



*The Institution of Railway Signal Engineers
Australasian Section Inc.*

COMMON LAW SAFETY CASES

Richard M Robinson, BE BA FIEAust MSFPE
Director, R2A Pty Ltd

ABSTRACT

A common law safety case is an argument as to why an organisation is confident that all statutory, regulatory and common law obligations have been met. It is primarily a demonstration that all sensible practicable precautions are in place.

This means that target risk levels are not strictly relevant. Legally at least, if a business or activity is prohibitively 'dangerous' then it must be stopped. Otherwise the common law principle, the balance of the significance of the risk versus the effort required to reduce it, applies. As such, 'risk' is only invoked to test the value of the possible precautions, rather than the significance of the 'hazard'

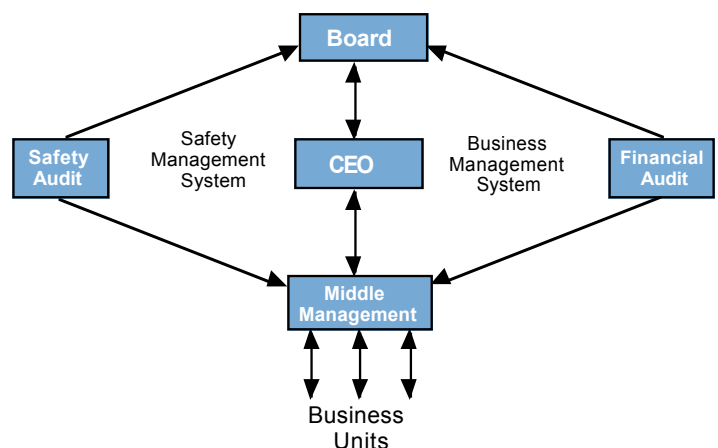
INTRODUCTION - TRADITIONAL TECHNICAL SAFETY CASES

The process of managing safety, health and environmental issues in large and/or complex processes and organisations usually requires a formal management system generally referred to as a safety management system. A safety case is developed as a reasoned argument by the technical people that all significant hazards have been identified, are properly managed and are 'safe', that is, an 'acceptable' or 'tolerable' level of risk has been achieved.

Historically, safety cases were developed by technical people using bottom up asset management hazard identification techniques to optimise safety performance. Regulatory safety case regimes cover such industries as offshore petroleum, gas safety, electrical safety management, major hazards, mining and rail transport.

There are parallels to a business case, which is usually developed to convince a financier that a business is viable (Redmill et al. 1997). The objective of the business case is to ensure that all significant factors affecting the business have been identified

and that appropriate measures are in place to maximise the positive factors and minimise the negative ones. A safety case is intended to provide the same assurance with respect to safety of a system, project or complex.



Idealised Safety Management System

Once established, a safety case effectively manifests itself as a contract between an organisation and a regulator that permits the

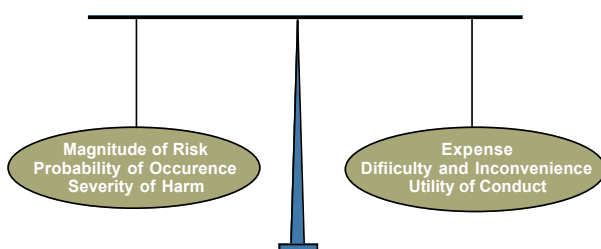
organisation to operate within defined limits in accordance with documented procedures. Compliance failure is a breach of contract. If damage to third parties, or injury or death occur due to such breaches then serious liabilities arise.

DUE DILIGENCE

It is the common law duty of employers to provide a safe workplace for employees and the obligation of owners and occupiers of premises to ensure they are safe with respect to members of the public and the surrounding environment. Failure to ensure such may be negligent, and can lead to the significant costs associated with common law claims. It may also lead to statutory penalties for 'responsible' individuals depending on local legislation and regulations.

In order to meet this common law duty of care, it would appear that risk management is shifting away from the concept of 'acceptable' risk to 'tolerable' risk. If an identified risk is found to be 'intolerable', that is prohibitively dangerous, then the activity must be stopped. The concept that risks can only be 'tolerable' (meaning 'not intolerable') seems to be supported in the recent revision (October 2004) of the Australian Risk Management Standard AS4360 which appears to have deleted all reference to the term 'acceptable' risk.

For risks not identified as 'intolerable', the common law principle applies, that is, the balance of the significance of the risk versus the effort required to reduce it. This is represented by the diagram below adopted from Sappideen and Stillman (1995).



How would a reasonable defendant respond to the foreseeable risk?

The overall situation is perhaps best summarised by Chief Justice Gibbs of the High Court of Australia:

Where it is possible to guard against a foreseeable risk, 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.

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

Liability can also arise if 'good practice' has not been implemented. For example, the UK Health and Safety Executive in a document titled, *Reducing Risks, Protecting People* (2001) states:

... the starting point should be an option which is known to be reasonably practicable (such as one which represents good practice). Any other options should be considered against that starting point, to determine whether further risk reduction measures are reasonably practicable. (Bolding by R2A).

For this reason it would appear that an effective safety case will have to demonstrate at least 'good practice' in a way that is transparent to non-technical personnel including the public and potentially the courts after a loss event. In terms of a common law due diligence sense liability appears to arise when there are unimplemented good ideas rather than the existence of hazards or vulnerabilities in themselves.

The impact of the adversarial legal system appears to have changed the nature of a safety case from being a statement by the technical people as to why they are confident that all relevant hazards are being managed to an 'acceptable' level of risk to a due diligence argument as to why the organisation is confident that all reasonable practicable precautions are in place.

This seems to be so because the courts appear to be consequence driven. Risk is generally considered to be a combination of

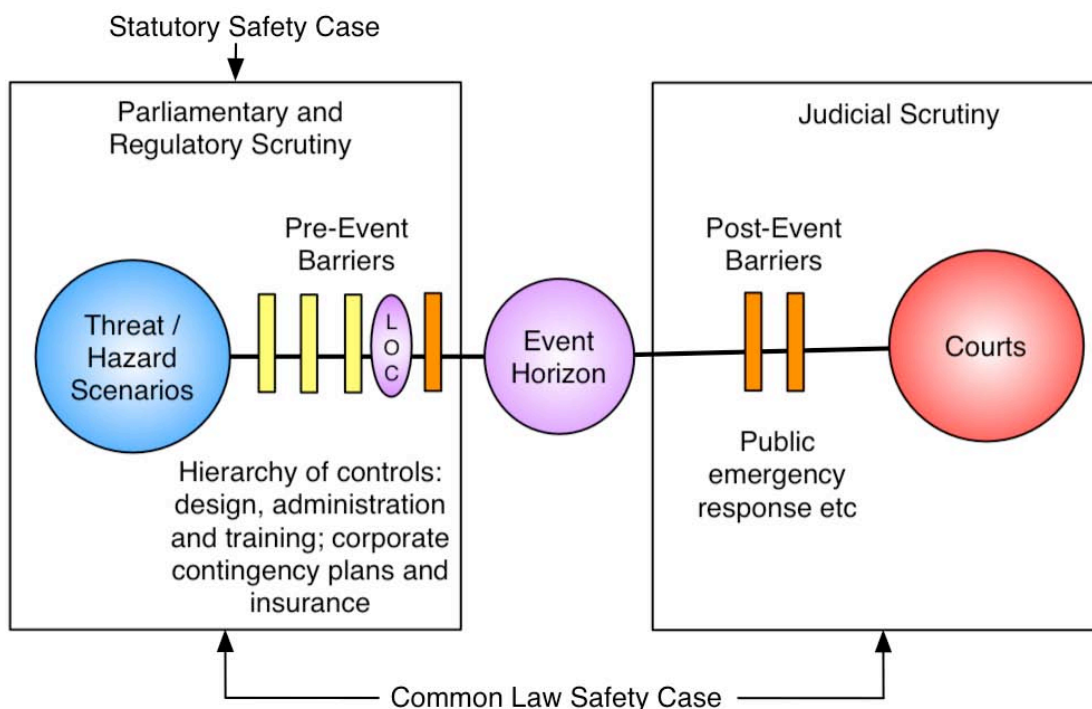
likelihood and consequence. However, after the fact, the likelihood is certain. Any view that the event occurs very, very rarely is not relevant. To paraphrase a judge in NSW: *'What do you mean you didn't think it could happen, there are seven dead'*. This is a very powerful argument after the event. The expert witnesses then look to see what could have been done, which if it had been done, would have prevented the occurrence. Risk per se is not relevant. It is only raised to assess the reasonableness of the possible precautions in view of the state of knowledge before the event.

Thus for senior management and board members at least, liability management is very nearly identical to consequence management. Frequency and therefore risk management is not really an issue. If a serious loss event can credibly occur then it must be (seen to be) managed.

required to reduce it. It also includes management contingency plans up until the event horizon. 'Good practice' is usually considered to be a starting point. It essentially ensures 'due diligence' is (seen to be) demonstrated, not that accidents / incidents won't happen.

Based on the due diligence arguments above, a common law safety case is a documented demonstration by an organisation that all statutory, regulatory and common law requirements have been met. The latter aspect distinguishes it from a statutory safety case which deals with statutory and regulatory requirements only.

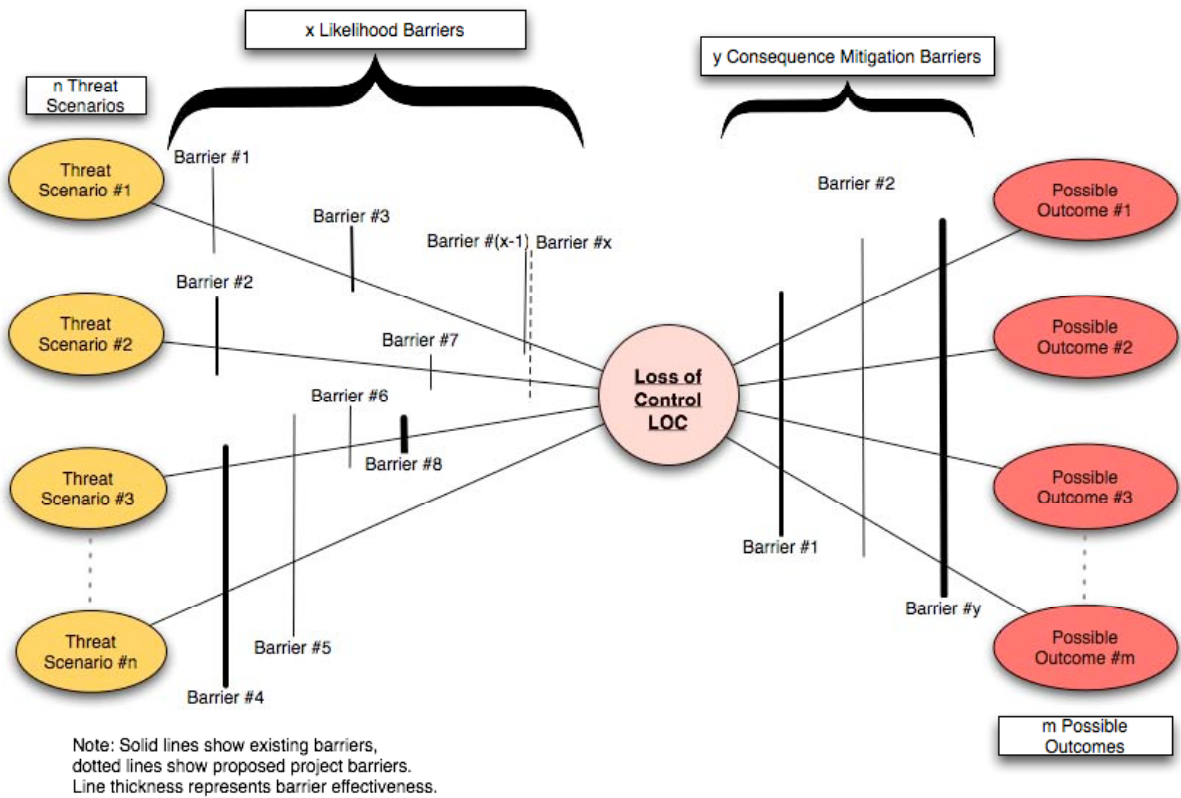
This is represented by the diagram below, which shows that a statutory safety case focuses on the left hand side of the event horizon. A common law safety case targets both sides simultaneously.



COMMON LAW SAFETY CASES

A common law safety case consists of a number of arguments that demonstrate that all reasonable practicable precautions are in place. This process includes the application of the hierarchy of controls consistent with OH&S legislation (elimination, engineering/design, training and administration) based on the balance of the significance of the risk verses the effort

The loss of control (LOC) point is the point at which it becomes technically unclear as to what the scale of the event may be. Contingency plans, especially for small events may be effective. The event horizon is the point at which perception and control of the event passes from the ken of management. The public response systems (emergency

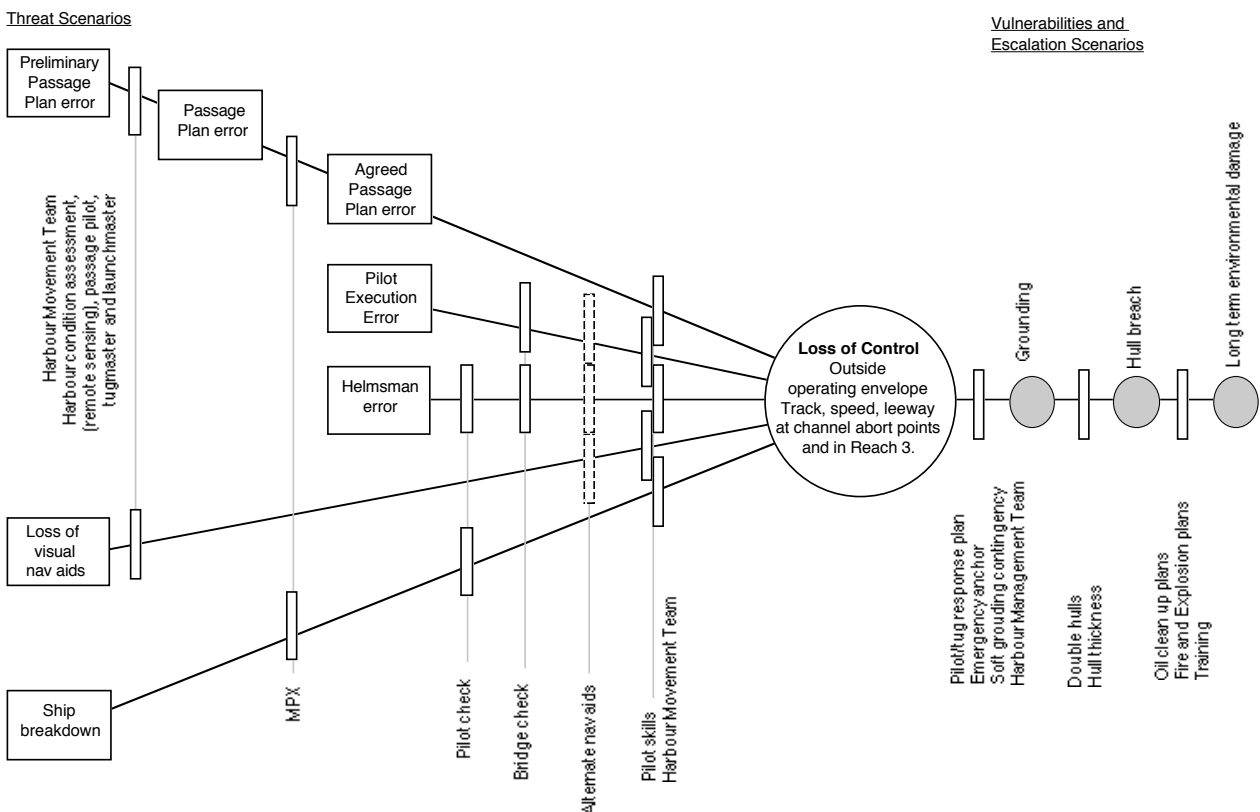


services like the Fire Brigade and Ambulance Services) and the courts are invoked.

developed for South Port, New Zealand in 2003 (shown with permission).

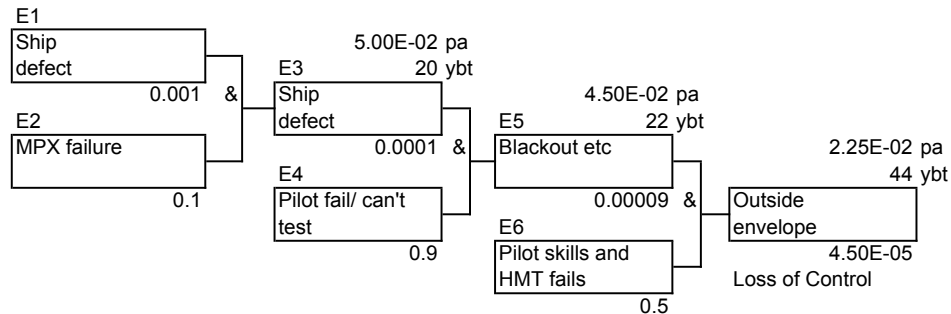
This page shows a concept threat barrier diagram and an actual threat barrier diagram

This seems to a powerful way to demonstrate the efficacy of existing and proposed controls.



Each of the threat scenarios can then be modelled as a fault tree. Loss of control due to mechanical failure is shown below.

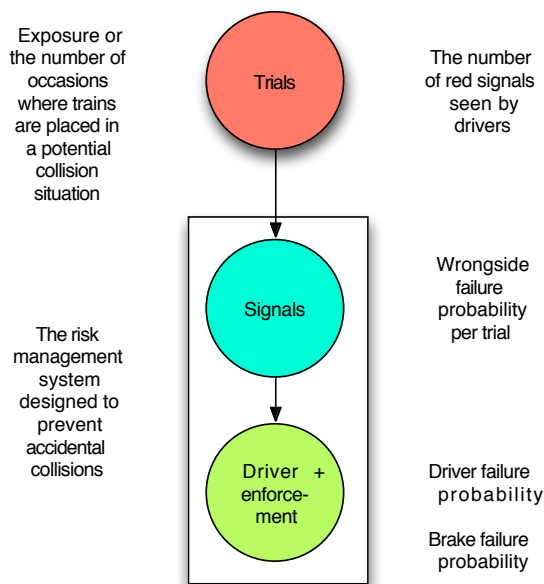
Loss of Control caused by Mechanical Failure



The presence of ship defects (E1) is tested during the Master/Pilot Exchange (E2) when the pilot asks the master if there are any known faults. If possible and necessary the pilot tests equipment / manoeuvres (E4) to ensure it is operational. The pilots then rely on experience and skills and the harbour management team (E6) to deal with a mechanical failure.

The vulnerabilities and escalation scenarios can be modelled as an event tree.

For train signalling, the overall risk model for this process would look like this.



Concept Signalling Model

COMMON LAW SAFETY CASE ARGUMENTS

Any argument that an expert witness could formulate after an event needs to be considered prior to the event.

The Engineers Australia Safety Case Guideline (available online through Engineers Australia <http://www.engaust.com.au/epub.html>) attempts to outline the different ways in which such risk arguments can be formulated. These are also expanded in the R2A text, Risk & Reliability - An Introductory Text 6th Edition (2006).

Efforts to demonstrate how risk should best be managed has given rise to a number of risk management paradigms. Here, a paradigm is defined as a universally recognised knowledge system that for a time provides model problems and solutions to a community of practitioners (after Kuhn, 1970). New paradigms based on more comprehensive or convincing theories may supersede older ones or exist co-jointly with them.

The most common risk management paradigms are:

- i) The rule of law.
- ii) Traditional risk management historically typified by the Lloyds Insurance and the Factory Mutual Highly Protected Risk (HPR) approaches.
- iii) Asset based risk management, typified by engineering based Failure Modes, Effects and Criticality Analysis (FMECA), Hazard and Operability (HazOp) and Quantified

- iv) Risk Assessment (QRA) 'bottom-up' approaches.
- Threat-based risk management typified by Strengths, Weaknesses, Opportunities and Threats (SWOT) and vulnerability type 'top-down' analyses.

- viii) The development of risk culture concepts including quality type approaches.

Many proprietary risk management systems integrate several of these approaches. One of the first tasks when developing a safety case is to determine which of the above paradigms are to be adopted.

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

- v) The comparatively recent market based risk management, which uses the notion of the risk being equal to variance with an equivalent risk of gain as well as risk of loss.
- vi) Solution-based 'good practice' risk management rather than hazard based risk management.
- vii) The development of biological, systemic mutual feedback loop paradigms, practically manifested in hyper-reality computer based simulations.

Although there are a number of risk techniques available, there appears to be only three generic methods by which organisations can proceed with strategic tasks to address the concept of risk. These are:

- a) Expert knowledge provided from experts, literature and research
- b) Facilitated workshops of experts and interested parties
- c) Interviews with selected players.

Each of these methods has different strengths and weaknesses depending on

the culture of the organisation and the nature of a particular task. The best methodologies that might be used to demonstrate due diligence in the implementation of a safety case are highlighted in the tale above.

CONCLUSION

The purpose of a (common law) safety case is to ensure 'due diligence', not to achieve target levels of risk or safety. That is, accidents may still happen but organisations, in addition to their regulatory and statutory responsibilities, also have a common law obligation to demonstrate that all reasonable, practicable precautions are in place.

REFERENCES

- Engineers Australia (2002). *Safety Case Guideline*. Published on-line by Engineers Australia Pty Ltd, Crows Nest, Sydney.
- Kuhn T S (1970). *The Structure of Scientific Revolutions*. 2nd Edition, enlarged, sixth impression. University of Chicago Press.
- Redmill, Felix and Jane Rajan (1997). *Human Factors in Safety Critical Systems*. Butterworth-Heinemann, Oxford.
- Risk & Reliability Associates Pty Ltd in association with Maritime Safety Management Systems (2003). *Formal Safety Assessment to Determine Guidelines / Decision Criteria for Pilotage Services and Risk Management of Marine Infrastructure*. South Port New Zealand Limited, Bluff, New Zealand.
- The R2A Text
Robinson, Richard M, Gaye Francis et al (2006). *Risk & Reliability - An Introductory Text*. 6th Edition. R2A 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.
- Sappideen C and R H Stillman (1995). *Liability for Electrical Accidents: Risk, Negligence and Tort*. Engineers Australia Pty Ltd, Crows Nest, Sydney.
- Standards Australia / Standards New Zealand (2004). *Risk Management. Australia / New Zealand Standard AS/NZS 4360:2004*.
- Standards Australia / Standards New Zealand (2004). *Risk Management Guidelines. Companion to AS/NZS 4360:2004*. HB 436:2004.
- Turner v. The State of South Australia (1982). High Court of Australia before Gibbs CJ, Murphy, Brennan, Deane and Dawson JJ
- UK Health and Safety Executive (2001). *Reducing Risks, Protecting People. HSE's decision making process*. Crown, Norwich.