SFAIRP vs ALARP

Richard Robinson
BE, BA, FIEAust, MSFPE, HonFAMPI

Gaye Francis
BE MIEAust

R2A Due Diligence Engineers, Victoria, Australia

SUMMARY

The Rail Safety National Law [1] and the model Work Health and Safety Act [2] both require safety risk to be eliminated or minimised *so far as is reasonably practicable* (SFAIRP). SFAIRP requires a positive demonstration of due diligence. Most technical safety work is done in the context of ensuring technical safety is *as low as reasonably practicable* (ALARP). There has been an on going attempt in many places to equate the SFAIRP and ALARP. This paper will describe why this cannot be done and explains why adopting the SFAIRP process is sensible and forensically defensible.

INTRODUCTION

There have been two primary paradigms of safety risk management co-existing uneasily over the last few decades. One is related to hazard based risk analysis driven by technical professionals. The other the precaution based risk analysis driven by the courts.

The hazard based approach to risk is the one popularly described in the risk management standard AS/NZS ISO 31000 [3], that is:

- Establish the context
- Risk assessment:
  - (Hazard) risk identification
  - (Hazard) risk analysis
  - (Hazard) risk evaluation (comparison to criteria)
- Risk treatment

In Figure 1, this means starting at the top identifying credible hazards and then, using the metric of risk, moving to hazard assessment on the left and then on to the control options on the right to establish risk treatments, very often using target levels of risk or safety as a decision making benchmark. This is a very input-based process. If the risk assessment is in error (not uncommon for high consequence, low likelihood events) then action may not be identified as being needed.

An alternative to hazard based risk management is precaution based risk management. In Figure 1, this starts at the top but then jumps straight to the right to see what practical options are actually available and then tests to see which are reasonable in the circumstances and ought to be done, especially recognised good practices.

That is:

- Establish the context
- Precautionary assessment:
  - Credible, critical issues identification
  - Practicable control options identification
  - Judgement (viable control options evaluation)
- Precaution implementation (action)

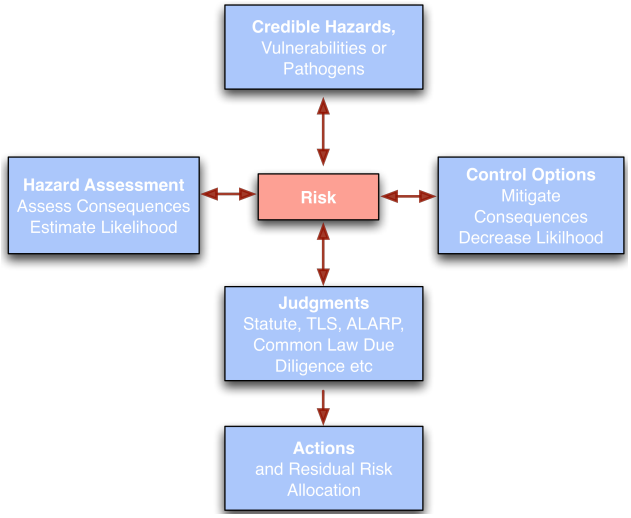

Figure 1. Hazard based risk assessment approach

The precautionary approach is very output-focussed. It is invariably the one adopted by the courts post event. Precautions and mitigations are implemented unless it is unreasonable to do so.

This paper builds on that presented by the authors at CORE 2012 [4] prior to the commencement of both the Rail Safety National

Law and the model Work, Health and Safety legislation in Australia.

SYSTEM OF LAW IN AUSTRALIA

There are two basic kinds of laws in Australia:

* Statute law, which is made by a Parliament consisting of democratically elected members. Statute law (also called legislation) may be made by the Commonwealth Parliament, or by the Parliament of a State or Territory.

* Common law, which is law made by judges when deciding cases [5].

Common law has its origins in England in the 12th century, before there was any Parliament in England, when the King of England at that time (Henry II) appointed members of his court to hear complaints and do justice on his behalf. Judges making decisions drew on their notions of justice or fairness, sometimes customs or traditions, sometimes Roman law. Reasons for judges' decisions were recorded, and this body of case law, known as the *common law*, became the most important source of law for judges. In time, judges considered themselves to be bound to follow the precedents set by other judges in earlier cases.

The High Court of Australia is the highest court in the Australian judicial system. It was established in 1901 by Section 71 of the Constitution [6]. The functions of the High Court are to interpret and apply the law of Australia; to decide cases of special federal significance including challenges to the constitutional validity of laws and to hear appeals, by special leave, from Federal, State and Territory courts.

Australia inherited the common law system from the UK. And with the passage of the Australia Acts of the1980s eliminating appeals to the Privy Council, the High Court of Australia become the ultimate 'reference' for Australian case law.

In Australia court cases are conducted under the adversarial system in which the court is asked to adjudicate upon 'issues' put forward by the parties upon evidence adduced by the parties. The presiding judge has no power of inquiry (the 'inquisitorial system'), unlike courts in parts of Europe [7].

There are several points about the adversarial system that need to be remembered. It is first and foremost a court of law. And the courts are always right even when they are in error as the decisions of appellate courts reveal.

For example, in Turner vs The State of South Australia [8] the judges of the High Court of Australia, when discussing why a lower court might have come to a particular decision noted that:

It is possible that their Honours were also influenced by the opinion of an orthopaedic surgeon, Mr Jose, that the upward force to required to raise a 400 lb drum from the prone to the upright position was 400 lbs. That evidence which was set out in the judgement of Williams J at the first instance is plainly mistaken. The upward force required to up-end a drum, with the bottom rim remaining on the ground, is an initial force of approximately 200 lbs which progressively decreases as the top end is raised.

That is, awkward situations will arise if the matter before the court is technically complex and the adversaries rely on purely legal advice, rather than relying on the technical insight from competent expert witnesses.

Engineers Australia also notes [7]:

Adversarial courts are not about dispensing justice, they are about winning actions.

In this context, the advocates are not concerned with presenting the court with all the information that might be relevant to the case. Quite the reverse, each seeks to exclude information considered to be unhelpful to their side's position. The idea is that the truth lies somewhere between the competing positions of the advocates.

Further, courts do not deal in facts, they deal in opinions [9]:

What is a fact? Is it what actually happened between Sensible and Smart? Most emphatically not. At best, it is only what the trial court - the trial judge or jury - thinks happened. What the trial court thinks happened may, however, be hopelessly incorrect. But that does not matter - legally speaking.

That is, in court, the laws of man take precedence over the laws of nature, which can be particularly astonishing to engineers. In the adversarial system innocence must be assumed or there is no case to try. If the defendant pleads guilty, for example, the case stops immediately other than for the determination of the penalty.

DUE DILIGENCE

Due diligence (or due care) is a legal concept, derived from the societal need to ensure fairness in dealings between human beings. It has been variously defined, for example:

The diligence reasonably expected from, and ordinarily exercised by, a person who seeks to satisfy a legal requirement or obligation [10] and,

A minimum standard of behaviour which provides against contravention of relevant regulatory provisions and adequate supervision ensuring that the system is properly carried out [11].

Such legal obligations can be created in the common law or by statute law as has occurred with the commencement of the Rail Safey National Law (RSNL) [1] and the Model Work Health and Safety (WHS) Act (2011) [2] in Australian jurisdictions.

One immediate reaction to such a definition is to institute a legal and regulatory compliance audit. The difficulty with this approach to safety (meaning a lack of harm) is that in a complex industrial society mere compliance with legislation and all the regulations made by regulators under such legislation will not necessarily make any particular situation or circumstance safe in reality. To be safe requires that the laws of nature be managed competently prior to compliance with the laws of man.

Due diligence engineering is about overcoming this practical difficulty by ensuring that the laws of nature and the laws of man simultaneously align. And, logically and practically, in order to be safe, it is better to manage the laws of nature first and then to confirm that the requirements of the laws of man have been met, rather than the other way around.

COMMON LAW DUE DILIGENCE

Due diligence has been a primary defence against the tort (or wrong) of negligence in the common law. In this context, what constitutes due diligence in Australian case law has been established by the High Court of Australia. In an appeal to the High Court from the Court of Appeal of the Supreme Court of NSW [12], Stephen J noted:

This appeal involves interpretation of the Hague Rules. During heavy weather in the Great Australian Bight, the severity of which was unusual but not unforeseeable, a number of drums of cleaning solvent stowed in a ship's hold broke adrift, were damaged and their contents lost. The means of securing them in place in the hold had been inadequate.

Under the Hague Rules (to which Australia is a signatory), *Article IV Rights and Immunities* states:

1. Neither the carrier nor the ship shall be liable for loss or damage arising or resulting from unseaworthiness unless caused by want of due diligence on the part of the carrier to make the ship seaworthy, and to secure that the ship is properly manned, equipped and supplied...

Whenever loss or damage has resulted from unseaworthiness, the burden of proving the exercise of due diligence shall be on the carrier or other person claiming exemption under the section.

Reynolds J.A. summed up the conclusion of the Court of Appeal of the Supreme Court of NSW in the following words:

Loss or damage does not arise or result from perils of the sea where negligence is a concurrent cause. Where negligence allows or facilitates the perils of the sea to inflict damage on cargo, then in all relevant respects the loss or damage arises or results from the negligence. The perils of the sea must be guarded against by the use of due care.

The judges of the High Court unanimously dismissed an appeal to the High Court and supported the view of the NSW Court of Appeal summarised by Reynolds J.A. above. And when 10 superior court judges unanimously agree on a particular point then this is robust case law and unlikely to change in the near future.

NATIONAL RAIL SAFETY LAW

National Rail Safety Law [1] adopts several key concepts, which parallel the model WHS legislation.

First and foremost is SFAIRP. Under Section 46 – *Management of risks*:

A duty imposed on a person under this Law to ensure, so far as is reasonably practicable, safety requires the person—

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

The meaning of reasonably practicable is then defined (Section 47):

… reasonably practicable, in relation to a duty to ensure safety, means that which is (or was at a particular time) reasonably able to be done in relation to ensuring 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).*

Section 48 then goes on to explain the relationship between the rail safety law and OHS legislation. It is absolutely clear that OHS (WHS) legislation takes precedence. For example the note to Section 48 (20):

For example, if a provision of this Law deals with a certain matter and a provision of the occupational health and safety legislation deals with the same matter and it is impossible to comply with both provisions, a person must comply with the occupational health and safety legislation and not with this Law. If provisions of both this Law and the occupational health and safety legislation deal with the same matter but it is possible to comply with both provisions, a person must comply with both.

The legislation, like the model WHS act spells out the duty of officers and how this obligation to demonstrate due diligence can be met (Section 55):

(1) If a person has a duty or obligation under this Law, an officer of the person must exercise due diligence to ensure that the person complies with that duty or obligation.

(3) In this section— due diligence includes taking reasonable steps—

- *(a) to acquire and keep up-to-date knowledge of rail safety matters; and*
- *(b) to gain an understanding of the nature of the railway operations of the person and, generally, of the risks associated with those operations; and*
- *(c) to ensure that the person has available for use, and uses, appropriate resources and processes to eliminate or minimise risks to safety from the railway operations of the person; and*
- *(d) to ensure that the person has appropriate processes for receiving and considering information regarding incidents and risks and responding in a timely way to that information; and*
- *(e) to ensure that the person has, and implements, processes for complying with any duty or obligation of the person under this Law; and*
- *(f) to verify the provision and use of the resources and processes referred to in paragraphs (c) to (e).*

The penalties for officers of persons conducting a business or undertaking are high (Section 58):

58—Failure to comply with safety duty—reckless conduct—Category 1

(1) A person commits a Category 1 offence if—

- *(a) the person has a safety duty; and*
- *(b) the person, without reasonable excuse, engages in conduct that exposes an individual to whom that duty is owed to a risk of death or serious injury or illness; and*
- *(c) the person is reckless as to the risk to an individual of death or serious injury or illness.*

Maximum penalty:

- *(a) in the case of an individual—$300 000 or imprisonment for 5 years, or both;*
- *(b) in the case of a body corporate—$3 000 000.*

Unlike the model WHS act, reckless conduct (knew or made it happen) does not appear to be a crime.

SFAIRP vs ALARP

Whilst the two approaches may set out to achieve the same outcome, that is, to demonstrate due diligence with regards to safety, the implication that having achieved ALARP will forensically satisfy SFAIRP post event is naively courageous. This is simply because the processes required to demonstrate each is different, especially for high consequence, low likelihood events, the ones that are the subject of judicial scrutiny.

* ALARP asks what is the risk associated with the hazard and then can that risk be made as low as reasonable practicable.

* SFAIRP asks what are the available practicable precautions to deal with the identified issue and then tests which precautions are reasonable based on the common law balance (of the significance of the risk vs the effort required to reduce it).

The possibility of the results of the two processes being identical is, in the authors' opinion, nil. In view of the requirements for SFAIRP under the Rail Safety National Law (Section 46) and the model WHS act (Section 17), and others, this is a serious issue for engineers.

The ALARP process requires that hazards be identified, the risk (likelihood and consequence) associated with them be determined and then compared to acceptable or tolerable risk criteria. If the criteria are not satisfied then risk treatments are applied until they are. Caveats to the approach can be applied such *as avoiding avoidable risk* and even testing if further precautions can be justified even if the target level has been met, but these are afterthoughts, not the primary process and presumably an attempt to legally recover the situation. Figure 2 shows the difference between the two approaches, especially for high consequence, low likelihood events. The top loop describes the hazard based, risk focused analysis. 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. And, 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 beyond-reasonable doubt proof of negligence. As a judge in NSW has been reported as saying to engineers after a major rail accident:

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

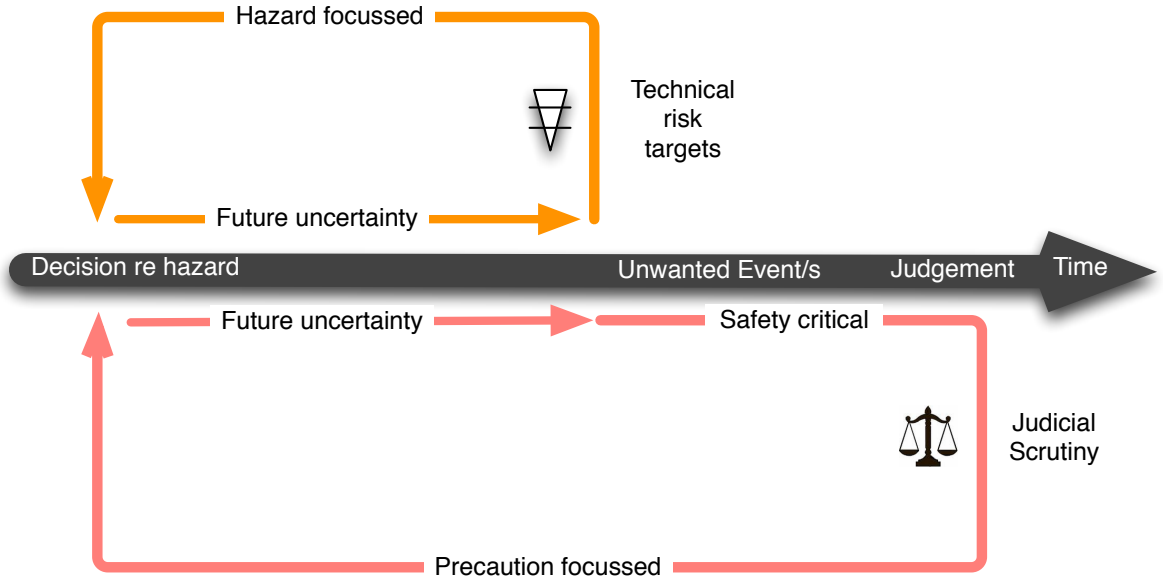

Figure 2: Hazard vs Precaution focussed risk management [13]

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 straight forward 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.

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) such as described in the model WHS legislation. Its purpose is to demonstrate that all reasonable practicable precautions are in place by firstly identifying the practicable precautions and then testing for reasonableness using relevant case law. As Work Safe Australia notes [14], 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 process might be as low as reasonably practicable (ALARP) 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. The SFAIRP concept embodies this outcome.

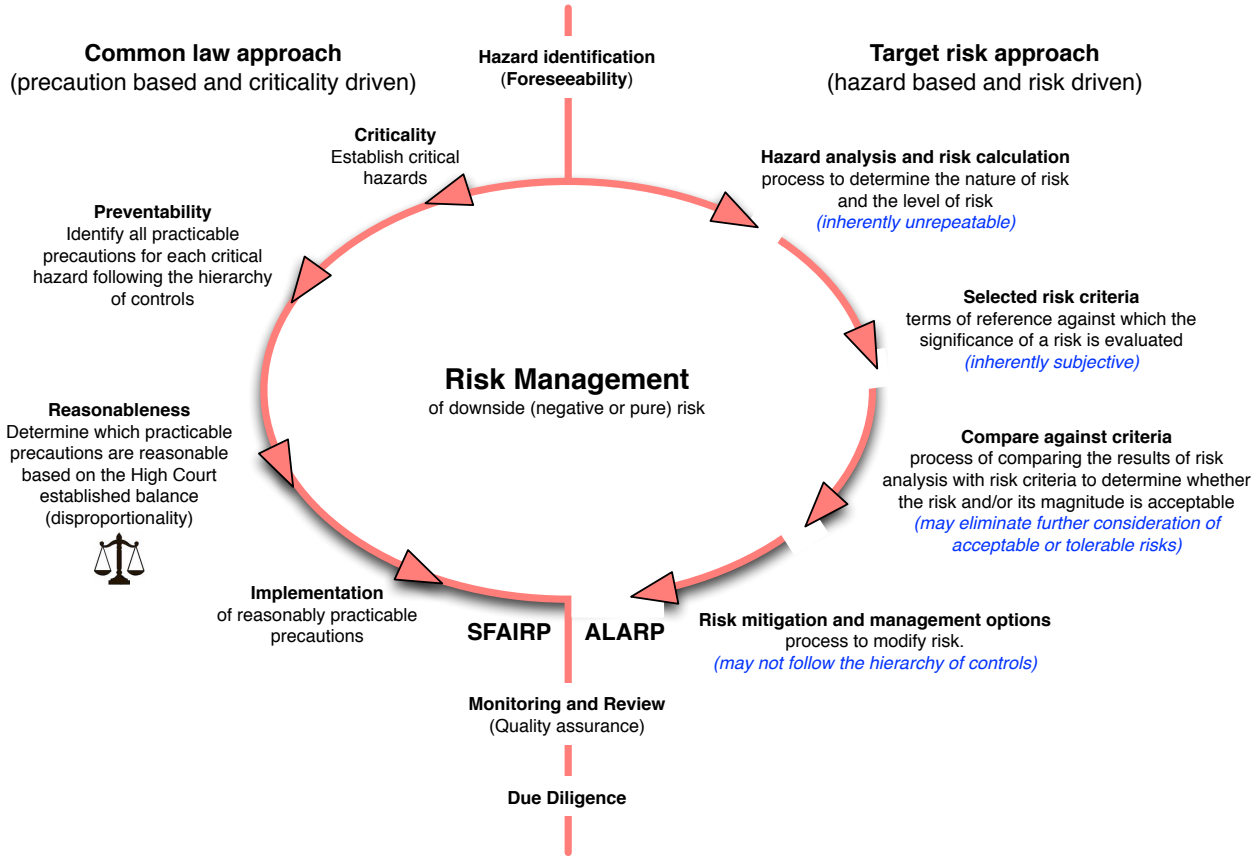

Figure 3. Precaution vs hazard based approaches to risk management [13]

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 major difficulties with each step of this approach as noted in blue.

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 always imperfect especially with regard to human failings and management systems. Quoting Mark Tweeddale [15]:

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 subjective. The old adage should probably be extended to; *there are*

lies, damned lies, statistics and then there are target risk criteria. 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 industries (dam and air safety for example) and states, especially Victoria and NSW dating from the mid-nineties is problematic.

Thirdly, if the risk associated with a hazard is below 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 [8]:

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 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.

Engineers often argue that, if you set the law aside, the only way to demonstrate due diligence is the ALARP approach. This is simply not a viable proposition. The laws of man may not be ignored. Our parliaments and courts necessarily reject this. It has always been clear that the courts will interpret the circumstances surrounding death, injury or damage in legal terms. This proposition is easily confirmed by consulting in-house legal counsel.

An example of the SFAIRP approach applied to a rockfall issue for Lapstone Cutting in NSW on behalf of Railcorp is described in the paper by the authors [4]. Another more recent example is described in the report to the Victorian cabinet by the Powerline Bushfire Safety Taskforce [16] arising from the Victorian Royal Commission into the Black Saturday bushfires that killed 173 people in 2009. This report explicitly uses the SFAIRP approach in the formulation of its recommendations which were all accepted by the Victorian government.

CONCLUSION

The Rail Safety National Law (and the model Work Health and Safety legislation) require, by statute, a positive demonstration of safety due diligence by responsible officers of railway businesses. This specifically rejects the ALARP approach, especially using target (acceptable or tolerable) levels of risk or safety.

The point of the SFAIRP approach is to demonstrate, that provided something is not prohibitively dangerous that it ought not to be done at all, that all reasonable practicable precautions are in place for foreseeable critical hazards. Essentially, arguing over degrees of rareness for high consequence outcomes pre-event is simply indefensible, post-event.

This has extraordinary and perhaps unintended consequences. These include:

* Rejection of the risk management standard (ISO 31000) approach as a competent method of demonstrating safety due diligence in Australia, at least of high consequence, low likelihood events.
* A number of well recognized technical standards encourage the use of risk targets including the SIL (Safety Integrity Level) standard, IEC 61508; the high voltage earthing standard EG(0) and others. Exclusive use of such approaches will probably render relevant *officer* practitioners *reckless* under the new legislation in the unlikely event of a death or injury resulting from subsequent designs.

However, the precaution based SFAIRP approach provides for better, legally explicable, output focused safety outcomes.

REFERENCES

1. South Australia. Rail Safety National Law (South Australia) Act 2012. Version: 20.1.2013.
2. Model Work Health and Safety Bill. Model Bill 23/6/2011
3. Standards Australia & Standards New Zealand, 2009. Risk Management Principles and Guidelines AS/NZS ISO 31000:2009. Sydney.

4. Francis G E & Robinson R M, The Implications of Common Law Due Diligence. CORE 2010, 14 September 2010, Wellington.
5. Adapted from: http://www.austlii.edu.au/au/other/liac/hot_topic/hottopic/2002/3/1.html viewed 5 April 2013.
6. Adapted from: http://www.hcourt.gov.au/about/role-of-the-high-court viewed 28 April 2013.
7. Adapted from: http://www.nswbar.asn.au/docs/resources/publications/structure.pdf viewed 5 April 2013.
8. Turner v. The State of South Australia (1982). High Court of Australia before Gibbs CJ, Murphy, Brennan, Deane and Dawson JJ.
9. Institution of Engineers, Australia (1990). Are You at Risk? Canberra.
10. Black's Law Dictionary, 4th Edition (2009)
11. LexisNexis Concise Australian Legal Dictionary, 4th Edition (2011)
12. Shipping Corporation of India Ltd v Gamlen Chemical Co. A/Asia Pty Ltd [1980] HCA 51; (1980) 147 CLR (12 December 1980)
13. Robinson Richard M, Gaye E Francis, Peter Hurley et al (2013). *Risk and Reliability: Engineering Due Diligence* (9th Edition). R2A Pty Ltd.
14. From: http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/607/Interpretive%20guideline%20-%20reasonably%20practicable.pdf viewed 24 July 2013
15. Tweeddale M, 2003. Managing Risk and Reliability of Process Plants. Boston: Gulf Professional Publishing.
16. From: http://www.esv.vic.gov.au/Portals/0/About%20ESV/Files/RoyalCommission/PBST%20final%20report%20.pdf viewed 5 April 2013. See Section 3.6 Precautionary approach to bushfire risk reduction (page 52) and Appendix E *Threat-barrier analysis* (page 146).