

## **When Organizations Fail: New Thinking on Catastrophes**

By CJ Pitzer

### **Introduction**

Disasters are often tragic outcomes of high-risk technologies such as mining and as the number of mines and worksites increases so does the risk of disaster.

Some accidents are inevitable and happen because of 'interacting failures' that have not been anticipated. The risk is higher when processes are fast and where technological risk control is used, as the control introduces further complexity.

Can we prevent these catastrophes or is risk increasing as a result of increasing complexity of technology and management systems?

Although risk control is perceived to have improved, is this activity just illusion with the likelihood of catastrophes increasing? By focusing on technology and procedures, are we applying the right solutions to the wrong problems?

Our problem is one of *production cultures ripe for error*.

### **Disasters in the international mining industry.**

Comprehensive statistics on international mining disasters are not readily available. Over the last 200 years it is estimated that for the USA alone more than 13,000 miners were killed, whilst internationally this figure could be over 100,000 deaths not including single fatal accidents. The mining industry globally is under public scrutiny for its poor safety records. Why do there seem to be more disasters than in other high-risk industries? Are there greater risks or is safety not being managed as well?

### **Risk exists in the eye of the beholder.**

Risk like beauty exists in the eye of the beholder.

The science of risk management with its complex modeling of probability, exposure and consequence, has created the misconception that risk can be quantified. Safety managers therefore mistakenly try to deal with risk as something that can be precisely measured and managed.

However, risk is not simply physical but is dependent on the 'beholder'. Everyone makes their assessments based on their own experiences. People tend to ignore,

'misperceive' or deny events that do not fit their worldview.

How we look at risk is extremely important. If we accept risk as a physical entity that can be managed, then management must be to blame when an accident happens. They know the risks, they violate safety rules and pursue economic goals at the cost of workers' lives.

If, instead, one accepts the argument that risk depends on the 'beholder', a totally new perspective on disasters and accidents emerges.

Three high profile disasters pointed to management culpability:

- The Challenger Shuttle disaster of 1986.
- The Piper Alpha disaster of 1986.
- The Moura disaster of 1994.

Using these examples, it is possible to suggest other explanations for major disasters and raise an alternative approach to preventing and inquiring into accidents.

### Lessons from Challenger

*An organisation is a complex set of dynamics, systems, power plays, actions and reactions.*

The Challenger disaster offers an excellent case study of these complexities.

#### **Countdown...**

On 26 January launch was rescheduled to 27 January because of poor weather.

On 27 January, during countdown, alarms indicated a problem with an exterior latch locking mechanism. Launch was postponed for a few hours.

Wind speeds at the launch pad increased above an acceptable level, and launch was re-scheduled for 28 January.

The weather forecast predicted launch temperatures below 20F, and Thiokol engineers, the manufacturer of the solid rocket boosters, were asked to assess the risk. They expressed concern as below 56F was their threshold, and recommended that the launch be postponed for a few hours.

NASA reacted harshly, with one senior administrator asking over the phone, 'My God, when do you want us to launch, next April?' Thiokol was asked to review their decision.

After discussion, three of the four top administrators in Thiokol changed their vote to launch, but the fourth, more junior, person still disagreed. He was told to 'take off his engineer's hat and put on his management hat'. He changed his vote. Thiokol changed their recommendation to 'OK to launch' and the launch procedure re-commenced.

#### **Launch...**

On 28 January 1986, at 11.38 am, Challenger was launched. 73 seconds later a huge fireball erupted and Challenger disappeared in a cloud of smoke and the seven crew members died.

#### **The cause...**

A cheap O-ring failure caused a multi-billion dollar project to fail. But was it that simple?

NASA had known for a long time about the O-ring problem. A year earlier, a budget analyst wrote a memorandum warning about the risks associated with the O-ring and seal failures. A NASA internal memorandum prior to the disaster also warned about suspect seal technology. Seal erosion on rocket boosters had occurred 12 times since 1977.

The night before the Challenger launch, Thiokol had warned NASA about the possible risks associated with O-ring failure. Charts and graphs were produced clearly showing the serious doubts Thiokol had about launching.

A separate contractor, Rockwell, builders of the shuttle, did a launch pad inspection prior to launch. They found ice on the rocket outlets and equipment, and they also recommended that the launch be postponed.

The final recommendation that NASA managers made to the senior NASA management the next morning was simply: 'OK to launch'. This communiqué said nothing of the cold weather, the launch postponement recommendations the previous night, or Thiokol's concerns about the O-ring problem. There was obviously an effort to avoid stirring up concerns at a senior level.

*The President's Commission of Inquiry into the Challenger disaster came to the following conclusions.*

#### **Enormous pressure to launch...**

NASA was under enormous pressure to launch for many reasons:

- Budget cuts by Congress.
- Competition from European space program
- Commercial and military viability of the shuttle program
- Inability to sustain the high launch rate needed to demonstrate its economic viability
- Previously postponed launches.

- Massive publicity because of the first civilian (teacher) astronaut on board.
- The media linking the timing of the launch to an important presidential speech by Reagan

### **Organizational causes...**

Organisational causes were identified as:

- Budget cuts and associated compromises to safety.
- A widening gap between NASA goals and the means to achieve them.
- Flawed decision making processes.
- Substantially reduced work forces.
- Managers overriding engineers concerns.

In short, production pressures and managerial wrongdoing appeared to be the culprits.

The NASA managers were highly competent people who thoroughly understood the engineering and managerial issues involved but to secure resources for their organisation's survival, and to please their shareholder, the U.S. Government, they took a calculated risk, violated safety requirements, and they lost.

Afterwards their decisions could be shown as flawed and even callous.

### **Why do good people do such 'dirty work'?**

The pressures and organizational problems experienced by the NASA managers are common in most organisations with production pressures compromising safety, and middle managers and workers routinely taking risks - despite commitment to safety.

When managers are well-qualified with positive intentions within their organisations, why do they violate rules and regulations, and make decisions that lead to loss of lives and property? In recent years, almost all public inquiries into mining and industrial disasters have supported such findings and blamed management. Why do good people

do such 'dirty work'? Are managers conscienceless 'amoral calculators' of risk?

The answer is 'no' and Challenger gives us two reasons to support this.

### **Anecdotal evidence...**

*A disaster inquiry performed by highly qualified people is flawed by the quality of information available at the time.*

Anecdotal evidence is:

- Often distorted (intentionally or unintentionally)
- Incorrectly assessed as linked to the disaster when it is not linked.
- Ignored if it doesn't fit the model of 'managerial wrongdoing'.

The President's Commission on the Challenger disaster found safety and production trade-offs. But an intensive revision of the same report showed most decisions were made in the interests of safety. Only exceptional cases of trade offs were found - made after competent consideration of opposing facts.

A similar review of the Moura Disaster shows the majority of decisions were made in the interests of safety and this is true in most companies today.

The logic behind the managerial safety/production trade-offs argument is flawed. In a production-oriented organisation, it makes no sense for managers to make decisions that risk their jobs, the lives of employees and the future of the organisation for relatively little gain.

Money spent on training, on systems and controls, and on most activities of a mine is inherently meant to ensure safety. This spending is so routine that its contribution to safety is no longer recognized. When driving your car try to identify any action which is *not* designed to ensure your or others' safety. Except for stepping on the accelerator to make the car go (production) everything else is focused on safety.

**Honest errors...**

The second argument against the 'manager as amoral calculator' is the possibility of making honest errors in risk calculation.

The science of risk management suggests that probability of an event can be calculated on the basis of the likelihood of it occurring e.g. 2 times per million per annum. Statistically this is correct, but people cannot relate such a figure to a specific task. How can a manager judge whether a task is 'too risky' unless perhaps the probability of an accident is approaching 1 (100%) and highly likely e.g. jumping off a cliff?

Most work place accidents are in the category of highly unlikely (e.g. 0.0000002%) a level that our minds cannot relate to. Managers use 'gut feel' in these circumstances. Even after the Challenger disaster, the engineers of NASA could not agree on the likelihood of the failure. Their estimates ranged from 1 in 100 launches to 1 in 100,000 launches which equates to a difference of one failed launch every ten years or one failed launch every ten thousand years!

In summary, the argument that managers are 'good people doing dirty work', and that their actions can actually be classified as 'criminal' is seriously flawed. Yet this is widely accepted, even by managers themselves. The many events that make up a catastrophe can be so trivial and banal by themselves that they are routinely overlooked, underestimated or ignored. In the catastrophic interaction of these events, however, the accusations of dirty work and management wrongdoing are often inescapable.

**Who is to blame?**

Unfortunately an inquiry or accident investigation is a blaming process with the operator, their superior or, more likely today management, being blamed for events over which they may have little control. These people cannot carry the blame automatically for two reasons: **interactive complexity** (and associated with this

operator/managerial incompetence) and **normalization of abnormal events**.

**Interactive Complexity**

Virtually every type of industry rates operator error high on its list of causal factors, generally at a level of about 60 to 80%. Is this valid? Let us look at the first reason for shifting the blame away from operators or managers - the issue of complexity.

From the earliest times there have been 'God-made' natural disasters. With industrialisation we created man-made disasters with devices that could crash, sink, burn or explode. We prevented these accidents by discovering and removing their causes with technology.

We then declared war on human error and did this by training, conditioning rewarding and regulating workers. This still continues with a proliferation of health and safety legislation, and the advent of risk and/or loss control management systems. Combined with a huge increase in technology over the last 25 years, we have added a new cause of accidents: 'interactive complexity'.

Perrow (1984) provides a classification system of types of industries which is a useful framework to identify high-risk or disaster prone circumstances. The two continuums used are *Complexity to Linearity* and *Tight and Loose Coupling*. See diagram.

Complex systems have tight spacing of equipment, proximate production steps, personnel specialisation, unfamiliar or unintended feedback loops, many control parameters with potential interactions and limited understanding of associated processes in the organisation.

Tightly coupled systems have time-dependent processes eg chemical reactions in a chemical plant. Sequences of activities are invariant, and the production processes are fixed. There is little 'slack' in tightly coupled systems.

	Linear	Complex
Tightly Coupled	<ul style="list-style-type: none"> <li>▪ Rail</li> <li>▪ Airways</li> </ul>	<ul style="list-style-type: none"> <li>▪ Nuclear</li> <li>▪ Space</li> <li>▪ Oil Rigs</li> <li>▪ Chemical Plants</li> <li>▪ Deep Underground Mines</li> </ul>
Loosely Coupled	<ul style="list-style-type: none"> <li>▪ Assembly line production</li> <li>▪ Most manufacturing</li> </ul>	<ul style="list-style-type: none"> <li>▪ High volume mines</li> <li>▪ Open Cut Coal</li> <li>▪ Military</li> </ul>

The working environment and organizational structures of the mining industry place it in the highest risk category for disasters. With the incidence of disasters far higher than other higher risk industries, Perrow concludes that the mining industry is simply 'not managing safety well enough'.

Mining employees are subjected to increasingly complex systems of management, engineering and legislation. Operators are expected to:

- make rational observations of the environment,
- rationally interpret requirements and procedures and,
- act rationally on those interpretations.

But it is unlikely that the average operator knows all possible links and interactions. *After an accident*, this operator would recognise his mistakes and identify the alternatives he should have selected. But this is only *after* the event. *Before* the event the possibilities can be complex and this can lead to error.

It is also the case that great events have small beginnings. On the Piper Alpha oil rig, an inadequately tightened flange on a gas pipeline leaked causing gas to ignite, but a complex interaction of factors prior to and at the time, led to the death of 162 people.

At Moura there were layers of systems in place including engineering knowledge, administration systems, legislative requirements, a quality management system, a safety management system and a risk management process. All had their own safety requirements, regulations and auditing. The level of complexity of each of these systems is mind-boggling but the interactive complexity was disastrous.

Is the only way to avoid disasters caused by human error such as in Piper Alpha, to train operators to tighten flanges, punish them if they don't, and reward them if they do?

In mining and other high risk industries, current workforces are probably over-trained, over-rewarded and under-punished. Accidents continue because we are fighting them through use of probability-based risk

assessments which introduce more rules and systems, and more interactive complexities. Ironically, the more risk assessments and analysis we introduce, the more we *increase* the risk.

*As low as reasonably achievable...*

Risk assessments can even lead us astray. Consider the following scenario:

The Board of a company is advised that if it does not install a safety device, there is likely to be the death of one more worker per year in a business employing 130,000. With a depressed labour market and an attitude amongst workers that fatalities happen to someone else, the company is not under pressure to install the device. By not installing the device, the Company will save \$50 million, and the saving will enable the Company to avoid a \$20 million price rise in their products and allow it to retain this year's merit bonus of \$30 million. Against a statistical probability of one worker death per year, the customers, the shareholders and the workers will greatly benefit. The Board considered that \$50 million is a high cost for the possible loss of a worker and the safety device was not installed.

In the real world a similar decision was made at the Ford Motor Company when they decided not to buffer the fuel tank in the Pinto car leading to a significant increase in fatal accidents where crash victims were burned to death.

Risk assessment is about getting risk down 'as low as *reasonably* achievable'. With this thinking, companies use risk assessment to try to quantify the cost of accidents, if only to express concern that accidents are costing money or prove that safety practice is good business.

There should be concern at assessing physical risk without considering *sociological risk* - the thinking patterns and the influences within the organisation. Without considering both, a potentially damaging definition of risk is created.

Is the situation as bad as shown here? Looking at our day-to-day operations it is not so bleak. Coal for instance is produced in

greater volumes, more efficiently, and with fewer accidents. Risk management, however, still seems to be the 'beast' within our organisations. So why is there a perception of 'risk-taking amongst management'?

### **Normalisation of Abnormal Events**

The second reason why employees cannot be blamed for a disaster is called the 'normalization of abnormal events'. Three factors explain this process of normalization - the **production of culture**, the **culture of production** and **structural secrecy**.

#### ***The production of culture...***

*A culture is a set of solutions produced by a group of people to meet specific problems which they commonly face. These solutions are passed on as the rules, rituals and values of the group.*

It is falsely assumed that a large organisation has one common culture but organisations are segmented and often have as many cultures as they have sub-units, although these may share some common features.

People in a work group are drawn together through the task they perform, and develop a culture that is unique to that task. Work group cultures ensure that new information is interpreted in terms of the culture concerned.

Before the NASA shuttle program existed, tests showed that the solid rocket booster (SRB) joints which contained the O-rings had unexpected performance deviations. The engineers alerted management who decided it was 'acceptable risk'. *There was no risk at this time because the shuttle program did not exist.*

The workgroup accepted this new standard of acceptable risk for the O-rings - the abnormality was 'normalised' to accept that the O-ring would withstand erosion by hot gases, and in the unlikely event it did not, the back-up O-ring would. Although problems with the O-ring were identified twelve times between 1977 and 1985, the workgroup culture that the O-ring joint was

an acceptable risk was never questioned. For 10 years this 'culture' prevailed, until that fateful morning in January, 1986, despite the occurrence of a new problem; cold temperatures never before experienced. This is the fatal effect of culture.

At most coal mines in Australia during the 1990s, a negative, mistrustful culture existed between the levels of the organisation. Culture surveys conducted by CJ Pitzer (1996) showed extremely negative safety attitudes, largely influenced by a negative industrial relations climate in the industry and Moura probably did not escape this.

### ***The culture of production...***

So why do people 'normalise' abnormalities despite all the evidence? The answer lies in the culture of production.

The engineering and production professions give the impression of precision, rule-making and qualified thinking. Without accidents, there is no opportunity to investigate the thoroughness of their processes. However, if an organisation was subjected to such investigation, it may well expose the production culture of '*flying with flaws*', *margin of error* and *redundancy of risk*.

### ***Challenger production culture***

NASA had two formal processes designed to facilitate the management of launches - the Acceptable Risk Process (ARP), and the Flight Readiness Review (FRR).

The ARP process classified all risks. The O-ring joints were reviewed over many years and, although they were accepted as a risk, there was never any serious doubt about them. Apollo programs had operated with the same design and a secondary O-ring was added as a back up.

'Flying with flaws' was not abnormal in the culture of NASA. This was regarded as 'residual risk' which had been analysed and rationalised through the Acceptable Risk Process. The high level of risk analysis, and the qualification process, created an impression of invulnerability. However, It is

folly to argue that risks are under control because they have been quantified and a control measure introduced - because, as discussed earlier, risks are also social phenomena.

Furthermore, no one in NASA had the ability to recommend that the whole Space Shuttle program be shut down until the SRBs joint was redesigned. Despite all attempts to flag the issue, there was a powerful production culture, which accepted the risk and proceeded with the flight.

### ***Piper Alpha 'flying with flaws'***

On the Piper Alpha Oil rig, the water deluge system, its main fire fighting capacity, was seriously deficient for four years. This deficiency had become 'acceptable and normal'.

Management of Piper Alpha were warned that the gas outlets were extremely dangerous and exposing the workers to enormous risks. The warnings were ignored, and everybody accepted the risks associated with it.

### ***Moura 'flying with flaws'***

The Warden's Inquiry report found:

- The Mine manager was informed that the increase in CO was linear not exponential and it was concluded that no problem was evident
- At Moura No.2 it was the practice rather than exception to continue to work underground as sealed panels passed through the explosive range. The risk was known, defined and accepted.
- Deficiencies in the ventilation system were 'normalised' and with this the lifeline of an underground mine was compromised.

### ***Margin of error and redundancy of risk***

With Challenger, there was a history of successful launches and the back up of the secondary O-ring which provided a 'margin for error' and with this came the next critical ingredient for a disaster: the *redundancy of risk*. With this culture in the organisation the

acceptance of risk slowly increases and with it the potential for disaster.

Data existed showing that of all flights launched above 65°F, 17% had O-ring anomalies during launch while those launched below 65°F had 100% anomalies. On 28 January, NASA launched at 27°F. The graph of this data was never drawn and an opportunity to avert the disaster was lost.

Similarly at Moura, a graph could have been drawn to show the increases in CO and the Graham's ratio, which, had it been used with other information, 'may have tipped caution in the right direction'. The inquiry also found other examples of the gradual risk acceptance through belief in margin of error.

The belief in a margin of error occurs in all high-risk work environments. In these organisations a 'mindset' develops that risk can and should be conquered. The most fundamental purpose of organisations such as NASA, oil rigs and mining companies is to conquer risk, through a belief in their ability to achieve, a culture of 'can do' and a belief in the redundancy of risk.

An organisation that does not believe in the redundancy of risk will find it impossible to continue as a business. And therein lies the irony – what makes us successful in a high risk industry is also our undoing.

### **Structural secrecy...**

This is our third factor that comes into play with 'normalisation' of risk and involves the phenomena of  *censorship*  and  *distortion* . The result is top people get very little of the information churning around in their organisations. The sheer quantities of information are such that they could not make sense of it all anyway unless it was drastically filtered. Decision-makers have to rely on 'signals' based on their experience but the bulk of the information remains unknown to them.

After the launch of Challenger it was revealed that the higher levels of NASA were not informed of the concerns expressed by Thiokol about launch. According to Centre Director Lucas' testimony, NASA's directors were only

afterwards informed of Thiokol's and Rockwell's warnings. He said that he had been told that "an issue concerning the weather had been resolved, and that the launch had been discussed very thoroughly by the people at Thiokol and the Space Flight Centre and it had been concluded agreeably that there was no problem". He said further that he had a recommendation by Thiokol to launch and the "most knowledgeable people and engineering talent had agreed with the recommendation".

The President's Commission found communication problems existed and lower levels of management had deliberately withheld information flowing to the senior levels.

*Was it just a question of deliberate withholding of information - a human failing - both understandable and punishable? Or were senior management to blame - if it was their autocratic, aggressive behaviour that led to the suppression of communication?*

The answer is not that simple. Secrecy is built into the structure of organisations. Knowledge about tasks and goals is segregated through geographic location, levels of management, specialisation and division of function. Communication systems are so complex that  *more*  communication frequently results in  *less*  knowledge.

Secrecy also develops as a result of weak signals. Even if people overcome their reluctance to voice opinions about danger, risks or threats, their signals may simply be too weak to be heard. One engineer at NASA explicitly recommended that launches be terminated until the problems with the O-ring failures were sorted out. This signal was not given to anybody with sufficient authority to do anything about it -  *it was too weak to be heard* .

### *Systematic censorship...*

One phenomenon of secrecy in the organisation is the process of 'systematic censorship' over which management has no clear control. At every level of all

organisations, information censorship takes place for several reasons.

There is a natural tendency at every level to withhold as much bad news as possible. Although this can lead to catastrophe, it is also a useful process, as it can result in decisions being taken at the appropriate level of the organisation, and only critical exceptions are communicated to senior management.

In the industrial relations arena, mines are implementing benevolent and very participative management systems, while unions struggle to establish a new role for themselves. Their old view of management exploiting workers means they still see their role as fundamentally that of protection. This results in philosophical conflict between the opponents with increased secrecy at the lower organisational levels. In this way unions may even contribute to the very processes that foster a high-risk culture.

Job specialisation contributes to the loss of information sharing in organisations. Specialists experience difficulty in sharing information even amongst themselves. Added to this is the tendency for engineers to become managers and administrators. They lose their hands-on exposure and understanding of production and engineering processes and consequently their ability to deal effectively with the technical information they receive from lower levels.

The creation of specialised safety departments and some kind of safety and/or risk management system in many organisations is another contributory factor. These departments and systems can create paperwork, terminology, information and interventions which managers have to accept on face value and visibly support.

#### *Systematic distortion...*

While 'systematic censorship' withholds as much bad news as possible from the top levels, 'systematic distortion' occurs where people tend seek out favourable information to the exclusion of negative information.

Such distortion lies in the tricky area of 'failure probabilities' or 'disqualification heuristic'. In simple terms, if you hold a conviction such as it is safe to fly or mining is a safe activity, you will neglect contradictory information and focus on supporting information.

With Challenger, remember how the retrospective estimates of the probability of the failure of the shuttle varied from 1:100,000 to 1:100? The higher probabilities came from engineers and safety officers and the lower probabilities from NASA managers. The engineers' estimates were higher because they had access to more information than the managers.

*In mining and other such organisations there is a 'can do culture' where high production volumes continuously demand a high achievement culture. Very few of these organisations have internal processes that encourage self-criticism and critical self-review. The focus is on survival and therefore normalisation of risk through organisational culture, production culture and secrecy thrives. At some point, these forces in the organisation may become so powerful that, if the right physical conditions exist, a disaster becomes almost inevitable.*

#### *A multitude of signals and probabilities...*

Through these examples *interactive complexity* and *normalization of abnormal events* can be seen to create an incredibly complex situation which clouds the whole issue blame. On top of this, it is practically impossible for any management team to act on the many signals that actually reach them. The levels of probability of the possible events often fall in the range where it is humanly impossible to prioritise between them.

A NASA manager was accused of neglect because prior to the launch he focussed on the problems of the SRB's parachutes instead of the O-ring problem. But, at that stage, the parachute problem of tearing and causing the large boosters to fall back to earth unrestrained was a very urgent, realistic problem. The O-ring was regarded as an acceptable risk. The critical issue here was that he could not make a rational

judgement between two risks of equal probability but of different perceived urgency.

At Moura, the management was dealing with safety problems far removed from the one of spontaneous combustion. Of sixty six risk assessments conducted on that mine site just prior to the disaster, only one dealt with the problem of spontaneous combustion. The management was dealing with urgent problems, reacting to signals which they received about the relative importance of these events. They could not be expected to rate one risk against another and make a 'mathematically correct' decision although after the event it is easy to demonstrate that their failure to do so was neglectful and wrong.

There was also criticism because: '*No one person or group of persons at any time had all the facts available to them on which to base their decisions*'. However, this is quite normal in any organisation where complex processes exist, where decisions are being made at all levels, and where the fundamental aim is to conquer risk. Many other communication issues appeared seriously flawed, such as reports on 'benzene-type' smells underground failing to raise concern and various assumptions being made - such as the *assumption* that workers knew of the risk of spontaneous combustion on the day of the event. All these issues point to the *distortion of information*.

On Piper Alpha, it was 'regretfully evident' to the inquiry that 'management failed in some very basic duties'. Even the decision the manager made to reduce the risk to divers in the water was slammed by the inquiry as a '*wrong decision*'. What this inquiry overlooked in this case that this was a decision in the interest of safety, as was the case with several decisions of the NASA and Moura managers. In hindsight, these decisions appear flawed, but they were not. They were realistic decisions made at the time under realistic circumstances.

The Piper Alpha manager stated in the inquiry that he 'knew that everything was all right because he never had any report of anything being wrong'. The statement may

appear to be extremely naïve but it is more likely that the information that reached him was simply distorted to the point that his only impression could be that everything was all right.

It was no different at NASA with what was reported to the launch director on the morning of the launch and it was no different at Moura. The inquiry of the Moura incident reported that the 'Mine Manager on return from leave was not aware of the condition of the panel even after discussion with the Safety/Training Manager'

*In summary our willingness to accept risk is often underestimated or not even taken into account. The factors which make it possible for us to accept risk and the possibility of disaster include:*

- *Risk assessment processes.*
- *The probability of an accident being incomprehensibly small.*
- *The culture of production.*
- *A margin of error developing misplaced confidence.*
- *Organisational pressures.*
- *Illusions of invulnerability that develop as a result of a 'can do' culture.*

### **The Social Organisation of Mistakes**

Inquiries into all work accidents tend towards the 'politics of blame'. The answers are seldom simple however and they fail to identify the organisational and cultural causes. The heart and mind of organisations are beyond the control of individual managers, because mistakes are socially determined in a highly complex, unpredictable manner.

The Challenger, Moura and Piper Alpha disasters happened because mistakes were made. None was a simple case of human error - the mistakes were 'socially' organised and systematically produced. The source of disasters can be found in the routines and the taken-for-granted aspects of organisational life.

The key questions about Challenger - why did they launch despite their knowledge of the O-ring deficiencies, and the prelaunch warnings by engineers? - can be asked about most disasters and accidents.

The answer lies in the three processes already described: *production of culture, the culture of production, and structural secrecy.*

Each factor on its own cannot explain the disaster examples given - or any other disaster. But in combination with the right combination of circumstances mistakes will happen, some of them leading to disasters.

*In looking for causes of disasters we need to shift our attention from the technical to the managerial, and then to the psychological and beyond - to the organizational and cultural factors. By doing this we highlight the influence of culture on risk assessment. Even if risk assessments are done daily, they can be fatally flawed with their biggest failing being the impression they create of being scientifically complete and sufficient to manage risks. It needs to be stressed that risk is not a 'quantity of threat'. It is a social construct that changes continuously and cannot be captured by simplistic categories or 'levels' of probabilities.*

Routine decisions in organisations are taken every day without resulting in disasters. When disasters are analysed many of these routine decisions can be demonstrated to be flawed and blame is cast on those making the mistakes. Decisions are made within the context of the culture of the organisation and this cannot be ignored, although public inquiries do just that.

*Disasters have long incubation periods during which warning signals are ignored, rationalised or accepted as normal. Organisations need mechanisms to counteract these organisational influences.*

### **The Aftermath of Disasters**

#### ***Public inquiries and accident analysis...***

Public inquiries, despite necessity, have a number of serious flaws which can erode their effectiveness:

#### ***Political Problems***

No inquiry is conducted in a vacuum. The process, and its findings, are a political compromise - sometimes slight, sometimes significant.

#### ***Terms of Reference***

Too often, the terms of reference of public inquiries are too narrow or unbalanced. Inquiries search too deeply into some aspects of disaster, and persistently ignore others.

#### ***Blame and Truth***

The quasi-legal nature of inquiries may also impede the findings, by focusing too much on the blame and guilt of individuals or institutions and too little on the 'heart and mind' of organisations.

#### ***Recommendations of Inquiries***

An overview of the typical recommendations made by public inquiries shows that typically their recommendations can be divided into 5 broad categories:

- Technical
  - Specific technical issues
  - Physical safety precautions
- Social - personnel-related e.g. staff training
- Authority - use of legislation to enforce rules.
- Information:
  - Improve communication and consultation
  - Improve hazard awareness
  - Review rules, standards and knowledge
  - Review existing work practices.
- Attempted Foresight:
  - Design analysis
  - Require experimental investigations
  - New codes of practices.

It is quite common for public inquiries to make a combination of these recommendations, but most focus on the technical and communication aspects. This suggests that inquiries seldom achieve more than a superficial analysis, despite their voluminous nature. The other possibility is that organisations typically make only

technical and communication mistakes - which is clearly not always the case.

### ***About biting dogs and accident analyses in organisations...***

There are many contributing factors to each accident, but accident investigations and analyses tend to focus on the immediate events, behaviours and hazards.

The 'muzzle' approach is often used to deal with accidents in industry. Accidents can be likened to aggressive dogs in the neighbourhood. When a dog bites, it is caught, fitted with a muzzle ('muzzle': a new procedure, a machine guard etc.) and released. Sometimes a dog loses its muzzle and comes back to bite again, but the muzzle is just refitted.

Instead of reacting in this way we should be asking more fundamental questions, such as: 'Why are the dogs so aggressive in the first place? Why are the dogs roaming the streets? Who are responsible for them? Do they have the means to restrain the dogs?' In other words why do the deficiencies in the system exist to cause accidents (or 'biting dogs')?

### ***Developing 'active foresight' from hindsight...***

Accident analysis is essentially hindsight. It may sound contradictory, but we should use this hindsight to produce foresight to prevent similar accidents.

Several authors in the field have proposed the idea of 'active foresight', which is an attempt to identify some of the more fundamental influences, forces and dynamics in organisations.

The analysis that follows in the wake of a disaster is very comprehensive. It includes lengthy official inquiries, recommendations and reports. It generally identifies the proximate causes of the accident and goes on to identify so-called 'root causes'.

Active foresight, on the other hand, goes further than this. More than one inquiry e.g. Piper Alpha has attempted to take the additional step of analysing the

organisation's culture and fundamental systems, to pinpoint deficiencies at these levels. This shows that there is a growing realisation that disasters and accidents cannot satisfactorily be explained by direct and immediate cause analysis.

An in-depth approach like this is very sound because accidents or disasters do not occur solely as a result of technical or operational deficiencies. They are complex phenomena, and symptoms of complex deficiencies in an organisation.

The most important aim of an in-depth analysis is to make it possible to accurately foresee how accidents can occur and introduce interventions that will comprehensively deal with the root causes.

### ***How can an organisation develop foresight?***

For an organisation to develop 'active foresight' it must first understand the various levels in the organisation where deficiencies can occur. These levels are:

- **Organisational** - management and supervision.
- **Systematic** - managerial and functional control such as training and responsibility.
- **Technical** - plant, equipment, maintenance and production systems.
- **Operational** - execution of tasks according to systems, policies, regulations etc.

All these levels are affected by the **behaviour** of people. This behaviour can vary from positively compliant with safety standards, to rule-breaking, short cutting or risk taking behaviour.

Deficiencies at any of these levels may interact and generate accidents. A superficial analysis will pinpoint the technical and operational deficiencies, but this approach will leave *two problems to contend with*:

- The same accident could have been produced by many other permutations of

technical and operational deficiencies which a superficial accident analysis may not identify.

- The systematic and organisational deficiencies are seldom identified, and lie 'dormant' in the organisation to eventually produce an incident or accident again and again.

Different types of instruments must continuously be used to measure each of these levels.

For example, at the most fundamental level, the organisational level, the measurements are done by safety culture surveys; at the systems level, they are done by system audits; at the technical level by risk assessments; and at the organisational level, by behaviour measurement and job safety analysis.

The analysis of accidents and incidents is a critical activity because it offers the organisation a rare insight into the breakdowns in the dynamics and interaction between all the levels. However, it is very rare for an in-house analysis of an accident or incident to go beyond the operational or technical level. Only if an accident results in a fatality or multiple fatalities does the inquiry normally become an in-depth probe into all kinds of 'deficiencies'.

And, of course, the existence of deficiencies cannot be disputed, because the fatal accident is 'evidence' of their existence.

#### ***Flaws in the analysis processes...***

Accident analysis is often the only means an organisation has to identify the breakdowns in its systems and processes. There are, however, major flaws in relying on the ordinary accident investigation process:

- It seldom analyses root causes. The depth in which we analyse accidents is often determined by the seriousness of the accident. Safety literature stresses that the difference between a near accident and a fatal accident is frequently no more than a few millimetres or a few seconds. As a result of this, sadly, most of the time we do not

analyse the root causes of minor incidents or accidents because of complexity and expense.

- The inquiry is subjective. This is especially the case if there were several fatalities - where the tragic loss of life provides proof of serious deficiencies in the organisation. This inevitably leads to an automatic assumption of guilt on the part of the company and its management - a reversal of the normal legal process of 'presumed guilty until proven innocent'. It is not argued here that the company where a disaster or fatality occurred can claim innocence. Instead, it is argued that if deficiencies are identified in one company, the very same deficiencies will most likely crop up in the most other similar organisations in the industry, without necessarily resulting in disasters or even fatal accidents.
- An inquiry can only identify and investigate what is apparent in the organisation at that particular point in time. This 'snapshot' of organizational deficiencies may be totally off the mark for the organisation over a period of time, even though it may be correct for the specific period being investigated. Organizational dynamics are just too complex. Such inquiries do not analyze trends and dynamics in the organisation over a *longer* period of time.
- However, public inquiries are almost without exception staffed with technical and managerial personnel. They will focus on technical and managerial issues. Every enquiry should perhaps be required to draw upon the expertise of social scientists.
- Investigators of accidents may themselves be extremely prone to commit a whole host of errors. The most obvious stems from the fact that they are *there to find something wrong* - a fact that may introduce serious biases to the investigative process.
- Because of the subjectivity of the analysis process, there is a real risk that the investigators may commit one of the so-called Type I or Type II errors. A Type I error is: 'Finding the right solutions to

the wrong problems', and a Type II is: 'Finding the wrong solutions to the right problems'. In everyday accident analysis, there is the possibility of the ultimate sin: 'Finding wrong solutions to the wrong problems'!

Is it possible for a company to have a disaster if 'nothing is wrong' with the organisation? Clearly not, but there may be nothing 'more wrong' with this company than with the one next door where no disaster happened.

Quite often organisations are locked into an ineffectual cycle of accident prevention, and, similarly, whole industries are limited in their ability to properly develop a pro-active approach to safety. The continuous occurrence of accidents creates a constant flow of revised operational and technical requirements, specifically aimed at preventing the re-occurrence of those accidents.

For a long time the mining industry was driven by this cycle of reactive changes to procedures and systems. It may still be today.

### **How to Overcome the Flaws of Accident Analysis**

An objective system of root cause analysis is needed.

- The company must investigate all incidents with the same level of commitment, irrespective of the seriousness of an incident. However difficult it may be, a mere laceration must receive the same depth of analysis as a fatal accident.
- An 'analysis of the analysis' must be made, ie. trends over a period of time must be identified and clusters of root causes isolated. This trend and cluster analysis helps prevent the typical knee-jerk reactions to accidents.
- Teams must conduct the analysis to ensure that individual perceptions and biases do not skew the results. Ideally, each team will be composed of representatives from different

departments or sections and levels, coordinated by an objective facilitator.

- The inter-relationship between strategic, tactical and operational levels must be reviewed and changes implemented following the trend and cluster analysis. Clear and specific outcomes for each intervention must be specified, actioned and then controlled. Ideally, cross-section teams will be involved in the implementation processes as well.
- The organisation must continuously review its overall safety approach to strike a balance between managing the physical working environment and managing behaviour at the coal face (getting people to comply with safety standards, getting them to recognize dangers and to demonstrate commitment to safety)
- The most important aspect, and the one most neglected by most organisations, is strategic safety planning. While it may be argued that safety is part of the strategic planning process, the reality is that safety is overlooked in many companies. Implementing a major safety management system is often seen as 'strategic'. Although these decisions often consume huge resources, they are at best only tactical decisions.

*The most striking example of the lack of strategic thinking in the safety field is the fact that most of the safety intervention and programs operated today in modern companies are the same as those used 10 to 15 years ago, under different names. Examples of these are safety management, loss control, risk management, total safety/quality management etc. Have we really progressed in our thinking and approaches to safety in the mining industry and supplemented these programs with approaches that reflect modern thinking in safety management?*

### **What else can organisations do?**

The following can be regarded as the issues which should be addressed:

- Select the right safety precautions

- Supervise and monitor the processes, procedures, individuals, departments
- Keep working practices, procedures, rules and regulations up-to-date.
- Exchange and manage information between individuals, departments, and organisations.
- Train staff and update skills.
- Focus on, analyze and manage the 'safety culture' of the organisation. In other words, develop 'foresight' or active imagination about potential safety problems in the organisation.

Unfortunately, all organisations have a specific approach to safety and this 'specific approach to analysis' influences the outcome of the analysis. If the organization's approach is a strongly technical-engineering one, the findings of accident analysis will be mostly technical.

### ***Shocking the system...***

At organisational levels complex issues are involved. It is at this level that the 'culture' of the organisation exists and it is at this level that it is most difficult to make interventions work. Ensuring that the culture of organisation does not produce a disaster requires bold actions from management. Management has to allow the organisation to be subjected to severe 'shocks and criticisms' in order to continuously break complacency.

Shocking the system (SOS) in an organisation ensures that ineffective systems or procedures are eliminated and a continuous state of readiness is promoted.

*A warning: the implementation of some of these recommendations require management to be either very brave, or very desperate:*

- Conduct culture/perception surveys and ensure that all news from these surveys (good and bad) is widely disseminated to all.
- Expect, elicit, demand and 'facilitate' bad news reaching the top of organisation. This is difficult because it makes open upward communication of mistakes possible.

- Subject the organisation to intense external review and criticism of systems, practices, procedures and regulations. Allow external persons to join with employees to form teams and identify specific areas of concern.
- Ensure that the organisation develops the willingness and skill to review, criticize and continually re-engineer itself. This can be achieved by intra-group reviews and self-assessment, eg. within departments or within workteams, or by inter-group or peer reviews.
- Consciously focus on 're-engineering' the organisation towards simpler management systems, less bureaucracy and less complex safety systems. Critically review the impact and increased complexity created by safety management systems introduced 'on top' of existing systems, and on top of legislative requirements.
- Review the role of safety staff in the organisation and reintroduce their earlier role of 'in-house policeman' on safety. The noble goal of safety staff being a safety resource, adviser or facilitator may appear elegant and correct, but by changing the role in this way organisations have lost a critical resource and the ability to keep a high level of internal alertness.
- There may be an intense obligation for employers and employer organisations to provide maximum resources for the achievement of safety goals, but a similar, although possibly not an equal, obligation rests with unions in the coal mining industry. The extremely high levels of conflict between management and unions strongly contribute to the creation of 'structural secrecy'. The advent of broader management practices has created the processes for positive cooperation between management and labour. However, this has not occurred in the Australian coal mining industry, and serious concerns exist that unions are not allowing this to happen. The unions' future role is potentially that of expert mediator between management and labour, and

not of protector of labour against an

'exploitative management'.

### **In Conclusion**

We are not talking of guilty people who should 'carry the can' for disastrous events. We are talking of people who are doing their job diligently and honestly.

Combine this with honest mistakes, misplaced risk perceptions, widespread organisational failures and a touch of coincidence, and the risk of disaster increases exponentially.

Miners are going about their tasks and if one or more of our controls falter, such as happened with Vaal Reefs, Challenger, Piper Alpha and Moura, disaster will strike, a disaster that has been created over a period of time and is in the process of creation now.

Is it then true, as stated in the Moura report that we can expect another spate of disasters in about ten years time, as soon as the current shock as reactions have waned?

It is not a question of *when*, it is a question of *who* will be the next victims...

### ***Learning from mistakes...***

In 1995, the Discovery space shuttle was successfully launched. It was lauded as one

of the most successful shuttle missions to date.

The following was reported in Avion, Summer 1995:

'Discovery's safety was brought into question by an examination of the solid rocket boosters retrieved after the launch of the space shuttle Atlantis two weeks prior to the launch of Discovery.... Burning rocket propellant had burned one of the primary O-ring seals in one of the booster rockets of Atlantis. This problem was not discovered until four days after Discovery's launch.... The problem was particularly worrisome due to the fact that it was a similar leak that had caused the explosion of the Space Shuttle Challenger in 1986'.

To their astonishment, the engineers discovered that the seals in the Atlantis solid rocket boosters had failed in the same way - but without the disastrous consequences of the 1986 Challenger O-ring failure. After many years and many millions of dollars, exactly the same failure re-occurred.

**Organisations have very poor memories.  
Whole industries have no memory at all.**