

LESSONS FROM CAUSE-CONSEQUENCE MODELLING FOR TUNNEL EMERGENCY PLANNING

Richard M Robinson, Risk & Reliability Associates, Melbourne, Australia
Gaye E Francis, Risk & Reliability Associates, Melbourne, Australia
Kevin J Anderson, Risk & Reliability Associates, Melbourne, Australia

ABSTRACT

The use of vulnerability assessments supported by cause-consequence models to assess risk in tunnels seems a peculiarly efficient form of 'due diligence' demonstrating that it is vital to give priorities to measures that will address matters before loss of control can occur. Regulators and corporate lawyers seem to find them attractive. A sample tunnel vulnerability assessment is presented together with a cause-consequence model (a form of combined fault and event tree) of a heavy commercial vehicle fire (50 MW) for a longitudinally ventilated tunnel. Such models show that automatic fire control systems like automatic deluge systems provide superior risk reduction for fires in stalled traffic compared to manually activated deluge and emergency longitudinal air handling systems, the usual design for Australian tunnels.

1.0 INTRODUCTION

There appears to be no single agreed approach to tunnel design and fire protection. Even within Australian states there appear to be different criteria and approaches. Australia has limited experience with long tunnels and then only for a comparatively short time compared to Europe especially. Australian tunnels provide deluge systems, which is not the overseas norm. Small fires occur regularly in Australian tunnels but there have been no recorded large fires to date. The performance of Australian tunnels for large fires appears to be empirically untested.

The conventional approach to tunnel risk management in Australia is exemplified by the "Emergency Response and Incident Management Plan" developed by the Roads and Traffic Authority of New South Wales. Risk assessment and mitigation strategies are nowadays developed through the Environmental Impact Statement (EIS) process and embodied in prescribed standards and services. For example, 50 MW maximum single incident hydrocarbon fire is to be fully controlled by mechanical ventilation and smoke control systems.

The authors note that until recently, Australian road safety authorities have not adopted a risk based approach. In addition to the generic Australian Risk Management standard AS 4360, reference can be made to transport domain standards such as AS 4292 (railways); the functional safety standard AS (IEC) 61508; tunnel specific standards such as NFPA and PIARC; the technological risk analysis standard AS/NZS 3931:1998 and the International dependability standards for failure mode and effects analysis, fault tree analysis, reliability block diagrams and human reliability as well as various defence standards applicable to the safety assessment process.

2.0 DUE DILIGENCE

Senior decision makers and the courts require a demonstration that all practicable reasonable precautions are in place. The underlying issue is that if something untoward occurs the courts immediately look to establish (with the advantage of 20:20 hindsight) what precaution/s that should have been implemented weren't. Risk is not strictly relevant since, after the event, likelihood is not relevant. It has happened. As an Australian judge has been reported as noting to the engineers after a recent train incident; "What do you mean you did not think it could happen, there are 7 dead".

That is, the notion of risk is really only used to test the value of the precaution it is claimed ought to have been in place. How risky a situation is before the event is not germane.

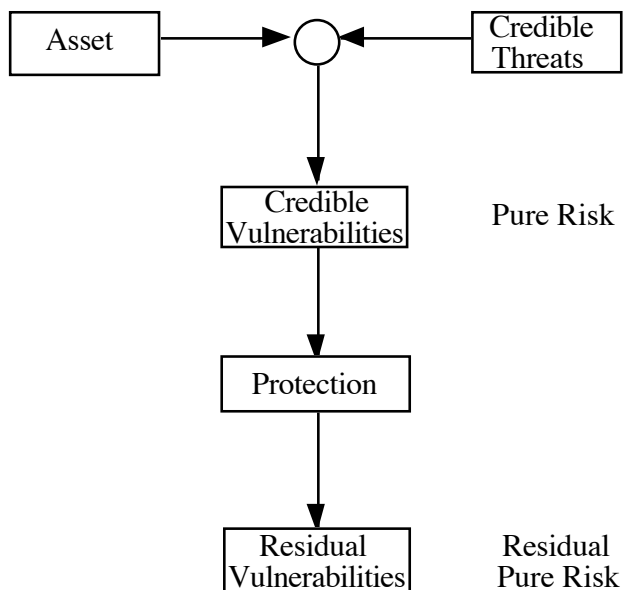
This means risk control is primarily focussed at rare, high consequence events. Arguments capable of legal scrutiny need to be developed. There are multiple possible arguments. The R2A position is documented in the R2A Text and also in the Institution of Engineers Safety Case Guideline available online through Engineers Australia (<http://www.engaustralia.com.au/epub.html>).

Two of the more persuasive techniques are vulnerability assessments and cause-consequence modelling.

3.0 VULNERABILITY ASSESSMENTS

Vulnerability assessments are a form of top down completeness check. Historically they are derived from military intelligence approaches. The vulnerability process can be shown as a simple flow chart.

Figure 1: Vulnerability Assessment Process



The power of the process rests on the fact that if all those 'assets' to be protected have been identified and all the credible 'threats' have been addressed, then there is a completeness check of the issues that must be addressed. Bottom up hazard based approaches find this difficult.

Table 1: Criticality Scoring System

xxx	Critical potential vulnerability that must be (seen to be) addressed
xx	Moderate potential vulnerability
x	Minor potential vulnerability
-	No detectable change in risk
va	Possible value adding

A vulnerability workshop can easily identify 10 assets and 10 threats resulting in 100 possible vulnerabilities. This can easily result in information overload. However, if a preliminary criticality assessment is made, that is a form of consequence analysis, then this figure is typically cut to around 10%. A preliminary criticality determination is made using the values in Table 2.

A very reduced sample for a tunnel is shown in Table 2 below. Note in this instance no items were assessed as 'value adding' (va) as the concerns were focussed on unwanted events for which there is no 'upside'.

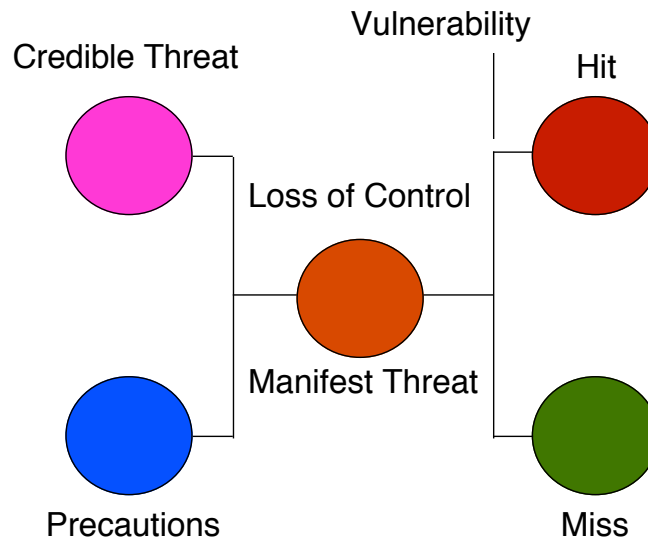
Table 2: Sample Vulnerability Table Note: Refer Table 1 for x, xx, xx notation

VULNERABILITIES exist at the intersection of assets (listed in columns) and threats (listed in rows)	ASSETS					
	Travelling Public Including Disabled, Elderly, small children, people who behave erratically	Operator Staff Including contractors, Breakdown services	Emerg- ency Services Fire brigade, ambulance and police	Local Residents	Habitat/ Environ- ment Air quality	Infra- structure & Third Party
THREATS						
Motorcycle breakdown	x	x	-	-	-	-
Passenger car breakdown	x	x	-	-	-	-
Bus Breakdown	xx	x	x	-	-	-
HCV load fire stationary vehicle in free flowing traffic	xx	xx	xxx	x	x	x
HCV vehicle fire burning vehicle in stalled traffic	xxx	xxx	xxx	x	x	x
Injury/entrapment accident - all lanes blocked	xx	x	x	-	-	-
Fatal accident - all lanes blocked	xx	x	x	-	-	-
Pedestrians in Tunnel on walkway	x	x	x	-	-	-
Cyclist in Tunnel	xx	x	x	-	-	-

4.0 CAUSE-CONSEQUENCE MODELLING

A concept cause-consequence diagram shown below (also see R2A Text Chapter 6). As will be noted it is a form of fault – event tree connected by the loss of control point.

Figure 2: Concept Cause-Consequence Diagram



To fully describe this model requires 3 parameters, threat likelihood, precaution failure probability and the hit and miss balance (degree of vulnerability). If the uncontrolled threat (the central "loss of control") affects the vulnerability, then there is a balance of probability between the null incident (near miss) and escalation of losses and accident severity leading potentially to a catastrophic outcome.

The loss of control point is a legal concept. It has been tested with numerous lawyers by R2A on many occasions. For example, with regards to airspace collision risk it is the point at which the two aircraft collision envelopes overlap. That is, become so close that the pilots cannot avoid each other (Jones et al). It does not mean that they will collide. In fact the collision envelope is large compared to the aircraft. It's just that the pilots have lost control over the outcome.

For level crossings it is the point at which the vehicle approaching the level crossing has inadequate stopping distance (R2A Text Chapter 6).

In terms of due diligence, the lawyers/courts always focus on the prevention side first. Trying to restore control after the event is always difficult. This actually parallels the OHS hierarchy of controls: elimination/engineering, administration and PPE (personal protective equipment). The latter can only be adopted if the other options are not viable.

Viable in this sense seems to mean the common law test of negligence. That is, the balance of the significance of the risk verses the effort required to reduce it. As cause-consequence models invariably demonstrate, control before the loss of control point is the only way to reliably prevent large scale multiple life loss scenarios when large energies and many people are involved.

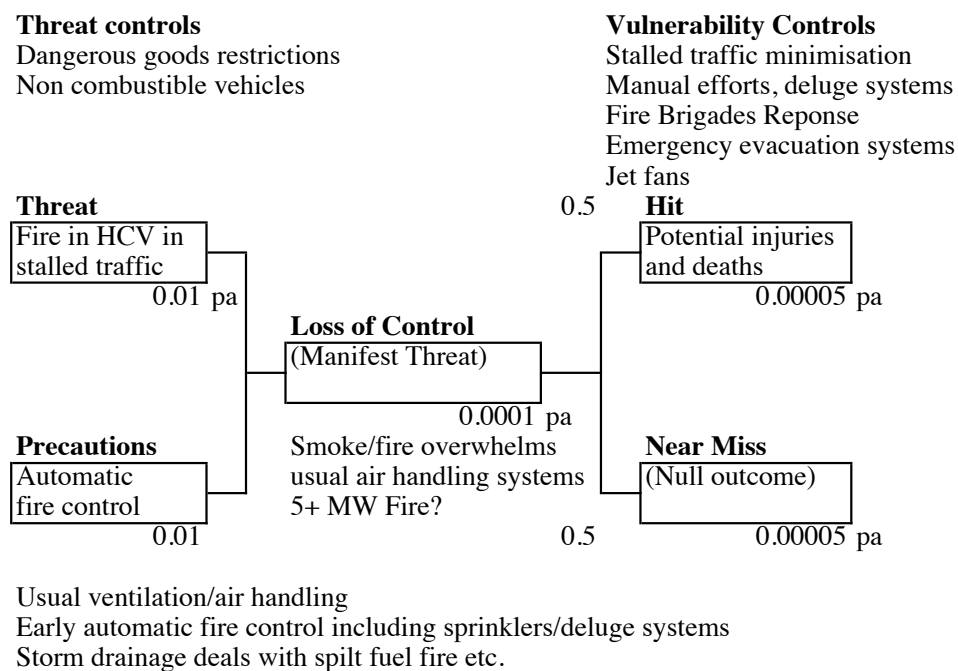
In practice, in ensuring no loss of control, at least three assessment levels of precautions need to be considered:

- i) Not less safe – comparison with the current situation
- ii) Best practice - what other organisations and comparable industries do to manage similar threats
- iii) As low as reasonable practicable - the balance of the significance of an additional precaution of defined safety integrity level versus its cost (a legally difficult process).

4.0 TUNNEL CAUSE-CONSEQUENCE MODELS

The figure below shows a preliminary cause-consequence model for a fire in a heavy commercial vehicle (HCV) in stalled traffic in a long two tunnel system using longitudinal emergency ventilation (jet fans).

Figure 3: Preliminary Cause-Consequence Model for HCV Fire in a Tunnel in Stalled Traffic



Loss of Control Point

The loss of control point appears to be that fire which overwhelms the usual air handling system. There are several arguments for this. The simplest, legally, probably revolves around confined spaces. The tunnels should only have sweet, decent air whenever they are occupied, even during a fire/smoke incident. Otherwise they would be considered a confined space. Emergency ventilation to prevent a situation becoming a confined space is an attempt to restore control and acts after the event.

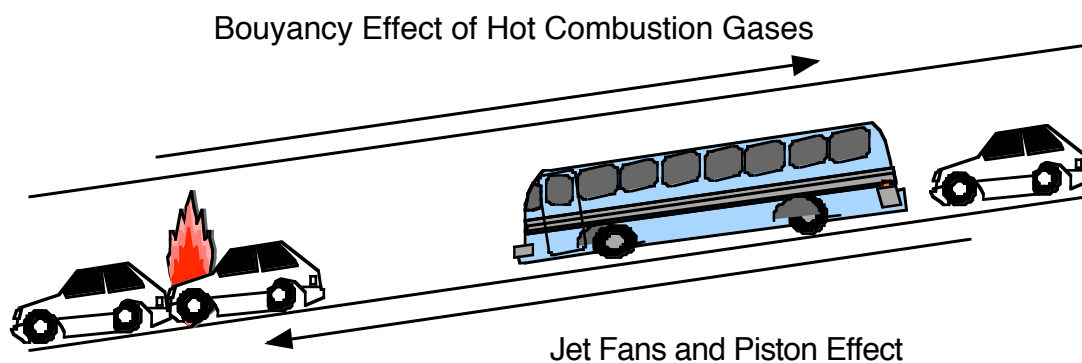
On an open freeway a fire is mostly an isolated event since the heat and smoke goes up and exposed persons (beyond those trapped in the vehicle/s) basically stay away from the inferno

until the brigade arrives or the fire burns out. In a tunnel this is potentially far more problematic because of the contained environment. Even an unmanaged 5 MW fire can create substantial problems for persons remote from the fire unless special precautions are taken. This means that it is the change of the tunnel environment by the fire that creates the loss of control.

Another way to think of this relates to different size fires in the tunnel. Suppose that a car engine catches on fire, the driver pulls over and a passing truck driver stops and extinguishes the fire with a fire extinguisher. Other than the lane restriction and the possibility of collision, from the point of view of the tunnel environment, there has been no loss of control since the smoke and heat will have been dissipated in the overall tunnel air movement (piston effect of cars and the jet fans etc).

However, there is a certain size fire that will disrupt the air flow, place remote persons at risk and thus bring about the need to impose emergency measures including an emergency ventilation system and the like. This appears to be the loss of control point.

Figure 4: Fire in Downward Facing Tunnel



Since tunnels can slope, cars travel in different directions and hot air rises, the fire loss of control point for two tunnels is potentially different. It is likely to be more severe in the tunnel where vehicles travel downhill. As suggested in the diagram above, fire in the downhill tunnel is far more likely to produce turbulence and mixing.

There are three primary risk control regions.

Threat Reduction

Firstly, threat reduction, in this case reduce the source of fire, for example, combustible trucks with large combustible loads. Small fires in any vehicle may occur once every two months, in a heavy commercial vehicle, say once per 10 years and in stalled traffic say once in 100 years.

Precautions

Secondly, precautions such as deluge systems that can control fire before the normal air handling system is overloaded (small fires are safe fires). A further consideration is the size of the uncontrolled fires. If the environment can be designed to manage, say a 5 MW fire and, for example, the proposed deluge system could be relied upon to control the fire 99% of the occasions on which it is called upon to act. Automatic activation is probably required to

achieve such reliability. In legal terms this may be considered to be beyond reasonable doubt?

Vulnerability Reduction

And thirdly, reduce vulnerability by ensuring no one is present during a fire (minimal stalled cars) and the provision of emergency response, ventilation and evacuation systems.

Three key scenarios appear on the consequence side.

- a) Low congestion meaning there are minimal vehicles around.
- b) Some congestion meaning vehicles stop behind the fire but those in front of the fire drive out which makes the jet fan emergency mode desirable since the smoke can be blown away from the stopped traffic.
- c) High congestion with stalled traffic meaning there are stopped vehicles both before and after the fire. This makes the use of the longitudinal (jet fan) emergency mode problematic since it would blow smoke over one column of stopped traffic hampering evacuation. That is, with stalled traffic and longitudinal emergency ventilation, a heavy commercial vehicle fire will expose a large number of people who would have to evacuate through a smoky environment on foot. To reliably achieve this is very, very difficult.

6.0 DISCUSSION

In the Australian context, some form of deluge protection is the norm. This is the option adopted by CityLink (Yarra River Tunnel in Melbourne) amongst others. Essentially a manually operated deluge (drencher) sprinkler system is provided, typically covering a 20 m section of a tunnel. On activation this whole 20m *slice* of the tunnel is provided with a spray of water averaging around 10 mm per minute. Such a system can be actuated remotely or locally. Thermal fire detection systems are provided to enable accurate identification of the position of the fire.

The proponents of this approach generally expect that the system will not be actuated until all persons in the tunnel are safely evacuated. The view is that all the combustion gases from the fire remain buoyant and above the heads of any person in the tunnel. Once such a system actuates, the hot gases will be cooled and fall placing any persons on the ground at risk. Spurious, hazardous activation such as may occur with automatic systems is eliminated.

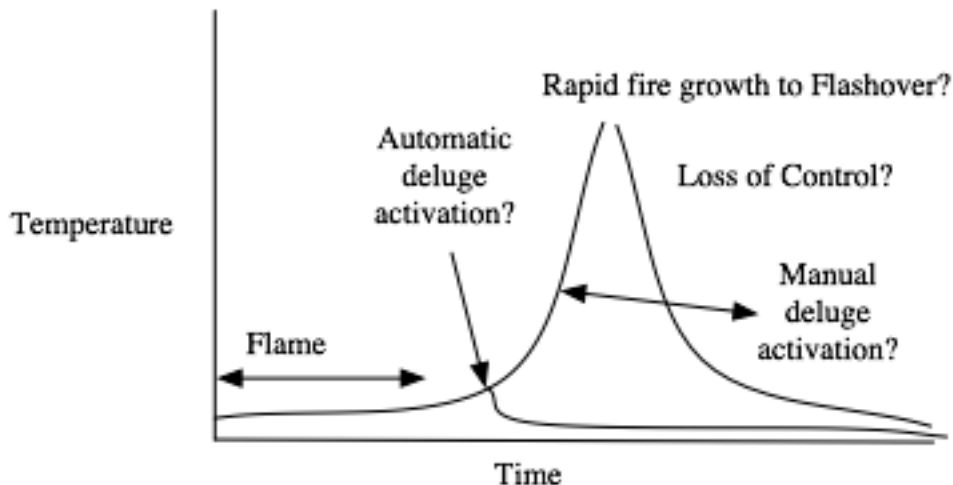
A supplementary argument often is that the presence of such a system means that the maximum size of fire that needs to be designed for can be reduced from 50 MW to 25 MW.

The issue being considered in this paper is whether or not the deluge system should be automatic. The authors favour the automatic deluge option. Figure 5 shows a representative fire curve summarising the argument.

There appears to be an empirical connection between the size of a fire and the number of deaths. That is, small fires are less likely to kill people. The larger the fire the less room for error there will be in any emergency response. With automatic operation, early in the

development of a fire, small fires should be the norm. That is, flashover (well after the loss of control point) should not occur. As Kumar (1992) comments; *It is the pre-flashover stage which is the most relevant to life safety, for, if escape is not completed then, there is no chance after flashover.*

Figure 5 Representative Fire Curve



This argument is particularly powerful if there is stalled traffic in long tunnels with longitudinal ventilation. If the fire has achieved flashover the smoke has to be blown one way or the other potentially exposing up to half the tunnel occupants.

The lawyers (and regulators to whom such arguments have been presented) have always confirmed that precautions implemented before the loss of control point are the best place for the precautionary dollar. Complex, expensive, hard to model and unpredictable emergency measures invoked after the loss of control point attempting to bring a situation back under control are legally difficult to defend, especially when a sensible pre-loss of control point precaution was available.

Obviously it is necessary to acknowledge and verify the reliability of the actual automatic systems that are proposed. In part, this is to address the accidental discharge question. Complex systems require commensurate safety assurance, such as through obtaining a Safety Integrity Level (SIL) pursuant to the Functional Safety Standard IEC (AS) 61508. Further, such automatic activation does not preclude manual intervention in the automatic sequence if required.

7.0 CONCLUSIONS

- 7.1 The combination of vulnerability assessments as a completeness check and cause-consequence modelling as a due diligence design tool seems to be attractive to Australian lawyers and regulators.
- 7.2 It is vital to give priorities to measures that will address matters before loss of control can occur.

The use of cause-consequence models suggest that:

- 7.3 Automatic fire control systems like automatic deluge systems provide superior risk reduction for fires in stalled traffic compared to manually activated deluge and emergency longitudinal air handling systems, the usual design for Australian tunnels. Provided auto-activation of the deluge system is reliable, then it should be provided in road tunnels. If provided, the possibility of a large fire occurring (5 MW to 50 MW and above) seems small.
- 7.4 Congestion management appears as the more desirable form of emergency control rather than ventilation systems capable of controlling up to 50 MW or larger fires. That is, full height smoke and heat exposure to un-evacuated persons downstream (stalled traffic) of large fires does not appear legally defensible.

8.0 REFERENCES

Fire Code Reform Research Program (1998). *Fire Safety in Shopping Centres*. Final Research Report, Project 6. Available from Standards Australia.

Kumar S (1992). *Fire Development and Smoke Spread in Tunnels - Some Modelling Considerations*. Safety in Road and Rail Tunnels Conference, Basle Switzerland, Nov, 1992.

Jones K, K Anderson, W Ely and R Phillips (1995). *Application of Risk Analysis to Airspace Planning*. Review of the General Concept of Separation Panel (RGCSP), ICAO, Gold Coast, Australia.

Massachusetts Highway Department, Federal Highway Administration (1996). *Memorial Tunnel Fire Ventilation Test Program*. Interactive CD-ROM & Comprehensive Test Report.

PIARC Committee on Road Tunnels (1995). *Road Safety in Tunnels. 05.04.B - 1995*

PIARC. *The risk of the transport of hazardous materials in tunnels 20.04.B - 1995* pages 43 - 55

Risk & Reliability Associates Pty Ltd (1999). *Fire Engineering Study*. Inner City ByPass Project. Brisbane City Council.

Robinson Richard M, Kevin J Anderson et al (2002). *Risk & Reliability - An Introductory Text* 4th Edition. (The R2A Text). Risk & Reliability Associates Pty Ltd, Melbourne.

SAE ARP 4761:1996 *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

Standards Australia/Standards New Zealand (1999). *Risk Management*. Australian/New Zealand Standard AS/NZS 4360:1999.

Standards Australia (1999). *Functional Safety of electrical / electronic / programmable electronic safety related systems*. Par 6.5: Examples of methods for the determination of safety integrity levels AS 61508.5 – 1999 / IEC 61508.5 – 1998.