
DUST EXPLOSIONS 2005 – Panthers World of Entertainment

ENSURING DUE DILIGENCE FOR THE MANAGEMENT OF TECHNICAL RISK

Richard M Robinson, Director, Risk & Reliability Associates, R2A Pty Ltd

ABSTRACT

Senior decision makers focus on large events. In safety terms they require confidence that all the big, potentially unpleasant issues have been competently addressed. This requires a completeness argument (usually a logical rather than a scientific argument) that all credible, critical issues have been addressed (the essence of due diligence). Explosion is one threat amongst many for most industrial facilities. Simply addressing explosion risks alone is not sufficient from a due diligence perspective. A range of risk management techniques and approaches are available and ought to be applied. A brief description of those noted in the Engineers Australia (Victoria Division) Safety Case Guidelines is described. One in particular, vulnerability assessments supported by cause-consequence modelling and reliability modelling, has proved very successful in obtaining legal sign off for major infrastructure project risks (including fire and explosion) in most Australian jurisdictions.

1.0 INTRODUCTION

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 (Robinson & Anderson et al, Fifth Edition 2004) and also in the Institution of Engineers Safety Case Guideline available online through Engineers Australia (<http://www.engaust.com.au/bookshop/epub.html>).

2.0 ENGINEERS AUSTRALIA SAFETY CASE GUIDELINES

A safety case is a documented demonstration by an organisation of the way in which hazards at a facility are managed to ensure an acceptable risk. It typically consists of a number of arguments, all converging on a single conclusion: 'The system meets its safety criteria and is therefore acceptably safe to be allowed to operate in accordance with its defined objectives and procedures.'

However, impact of the adversarial legal system on the development of safety cases appears to be moving them from being strictly a technical safety management tool to an approach that includes liability management devices. Effectively they have become a legal argument as to why an organisation believes that there are no outstanding precautions appropriate to their particular facility or operation that ought to be implemented.

To act effectively as both a technical and liability management tool, a safety case needs to have an initial argument for the approaches selected to demonstrate effective safety management.

Eight paradigms for assessing risk and three inquiry methods of "risk sign off" are described in the table below.

Technique>>> Risk Management Paradigm		Expert reviews	Facilitated workshops	Selective interviews
0.	The rule of law	Yes (Legal opinions)	Yes (Arbitration, moot courts)	Yes (Royal Commissions)
1.	Insurance approaches	Yes (Risk surveys, Actuarial studies)	Yes (Risk profiling sessions)	Yes (<i>especially moral risk</i>)
2.	Asset based, 'bottom-up' approaches	Yes (QRA, availability & reliability audits)	Yes (HazOps, FMECAs etc)	Difficult
3.	Threat based 'top- down' approaches	Difficult in isolation	Yes (SWOT & vulnerability)	Yes (Interviews)
4.	Business (upside AND downside) approaches	Yes (Actuarial studies)	Difficult in isolation	Yes (Fact finding tours)
5.	Solution based 'good' practice' approaches	Difficult to be comprehensive	Difficult to be comprehensive	Yes (Fact finding tours)
6.	Simulation	Yes (Computer simulations)	Yes (Crisis simulations)	Difficult
7.	Risk culture concepts	Yes (Quality audits)	Difficult	Yes (Interviews)

Risk Management Paradigm - Technique Matrix

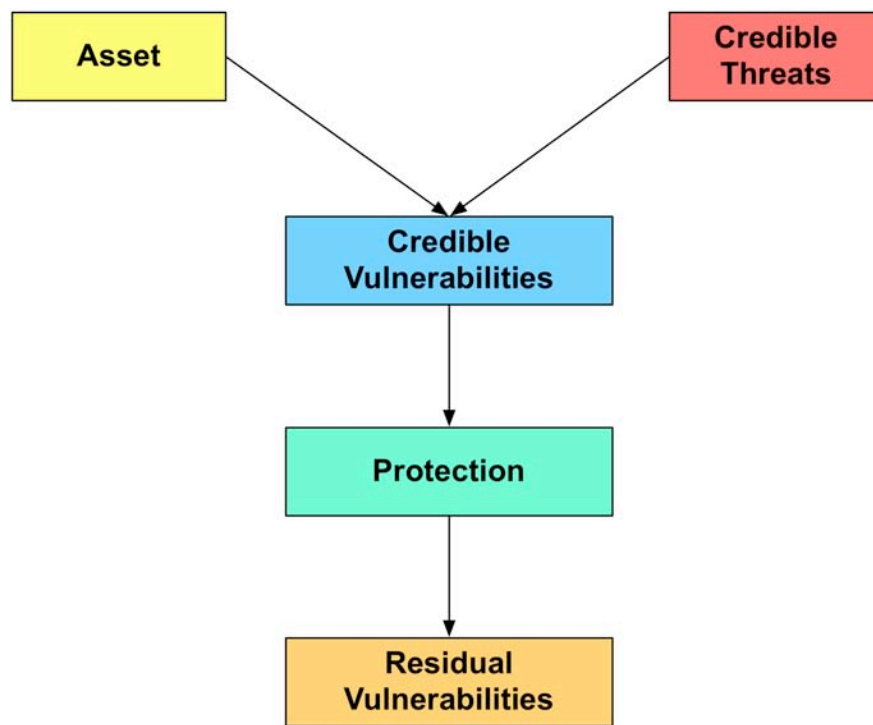
The techniques and paradigms highlighted in the table would be the suggested minimum to be used in developing a safety case. The opening argument of the safety case should be which of the approaches are to be adopted and why.

The methods applied in generating a safety case will depend on the organization and project under consideration. The choice will depend on a number of factors including the hazards, the technology, along with the business and legal environments.

One of the more persuasive techniques is threat and vulnerability assessments supported by cause-consequence modelling and reliability modelling.

3.0 VULNERABILITY ASSESSMENTS

Vulnerability assessments are a form of top down completeness check. Historically they are derived from military intelligence approaches (Australian Defence Force). The vulnerability process can be shown as a simple flow chart. The technique is described in detail in the R2A text, especially Chapter 9.



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.

If a matrix of assets and threats is established on a spreadsheet then a single representation of the risks associated with a project can be made. However, there are two complications.

Firstly, a 10 x 10 matrix yields 100 potential vulnerabilities. Information overload is nigh. The simplest and legally most appropriate way to deal with this is to undertake a preliminary criticality analysis first. The reason is twofold. Likelihood is probably unknown at this time. But if the threat is credible and the consequences of its manifestation critical then it must be managed. It is otherwise a potential *show stopper* at many levels probably including the law.

Secondly, there is a tendency for the assets and threats to overlap creating unnecessary complexity and confusion. However, if an initial criticality assessment is completed it usually becomes obvious that such overlapping has been made since duplicate patterns of criticality arise. Moreover, proposed precautions address many potential vulnerabilities at once.

Criticality

A preliminary criticality determination can be made using the values in the table below.

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

Table of Criticality Values

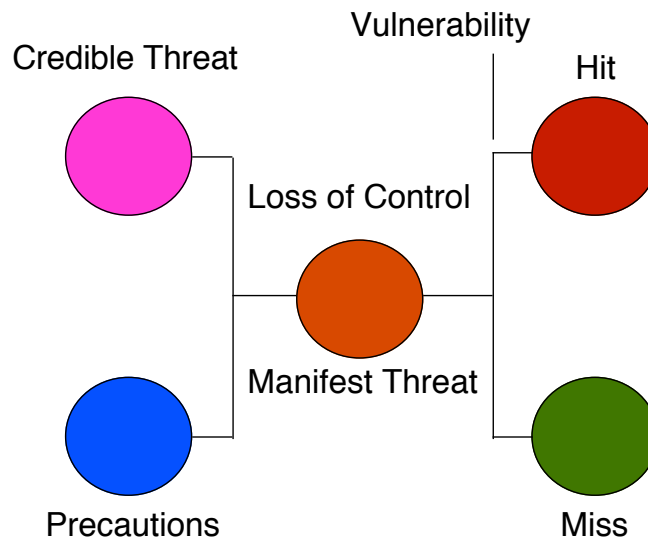
Several sample vulnerability matrices follow. If this is correctly done then around 10% or so of the cells will have three x's. This is the Pareto principle. Typically 80% to 90% of the risk comes from 10% to 20% of the vulnerabilities. Dealing with the 10 to 20% is the primary purpose of the analysis. A very reduced sample for a tunnel adapted from Robinson, Francis & Anderson (2003) is shown in the table below.

Assets>>	Travelling Public Including Disabled, Elderly, small children, people who behave erratically	Operator Staff Including contractors, Breakdown services	Emergency Services Explosion brigade, ambulance & police	Local Residents	Habitat/ Environment Air quality	Infrastructure & Third Party
Threats						
Motorcycle breakdown	x	x	-	-	-	-
Passenger car breakdown	x	x	-	-	-	-
Bus Breakdown	xx	x	x	-	-	-
Heavy commercial vehicle (HCV) load fire: stationary vehicle in free flowing traffic	xx	xx	xxx	x	x	x
HCV vehicle fire; burning vehicle in stationary 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	-	-	-

Sample Vulnerability Table

4.0 CAUSE CONSEQUENCE MODELLING

A concept cause-consequence diagram shown below (also see the R2A Text Chapter 9). As will be noted it is a form of fault – event tree connected by the loss of control point.



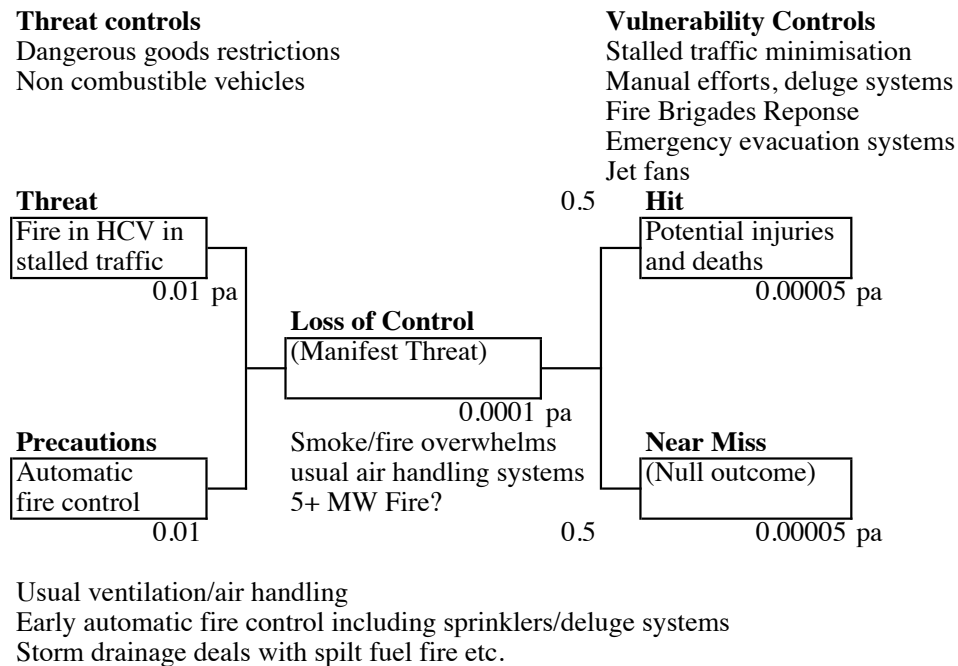
Concept Cause Consequence Diagram

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, Anderson and Phillips). 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.

5.0 FIRE IN TUNNEL EXAMPLE

The following example is summarised from Robinson, Francis & Anderson (2003). 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).



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

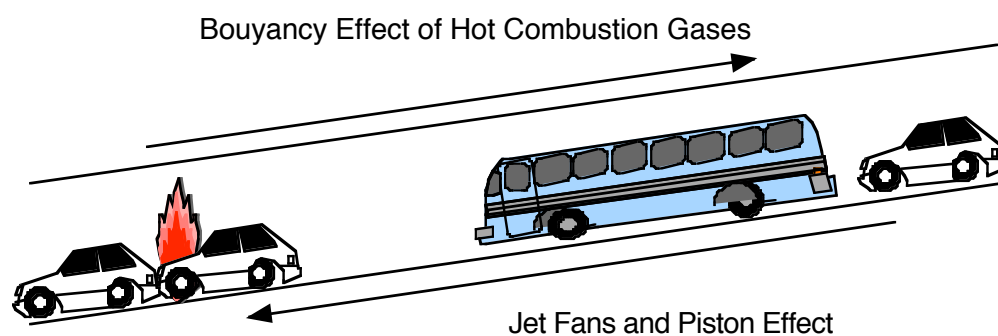
5.1 Loss of Control Point

The loss of control point appears to be a fire which overwhelms the usual air handling system. There are several arguments for this. The simplest, from a legal standpoint, 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.



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 down tunnel is far more likely to produce turbulence and mixing.

5.2 Primary Risk Control Regions

There are three primary risk control regions.

5.2.1 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.

5.2.2 Precautions

Secondly, precautions such as deluge systems that can control a 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?

5.2.3 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.

The critical scenario is 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 a safe evacuation is very, very difficult.

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.

5.3 Reliability of Automatic Systems

Obviously it is necessary to acknowledge and verify the reliability of the actual automatic systems that are proposed. Complex systems require commensurate safety assurance, such as through obtaining a Safety Integrity Level (SIL) pursuant to the Functional Safety Standard IEC (AS) 61508. The Functional Safety standard IEC 61508:1998 and now also AS 61508:2000 sets out requirements for electrical/electronic and programmable electronic (E/E/ES) systems. A system is said to be safety-related if any failure to function can present a prospect of harm to people.

SIL (Safety and Integrity Level) ratings after IEC 61508:1998 are used to characterise the required functional safety of computer control systems. SIL is a measure of the probability that the safety related system will fail dangerous. The value of SIL ranges from 1 (the lowest) to 4 (the highest). The table below is adapted from IEC 61508-1:7.6.2.9; via Factory Mutual.

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its designed function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

SIL Targets

For example, SIL 4, the highest rating is for fly by wire aircraft and weapons systems and SIL 3 is typical of track circuited train signalling systems. Explosion / fire systems have not been SIL rated to date even though organisations like Factory Mutual provide SIL ratings for various PLCs in their approvals guides.

SIL ratings are a powerful performance based safety statements. They are being quoted in emergency control systems for tunnels and other major infrastructure works and are thus defining fire control system performance in some instances. Yet fire and explosion control systems are not SIL rated. The issue as to whether SIL ratings ought to be provided for fire / explosion systems and fire control panels in particular is becoming integral with the reliability determined in cause-consequence models. Why shouldn't fire systems and panels be SIL rated if all the other control systems of a major facility are SIL rated? Recent private communications with FM Approvals in Norwood, Massachusetts (David Baer, 2003), confirms that fire panels are not yet SIL rated but that they ought to be.

However, instances of product compliance remain rare and certification can add considerably to the cost of a product. For example, the Allen Bradley range of programmable logic controllers (PLC) are certified by TUV, Germany. (www.ab.com/logix/controllogix/sil2.html). Certification includes field data to confirm reliability metrics including Mean Time Between Failures (MTBF) and independent analysis of Safe Failure Fraction and probability of Failure on Demand. TYPE approval includes restricted sub-sets of programming languages and Coding Standard.

Such certification can considerably increase costs and industry has been reluctant to follow such leads. Critics of the standard have also been strident. For example, O'Connor (2002):

The standard (IEC 61508) is without practical value or merit. The methods described are inconsistent with accepted industry practices, and many of them are known only to specialist academics, presumably including the members of the drafting committee.

As a contractually enforceable document, the authors agree with O'Connor, unless there is some form of third party certification such as TUV Germany or Factory Mutual USA which provides an agreed interpretation.

Alternately, the standard can be employed to conduct an independent Functional Safety Assessment (FSA) taking an inquisitorial approach. This role, pursuant to part 1 clause 8 is 'to investigate and arrive at a judgement as to the level of functional safety afforded by the safety-related system'. This should take account of necessary risk reduction afforded by external risk reduction facilities (ERRF) and other technology. This is a very continental inquisitorial approach as opposed to an adversarial approach. A functional safety assessor goes in search of evidence until sufficient has been gathered to come to a judgement. It is very European way of fighting the liability dragon. It often seems difficult to understand for those in an adversarial liability system.

6.0 CONCLUSIONS

Explosion is one threat amongst many for industrial facilities. Simply addressing such risks in isolation is not sufficient from a due diligence perspective. Senior decision makers and the courts require a demonstration that all practicable reasonable precautions are in place. Risk is not strictly important since after the event, likelihood is not relevant. In court the notion of risk is practically used to test the value of possible precautions.

A range of risk management techniques and approaches are available and ought to be applied such as those noted in the Engineers Australia (Victoria Division) Safety Case Guidelines. A combination of vulnerability assessment, cause-consequence modelling and reliability modelling is useful to address the threat of fire or explosion and assess the efficiency of precautions.

SIL ratings (Safety and Integrity Levels) are being used in a large number of risk situations and are impacting fire protection systems. They are being used to provide independent reliability and available targets in turn providing excellent support to the technical risk business generally including process controls and emergency response systems.

However, fire control systems are not generally SIL rated. In view of the widespread use of SIL ratings in the process industries and that functional safety assessors are being required to determine the SIL ratings of fire systems during the design of emergency management systems for large infrastructure projects, it would seem desirable for the fire protection industry to come to grips with the concept promptly.

7.0 REFERENCES

Australian Defence Force (1998). *Joint Military Appreciation Process*, Chapter 8. ADF Canberra.

Baer David (2003). FM Approvals in Norwood, Massachusetts. Email dated 4 June 2003.

Engineers Australia , Risk Engineering Society, Victorian Chapter (2002). *Safety Case Guidelines*. Engineering Guidelines Online. (<http://www.engaust.com.au/epub.html>)

Factory Mutual Research Approval Guide (2001). Chapter 4. *Functional Safety of Safety Related Systems and Components*.

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.

International Electrotechnical Commission (1998). *Functional safety of electrical / electronic / programmable electronic safety-related systems*. IEC 61508:1998. Also known as AS 61508:2000.

The Institute of Electrical and Electronics Engineers, Inc. (1980) *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. IEEE Std 493-1980.

O'Connor Patrick D T (2002). *Practical Reliability Engineering*. John Wiley & Sons. Fourth Edition.

Robinson Richard M, Kevin J Anderson et al (2004). *Risk & Reliability - An Introductory Text*. 5th Edition. (The R2A Text). Risk & Reliability Associates Pty Ltd, Melbourne.

Robinson Richard M, Gaye E Francis, Kevin J Anderson (2003). *Lessons from Cause-Consequence Modelling for Tunnel Emergency Planning*. Proceedings of the Fifth International Conference on Safety in Road and Rail Tunnels. University of Dundee. pp 149-158. ISBN 1 901808 22 X.

Standards Australia/Standards New Zealand (2004). *Risk Management*. Australian/New Zealand Standard AS/NZS 4360:2004.