

---

**JAMES REASON IN ACTION**  
**PILOTS ASSOCIATION PAPER**  
Thursday 15 September 2002

RICHARD M ROBINSON  
Director  
Risk & Reliability Associates Pty Ltd

**CONTENTS**

0.0 ABSTRACT

1.0 CONTEXT

1.1 20th Century Risk Paradigms

1.2 21st Century Safety Cases

2.0 SOME OF JAMES REASON'S IDEAS

2.1 Resident Pathogen Metaphor

2.2 Three Risk Models

2.3 Three Culture Models

2.4 "Swiss Cheese" Model

3.0 SOME DIFFICULTIES

3.1 Latent Conditions

3.2 High Level - Low Level Connections

4.0 SOME APPLICATIONS

4.1 Generative Interview Technique

4.2 Generative Solutions Technique

5.0 CONCLUSIONS

6.0 REFERENCES

**0.0 ABSTRACT**

James Reason's risk control ideas are contextually described in terms of risk paradigms of the 20th century. His biological pathogen metaphor and his culture based models of risk control are described. The strengths and weaknesses of his approaches are briefly discussed and two applications of two generative risk techniques resulting from such ideas explained, namely, a generative interview technique and a generative best practice solutions technique.

## 1.0 CONTEXT

Contextually, James Reason appears as a psychologist ascendant in the last decade of the 20th Century supplementing (with others) the concept of the safety case regime.

### 1.1 20th Century Risk Paradigms

'Risk' means different things to different people although there is common ground based on the notion of uncertainty. If we knew what would happen next then there would be no 'risk'. Demonstrating that risk has been properly managed has given rise to a number of risk management paradigms.

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

The paradigms (from Robinson, Anderson et al) 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 Risk Assessment (QRA) 'bottom-up' approaches.
- iv) Threat based risk management typified by Strengths, Weaknesses, Opportunities and Threats (SWOT) and vulnerability type 'top-down' analyses.
- 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 'best 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.
- viii) The development of risk culture concepts including quality type approaches.

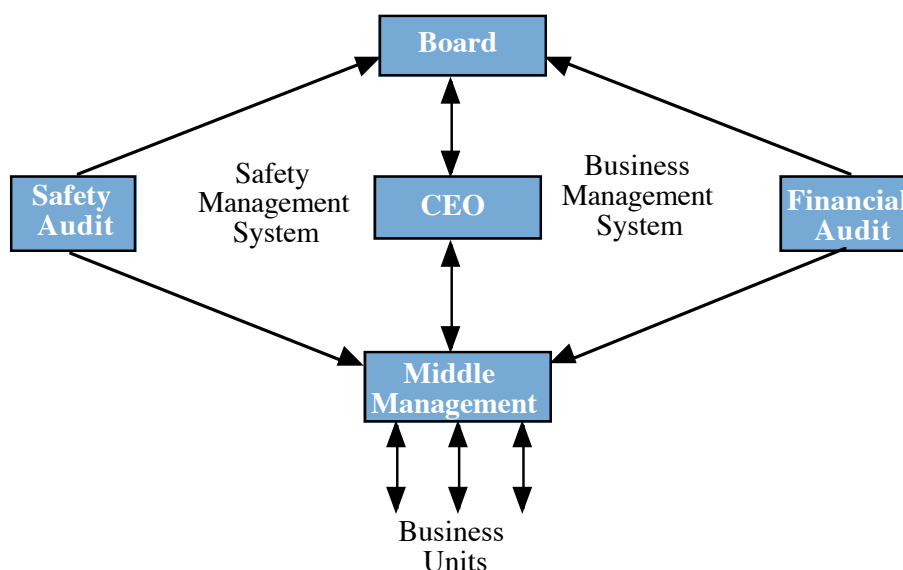
Many proprietary risk management systems use a combination of some of these approaches. As will be seen, James Reason's ideas have been particularly applied in the last three paradigms, namely; best practice, biological simulation and risk culture.

## 1.2 21st Century Safety Cases

With large and complex technological systems, the process of managing safety, health and environmental issues requires a formal management system. The formal approach adopted is usually referred to as a safety management system (SMS). An argument or case that the operation of a facility is performed with acceptable risks is often termed a safety case.

There are parallels to business cases, which are usually drawn up to convince a financier that a business is viable (Redmill). The object of a 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. It is usually the responsibility of the highest levels of management within the organisation. Accordingly, responsibility for the businesses failure usually rests there too.

A safety case is intended to provide the same assurance with respect to the safety of a system or facility. Again it is primarily the responsibility of the operating company, at its highest levels. The Victorian major hazards legislation, for example, requires that the safety case be signed off by the CEO or the most senior company officer resident in the State of Victoria.



**Idealised Safety Case Structure**

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 death and injury occur due to such breaches then serious liabilities arise. Because of this, it appears to the authors that the legal system has converted the safety case concept to a liability management device.

This means that an overriding consideration is that any safety case work be to the satisfaction of legal counsel. This is difficult if the safety task is assigned to technical 'experts' in isolation.

What constitutes a safety case varies from industry to industry. The paradigm discussion from section 1 is relevant. Based on a number of presentations made to various lawyers, those techniques and paradigms highlighted in the table at least can be used in developing a safety case.

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

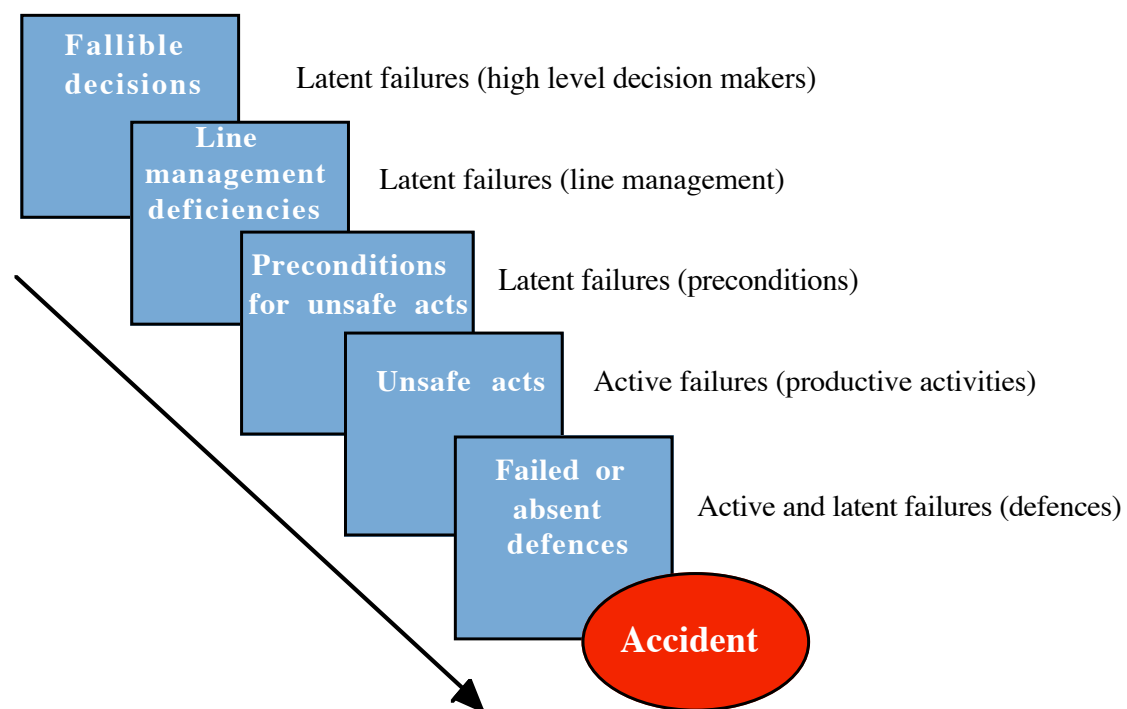
### Risk Management Paradigm - Technique Matrix

Each of the approaches in the cells above has particular strengths and weaknesses. They can be combined in different ways. James Reason's ideas are particularly relevant to the bottom four shaded rectangles.

## 2.0 SOME OF JAMES REASON'S IDEAS

### 2.1 Resident Pathogen Metaphor

James Reason's (1993) resident pathogen model of how things go wrong is described in the figure below. The idea is that latent failures in technical systems are analogous to resident pathogens in the human body, which combine with local triggering factors, for example, life stresses or toxic chemicals, to overcome the immune system and produce disease. Like cancers and cardiovascular disorders, accidents in defended systems do not arise from single causes. Rather, they occur as a result of the adverse conjunction of several factors, each necessary but none sufficient to breach the defences alone. And, as in the case of the human body, no technical system can ever be entirely free of pathogens.



**"Reason" Resident Pathogen Metaphor Model**

Such a view leads to a number of views about accident causation:

- a) Accident likelihood is a function of the number of pathogens within the system.
- b) The more complex and opaque the system, the more pathogens it will contain.
- c) Simpler, less well defended systems need fewer pathogens to bring about an accident.
- d) The higher a person's position within the decision making structure of a system, the greater the opportunity to spawn pathogens.
- e) Local triggers are hard to anticipate.
- f) Resident pathogens can be identified pro-actively.
- g) Neutralising pathogens (latent failures) are likely to have more and wider ranging safety benefits than those directed at minimising active failures.
- h) The establishment of diagnostic organisational signs will give general indications of the health of the high-hazard technical system.

Some form of risk auditing and scoring system could provide an indication of the general health of the risk control system. But the difficulty, as Reason notes, is that even if given a clean bill of health (a 10 out of 10) today, there remains the possibility that something will still occur tomorrow. And predicting precisely which pathogen 'success' and/or control system failure brings about the loss is difficult to know. Reason (1997) notes three types of risk models.

## 2.2 Three Risk Models

### 2.2.1 The Person Model

The Person Model is exemplified by the traditional occupational safety approach. The main emphasis are upon individual unsafe acts and personal injury accidents. It is usually policed by safety departments. The most widely used counter measures are 'fear appeal', unsafe act auditing, new procedures, training and selection.

### 2.2.2 The Engineering Model

The Engineering Model is system based and quantified where possible. Counter measures are engineered into the system using devices such as HazOps, FMECA's etc. Measures include quantified individual risk and societal risk.

### 2.2.3 The Organisational Model

The Organisational Model is allied to crisis management. Human error is a consequence and not a cause. Countermeasures aim at an 'informed culture'. Safety may be measured as quality.

Reason (1993) suggests a 7-point rating scale for overall organisational risk control:

- i) Pathological  
barest minimum industry safety practices
- ii) Pathological /low reactivity  
one step ahead of regulators, some concern re adverse trends
- iii) Worried /reactive  
anxious about a run of incidents or accidents
- iv) Repair /routine  
sensitive to events, safety data collection /analysis but local repair only
- v) Repair /some proactivity  
wide range of auditing but "technocratic" remedial measures
- vi) Reform /generative  
aware that engineering, selection, training not enough, looking for better
- vii) Truly generative  
proactive measures in place, safety measures under continuous review, range of diagnostic/remedial measures being considered, not complacent or self-congratulatory, still afraid of the hazards.

## 2.3 Three Culture Models

Audit systems can often be seen to favour one or more of these models. Reason also notes three types of culture, each having particular characteristics.

### Pathological Culture

Don't want to know  
Messengers are 'shot'  
Responsibility is shirked  
Failure is punished or concealed  
New ideas actively discouraged

### Bureaucratic Culture

May not find out  
Messengers are listened to if they arrive  
Responsibility is compartmentalised  
Failures lead to local repairs  
New ideas often present new problems

### Generative Culture

Actively seek it  
Messengers are trained and rewarded  
Responsibility is shared  
Failures lead to far reaching reforms  
New ideas are welcomed

For Reason, an informed culture = a safety culture.

It has the following components: a reporting culture, just culture, a flexible culture and a learning culture.

### 2.3.1 A Reporting Culture

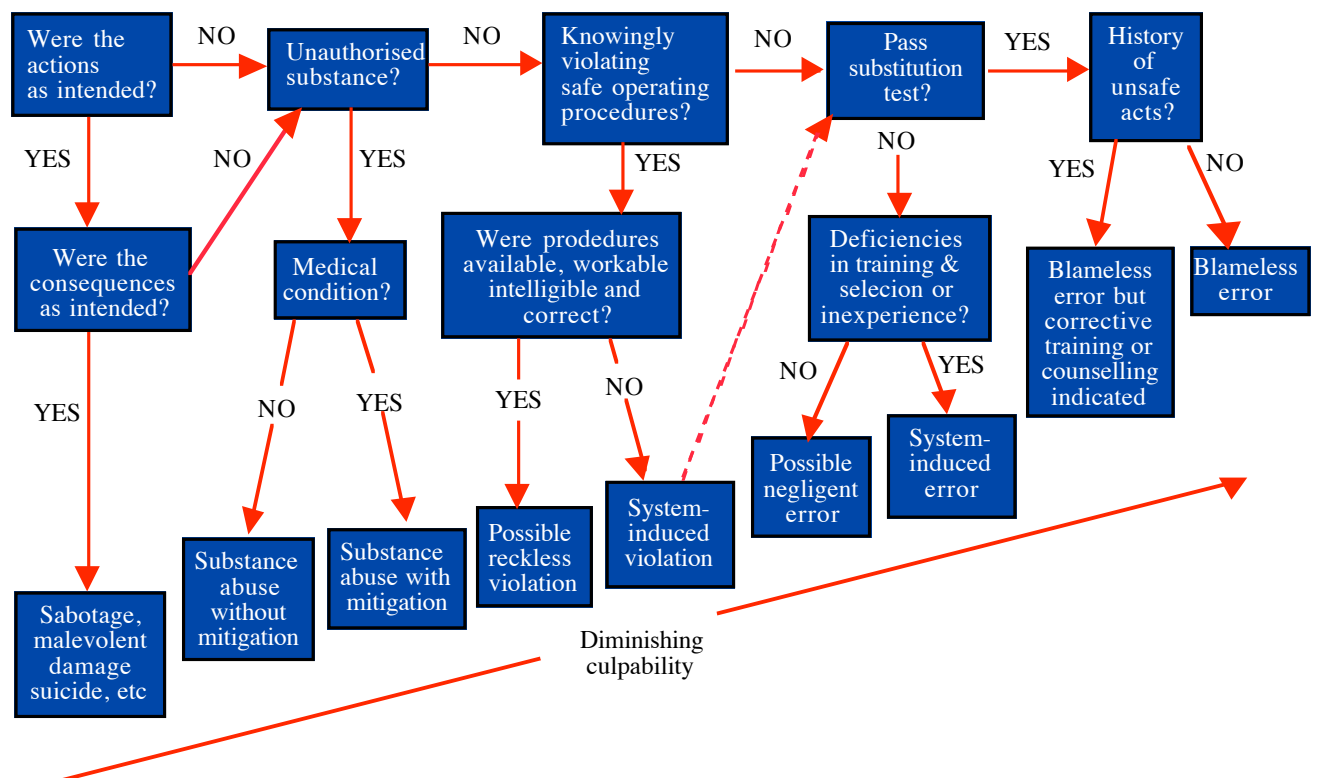
#### *Disincentives*

- Extra work
- Scepticism that anything constructive to prevent it will happen
- A desire to forget all about it
- Lack of trust and
- Fear of reprisals

#### *Incentives*

- Indemnity against disciplinary proceedings
- Confidentiality or de-identification
- The separation of the agency or department collecting and analysing reports from those bodies with the authority to institute disciplinary proceedings and impose sanctions
- Rapid, useful, accessible and intelligible feedback to the reporting community
- Ease of making a report

## 2.3.2 A Just Culture



**A decision tree for determining the culpability of unsafe acts**

## 2.3.3 A Flexible Culture

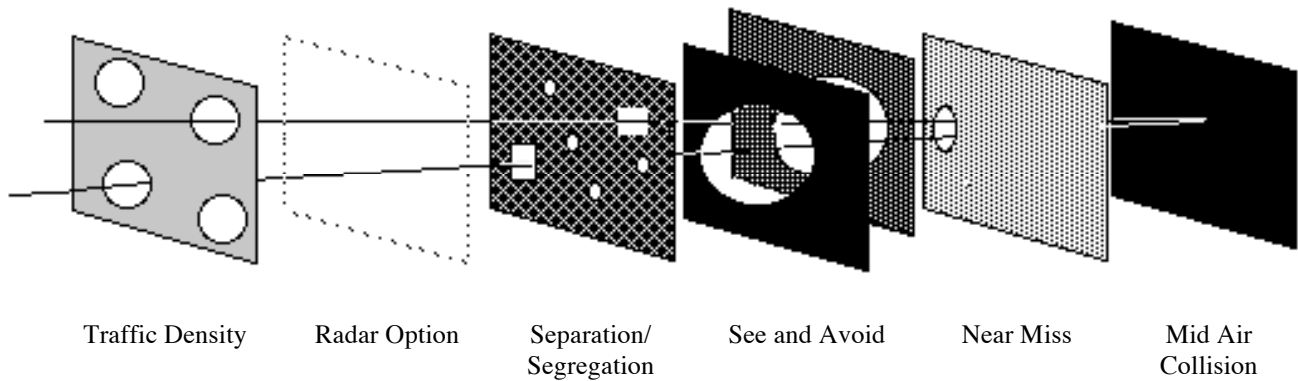
- \* A culture that favours face-to-face communication
- \* Work groups made up of divergent people (with shared values and assumptions)
- \* Able to shift from centralised control to decentralised mode in which the guidance of local operations depends largely on the professionalism of the first-line supervisors

## 2.3.4 A Learning Culture

- \* Observing (noticing, attending, heeding, tracking)
- \* Reflecting (analysing, interpreting, diagnosing)
- \* Creating (imagining, designing, planning)
- \* Acting (implementing, doing, testing)

## 2.4 "Swiss Cheese" Model

James Reason is also noted for his so called "Swiss Cheese" model which is an interesting method of presenting decision tree theory (Robinson, Anderson et al).



**Series of Failure Required for a Mid Air Collision to Occur**

## 3.0 SOME FRUSTRATIONS

### 3.1 Latent Failures

Latent failures, are failures which is not detected and/or enunciated when it occurs, disable protective mechanisms or reduce safety margins thereby increasing the risk associated with hazards due to subsequent conditions or failures. Latent failures, by themselves, do not constitute a hazard (that is, by themselves they have no effect which would make them noticeable, otherwise they would not be latent, by definition). Usually latent failures affect only functions which are not relied upon in normal operation, but which provide fail-safe coverages and/or protection against abnormal conditions. (SAE ARP 4761, appendix D)

The notion of latent conditions has re-emerged in causation recently, largely as a result of James Reason's (1997) promotion of *latent conditions*. J L Mackie (1965) outlines a situation which can be used to explore the concept:

Suppose that a fire has started in a house which is extinguished before it consumes the house completely. Fire investigators will investigate the cause and may conclude that it started in some wiring due to a short circuit. However, this is not a simple concept.

#### 3.1.1 Necessary Conditions

A necessary condition is a positive condition that must be present for the incident to occur. In the example of a house fire, necessary conditions include combustible materials and an ignition source. From this definition a short circuit is not a necessary condition in a house fire as hot oil fires on stoves and children playing with matches are other well known domestic fire sources.

### 3.1.2 Sufficient Conditions

For an incident to occur there must also be sufficient conditions. For example, there has to be sufficient nearby combustibles in an appropriate configuration with an adequate supply of air (oxygen) to cause a fire.

### 3.1.3 Negative Conditions

Negative conditions are the absence of certain conditions causing a fire. For example:

- \* a correctly sized fuse (which would have prevented the short circuit in the first place),  
or
- \* the failure to enclose the cable in metal pipe to shield it from combustibles, or
- \* the absence of a nearby automatic sprinkler which would have minimised the fire, or
- \* the absence of a micro-meteorite that would have crashed through the area just as the fire was about to start.

Obviously, negative conditions are problematic because they can include a vast array of unpredictable 'what if' possibilities.

### 3.1.4 Controllable Conditions

What the fire investigators may be attempting to do is to describe those conditions that they believe should have been considered *controllable*. This is in some ways problematic since establishing all the relevant conditions can be a very difficult task, especially if it is deemed to include all aspects of human behaviour in the context of underlying cultural, social and economic circumstances.

To establish what might be practicable, some form of probability test seems to be applied. The legal tests of causation appear to be relevant. If a *negative* condition was removed would it have:

- \* controlled the situation beyond reasonable doubt? or,
- \* controlled the situation on the balance of probabilities?

### 3.1.5 Latent Conditions

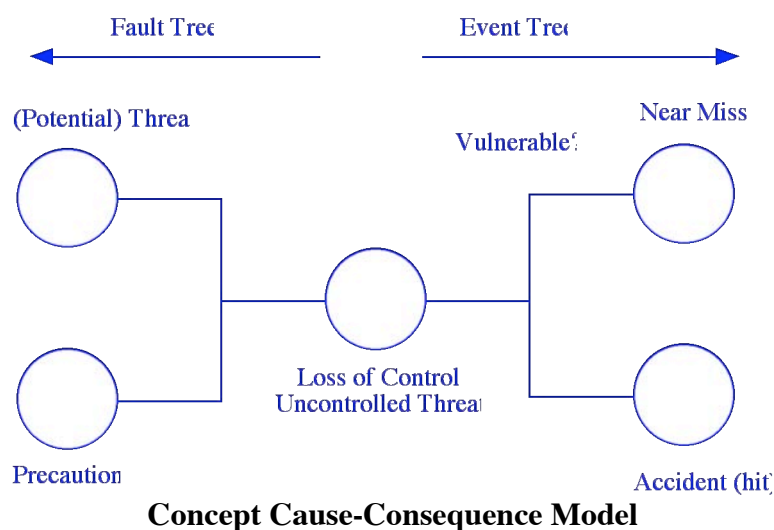
The notion of latent conditions seems to rest around some form of failure that is not apparent when it occurs, similar to a hidden or concealed failure in FMECA (Fault Modes, Effects and Criticality Analysis). So, like a software error, a latent condition waits until a particular pattern of circumstances arises enabling a catastrophe. In this sense, latent conditions would be *controllable*, possibly *negative* and *necessary* not but *sufficient*.

### 3.2 High Level - Low Level Connections

Cultural models tend to generate key safety indicators, where trends are observed in numbers of faults and incidents. A poor trend indicates ill health of the systems and vice versa. However, such indicators do not necessarily give an overall indication of safety system functionality as:

- i) They are reactive indications in that they rely on trends observed in “undesirable incidents”.
- ii) There is no explicit consideration of the importance of the various faults measured.
- iii) There has been no systematic development of the indicators as a group to ensure that all issues relevant to safety are addressed.
- iv) This method assumes that controlling the number of small incidents will necessarily prevent major incidents.
- v) Trends indicate changes from the current state, rather than indicating the absolute performance.

These are all serious difficulties. One answer is to use cause-consequence modelling to create a Safety Lead Indicator Model (SLIM). In its simplest form, a cause-consequence model for a particular “hazard” can be expressed as a combination of a fault tree and event tree as shown below.



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

For a single severity of outcome to an accident this can be presented conceptually as a table shown below.

	Threat 1	Threat 2	Threat 3	Threat i	Threat j	Totals
Threat (hazard) frequency	10 pa	1 pa	100 pa	etc	etc	85 pa.
Precaution failure probability	0.1	0.01	0.001	etc	etc	? pa
Vulnerability (hit/miss) ratio	0.5	0.01	0.2	etc	etc	? pa
Accident Frequency	0.5 pa			etc	etc	0.1 pa

**Concept SLIM Table**

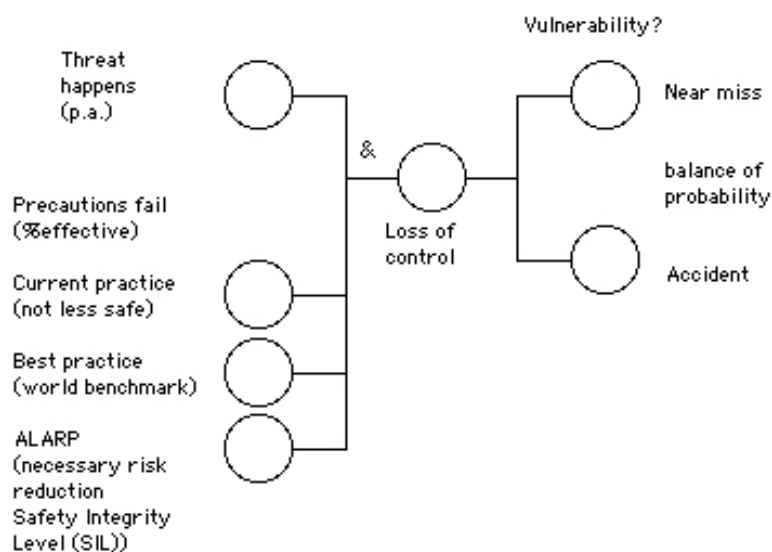
The performance of the area in grey are Lead Indicators since these should be assessable before an accident or near miss. However, the whole process can be calibrated to historical experience. A projected change in threat frequency, or precaution failure or degree of vulnerability can be easily assessed in the model.

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

- "not less safe" - reliability of existing defences
- "best practice" - what other organisations and comparable industries do to manage similar threats
- "as low as reasonable practicable" - the balance of the significance of an additional precaution of defined safety integrity level versus its cost.

For example, if the reliability of existing defences is assessed as 999 in 1000 demands (1 in 1000 failure rate) then the safety requirements as regards the incidence of threat become:

- threat shall not happen say, no more than 100 events per annum, and
- precautions shall not fail, no more than 1 in 1000 demands.



**Legal Focus of Cause-Consequence Model**

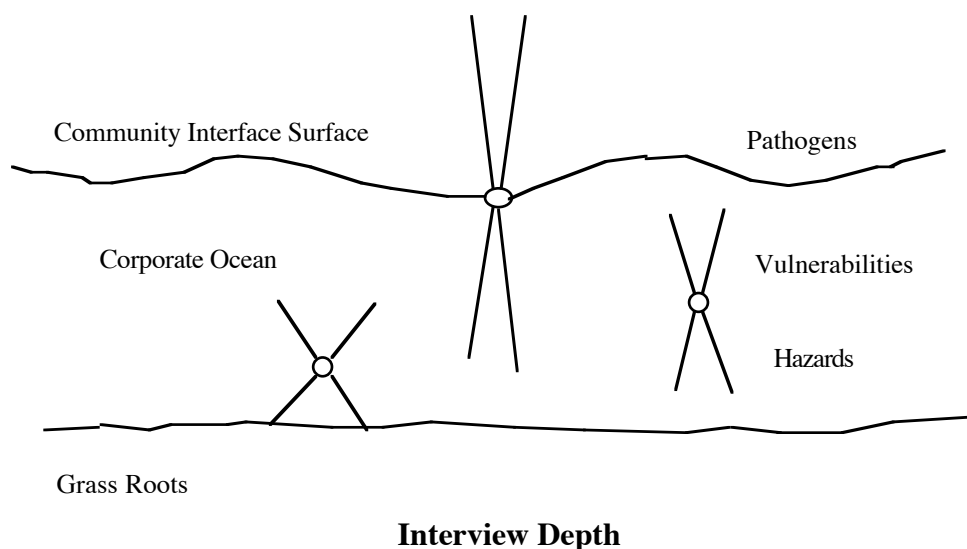
## 4.0 SOME APPLICATIONS

### 4.1 Generative Interview Technique

An alternative approach to the traditional auditing processes would seem desirable to ensure a growing, generative process in accord with James Reason's ideas rather than a negative, constraining, encrypted framework.

Such an approach is safety culture and safety case focussed. It recognises that accidents within an organisation are not primarily the result of an individual's action at the time of an accident (the *active error*). Rather accidents are really the result of a combination of *latent* errors in the organisation that may have existed years before the accident took place.

This is a top down enquiry and judgement of unique organisations rather than a bottom up audit for deficiencies and castigation of variations for like organisations. The object is to delve sufficiently until evidence to sustain a judgement is transparently available to those who are concerned. (Enquires should be positive and indicate future directions whereas audits are usually negative and suggest what ought not to be done).



The idea is that team interviews recognised 'good players' at each level of the organisation. If a commonality of problems and solutions is identified consistently from individuals at all levels then adopting such ideas would be fast and reliable. Other positive feedback loops should be created too. The process should be stimulating, educational and constructive. Good ideas from other parts of the organisation ought to be explained and views as to the desirability of implementation in other places sought. As a preliminary guide, the Table on the following page can be used.

This is really a best practice focus by identifying success factors (what is being done well) and how this can be extended. It is also a recognition that all organisations are unique and that there are different ways of achieving success.

## SAMPLE GENERATIVE INTERVIEW GUIDE OVERVIEW

### A WHAT IS UNDERSTOOD BY RISK AND RISK MANAGEMENT?

*The purpose of the section is to obtain the interviewee's initial perception on risk management in the organisation.*

- A.1 What is risk? (pure/business/speculative).
- A.2 What is risk management? (AS 4360 vs other concepts like assurance, quality etc)
- A.3 What risks are relevant to you? (Types, concerns etc).
- A.4 What risk management approaches do you currently use?
- A.5 How effective do you believe your risk management systems are?
- A.6 Are you familiar with the requirements of AS/NZ 4360?

### B. WHAT RISK/DEPENDABILITY/ASSURANCE MEASURES AND TECHNIQUES ARE IN USE?

*This section tests knowledge of formal risk related processes.*

- B.1 What specific risk skills have you and/or your people been trained in?
- B.2 What makes you believe that when a (potential) emergency occurs your people will respond well?
- B.3 Have you or others attended courses in risk management?
- B.4 Do you have knowledge of the following techniques?
- B.5 Do you have knowledge of the following codes and standards?
- B.6 Do you have access to and does your staff use the library of past incidents?

### C. WHAT IS THE PRESENT RISK/SAFETY CULTURE?

*This section reflects the issue that systems must match cultures for optimum results.*

- C.1 Is your culture risk pro-active?
- C.2 Does your section have a clear understanding of the organisation's aims?
- C.3 Do your people have a clear understanding of your section's aims?
- C.4 Do you feel there is a good active knowledge of past organisation risk failures?
- C.5 What are your measures of risk performance?
- C.6 Do you receive management feedback on risk performance?

### D. WHAT RISK INFORMATION SYSTEMS ARE IN PLACE?

*This is to test not only the types of risk information collected, but how it is used and the overall integration of these systems.*

- D.1 What are your claims management/insurance/legal response systems?
- D.2 How does your OSH&E function operate?
- D.3 How does the internal audit system function?
- D.4 Is the whole of life cost of risk available in the organisation information and planning systems?

### E. WHAT CHANGES WOULD YOU SUGGEST FOR RISK MANAGEMENT?

*This section is particularly focussed at what positive things could be done to enhance risk management in the subject organisation.*

## 4.2 Generative Solutions Technique

Hazard based approaches to risk focus on identifying problems, and how they should be controlled. Concepts such as ALARP (as low as reasonably practicable) are often used.

Another approach is just to put up solutions, try them and see which work.

Such an approach was used to develop the “best way forward” for Silver Fern Shipping (Kneller at al 2002).

A top down threat and vulnerability approach was adopted to determine primary issues with regards to potential fires with unmanned engine rooms for the “Taiko” and “Kakariki” following from fires in the “Westralia” and “Helix”.

Such a review concluded (amongst other matters) that stopping all fires from starting is very difficult indeed. But it was also noted that fires in manned engine rooms were generally detected early and managed quickly. Further such detection occurred via various human senses. In addition to sight and smell, a change in the sound pattern or altered vibrations. That is, early detection was achieved by more than just typical fire detection systems. This prompted speculation as to the best early detection system. No crisp answer was available. Much expensive research could be undertaken, but this would commit the organisation to an endless series of unresolvable “what if” problems and possibly an untested technology thereby sapping organisational resources and enthusiasm generally.

It was also noted that the ships engineers received the greatest respect and pleasure from fixing problems and that if they had spare time at sea, there seemed to be an uncontrollable urge to 'fiddle' with things.

In view of this a generative solutions approach was recommended. Basically the two ships chief engineers were each given a budget to buy detection equipment. This potentially included sniffers, cameras (thermal imaging & others) vibration monitors (torsional and longitudinal) sound and noise analysers and the like. For the next few months they fiddled and then returned to the advise of that which worked well on their ship.

This was seen to be cheaper than hiring engineering consultants or researchers to attempt to determine a solution, which might or might not operate in a harsh marine environment. It was also constructive, agreeable and interesting to the crew.

## 5.0 CONCLUSIONS

The psychologists (especially James Reason) in the last decade of the 20th century have added a further dimension to the risk management process, especially in the biological and cultural view.

This has provide a much needed positive focus to risk control resulting in the development of various techniques, including the generative interview approach and the generative solution approach, both of which seem initially at least to be powerful and useful.

However, like many new risk control endeavours, this may only be because the are new. The actual value of the risk culture endeavour may take several more years to evaluate.

## 6.0 REFERENCES

Kneller, A, R Robinson & D McCann (2002) *A Fire Risk Assessment*. Paper presented at the Pacific 2002 Conference. Darling Harbour, Sydney.

Kuhn T S (1970). *The Structure of Scientific Revolutions*, 2nd Edition, enlarged, sixth impression. University of Chicago Press.

Mackie J L (1965). *Causes and Conditions*. American Philosophical Quarterly, 2.4 (October 1965), pp 245-64 and 261-4. Reprinted as Chapter I of *Causation and Conditionals* edited by Ernest Sosa. Oxford Readings in Philosophy. Oxford University Press (1975). pp 15-38.

Reason J (1990). *Human Error*. Cambridge University Press.

Reason J (1993). *Managing the Management Risk: New Approaches to Organisation Safety* Chapter 1 of *Reliability and Safety in Hazardous Work Systems: Approaches to Analysis and Design*. Eds I Wilpert et al. Lawrence Erlbaum Associates Ltd, East Sussex. ISBN 0-86377-309-5.

Reason J (1997). *Managing the Risks of Organisational Accidents*. Ashgate Publishing Limited.

Redmill Felix and Jane Rajan (editors 1997). *Human Factors in Safety-Critical Systems*. Butterworth Heinemann.

Robinson Richard M, Kevin J Anderson et al (2002). *Risk & Reliability - An Introductory Text* 4<sup>th</sup> Edition.

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

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

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