levels are deemed below the threshold. Once this transition from ‘intolerable’ to ‘tolerable’ takes place, no further measures are considered justified.

For major projects the ONRSR guidance requires this process to be undertaken quantitatively [13], using a ‘Value of Statistical Life’ and a ‘gross disproportionality factor’ in order to compare the estimate financial cost of proposed risk-reducing measures against the estimated financial saving of preventing a safety impact. A range of other factors may be included to estimate the equivalence of, for instance, a serious injury compared to a fatality. Various Values of Statistical Life are published internationally, including in New Zealand [17], however there is no current Australian figure.

This hazard-based risk management process provides the answer to the second question in any post-event investigation. However, it provides a poor response.

When determining what ought to have been in place to prevent the event, the court identifies, firstly, what has been shown to be reasonable in similar situations. That is, the court looks at recognised good practice, such as that described in Sections 2-6 above, to determine if it would have been appropriate in the scenario being investigated.

Secondly, the court identifies other practicable measures that would have influenced the occurrence or outcome of the event. These are
each tested to determine if they were reasonable given the state of knowledge before the event. This calculus compares the benefit each measure may provide through risk reduction against the cost in time, difficulty and expense to implement and maintain it.

Through the good practice review and the cost-benefit comparisons the court identifies measures considered appropriate for the event in question. Problems arise with the hazard-based risk management approach if any of these measures were not implemented due to the risk of the hazard in question being deemed ‘tolerable’ in comparison to selected risk criteria.

If this is the case the court may find the decision-maker negligent (in litigation) or guilty (in a criminal trial).

Although the ONRSR guidelines [8, 13] discuss the importance of recognising, assessing and implementing good practice in a rail industry context, the conflation of this approach with ONRSR’s requirement for the use of risk criteria does not provide a clear decision-making approach to demonstrate why risks have been reduced so far as is reasonably practicable.

The problems that this hazard-based approach presents to convincingly answering the two key questions ought to be of significant concern to rail tunnel fire safety system designers and operators. Current decision-making processes may not identify credible risks and reasonable measures that ought to be considered. And even with best intentions and efforts, post-event, owners and operators may not be able to demonstrate diligence in their safety-related decisions, even if they believe that the options they have chosen to address a safety issue are ‘right’.

Overall, the difficulty in determining reasonable safety measures for rail tunnel fire safety systems through compliance with legislation, standards and risk management may lead to safety considerations being ignored, neglected or given cursory attention, or, more likely, significant design and operations inefficiencies being introduced in an attempt to show compliance with the various conflicting requirements.

11 PROPOSED APPROACH TO RAIL TUNNEL FIRE SAFETY SYSTEM DESIGN

To address these issues a better approach is needed. The approach presented here considers the court’s point of view and works backwards to find the best way to answer the questions that would be asked after an event.

This requires extrapolating backwards from the court’s two tightly focused questions for a past single event to provide answers to these questions for all safety issues that could occur with the system in question. Care must be taken that these answers are readily comprehensible by a judge and jury.

In this way, the court’s post-event questions of:

1. Was it considered that this particular event was a credible issue? (And if not, why not?)
2. Was there anything else that ought to have been done to prevent it?

become, for rail tunnel fire safety system designers, owners and operators, prior to any event:

1. Why are we confident that we’ve identified all credible, critical safety issues?
2. Why are we confident that all reasonable measures are in place for all identified issues?

Answering to these two questions leads to much more convincing responses to any post-event questions. The required steps and associated outcomes for this approach are presented in Sections 12-15.

12 A COMPLETENESS CHECK

To address the first question requires not only identifying the risks associated with the system in question, but also undertaking a completeness check to provide confidence that no credible, critical issues have been overlooked.

This approach is most effective and valuable when it is tightly coupled to the assessment context; that is, the boundaries of the assessment in time and space. These are determined by understanding the limits of a system’s influence on people’s safety. By considering these groups of people (for example, system users, system maintainers, system patrons, the general public) in the different areas and times that the system could impact on threats presented to them, an overarching safety vulnerability matrix can be developed.

This matrix is a high-level, top-down completeness check which addresses system designers’, owners’ and operators’ first key question in Section 11, and provides guidance on where further analysis of key risks may be beneficial.

13 PRECAUTION-BASED DECISIONS

With this completeness check in place the identified vulnerabilities can be analysed. An effective method for this is timeline analysis, identifying the sequences of events that may lead to undesired scenarios, and the interactions of these timelines.
Using this framework, points of influence become apparent in the period from an initial event to an undesired scenario. At these points of influence, measures may be introduced to eliminate, or reduce the likelihood or severity of an event.

It is always wise to first consider measures that eliminate the threat. If these are not considered reasonable, next consider those that act earliest in the timeline before moving along until post event measures are considered.

An effective way to do this is to identify the point of loss of control for each undesired event. This is the point at which, although it is not certain that the event will occur, control is lost over whether or not it does.

This approach is borne out by the obvious order of preference of, for example, eliminating diesel services in a rail tunnel to remove a major fuel source, followed by minimising diesel services using the tunnel through timetabling, followed by ensuring appropriate tunnel fire suppression and evacuation measures are in place. This line of reasoning is followed by the courts.

To identify measures that may be considered reasonable, consider the court’s approach to determining reasonable measures. First, review recognised good practice and either implement it, or provide sound reasoning why in this case it is not considered appropriate.

Following this, consider other good ideas to understand their benefits, in terms of risk reduction, and their costs, in terms of time, difficulty and expense of implementation and maintenance. In a legislative (i.e., criminal) context an option’s safety benefits are compared against the costs to determine if they are “grossly disproportionate”, i.e., if the benefits are dramatically outweighed by the costs. In a litigative (i.e., common law) context the costs and benefits are considered “on balance”, i.e., if the costs outweigh the benefits. Where the costs are considered either greater than the benefits (for the latter) or grossly disproportionate to the benefits (for the former), an option can be considered not justified.

Where a number of options are identified to address a risk this approach provides a clear basis for prioritisation. The diminishing returns of multiple measures addressing a single event typically result in a cost-justified and effective suite of measures.

This approach provides clear, cost-justified arguments for the adoption or rejection of the options identified. This gives a clear answer to designers’, owners’ and operators’ second key question in Section 11.

The quantification of risk as part of this process may provide value if it is used to compare the potential effects of competing measures proposed for implementation. For instance, in a rail tunnel fire safety system context (assuming good practice has already been appropriately implemented), the quantified costs and benefits of decreasing cross passageway separation distances could be compared to the quantified costs and benefits of increasing evacuation pathway widths. This type of quantitative risk comparison can provide guidance when deciding which suite of options may be considered reasonable for a specific tunnel design. This process provides a means of demonstrating diligence in decision-making without requiring the comparison of quantified risk values to selected tolerability criteria, an approach with an inherent weakness under post-event review.

14 OTHER CONSIDERATIONS

When undertaking this process it is critical to ensure good information is used to feed into the assessment.

This information can be sourced from reviews of literature such as standards and other good practice, targeted interviews with key stakeholders, and discussions of the issues with groups of people from different knowledge bases such as in facilitated workshops.

For a rail tunnel fire safety system design this would be expected to include tunnel designers, tunnel owners, fire safety system operators, general rail operations and maintenance staff, train drivers, fire and emergency response personnel, and any other relevant stakeholders.

15 OUTCOMES OF A PRECAUTION-BASED APPROACH

Used together, the approach outlined in Sections 12-14 puts in place a clearly documented and explicable decision trail for safety issues.

The emphasis on clear and concise decisions helps ensure effective communication to all relevant parties, including those vulnerable to the identified risks, and those who may conduct an inquiry after an event.

Through this process, designers, owners and operators of rail tunnel fire safety systems can have comfort in their safety-related decisions, and confidence that due diligence has been demonstrated.

16 EXAMPLE APPLICATION OF PROPOSED APPROACH

The following is an example of how this process could be applied to a major rail tunnel fire safety system design with the aim of providing an argument as to why it is believed risks addressed by the tunnel fire safety system have been
eliminated or reduced so far as is reasonable practicable.

The tasks completed as part of this assessment are described in Sections 17-18.

**17 Completeness Check**

The first step is to address the key question: Why are we confident that we’ve identified all credible, critical safety issues? These may be identified through, firstly, a vulnerability assessment considering the critical exposed groups and high level threats as shown in Figure 1.

![Figure 1. Vulnerability assessment](https://via.placeholder.com/150)

**Figure 1. Vulnerability assessment**

This approach carefully considers the context in a systematic and top-down manner, with an emphasis on communicating findings. To more clearly show the findings of this assessment timelines can be developed to understand how they could occur. Figure 2 shows an example of a generic tunnel fire timeline.

![Figure 2. Threat timeline structure.](https://via.placeholder.com/150)

**Figure 2. Threat timeline structure.**

More detailed timelines can then be developed for specific scenarios, and their interactions analysed. This can develop a comprehensive timeline analysis suitable for identifying precautions. An example combined timeline for rolling stock tunnel fires is shown in Figure 3. This could be expanded to include, for instance, the effect of station fires on rolling stock.

![Figure 3. Combined detailed timeline of fire scenarios and consequences.](https://via.placeholder.com/150)
At this point there is confidence that all critical, credible threats are identified and understood, providing an answer the first key question, and a good foundation to identify reasonable precautions.

18 PRECAUTIONS IDENTIFICATION

Following this a precautions identification process is needed to answer the question: Why are we confident that all reasonable measures are in place for all identified issues?

This involves two steps: What are the practicable options? And, of these, what are the reasonable measures? This takes into account both initial and ongoing implementation.

One technique for presenting the threat and consequence scenarios and existing precautions is a threat-barrier diagram. This is a timeline analysis which clearly shows the point of loss of control, and where precautions (barriers) act along the event sequences. It also shows how barriers may address more than one threat mechanism.

To develop threat-barrier diagrams for the system as a whole critical events may be identified in the timeline in Figure 3 at which significant influence exists to prevent timeline progression. Such events are shown in the numbered orange boxes.

A threat-barrier diagram for one of these events is presented in Figure 4, showing precautions to address the threat and consequence scenarios around the point of loss of control.

Further options and enhancements are identified through considering a range of factors, including:

- Identified consequence scenarios,
- The geographic zones in which the threat and consequence scenarios could occur and the precautions could be influential,
- Construction and maintenance activities for potential precautions,
- Receptors of the consequence scenarios (ie the critical exposed groups),
- Operations requirements,
- Good practice requirements precautions in place for similar structures, including measures presented in the standards discussed in Sections 3-6. If there is conflict between these, the assumptions underlying each should be considered, for example the rolling stock fuel load assumptions and how they relate to cross passageway separation distances, as discussed in Section 9,
- Benefits of precautions already in place, and
- Interactions between each potential precaution and the other existing and potential precautions.

When identifying practicable options consideration is given to options for elimination of all or some of the risks, engineering measures, management measures, emergency response measures and consequence mitigation measures.
To determine which of these may be considered reasonable they are each reviewed to understand their costs and benefits for various stakeholders, including the constructor, the owner, operators and emergency response personnel.

Cost is considered in terms of time, difficulty and expense. Benefits are considered in terms of risk reduction, informed by, for example, fire and consequence modelling of fire and smoke effects on critical exposed groups such as rail patrons. Potential precautions should only be rejected if they are considered grossly disproportionate to the benefits they provide. If more detail is considered useful risks may be quantified to better understand potential safety and financial impacts. In this manner the requirement to quantify risks under the ONRSR guidelines [8, 13] may be addressed without require risk tolerability criteria in an attempt to justify no further measures being reasonable.

19 CHALLENGES

Although the process detailed above is straightforward, it brings to the fore the requirement for designers, owners and operators of complex rail safety systems to use their judgement in safety-related decisions. This understanding is crucial, as ignoring or not making a decision is not viewed kindly after an event.

Resistance to this can be addressed through clear discussions of the process to be followed and how it helps persons responsible for making judgements build defensible decision trails.

We address this through project briefings given at stakeholder meetings and interviews early in each assessment. The earlier stakeholders are comfortable with the process to be undertaken, the smoother the assessments tend to go, particularly where challenges are presented by different codes or standards that have conflicting safety measures.

Challenges presented by conflicting standards have been discussed elsewhere in this paper.

The question of quantification of risks also arises at times. In general quantification is useful as a basis for comparison, for example, to estimate the effectiveness of two competing options in order to select one.

However it is not often of benefit to quantify all risks as, firstly, it can provide a false sense of confidence in predictions of the future, and secondly, the amount of detail used may impede clear communication of safety-related decisions if not undertaken with care and discretion.

The use of measures such as the value of statistical life, gross disproportionality factors and the comparison factors between fatalities and different levels of injuries can also raise difficult questions post-event. Whilst these approaches provide a means of decision-making, they often contain underlying assumptions that may not be applicable to specific scenarios.

Although quantification may in some cases be mandated [eg 8, 13] the process demonstrated above provides a context in which it can be applied to the risks where it will enhance rather than cloud the decision-making process.

20 CONCLUSION

This paper discusses the current approach to the design of rail tunnel fire safety systems. Through discussion of the issues arising from current practices and presenting an alternative approach which we believe presents a more rigorous, explicable and diligent argument as to what may be considered ‘reasonably practicable’, we hope to enhance the state of the art in rail tunnel fire safety system design, as well as in wider contexts.

21 ACKNOWLEDGMENT

The authors gratefully acknowledge the valuable discussions with Peter Johnson of Arup on the ideas presented in this paper.

22 REFERENCES

1 Model Work Health and Safety Act, 2012


11 Henderson, L; Barber, D; Johnson, P; Do rail tunnels require mechanical tunnel ventilation for smoke management? World Tunnel Congress; San Francisco, USA, April 22-28, 2015.

12 Henderson, L; Kollevris, V; Caplan, M; Inglis, S; Passenger Rolling Stock – Blast, Fire, Passenger Flow and Intercar Doors, CORE, Adelaide, May 2014.


