ENGINEERS
AUSTRALIA

Safety Case Guideline

Third edition

Clarifying the safety case concept to engineer due diligence under the provisions of the model Work Health & Safety Act 2011.

RISK ENGINEERING
SOCIETY

RISK ENGINEERING SOCIETY

Prepared by a committee of the Risk Engineering Society of Engineers Australia.
The members of the committee were:
Geoff Hurst FIEAust CPEng MSIA RSP(Aust), ENGENEOHS, Chair and Editor
Gaye Francis MIEAust, R2A Due Diligence Engineers
Richard Robinson FIEAust MSFPE, HonFAMPI, R2A Due Diligence Engineers
Robert Relf MIEAust, Australian Engineering Exports
Mark Harding AMIE FSIA RSP Aust, Regional Manager HSSE (Asia Pacific) at AT&T
Barry Miller, Miller Impact Engineering
Ian Thomas FIChemE, FIEAust, FRACI, FSIA, CEng, CPEng, CChem, RSP(Aust), I F Thomas & Associates
Sharyn Durley LLB (Barrister), Legal review

Endorsed by the Risk Engineering Society National Committee.
The members of the committee were:
Geoff Hurst FIEAust CPEng MSIA RSP, ENGENEOHS, National President
Brian Truman, Immediate Past National Chair
David Cox MIEAust CPEng RPEQ, Brisbane City Council, RES Qld Chair
Pedram Deneshmand Aquenta, Consulting Pty Ltd, RES NSW Chair
Subash Dang Engineers Australia, RES ACT Chair
Dr Edward Lewis UNSW@ADFA, Layrib PTY LTD, RES ACT Deputy Chair

Editorial Adviser: Dr Dietrich Georg

Published by Engineers Media, Crows Nest, Sydney, www.engineersmedia.com.au on behalf of Engineers Australia

Cataloguing-in-Publication entry is available from the National Library of Australia at http://catalogue.nla.gov.au/

ISBN: 9781-922107-45-9

CONTENTS

INTRODUCTION

This guideline was first authorised in 2002 by the Victorian Chapter of the Risk Engineering Society of the Institution of Engineers Australia at its committee meeting on 7 October at the Victoria Division Office in Melbourne.

The guideline was revised in 2007, also by the Victorian Chapter of the Risk Engineering Society of Engineers Australia primarily to address changes in the Risk Management Standard (2004) and the Victorian Occupational Health and Safety Regulations (2007). The revision was authorised at the Guideline Review Committee meetings of 31 May and 10 July at the Victoria Division Office in Melbourne.

This third edition of the Safety Case Guideline considers how a safety case argument can be used as a tool to positively demonstrate safety due diligence consistent with the model Work Health and Safety (WHS) legislation (Work Safe Australia 2011) and to provide general information concerning the concepts and applications of risk theory to safety case arguments. The material is used by Engineers Australia (Engineering Education Australia Pty Ltd) in its training courses on Due Diligence and Risk Management. It provides practical guidance to engineers on preparing and presenting a safety case argument.

The guideline has been developed by a working committee of the Victorian Risk Engineering Society (RES) and approved by the National Risk Engineering Society. The Risk Engineering Society has the primary purpose to assist engineers better understand and apply the concepts of risk across engineering practices and projects.

A safety case provides the structure for considering and documenting the safety argument and the consultation process with stakeholders. It verifies in a practical sense that through the eyes of a reasonable person at the time of preparation or review, all foreseeable hazards have been considered and treated for risk control (see Figure 1).

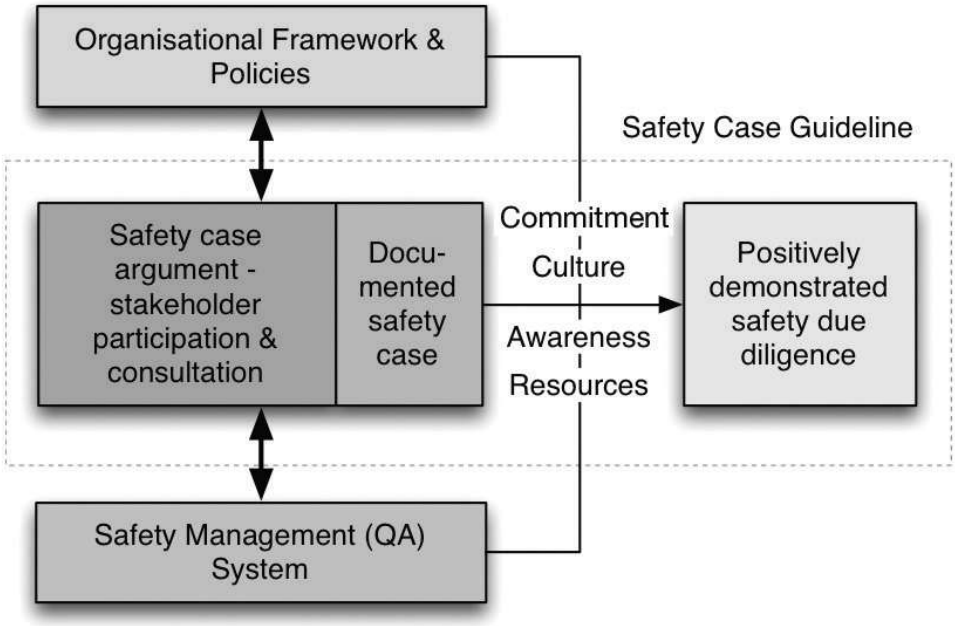

Figure 1: Safety Due Diligence Management Model (after Hurst 2002)

The safety case guideline has been developed in the context of engineering philosophy. That is, it applies a common process to safety issues whilst encouraging a collaborative, creative and innovative approach to ensure superior safety outcomes. It is not about compliance but rather governance to improve safety outcomes in a modern technological society.

The process consists of the following steps:

- What is the scope of the problem?
- Define the context in terms of the wider environment in which the scope is prepared.
- What are the optional actions available to address the scope (current and future)?
- What is the (best) optimal course of action given the current and reasonably foreseeable circumstances and wider environment?
- Implement the optimal action/s checking for effectiveness, safety and efficiency.
- Continue to monitor to ensure the safety case (scope, circumstances, wider environment and course of action) remains relevant and optimal.

Overall, a well structured, coherent safety case argument will facilitate an organisation's ability to demonstrate to others that they have a clear understanding of the factors that influence safety risk and the precautions / controls that are critical to eliminate or minimise the risks to health and safety of all people in and around the plant, process or facility so far as is reasonably practicable.

This document is not intended to be the final word. Rather it is hoped that it provides the basis for constructive discussion and thought leadership around the management and engineering of safety.

The authors accept no responsibility for any errors or omissions in the material, or for the results of any actions taken as a result of using this guideline. Users should seek their own legal counsel when developing a safety case.

SUMMARY

In reality, to be safe means to be free from harm. In court, safe means that despite something apparently unsafe having happened, due diligence has been applied and demonstrated. In engineering terms this means that to be safe requires managing the laws of nature for credible events in a way that is consistent with the requirements of the laws of man, in that order.

This third edition of the Safety Case Guideline considers how a safety case can be used as one tool to positively demonstrate safety due diligence consistent with the requirements of the model Work Health and Safety (WHS) legislation that has commenced in all Australian jurisdictions except, at the time of writing, Western Australia and Victoria. It provides practical guidance on preparing a safety case.

It adopts the precautionary principle for the demonstration of due diligence as a defence against claims of negligence, namely:

- A completeness argument as to why all credible critical safety issues affecting all parties have been identified;
- An argument as to why all *practicable* precautions for each credible critical issue has been identified;
- An argument as to which practicable precautions are *reasonable* consistent with decided court cases; and
- The establishment of a safety quality assurance regime to confirm that all *reasonably practicable* precautions are maintained on an ongoing basis.

Such an approach does not mean bad things can't happen. Apart from activities that are prohibitively dangerous, the approach above means that all reasonable practicable precautions for all foreseeable, critical hazards to all affected parties are in place, based on the balance of the significance of the risk vs. the effort required to reduce it. This also means that risks should be eliminated or minimised so far as is reasonably practicable (SFAIRP).

In a practical sense, this means that *you start with what can be done and only do less when it is reasonable to do so* (Sherriff 2011).

Such a position should provide superior safety outcomes for all and offer protection against criminal charges for responsible officers under the provisions of the model WHS Act.

It is recommended that this guideline be tested with the readers' own legal counsel before adopting this approach.

1. OBJECTIVE

The objective of this guideline is to provide practical guidance to engineers on preparing and presenting a safety case to positively demonstrate safety due diligence consistent with the requirements of the model Work Health and Safety Act.

2. BACKGROUND

What constitutes a safety case has been variously described in many places, including the earlier editions of this guideline. There are many industries in Australia including rail, gas, off-shore petroleum, aviation, electrical, mining and hazardous facilities that currently utilise a safety case concept. However, the safety case concept can be expanded to all technological industries where a robust, transparent demonstration for the management of safety is essential.

One of the least controversial in the experience of the authors is that of the English law lord Cullen. In a Transport Research Institute lecture given in Edinburgh, Lord Cullen (2001) noted that a safety case serves two purposes: to ensure adequate internal management of safety, and to provide documentation of diligence to examining parties to maintain the public confidence.

> *A safety case regime provides a comprehensive framework within which the duty holder's arrangements and procedures for the management of safety can be demonstrated and exercised in a consistent manner. In broad terms the safety case is a document – meant to be kept up to date – in which the operator sets out its approach to safety and the safety management systems which it undertakes to apply. It is, on the one hand, a tool for internal use in the management of safety and, on the other hand, a point of reference in the scrutiny by an external body of the adequacy of that management of safety – a scrutiny which is considered to be necessary for maintaining confidence on the part of the public.*

The earlier editions of this guideline encouraged the adoption of a 'common law' safety case, using the common law concept of due diligence. Nevertheless, it was recognised that at that time regulators could continue to impose the hazard based approach to safety cases using their existing enabling legislation, as statute law takes precedence over common law.

The model WHS Act now recognises the concept of a 'due diligence' approach.

In reviewing this guideline, Sharyn Durley LLB (Barrister) commented on the subject of dealing with the two methodologies apparent in the legislation: Hazard based risk assessment and/or Precaution based due diligence (see section 4).

> *It may be that the courts will modify the basis of their decisions to reflect the 'due diligence' approach. However, it is not as clear-cut in the legislation as it might appear, and it is unlikely that the intricacies of the two methodologies would be argued in isolation of the facts of a case.*
>
> *This is particularly supported by the changes in the definition of 'due diligence' in the various drafts of the legislation (see section 3).*

3. WORK HEALTH & SAFETY ACT

The model WHS Act has commenced in most Australian jurisdictions (with appropriate local provisions including relevant court and regulator), presently excepting Western Australia and Victoria. The act requires that *responsible officers* of PCBU's (*persons conducting a business or undertaking*) to positively demonstrate safety *due diligence*. Penalties are criminal in nature and can provide for up to 5 years jail for responsible officers for recklessness (knew or made or let it happen). These responsibilities cannot be delegated, although such criminal charges must be proved beyond reasonable doubt.

The meaning of *due diligence* is considered in Part 2, Division 4 (27) of the model WHS Act:

(5) In this section, due diligence includes taking reasonable steps:

(a) to acquire and keep up-to-date knowledge of work health and safety matters;

(b) to gain an understanding of the nature of the operations of the business or undertaking of the person conducting the business or undertaking and generally of the hazards and risks associated with those operations; and

(c) to ensure that the person conducting the business or undertaking has available for use, and uses, appropriate resources and processes to eliminate or minimise risks to health and safety from work carried out as part of the conduct of the business or undertaking; and

(d) to ensure that the person conducting the business or undertaking has appropriate processes for receiving and considering information regarding incidents, hazards and risks and responding in a timely way to that information; and

(e) to ensure that the person conducting the business or undertaking has, and implements, processes for complying with any duty or obligation of the person conducting the business or undertaking under this Act; and

(f) to verify the provision and use of the resources and processes referred to in paragraphs (c) to (e).

The first approved draft of the model act left *due diligence* to be determined by case law. The next cut defined due diligence to be the six points listed above. The third and subsequent revisions advised that due diligence *includes...* these six points.

This single word change is perhaps significant. For example, the Workcover Authority of NSW advises that *exercising due diligence includes, but is not limited to:* the six points listed above.

The Australian Government Comcare has provided the following definition in "Guidance for Officers in Exercising Due Diligence" under the WHS Act:

Due diligence – in the context of work health and safety – means taking every precaution that is reasonable in the circumstances to protect the health, safety and welfare of all workers and others who could be put at risk from work carried out as part of the business or undertaking.

"Reasonably practicable" is defined as follows. According to the model WHS Act (Part 2, Division 1, Section 17):

A duty imposed on a person to ensure health and safety requires the person:

(a) to eliminate risks to health and safety, so far as is reasonably practicable; and

(b) if it is not reasonably practicable to eliminate risks to health and safety, to minimise those risks so far as is reasonably practicable.

The meaning of "reasonably practicable" is defined in Subdivision 2:

18 What is reasonably practicable in ensuring health and safety?
In this Act, reasonably practicable, in relation to a duty to ensure health and safety, means that which is, or was at a particular time, reasonably able to be done in relation to ensuring health and safety, taking into account and weighing up all relevant matters including:

(a) the likelihood of the hazard or the risk concerned occurring; and

(b) the degree of harm that might result from the hazard or the risk; and

(c) what the person concerned knows, or ought reasonably to know, about:

(i) the hazard or the risk; and

(ii) ways of eliminating or minimising the risk; and

(d) the availability and suitability of ways to eliminate or minimise the risk; and

(e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk,

the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

In other words (quoting Barry Sherriff[1], one of the lawyers who helped draft the legislation), the model WHS Act:

Simply makes clear that you start with what can be done and only do less where it is reasonable to do so.

[1] Barry Sherriff (March 2011) from a presentation to Engineers Australia, Brisbane.

4. DUE DILIGENCE AND THE RISK MANAGEMENT STANDARD

The approach encouraged by the risk management standard ISO 31000 (Standards Australia & Standards New Zealand 2009) uses a hazard based approach to risk, whereas the model WHS Act follows the precautionary due diligence approach. The differences between the two approaches, especially for high consequence, low likelihood events are summarised in Figure 2 and Table 1.

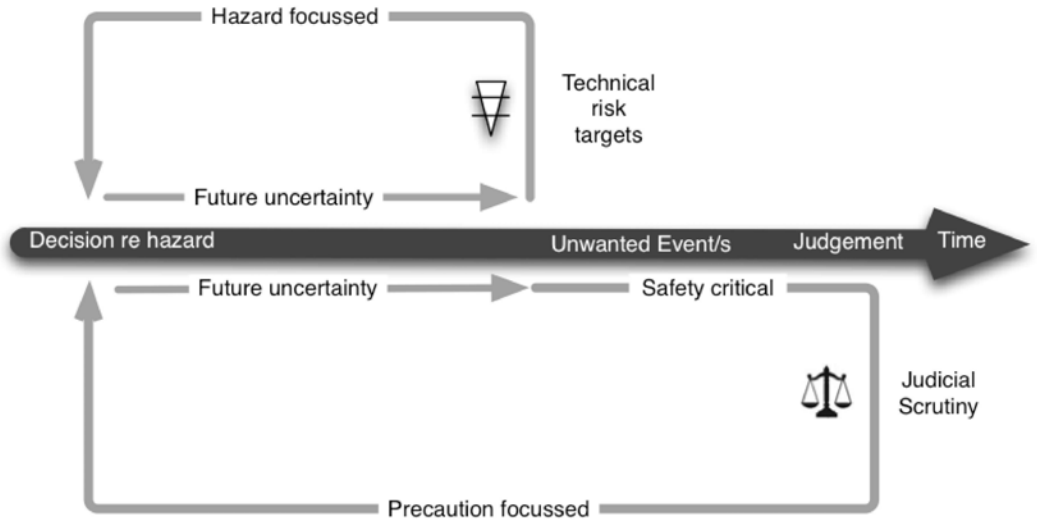

Figure 2: Precaution based due diligence vs hazard based risk assessment (Robinson & Francis et al 2013 page 26)

Table 1: Differences between the precautionary and hazard based approaches.

Precaution based due diligence (WHS Act)	**Hazard based risk assessment (ISO 31000)**
Precaution focused by testing all practicable precautions for reasonableness, that is, on the balance of the significance of the risk vs. the effort required to reduce it.	Hazard focused by comparison to acceptable or tolerable target levels of risk. From the definition in AS/NZS ISO 31000: ***2.24 risk evaluation*** *process of comparing the results of risk analysis (2.21) with risk criteria (2.22) to determine whether the risk (2.1) and/or its magnitude is acceptable or tolerable."*
Establish the context Risk assessment (precaution based): Identify credible, critical issues Identify precautionary options Risk-effort balance evaluation Risk action (treatment)	Establish the context Risk assessment (hazard based): (Hazard) risk identification (Hazard) risk analysis (Hazard) risk evaluation Risk treatment
Criticality driven Usual interpretation of WHS Act & common law.	Risk (likelihood and consequence) driven Usual interpretation of AS/NZS ISO 31000

The top loop in Figure 2 describes the traditional hazard focused analysis listed above. This approach never satisfied common law judicial scrutiny in Australia. That is because if the technical risk target were achieved in reality, the hazards of concern would not eventuate in the analyst's lifetime. But this is not the way of the world. Sometimes bad things will happen and the courts will examine the results.

The bottom loop describes the precautionary legal process applied by the courts. This is necessarily hindsight biased. The courts simply do not care how often matters went well. By definition, the courts only examine the

minority of things that went wrong. After the event, the fact is certain. This means that, from the court's viewpoint, prior-to-the-event estimates of rarity for serious events were presumably flawed and that, prima facie, those who made such estimates have provided proof of negligence. As a judge in NSW has been reported as saying to engineers after a major accident:

What do you mean you did not think it could happen? There are 7 dead.

The way the courts assess the situation is to consult post-event expert witnesses as to what could have been done to have prevented the disaster. Being an expert with the advantage of hindsight is a comparatively straightforward task. The only time the notion of risk is used in court is when the court is testing to see if the precautions suggested by such experts (after the event) were reasonable in view of what was known at the time of the decision.

The WHS Act requires a positive demonstration of due diligence, that is a demonstration that all reasonable practicable precautions are in place, so that risks are eliminated or minimised so far as is reasonably practicable or SFAIRP. This demonstration cannot be achieved through the application of the risk management standard on its own.

5. SFAIRP VS ALARP

Figure 3 describes the two approaches in a different way. The left hand side of the loop describes the legal approach which results in risk being eliminated or minimised *so far as is reasonably practicable* (SFAIRP) as described in the model WHS legislation.

The hazard based loop, shown on the right hand side, attempts to demonstrate that risk is *as low as reasonably practicable* or ALARP. But there are significant warnings to be heeded with each step of this approach as noted in blue.

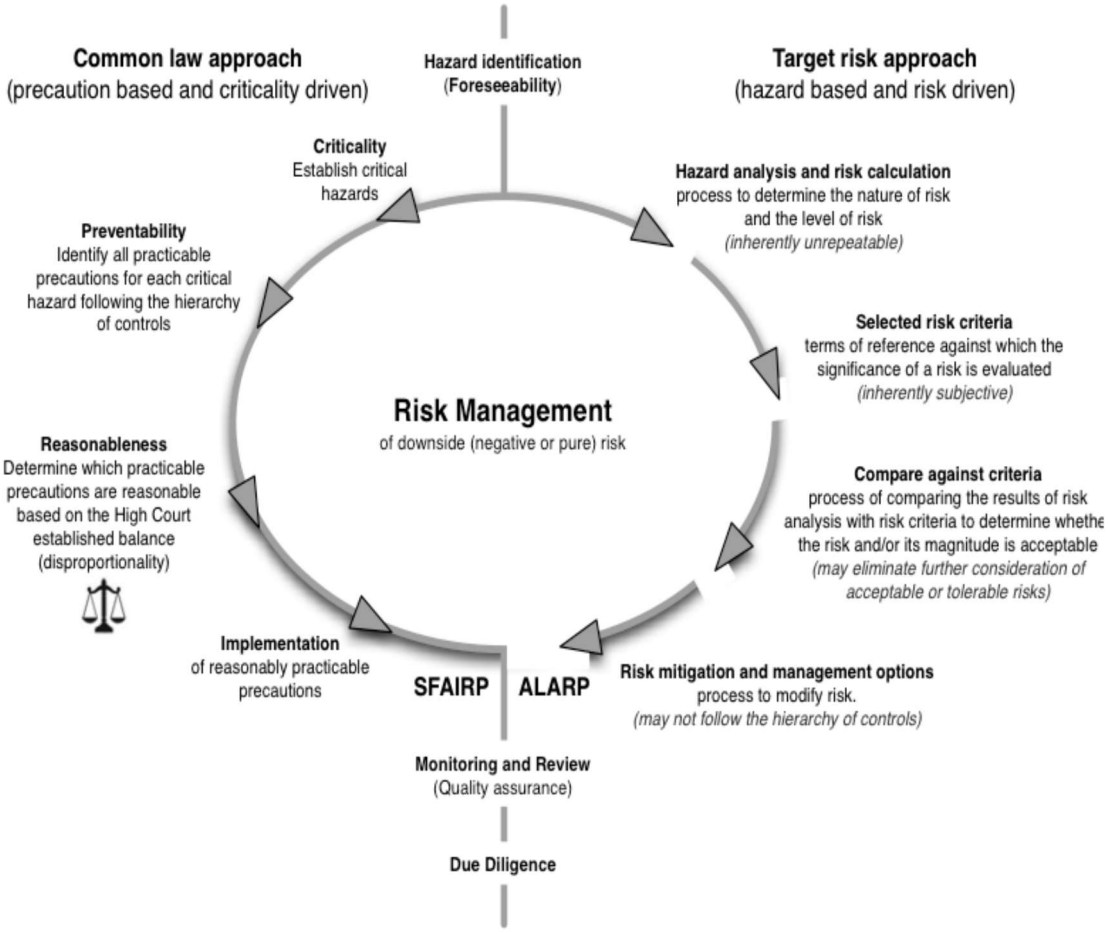

Figure 3: Precaution vs hazard based approaches to risk management (Robinson & Francis et al 2013 page 167)

Firstly, hazard analysis and risk calculations are inherently unrepeatable. Two independent risk experts assessing the same circumstances or situation never come up with the same answer (unless they use deliberately identical assumptions and processes in which case the assessment is not independent).

Risk calculations and characterisations to enable a comparison with risk criteria are by design always imperfect especially with regard to human failings and management systems. Quoting Mark Tweeddale (2003):

> *In the case of the process industry, most of the major disasters in recent years have resulted primarily from failures of management systems, which would not have been included in the quantitative assessment of risk, and not from random equipment failures such as are statistically assessable using data from data banks. This is a most serious limitation...*

Secondly, risk criteria are inherently subjective. Most risk criteria are based on statistical analyses. The traditional way to determine them is to consider mortality and injury statistics. But they are just that, statistics. The numbers change according to the exposed group selected. For example, the lightning strike death rate of around 1 in 10 million (for the whole population) is often selected as the lower limit to risk scrutiny for individual risk. However, if the mortality figures for the group of people who play golf during lightning storms is considered, it will be much higher. Which number ought to be used? Further, the inconsistency in individual and societal risk criteria between states, especially Victoria and NSW dating from the mid-nineties is problematic.

Thirdly, if the risk associated with a hazard is below the acceptable or tolerable threshold, there is a tendency to say that nothing further needs to be done, which is always problematic with low frequency, high severity events. The overall situation is perhaps best summarised by Chief Justice Gibbs of the High Court of Australia (*Turner v. The State of South Australia 1982*):

> *Where it is possible to guard against a foreseeable risk, which, though perhaps not great, nevertheless cannot be called remote or fanciful, by adopting a means, which involves little difficulty or expense, the failure to adopt such means will in general be negligent.*

That is, it does not matter how low the risk estimate is, if more can be done for very little effort, then the failure to do so will be negligent, in the event of an incident.

This leads to the fourth concern; that the temptation is to implement a precaution that reaches the target risk threshold without formally considering the hierarchy of controls.

The hazard based approach for safety seems to address its legal limitations with regard to mitigations by adding caveats, for example from the NSW Land Use Safety Planning Guidelines (NSW Department of Planning (2011)):

While it is useful to have objective, quantitative risk criteria, qualitative principles are equally important. These include:

1. *all 'avoidable' risks should be avoided;*
2. *particular attention needs to be given to eliminating or reducing major hazards, irrespective of whether numerical criteria are met; and*
3. *as far as possible, the consequences of significant events should be kept within facility boundaries.*

The legal system (which requires a demonstration of due diligence following the left hand side of the diagram) does not have this problem. As Andrew Hopkins (2005) notes:

> *At law, employers must drive down risks as far as is reasonably practicable, and there is no level of risk which, a priori, can be said to be acceptable. Moreover, the law has a well-defined set of principles for determining whether risks are as low as reasonably practicable, and despite the indeterminacy of these principles, it is by no means clear that QRA and the tolerability / acceptability framework offers a better way of deciding how low is low enough.*

All this was not a legal issue whilst relevant statute law enabled the hazard-based approach, as statute law always takes precedence over the common law. However, once the legal concept of due diligence is called up by statute via the model WHS Act the issue can no longer be side stepped.

In reviewing this guideline, Sharyn Durley LLB (Barrister) commented on the potential of the courts adopting either or both of the risk methodologies:

> *As stated previously, it is not likely that courts will assess risk in strict accordance with the two risk methodologies. The concept of 'due diligence' as a defence for negligence is well established in law, but it is possible that both/either methodologies may be applied, wholly or in part. In essence, the words 'due diligence' may not equate precisely to 'due diligence risk methodology'.*

The point of the shift from ALARP to SFAIRP is to ensure that all reasonable practicable precautions are in place rather than to achieve a tolerable or acceptable level of risk or safety, which is the result of the hazard-based approach. As Work Safe Australia notes in its "Interpretive Guideline – Model Work Health and Safety Act: The meaning of 'Reasonably Practicable'", this is an objective test.

> *There are two elements to what is 'reasonably practicable'. A duty-holder must first consider what can be done - that is, what is possible in the circumstances for ensuring health and safety. They must then consider whether it is reasonable, in the circumstances to do all that is possible. This means that what can be done should be done unless it is reasonable in the circumstances for the duty-holder to do something less.*

The level of risk resulting from this SFAIRP process might be as low as reasonably practicable but that's not the test that's applied by the courts after the event. The courts test for the level of precautions, not the level of risk.

Some published definitions of ALARP (excluding AS/NZS ISO 31000) imply that risk tolerability levels should only be applied after the SFAIRP test has been applied. Whatever the definition of ALARP, these Safety Case Guidelines advise that 'due diligence' may be better satisfied if SFAIRP is considered first before risk

tolerability is assessed. In this way SFAIRP and ALARP could be considered the same by this defined usage.

6. PREPARING A SAFETY CASE

This section provides guidance on how to develop a safety case including context, content, level of detail and structure that should be included in relation to each of the major aspects of the safety case document.

6.1 Content

The primary purpose of the safety case is to demonstrate and communicate the argument for the management of safety for an organisation, activity or project for all intended parties and stakeholders. In preparing a safety case, the key elements that should be included but not be limited to are:

- Description of the organisation, activity or project under consideration.
- Assessment identifying the safety critical aspects (both technical and managerial) of the organisation, activity or project as well as the control measures to be adopted (as well as those not implemented) to eliminate or minimise risks to health and safety so far as is reasonably practicable (SFAIRP).
- Safety Management System (SMS) overview to provide evidence that the SMS is comprehensive and integrated for all aspects of the safety case argument including the maintenance of control measures to ensure performance.

The safety case should document an argument that includes sufficient detail to allow the decision maker/s to gain a full understanding of the safety issues and the practicable control measures to make a fully informed judgement as to the reasonableness of these control measures.

It should be a stand-alone document that is sufficient without the need to refer to other documents external to the safety case so as to avoid the need to update attachments or the risk of attachments becoming out-dated or missing. All the information in the safety case should be reviewed and kept up-to-date during the various stages of the lifecycle or the organisation, activity or project.

Overall, a well structured, coherent safety case will facilitate an organisation's ability to demonstrate to others that they have a clear understanding of the factors that influence safety risk and the precautions / controls that are critical to eliminate or minimise the risks to health and safety of all people in and around the undertaking (organisation, activity or project) so far as is reasonably practicable.

6.2 Safety Case argument

Most legal advice regarding demonstrating due diligence as required by the model WHS Act is focused on a compliance audit to the relevant section and clauses. But compliance should be the outcome of the due diligence process. That is, in order to be safe, it is first necessary to manage the laws of nature. Confirming that this has been achieved to the satisfaction of the laws of man is a secondary exercise and one to which lawyers can be usefully and efficiently tasked.

Efforts to demonstrate how risk should best be managed have given rise to a number of risk management paradigms[2]. These have been articulated in the earlier editions of this guideline. A summary is shown below. The paradigms are (in historical order of development):

1. The rule of law.
2. Traditional risk management historically typified by the Lloyds insurance and the Factory Mutual Highly Protected Risk (HPR) approaches.
3. Asset based risk management, typified by engineering based Failure Modes, Effects and Criticality Analysis (FMECA), Hazard and Operability (HazOp) and Quantitative Risk Assessment (QRA) 'bottom-up' approaches.
4. Threat-based risk management typified by Strengths, Weaknesses, Opportunities and Threats (SWOT) and vulnerability type 'top-down' military intelligence type analyses.
5. Recognised 'good practice' risk management using published Codes of Practice, Guidelines and Standards.
6. The development of biological, systemic mutual feedback loop paradigms, practically manifested in hyper-reality computer based simulations.

[2] A paradigm is a universally recognised knowledge system that for a time provides model problems and solutions to a community of practitioners. (Kuhn 1970)

7. The development of risk culture concepts (following the work of James Reason) including quality type approaches.

These paradigms can overlap or coincide. Whilst there appears to be a number of risk paradigms available there seems to be only three generic methods by which organisations can proceed with strategic tasks to address the concept of safety risk, that is:

1. Expert knowledge provided from specialists, literature and research;
2. Facilitated workshops of experts and interested parties;
3. Interviews with selected players.

These can be summarised as a single table (see Table 2), with representative processes and techniques in the intersections.

Table 2: Risk management paradigms and ways of addressing them.

No.	Technique > Sign off paradigm	A. Expert opinions	B. Selective interviews	C. Facilitated workshops
1	**The rule of law**	Legal opinions	Coronial inquiries, Royal Commissions	Adversarial courts, arbitration
2	**Insurance approaches**	Surveys, actuarial studies	Moral risk focus	Risk profiling sessions
3	**Bottom-up asset based techniques**	QRA, availability and reliability audits, fault & event trees	Difficult	FMECAs and HazOps
4	**Top-down vulnerability techniques**	Difficult in isolation	Interviews	SWOT & vulnerability techniques
5	**Recognised good practice**	Codes of practice, guidelines and standards	Fact finding tours, conferences etc.	Collective experience of the group
6	**Simulation**	Computer simulations	Difficult	Crisis simulations
7	**Culture**	Quality processes	Generative interviews	Difficult

Each of these methods has different strengths and weaknesses depending on the culture of the organisation and the nature of a particular safety case.

The point is to determine those techniques that satisfy the requirement to manage the laws of nature that can retrospectively satisfy the laws of man. The steps required to positively demonstrate due diligence are:

1. A completeness argument to establish all credible critical hazards,
2. Identification of all practicable precautions for each hazard,
3. Determination of the reasonableness of the practicable precautions, and
4. Implementation of a safety quality assurance (QA) system to ensure precautions are sustained into the future.

This can be diagrammatically represented in the R2A "Y" model (see Figure 4).

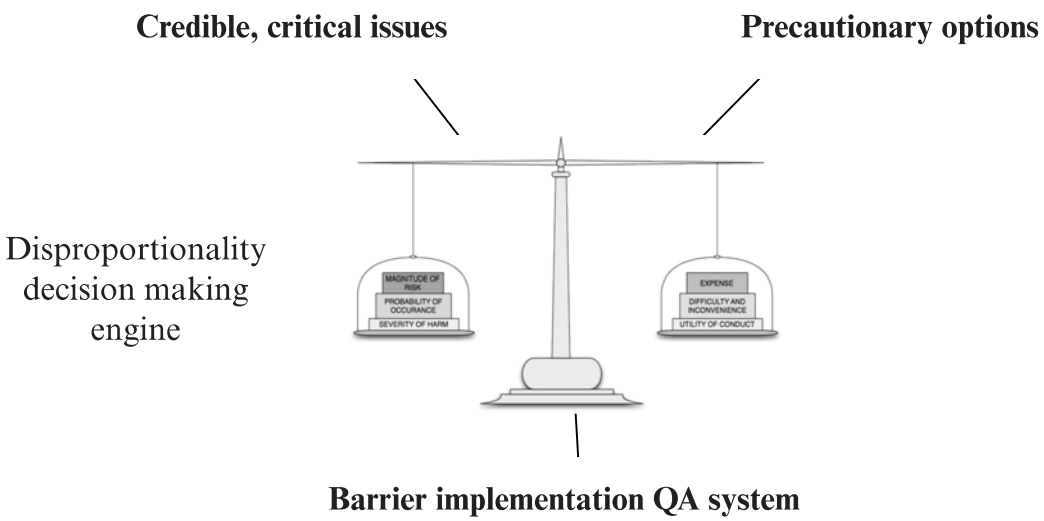

Figure 4: Steps required to positively demonstrate due diligence. (Robinson & Francis et al page 176.)

6.3 Consultation

The safety case argument document should be prepared following effective consultation and participation of relevant stakeholders to ensure informed opinions of the issues and practicable control measures have been obtained.Consultation is a legal requirement and an essential part of managing health and safety risks. The model WHS Act (Part 5, Division 1 (Section 49) identifies specific matters that trigger the requirement for consultation:

Consultation under this Division is required in relation to the following health and safety matters:

a. when identifying hazards and assessing risks to health and safety arising from the work carried out or to be carried out by the business or undertaking;

b. when making decisions about ways to eliminate or minimise those risks;

c. when making decisions about the adequacy of facilities for the welfare of workers:

d. when proposing changes that may affect the health or safety of your workers:

e. when making decisions about procedures for:

(i) consulting with workers; or

(ii) resolving health or safety issues at the workplace; or

(iii) monitoring the health of workers; or

(iv) monitoring the conditions at any workplace under the management or control of the person conducting the business or undertaking; or

(v) providing information and training for workers; or

f. when carrying out any activity prescribed by the regulations for the purposes of this section.

A safe workplace is more easily achieved when everyone involved in the work communicates with each other to identify hazards and risks, talks about any health and safety concerns and works together to find solutions. This includes cooperation and, better still, collaboration between the people who manage or control the work and those who carry out the work or who are affected by the work.

By drawing on the knowledge and experience of workers, more informed decisions could be made about how the work should be carried out safely compatible with the observed culture of the workplace.

Effective health and safety consultation also has other benefits:

- greater awareness and commitment – because workers who have been actively involved in how health and safety decisions are made will better understand the decisions.
- positive working relationships – because understanding the views of others leads to greater trust and hence co-operation and collaboration.

6.4 Legal counsel review

When complete, the safety case provides and argues a documented demonstration that the organisation has adopted safety precautions and mitigations that make the organisation, activity or project as "safe" as is reasonably practicable.

This should be tested with relevant legal counsel to confirm that the arguments satisfy the model WHS legislation.

Legal counsel should be briefed to assess whether the safety case is a complete, reasonable and practical document. The specific objective of any review should be whether the safety case forms the basis of a sound defence to breaches of the model WHS Act.

7. DEVELOPING A SAFETY CASE

7.1 Defining the problem

Defining the problem considers "Whatever can go wrong will go wrong, and at the worst possible time, in the worst possible way." This is a consequence driven test only. Likelihood is not considered at this point.

Therefore, an argument has to be mounted as to why all credible, critical safety issues have been identified. This can be done in a number of ways using well-established risk engineering tools and techniques. This will improve certainty that all foreseeable hazards have been identified.

One way to achieve such a completeness check is to use the military intelligence derived threat and vulnerability technique. In essence this asks the question: Who are the *exposed groups* that are to be protected, and what are the *credible threats* to which they are exposed? All stakeholders should be listed including, but not limited to, workers, contractors, visitors, volunteers, the in attendance/using public and the public at large. This can be presented in a table that is a succinct way of describing all those to whom a duty of care is owed.

An exposed group can be *vulnerable* to a number of threats. The identified vulnerabilities are examined for criticality (potential consequence) not risk (which includes likelihood). A simple example for a tunnel is shown in Table 3.

Table 3: Simplified Vulnerability Table (Robinson & Francis et al page 249).

	Critically Exposed Groups			
	Travelling Public	Operations & Maintenance Staff	Incident Response Personnel	Local Residents
Credible Threat Scenario	incl. disabled, elderly, non-English speaking, small children, people who behave erratically		including emergency services personnel	
Collision	XXX	XX	XX	–
Fire/Explosion (including dangerous goods)	XXX	X	XXX	XXX
Toxic Release	XXX	–	XXX	XXX
Sabotage/ Vandalism/ Terrorism	XXX	XXX	XXX	XXX
Falling objects – infrastructure	XX	XX	–	–
Falling objects – thrown	XX	–	–	–

XXX	Critical vulnerability (multiple fatalities)
XX	Major vulnerability (single fatality)
X	Minor vulnerability (injuries)
–	No vulnerability detected

Selective interviews of key staff and stakeholders supported by top-down workshops (paradigm 4) are central to this outcome.

HazOp and HazId completed in a workshop environment can also be used to identify the credible critical safety issues for further consideration. Fault and event trees can be constructed to examine issues in further detail.

A check of past history should be completed to ensure no credible safety issues have been overlooked.

7.2 Defining the context of the wider environment

It is important to define the context of the safety case upfront in relation to the organisation, activity or project for which the safety case is being prepared. This should be done using a lifecycle approach to ensure a full understanding of the situation is obtained. It may consider going as wide as to include considerations of financial climate, monetary policy, supply of labour and resources, availability of skill and knowledge.

The boundaries being considered by the safety case should be specified and should detail what is included as well as what is excluded from the assessment to make it quite clear.

7.3 Identifying the precautionary options

Identifying and describing all *practicable precautions* (those that could actually be implemented) for each credible critical issue can be done in a number of ways including, but not limited to, identified industry good practice contained in relevant standards, codes and guidelines, expert advice as well as the experience of the larger stakeholder group.

The authors believe that threat-barrier (sometimes known as *bow-tie)* diagrams are one of the best ways to clearly and simply present this information. A concept example is shown in Figure 5.

The loss of control (LoC) point is very important legally. It is always better to prevent the problem, either by eliminating the threat or enhancing the precautions, than to try to recover the situation with mitigations, after control is lost.

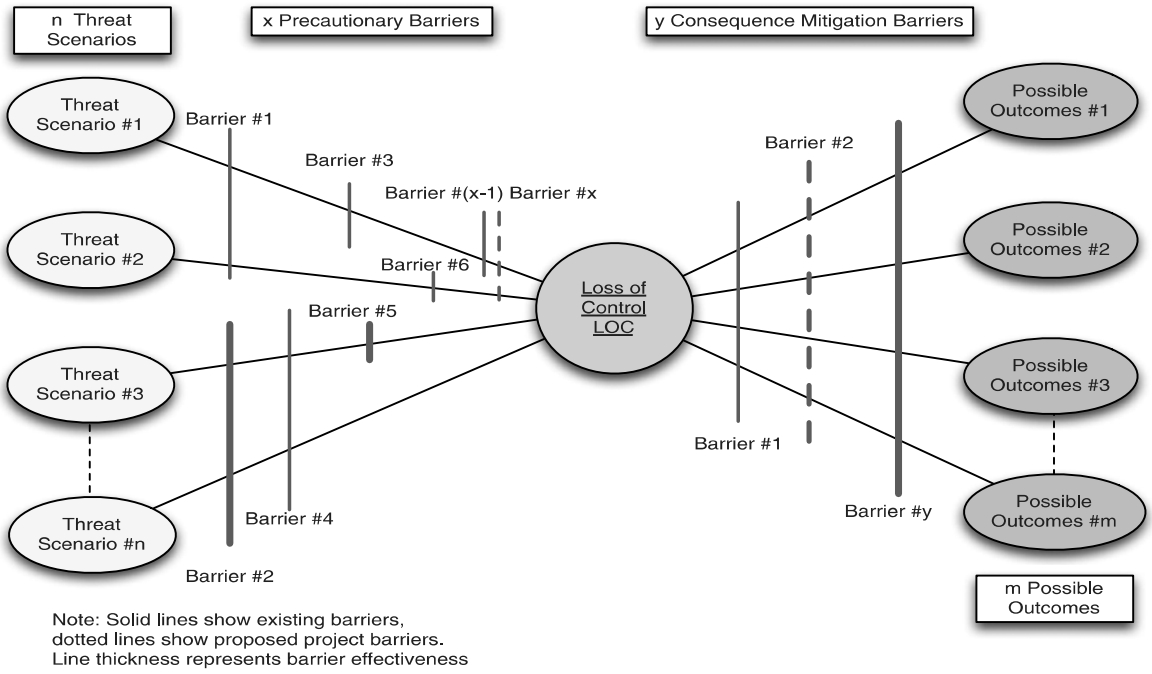

Figure 5: Sample Threat Barrier Diagram (Robinson et al page 88).

The legislation requires that risk control must be based upon the Hierarchy of Controls that is typically, in the order of most to least preferred:

1. Elimination
2. Substitution
3. Isolation

4. Engineering controls
5. Administrative controls
6. Personal Protective Equipment and Clothing.

In the threat barrier diagram, precautions are before the LoC whilst mitigations are after the LoC. That is, the hierarchy of controls is described from the left to the right of the page. The LoC is in fact the point at which the laws of nature and man align.

7.4 Determining the optimal course of action

In determining the optimal course of action, additional precautions (or combination of) need to be assessed for reasonableness in view of the controls already in place. The WHS Act (Section 18) describes what is *reasonably practicable* in ensuring health and safety. In particular, when weighing up all relevant matters, point (e) notes:

> *(e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.*

The High Court has considered precautionary *reasonableness* in the context of balancing cost against risk as reported in Sappideen and Stillman (1995) and described diagrammatically in Figure 6. Effort includes expense, difficulty and inconvenience and utility of conduct. *Expense* includes financial considerations, *difficulty and inconvenience* refers to the inconvenience of taking alleviating action and *utility of conduct* refers to the other aspects of conflicting responsibilities such action incurs.

The point here is that if the test of reasonable practicability is arguable at a common law balance (the 50:50 tipping point), then the likelihood of being successfully prosecuted on a beyond reasonable doubt basis is very small, but this is a proposition that ought to be tested with the readers' own legal counsel.

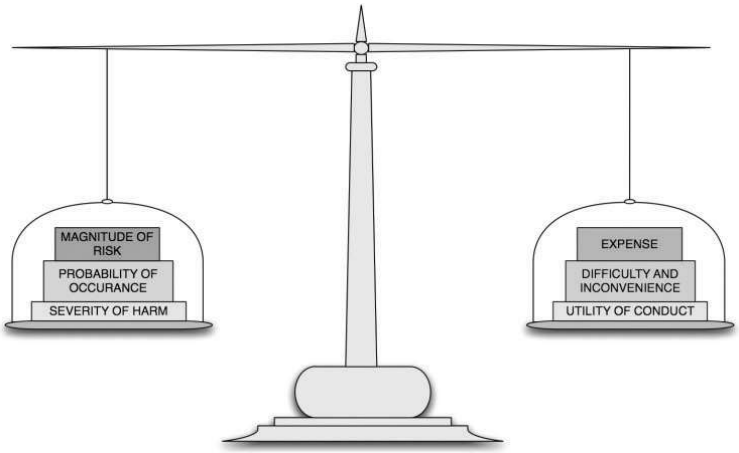

Figure 6: Decision-making scales for deciding which precautions are reasonably practicable.

Controls (or combinations of controls) that can be justified, *on the balance of the significance of the risk vs. the effort required to reduce it,* can then be implemented. This decision can involve quantitative risk assessment (QRA) on a relative risk basis.

It is also essential that documentation is included in the safety case that details why the discarded controls/precautions have been considered not reasonably practicable at this time. This avoids trying to recall the reasons during post event scrutiny. Conditions may have changed at the time of an event and the power of hindsight may cloud the rationale that was previously considered.

However, it is important that controls that are not considered reasonably practicable are reassessed regularly (especially if circumstances change) to ensure they do not become reasonably practicable.

In complex designs where engineering is extensive and innovative, it may be necessary to determine the residual risk. This risk can then be tested/compared with community standards of risk acceptability to ensure that it is acceptable to community standards. This process is known as determining safety as low as reasonably practicable (ALARP), the right hand of the loop in Figure 3. In most situations, engineering can be done and redone until innovation reduces risk to a notional level. The point at which innovation ceases to be reasonable may need to be argued as part of the safety case. Any such ALARP argument may need to be checked by legal counsel.

7.5 Implementation of the optimal action/s

Precautions considered reasonably practicable should be implemented and effectively maintained. The safety case should make it clear to all stakeholders why a precaution is in place and how it is effective in controlling the laws of nature. Documentation ensures the purpose of each precaution is understood and that this understanding is not lost or misunderstood over time.

7.6 Continuous monitoring and review

Some form of quality assurance system also needs to be shown as being in place to ensure that the relevant precautions and mitigations are sustained or maintained over time to the designed standard of effectiveness. SOPs (standard operating procedures) and work method statements contain the precautions in place to carry out each activity. Inspections, spot checks, toolbox meetings, consultation and audits etc. ensure precautions and mitigations (barriers) are being sustained or maintained.

This process can be managed as part of the organisation's larger Safety Management System (SMS) that describes the work environment and how management ensures the workplace is safe on an ongoing basis. This details all relevant policies and procedures. AS4801 and AS4804 may assist in designing the structure of a SMS.

8. CONCLUSION

The WHS legislation requires, by statute, a positive demonstration of due diligence by responsible officers of PCBUs. This means that provided something is not prohibitively dangerous that it ought not be done at all, all reasonable practicable precautions must be in place for all foreseeable critical hazards.

This essentially means that arguing over degrees of rareness for high consequence outcomes pre-event is indefensible, post-event.

This has extraordinary and perhaps unintended consequences. These include:

- Limitations around the use of the risk management standard (ISO 31000) approach for safety as it cannot in itself demonstrate safety due diligence in Australia under the model WHS Act.
- The WHS Act repeals the relevant Dangerous Goods legislation and becomes the enabling legislation for major hazard facilities. This has significant flow-on implications in this domain. Many dangerous goods and major hazard regulators continue to impose a hazard-based approach to major hazard safety cases for a license to trade. However, this in itself will not satisfy the due diligence requirements under the enabling WHS legislation.
- The land use planning guidelines in most states use the target risk approach. This is similarly affected and a so-far-as-is-reasonably-practicable approach should be followed.
- A number of well recognised technical standards encourage the use of risk targets including the SIL standard, IEC 61508; the high voltage earthing standard EG(0) and others. Exclusive use of risk target approaches expose officers under the Act to being considered *reckless* under the new legislation, in the unlikely event of a death or injury resulting from subsequent designs. These standards often provide guidance as to what are considered to be *practicable* precautions but the determination of *reasonableness* is now presently beyond their scope.

A precautionary-based safety case approach provides for better, more explicable, output focused safety outcomes. This requires that convincing, prior-to-the-event arguments be established along the lines described in this document, extensive consultation with stakeholders occur and that legal counsel review all this before being adopted as a safety case.

An example of the precautionary approach is described in the report to the Victorian Cabinet by the Powerline Bushfire Safety Taskforce (2011) arising from the Victorian Royal Commission into the Black Saturday bushfires that killed 173 people in 2009. This report explicitly uses the precautionary approach in the formulation of its recommendations that were all accepted by the Victorian government.

9. REFERENCES

Australian Government Comcare. Guidance for Officers in Exercising Due Diligence, Available from and viewed on 1 April 2013: http://www.comcare.gov.au/WHS/guidance_and_resources/guidance/guidance_for_officers_in_exercising_due_diligence/due_diligencewhere_to_start_and_what_does_it_mean_to_you.

Cullen (The Hon Lord) (2001). Transport, Regulation and Safety: A Lawyer's Perspective. The Transport Research Institute. Fifth Anniversary Lecture, Edinburgh, 10 December 2001.

Hopkins, Andrew (2005). Safety, Culture and Risk. The Organisational Causes of Disasters. CCH Australia. p 137.

Hurst, Geoff (2002). Safety in Action Conference 2002.

Kuhn, T. S., 1970. The Structure of Scientific Revolutions. 2nd ed. Chicago: University of Chicago Press.

NSW Department of Planning (2011). HIPAP 4: Risk Criteria for Land Use Safety Planning. Page 3. Available from and viewed on 5 April 2013: http://www.planning.nsw.gov.au/LinkClick.aspx?fileticket=mEA7owrSNTg%3d&tabid=168&language=en-AU.

Powerline Bushfire Safety Taskforce (2001). Final Report. Available from and viewed on 5 April 2013 http://www.esv.vic.gov.au/Portals/0/About%20ESV/Files/RoyalCommission/PBST%20final%20report%20.pdf. See Section 3.6 Precautionary approach to bushfire risk reduction (page 52) and Appendix E Threat-barrier analysis (page 146).

Robinson, Richard M, Gaye, E Francis, Hurley, Peter et al (2013). Risk and Reliability: Engineering Due Diligence (9th Edition). R2A Pty Ltd.

Safe Work Australia. Model Work Health and Safety Act (revised draft 23 June 2011). Available from and viewed on 5 April 2013: http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/model-work-health-safety-act-23-june-2011. Note that each jurisdiction has implemented the legislation slightly differently although the general principles remain consistent. For example, the NSW Act uniquely imposes strict liability (Clause 12A).

Safe Work Australia. Interpretive Guideline – Model Work Health and Safety Act. The meaning of 'Reasonably Practicable'. Available from and viewed on 24 July 2013: http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/607/Interpretive%20guideline%20-%20reasonably%20practicable.pdf.

Sappideen, C & RH Stillman, (1995). Liability for Electrical Accidents: Risk, Negligence and Tort. Engineers Australia Pty Ltd. Sydney.

Standards Australia & Standards New Zealand, 2009. Risk Management Principles and Guidelines AS/NZS ISO 31000:2009. Sydney.

Turner v. The State of South Australia (1982) High Court of Australia before Gibbs CJ, Murphy, Brennan, Deane and Dawson JJ.

Tweeddale, M, 2003. Managing Risk and Reliability of Process Plants. Boston: Gulf Professional Publishing.

WorkCover Authority of NSW, Available from and viewed on 19 October 2012: http://www.workcover.nsw.gov.au/newlegislation2012/Directorsandofficers/Pages/Duediligence.aspx.

APPENDIX A (INFORMATIVE)

This Safety Case Guideline describes the requirements to create a safety case argument to satisfy the provisions of the model WHS act as passed in all Australian jurisdictions, except at the time of writing, Western Australia and Victoria.

Each jurisdiction may limit the application of the Act within their jurisdiction (Section 12A). For example, the Queensland *Work Health and Safety Act 2011*, Section 12A refers to Schedule 1 which there describes the relationship with Mining Safety, Petroleum and Gas Safety, Electrical Safety and Rail Safety and others. The Commonwealth WHS Act excludes the vessels to which the *Occupational Health and Safety (Maritime Industry Act) 1993* applies (Section 12A (1)) and facilities to which Schedule 3 of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* applies (Section 12A (2)).

Historically, different individual regulators in each jurisdiction have their own enabling legislation in each industry and have different understandings of what constitutes a safety case, as it should be presented to them. To assist engineers in this area a list of jurisdictions and relevant representative regulators, their enabling legislation and a reference to each regulator's understanding of what constitutes a safety case follows.

Commonwealth

- ***Safe Work Australia***

  Enabled under the *Safe Work Australia Act 2008*. For information on major hazard safety cases see: http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/mhfsafetycasecontrolmeasures

- ***NOPSEMA***

  Enabled by the *Commonwealth Offshore Petroleum and Greenhouse Gas Storage Act 2006*. Can also be the designated regulator under state and territory legislation. For information on safety cases see: www.nopsema.gov.au/safety/safety-case/

Australia Capital Territory

New South Wales

Northern Territory

Queensland

Referred to in the Major Hazard facilities guidance material and is required by the *Work Health and Safety Regulation 2011*. For information on MHF safety cases see: http://www.deir.qld.gov.au/workplace/major-hazard-facilities/regulation/index.htm#.VC5C_1Y73fM

South Australia

- ***Office of the National Rail Safety Regulator***

  Enabled by the Rail Safety National Law (South Australia) Act 2012 and complementary enabling legislation in most other jurisdictions.

  The ONRSR provides guidance on rail safety management at: http://www.onrsr.com.au/rail-operation-requirements/safety-management

Tasmania

Victoria

- ***WorkSafe Victoria***

  Enabled by the Victorian Occupational Health and Safety Act 2004 and administers the Occupational Health and Safety Act 2004, the Dangerous Goods Act 1985, the Equipment (Public Safety) Act 1994, the Road Transport (Dangerous Goods) Act 1995, the Accident Compensation Act 1985, the Accident Compensation (WorkCover Insurance) Act 1993 and the Workers Compensation Act 1958.

  For information on MHF safety cases see: http://www.worksafe.vic.gov.au/forms-and-publications/forms-and-publications/safety-case-outline-for-a-major-hazard-facility.

- ***Energy Safe Victoria***

  Enabled by the Energy Safe Victoria Act 2005. Administers the Gas Safety Act 1997, and the Electricity Safety Act 1998, and the Pipelines Act 2005.

  For information of gas safety cases see the Gas Safety (Safety Case) Regulations 2008 available at: http://www.esv.vic.gov.au/Legislation-Regulations/Legislation-administered-by-ESV.

  For information on electrical safety management systems see: http://www.esv.vic.gov.au/Electricity-Professionals/Electricity-Safety-Management-Schemes-ESMS.

Western Australia

The *Dangerous Good Safety (Major Hazard Facilities) Regulations 2007 (MHF Regulations)* are one of seven sets of regulations that give effect to the *Dangerous Goods Safety Act 2004*. For information on MHF safety reports see: http://www.dmp.wa.gov.au/7264.aspx.

NB. Doing what a regulator asks will facilitate a licence to trade (very necessary) but may not discharge your obligations under the WHS legislation if that legislation applies. The regulator is not the one who will be prosecuted in the event of legislative misinterpretation as their enabling legislation invariably provides a statutory defence for the regulators' agents so long as those agents are acting in good faith. Hence the reason for the emphasis in this Safety Case Guideline that internal legal counsel confirm the appropriateness of any submitted safety case in view of all the legislation that may apply.

To provide an example of the complexity of the issues, the *Rail Safety National Law* which is presently being enacted in most jurisdictions indicates in Section 28 that OHS legislation always takes precedence over the rail law, that compliance with the rail safety law is not a defense for an OHS breach and that a breach of the rail safety law is also a breach of relevant OHS legislation.