

# **Why safe organizations fail...**

**Corrie Pitzer (BA Hons, Psych, B Hons Bus, MBA)**

*This study into mine disasters, originally commissioned by the NSW Minerals Council, started in 1997, resulted in several reviews of subsequent disasters, also outside the mining industry and in North America.*

*The findings in this study were reported at international conferences since then, including IAPA, Pacrim, AIMM and ASSE.*

## **1. Introduction**

Disasters are often tragic outcomes of high-risk technologies such as mines. Internationally, more mines are being developed every day, and the risk of disasters is ever increasing.

No matter how effective our conventional safety devices are, there is a form of accident that is inevitable. These relate to accidents that result from “interacting failures” in a way that could not be foreseen by the designers. In so-called “tightly coupled production systems” (processes that happen very fast, such as on a high producing mine) the risk is even higher and our risk controls mostly introduce some sort of a technological fix. While we are at the one hand attempting to control the risk, we are also introducing another level of complexity. Are we really controlling the risk?

This is one of the fundamental questions that will be addressed in this paper: Do we have the ability as an industry to effectively prevent these catastrophes, or are we, on the contrary, faced with an increasing risk as a result of increasing complexities of our mining technology and management systems and practices.

This paper will contend that a perceived improvement in risk control is an illusion of activity, and that the likelihood of catastrophes may be increasing.

This paper will further contend that we are applying the right solutions to the wrong problems. Our focus is technological and procedural, while our problem is one of *production cultures ripe for error and failure*.

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

### *2.1 Mine disasters Internationally*

Finding comprehensive data on mining disasters internationally is an impossible task. Most countries have all the data, but may be reluctant to publish this widely, and even reluctant to make this available if requested. However, some information was obtained, for instance just in the period of 1959 to 1974, more than 8000 miners died in catastrophes. A list of major mine disasters in each of those years are attached.

It is impossible to determine the total number of mining employees killed in disasters. In the USA alone, it is estimated that more than 13 000 miners were killed in disasters during the past 200 years, while internationally the figure would be in excess of 100,000 people. It would not include single fatal accidents.

---

Death is part of the process, it had been said many times. The mining industry is very much under public scrutiny for its poor safety records, in every mining country in the world. Why is that we seem to have more disasters than many other high-risk industries? Are we inherently more risky than, say, chemical and construction industries, or are we simply not managing safety as well as they do?

### 2.2 Risk - In the Eye of the Beholder.

Risk is like beauty - it exists in the eye of the beholder.

We make a fundamental mistake when we, as safety managers, deal with risk as a "fixed attribute", something physical that can be precisely measured and managed.

The misconception of risk as a fixed attribute is ingrained into our industry and is a product of the so-called science of risk management. Risk management has created the illusion that risk can be quantified on the basis of probability, exposure to risk, and from the likely consequences of accidents occurring. Risk management science can even produce highly technical and mathematically advanced models of the probabilistic nature of a risk.

The problem with this is that risk is not a physical quantum. It is, instead, a social construction. Everyone has a unique set of assumptions and experiences that shape their interpretations of objects or events. People tend to ignore, "misperceive" or deny events that do not fit their worldview. People find what they expect to find.

### 2.3 Management Stands Accused

This is not a game of semantics. How we look at risk is extremely important. If we accept risk as a physical quantum, we are inevitably led to the view that management, as an "amoral calculator", is responsible for accidents - an accusation that is hard to escape or disprove.

What happens when a post tragedy analysis is conducted? Management stands accused of culpability by unions and the public: "They knew about the risks, they violated safety rules, yet they pursued economic goals at the cost of workers' lives".

If, instead, one accepts the argument that risk is a social construction, a totally new perspective on disasters and accidents emerges. This will be explored in detail later on.

Three high profile disasters pointed to 'management culpability':

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

---

In each of these events, the blame was squarely placed at the door of management. By looking at one of these events - the Challenger disaster - in some detail I would like demonstrate or, at least, suggest, other explanations for the Moura disaster and possibly for many other mining disasters where the common accusation was that of gross neglect and poor attitudes. This paper asks why.

I would also like to offer an alternative approach of preventing accidents and, when accidents do happen, I propose another way of inquiring into them.

### **3. Lessons from Challenger**

An organization is a complex set of dynamics, systems, power plays, actions and reactions. Organizations are able to take risky decisions because of the large quantity of expertise available to it, and they are willing to take these decisions because the responsibility for them is often absolved and dissolved.

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

#### *3.1 Countdown...*

On 26 January, the date the Challenger space shuttle was scheduled for launch, the weather forecast predicted poor conditions, and the launch was rescheduled for 27 January.

On 27 January, during countdown, alarms indicated that an exterior latch locking mechanism had not closed properly. Launch was postponed for a few hours to fix the problem.

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

The weather forecast predicted that the temperature would drop below 20F, and the engineers attached to Thiokol, the contractor who manufactured the solid rocket boosters, were asked, via teleconference, to assess the risk.

The Thiokol engineers expressed concern about the low temperatures (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?". The meeting was adjourned, with Thiokol being asked to review their decision. A recorded teleconference was arranged a few hours later to listen to Thiokol's "reviewed response".

In those few hours, Thiokol changed their recommendation to "OK to launch". The four top administrators in Thiokol had met to discuss NASA rejection of their

---

original recommendation, and three of the four changed their vote to launch, with the fourth, more junior, person still dissenting. He was told to "take off his engineer's hat and put on his management hat".

He changed his vote.

Their decision was communicated during the second teleconference, and the launching procedure re-commenced.

### 3.2 *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. The seven crew members trapped in their seats were apparently still alive as they fell back to earth, dying instantly when the capsule hit the water at 200 miles per hour.

A cheap O-ring had failed causing a multi-billion dollar to fail. But was it that simple?

Of course not. 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.

Even worse, a NASA internal memorandum prior to the disaster warned about suspect seal technology. Seal erosion on rocket boosters had occurred 12 times since 1977!!

The night before the fateful 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 just prior to the launch. They found ice on the rocket outlets and equipment, and they also recommended that the launch be postponed. This was overridden by NASA mission management who recommended launch to senior NASA management.

The final recommendation that these NASA managers made to the senior NASA management the next morning was simply: "OK to launch". This communique said nothing of the cold weather or the launch postponement recommendations the previous night, and 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 discovered these glaring anomalies and deficiencies during its investigations. The Commission's conclusions are summarized below.

---

### 3.3 Enormous pressure to launch...

NASA was under enormous pressure to launch. This pressure arose from numerous associated events:

- Budget cuts by Congress.
- Commercial concerns that the European space program was gaining on them.
- The need to prove that the shuttle program was viable for commercial and military reasons (this was the time of the Reagan Star Wars program).
- Previous postponed launches.
- Inability to sustain the high launch rate needed to demonstrate and justify the economic viability of the shuttle program.
- The massive publicity accompanying this launch because of the first civilian (teacher) astronaut on board.
- The media linking the timing of the launch to an important presidential speech by Reagan that was scheduled to take place during the mission.

### 3.4 Structural causes...

Structural causes were identified as:

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

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

The structural origins of the disaster - competition, scarce resources and production pressure - permeated the NASA organization and dominated decision-making on the eve of the launch. The NASA managers were highly competent people who thoroughly understood the engineering and managerial issues involved.

But, in order to secure resources for their organization's survival, and to please their shareholder, the U.S. Government, they took a calculated risk, violated safety requirements, and they lost.

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

---

#### 4. Why Do Good People Do Dirty Work?

The pressures and structural problems experienced by the NASA managers happen routinely in most, if not all, organizations.

If any organization were analyzed with the same intensity and magnification of the Challenger Inquiry, the conclusion would be the same: production pressures compromising safety, and middle managers and workers routinely taking risks.

Risks are taken as a matter of routine in most organizations, for who is to know exactly what the level of risk is, how safe is safe enough? Despite the best intentions and commitment to safety, trade-offs have to occur.

Why do competent experienced managers make decisions that lead to accidents and the loss of lives and property? Why do good people do such "dirty work"?

Managers are normally well-qualified and experienced, and most have positive intentions to further the goodwill of the organizations they work for. Why do these law-abiding citizens violate rules, laws, and regulations, knowingly risking the lives of their subordinates or workmates?

Are managers conscienceless "amoral calculators" of risk?

If we accept the majority of public inquiries into mining and industrial disasters they certainly seem to be. In the past five to ten years, almost all public inquiries have blamed management. Prior to that, blame was cast on human error and, before that, God got the blame.

##### 4.1 Mine Managers - Amoral Calculators of Risk?

Let's return to the question posed in the beginning of this paper: are mine managers "amoral calculators of risk"?

Despite the apparently overwhelming evidence against management, the answer is emphatically "no".

There are at least two reasons to assert this. Let's go back to the Challenger example to explain.

##### 4.2 Anecdotal evidence...

The first reason is a peculiar one. It concerns anecdotal evidence and the powerful influence it has over the judgment process. A disaster inquiry should be a scientific analysis of an event, performed by highly qualified and experienced people. The flaw in the process is the quality of information the investigators use.

---

Not only are inquiries restricted to information that is available at the time, but this information is:

- Often very distorted, twisted or slightly changed by the "accused" - intentionally or unintentionally.
- Incorrectly assessed as linked to the disaster event. Information that seems to offer clues or indicate problems contributing to the event may in fact not be linked at all. It is seldom possible to link prior incidents or events to a disaster event in a way that would withstand scientific scrutiny.
- Ignored if it doesn't fit into the paradigm of "managerial wrongdoing".

As an example of the last point, NASA management stood accused, and was found guilty, of safety and production trade-offs. Production demands overrode safety (recognize this accusation?). Yet, what was not scrutinized was the number of times safety was *not* traded off against production demands. The reality was (and is in most companies today) that the vast majority of daily production decisions are made with a clear focus on safety. A comprehensive review of the NASA decision-making processes found only exceptional cases of such tradeoffs and these were always done within a context of a competent consideration of opposing facts.

The problem that eventually led to the "flawed decisions" prior to the Challenger disaster was that the engineers and managers together developed a definition of the situation that allowed them to carry on as if nothing was wrong even though they were continually faced with evidence that something was wrong.

The logic behind the statement that safety/production trade-offs were made is flawed. If an organization is heavily production-oriented it makes no logical sense for managers to make decisions that risk the very existence of a whole project, such as the Challenger program.

In effect, the critics are saying that the management would risk the project for the same reasons that they would not risk the project.

Why would a mine manager, knowingly and willingly risk his job, his career, the lives of fellow employees and the very future of his organization to win so relatively little? He would have to be very stupid indeed!

What was not scrutinized at Moura was the hundreds and thousands of times the management made routine decision in the interest of safety.

The President's Commission on the Challenger disaster found a host of decisions that supposedly demonstrated cost/safety tradeoffs. But an intensive revision of the very same Commission's report showed many, if not most, decisions were made in the interests of safety. A similar review of the report on the Moura Disaster shows numerous decisions were made in the interests of safety or as precautionary measures.

---

Every training dollar, every dollar spent on systems and controls, and all the money spent on most activities on a mine is inherently meant to ensure safety. Unfortunately so much of this spending has become "routinized" that it is hard to identify its contribution to safety. To make this clearer, think of driving your car, and 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.

#### 4.3 *Honest errors...*

The second reason why the "manager as amoral calculator" theory does not hold water is the complex question of risk evaluation, and the possibility of making honest errors in risk calculation.

The risk management discipline often gives the impression that the probability of an event is calculable and that it can be classified on the basis of the likelihood of it occurring. From a statistical point of view this approach is correct; it is possible to calculate the likelihood of any event occurring, say at 2 times per million per annum.

However, any manager individually faced with a single event is in no position whatsoever to make any sense of that statistical number. It is humanly impossible to work with a figure of the magnitude of 2 per million per annum. How can a manager judge whether a task is "too risky"? He simply cannot, unless the probability of an accident approaches 1 (100%), like jumping off a cliff.

Unfortunately most work place accidents are on the category of highly unlikely, and can approach likelihood so small (0.0000002%) that no human mind can come to grips with it. Managers, like everyone else, use "gut feel" in these circumstances. Even the highly specialized engineers of NASA could not agree afterwards on the likelihood of the Challenger disaster. Their estimates ranged from 1 in 100 launches to 1 in 100,000 launches. These differences are, in statistical terms, enormous. The difference between the two is one failed launch every ten years or one failed launch every ten thousand years!

In summary, the assertions that management are "good people doing dirty work", and that their actions can actually be classified as "criminal" is seriously flawed, yet these assertions are 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.

#### 4.4 *Who is to be blamed?*

It is unfortunate that an inquiry or even a simple accident investigation is a blaming process. If it is not the human operator, then it is his/her superior or,

---

more likely today, the manager, or management, that gets the blame, often for events over which they had little or no real control.

If none of the above can be blamed, and God can't be blamed, who then is responsible for the event? Someone or something must be!

There are two main reasons why operators, supervisors or managers cannot automatically be blamed for these events.

Firstly, it has to do with the complexity of even the most trivial events, a complexity that renders any operator or manager instantly incompetent to deal with the situation at hand.

Secondly, it has to do with a situation in which people, whether they are operators or managers, often find that they are forced to carry on as if nothing is wrong, even though they are continually faced with evidence that something is wrong. In other words, a process in which abnormalities are "normalized".

### **5. Interactive Complexity**

Let us look at the first reason for fixing the blame elsewhere than the operators or managers, namely the issue of complexity and operator/managerial incompetence.

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, and is it logical? I shall argue "no" to each question.

From the beginning of human time, we have had natural disasters, and for many centuries, our definition of a disaster was that it was God-made. As we marched ahead in the process of industrialization, we built devices that could crash, sink, burn or explode and, when these events happened, our answers were relatively simple and effective: We prevented accidents by removing the causal factors and, through trial-and-error, we eliminated most of the problems, for example safety relief valves became a requirement for pressurized vessels.

Our focus then turned to the actions of people. (This factor had, of course, always been there, but had not been as noticeable because of the preponderance of technical accidents). We declared war on human error and did this, at least since the 1920's, by treating workers as chimpanzees that needed to be trained, conditioned, rewarded, and regulated. This has continued to modern times through the proliferation of vast volumes of safety and health legislation, and through the advent of risk and/or loss control management systems. Combining this with a huge increase in technology over the last 25 years, we have added a new cause of accidents: "interactive complexity".

A production system on a large high production coal mine today is extremely prone to these interactive complexities. And this happens even though the mining

methods may be less complex than underground mining, simply because of the speed and volume of production activities.

Perrow (1984) provides a classification system of types of industries, which in many ways is a useful framework to identify high-risk or disaster prone circumstances.

The two continuums used are Complexity – Linearity and Tight and Loose Coupling.

Complex systems are characterised by features such as 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 process in the organization.

Tightly coupled systems are characterized by having time-dependent processes eg in chemical plants, reactions are instantaneous and cannot be allowed to be allowed at certain stages of the process, as with underground mines. Sequences of activities are invariant, and the production processes are fixed. There is little “slack” in tightly coupled systems.

A classification of different types of organizations follows:

	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>▪ Underground Coal Mines</li> <li>▪ High volume mines</li> <li>▪ Open Cut Coal</li> <li>▪ Military</li> </ul>

---

The mining industry, especially the underground and high volume surface mines, belong the highest risk category for potential disasters, by design and by organizational structures. (But even so, the incidence of disasters in the mining industries is far higher than the in higher risk industries such as the nuclear, chemical and space industries. Perrow concluded that the mining industry is simply “not managing safety well enough”)

Furthermore, in the social environment of employees, they are subjected to increasingly complex systems of management, engineering and legislation.

We have placed the operator in a production environment in which he/she is expected to:

- Make rational and logical observations of his/her environment;
- Rationally interpret events, requirements and procedures; and
- Act and react rationally on those interpretations.

Yet it is very seldom possible for the average operator to really know all the possible links between systems or the effect of one on the other. Of course the same operator would, after an accident has occurred, be able to recognise his mistakes and correctly identify the alternatives he should have selected. It can therefore safely be concluded that the operator made a mistake, and that a repetition of the error can be eliminated with better training, simpler systems, or with another more back-up systems or alarms.

But, of course, these things are only possible *after* the event. *Before* the event the possibilities can be complex, or at least confusing, and in a tightly controlled high volume work environment, you don't need much more than this to create havoc.

Something else to bear in mind is that great events have small beginnings. On the Piper Alpha oil rig, the small beginning was an inadequately tightened flange on a gas pipeline which leaked causing gas to ignite, followed by explosions and fire and the death of 162 people.

At Moura, several management systems were in place:

- The basic skills and **engineering knowledge** of the management and supervision introduce numerous requirements
- Management and **administration systems** are implemented on top of that
- **Legislative requirements** are to be maintained on top of that.
- The **quality management system** is implemented on top of that, bringing with it its own volumes of standards, inspections and audits.

- 
- The **safety management system** is implemented on top of that, with safety requirements and regulations to be maintained, and another level of auditing.
  - **Risk management process** are implemented on top of that, with new risk controls to be maintained

The level of complexity of each of these systems on their own is often mind-boggling. The level of interactive complexity could be disastrous.

#### *5.1 Over-trained, over-rewarded and under-punished...*

Is the only way to avoid disasters attributable to human error, like Piper Alpha, to train them to tighten flanges, punish them if they don't, reward them if they do, and put the problem in the "too hard basket" if none of these work?

This is an approach followed in the coal mining industry to the point where we now probably have a workforce that is over-trained, over-rewarded and under-punished. And we're not winning the war against accidents because we are fighting it with more and more risk assessments, involving Bayesian probabilities, ALARA principles, discounted future probabilities, F-curves, isopleths and the like. All this results in more rules, alarms, systems, and more interactive complexities.

Ironically, the more risk assessments and analysis we throw at the problem, the more we *increase* the risk.

Risk assessments can seriously lead us astray. Consider the following scenario at a board meeting of a large corporation:

#### *5.2 As low as reasonably achievable...*

The Financial Director announces that he has received advice from his risk assessors: If the Company does not install a planned safety device, the outcome 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 always happen to someone else, the Company is not facing a lot of pressure to install the device.

On the benefit side, by not installing the device, the Company will save \$50 million dollars. This 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 this year, the customers, the shareholders and the workers will greatly benefit. What is a life worth? Well, the Board considers that \$50 million is pretty high for the possible loss of a random anonymous worker and the safety device is scrubbed.

If this story appalls you, just remember that the risk analysis presented by the Financial Director is correct. It is a good bargain. Risk assessment is, after all, about getting risk down "as low as *reasonably achievable*".

---

If you consider the story as immoral and irrelevant and refuse to believe that no one could think like that, you will be surprised to learn that a similar decision was made at the Ford Motor Company when they decided not to buffer the fuel tank in the Pinto car and which led to a significant increase in fatal accidents where crash victims, trapped in their cars, were burned to death. Ford Pintos were known to easily catch fire during rear-end accidents...

This type of thinking is encouraged, even facilitated, by risk assessment procedures. Most companies, at some stage, try to quantify the cost of accidents, if only to express concern that accidents are costing money, or substantiate a statement that safety is good business.

I am not criticizing this thinking, but I am expressing concern that assessing physical risk without also assessing sociological risk, the thinking patterns of the organization, the forces, and the influences within the organization all lead to the creation of a very poor, restricted and potentially damaging definition of risk. And of course risk is one step away from disaster. That is the focus of this paper.

Can the situation be so desperately bad as portrayed here?

In practical terms and looking at our day-to-day operations the situation is not so bleak. We produce coal in greater volumes more efficiently, and with fewer accidents. Risk management, however, still seems to be the “beast” within our organizations. Management still seems to make amoral decisions and ignore risks. So why is there a perception of “risk-taking amongst management”?

The answer to this is not simple.

## **6. Normalization of Abnormal Events**

Earlier I said that there were two reasons why operators, supervisors and managers cannot be blamed for a disaster. We have looked at the first one, namely the complexity of events.

The second factor is called the “normalization of abnormal events”, and I said that such a process commonly exists within organizations, as it did in the NASA management prior to the Challenger launch.

Three factors explain this process of normalization:

- The production of culture.
- The culture of production.
- Beliefs in margins of error.

### *6.1 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 become institutionalized and passed on as the rules, rituals and values of the group.

---

It is falsely assumed that each large organization has a common culture. Most organizations are segmented and frequently have as many cultures as they have sub-units. Although there may be some commonalities between sub-unit cultures, the degree to which sub-units hold these commonalities will always differ.

The culture within a workgroup, or sub-unit, may be even more focused. People in a unit, or from different units, may be drawn together because they have a certain task to perform, and they develop a culture that is unique to that specific task. When the task ends the group and its culture dissolves, while new ones form around new tasks. The work groups develop and share certain definitions of each situation, definitions that often persist.

The creation of work group cultures ensures that new information is interpreted in terms of the culture concerned.

To illustrate this point, I'll return to the Challenger disaster. Prior to the shuttle program, early tests showed that the solid rocket booster (SRB) joints (which contained the O-rings) had unexpected performance deviations. The engineers alerted management in accordance with procedures, who re-interpreted the deviation and officially labeled it "acceptable risk". (Naturally there was no risk in this decision, because the shuttle program had not been launched yet!)

The workgroup accepted this new standard and treated each new program deviation within the wider band of acceptable risk thus created. Between 1977 and 1985 the first abnormality was normalized to accept that the primary O-ring would withstand erosion by hot gases, and in the unlikely event it did not, the secondary O-ring would. Although problems with the O-ring were identified twelve times, and there were discussions and disagreements about mechanics, 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 many mines a very fixed and pronouncedly negative culture existed between the levels of the organization. There exist little trust between operators, supervisors and management. A report on culture surveys conducted previously by CJ Pitzer (2000) in the mining industries of Australia and South Africa showed extremely negative safety attitudes, largely influenced by a negative industrial relations climate in the industry.

So why did they continue to "normalize" these abnormalities despite all the evidence? The answer lies in the culture of production.

### 6.2 The culture of production...

The engineering and production professions give the impression of precision, rule-making and qualified thinking. The reality, often overlooked, is often the opposite.

---

When accidents do *not* happen, the opportunity to investigate the engineering process in depth does not often present itself. If an organization, any organization, were subjected to an on-the-spot investigation, the public would discover the real messy inside story of "normal" engineering practice which, after a disaster investigation, looks like an accident waiting to happen.

There are some powerful processes in organizations, focused on creating satisfaction and minimizing stresses, strains and conflict. No dynamic organization (and that includes individuals) can constantly function under stress. There is therefore a powerful drive towards equilibrium.

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

The ARP process classified all risks, to enable a comprehensive analysis of risks and a proper classification record. The O-ring joints were investigated, tested and reviewed over many years and, although they were accepted as a risk, there was never any serious doubt about their resistance, because:

- The Apollo programs had, for many years, operated with the same design on Titan rockets.
- A secondary O-ring was added as a back up should the primary ring fail. Plus, many laboratory tests showed that the O-ring would hold.
- Most of the Challenger and SRB parts and systems could only ever be fully tested under real flight conditions. When the SRBs' of previous launches were disassembled (a routine process) no problems with the O-ring were found.
- "Flying with flaws" was not abnormal in the culture of NASA. It was normal, acceptable, even essential. While outsiders may have seen them as "known flaws", insiders saw them simply as "residual risk" which they had analyzed and rationalized through the Acceptable Risk Process.
- Organizations that constantly have to deal with high risks develop the means (or mindsets) to deal with them. If they don't, the continuous risk will destroy them.
- The high level of risk analysis, and the qualification process, created an "impression of invulnerability" in the organization - which it wanted to assume as quickly as possible. The more risk assessments were done, and the more successful the organization became at managing the risks, the less they expected risks. (It is folly to argue that risks are under control as soon as they are qualified and quantified and a control measure introduced - because, as discussed earlier, risks are a social phenomena.)

- 
- No one in NASA had the ability to recommend that the whole Space Shuttle program should be put on ice until the SRBs joint was redesigned. Those pressures would have been simply too excessive for any team or individual to handle. And, despite all the numerous attempts to flag the issue, no-one was ultimately brave enough to go against the production culture.

All this created a powerful culture, which accepted the risk and proceeded with the flight.

On the Piper Alpha Oil rig, the water deluge system, its main fire fighting capacity, was seriously deficient for four years. It is difficult to understand why this could occur, but on the oil rig, it had become “acceptable and normal”.

An engineer warned the management of Occidental Petroleum, owners of Piper Alpha, that the gas outlets on Piper Alpha are extremely dangerous and exposing the workers on the rig to enormous risks. These warnings were ignored, and everybody accepted the risks associated with it. They even considered to get rid of the emergency ship.

They were “flying with flaws”.

Let us look at the Moura Mine, and the prevailing “culture” prior to the explosion. The following are extracts from the Warden’s Inquiry report:

The Mine manager was informed that the increase in CO was linear not exponential and they concluded that no problem was evident – no different than “flying with flaws”

“The background of sealing panels at Moura No.2 was that, apart from a couple times, practice rather than exception was to continue to work underground as sealed panels passed through the explosive range”. The risk is known, defined and accepted, in the same way the risk of O-ring failures were.

The following deficiencies and practices all became “normal” and “acceptable” to the people dealing with and working in these conditions every day.

- “Ventilation was sluggish...”
- “In practice there was evidence that these appliances were affected by roof falls or local strata stability and that their function was, at times, compromised...”
- “There was evidence of ventilation problems...”
- “The likely compound effect of all these ventilation alterations was considered undesirable...” (by the Inquiry)

---

In an underground coal mine, the lifeline is ventilation, and this lifeline was compromised. They also, were “flying with flaws...”

### 6.3 *Belief in margin of error*

All the risk assessment processes and engineering history of the SRB's pointed to one thing: there is margin for error. They have had many successful launches, many laboratory tests showed that the secondary O-ring provided a margin of error which did not exist before, and the engineers of Thiokol and NASA turned their attention to more immediate and more urgent problems. With that, the next critical ingredient for a disaster has been created: the redundancy of risk.

As soon as this cultural feature becomes fixed in the organization, the “bandwidth: for accepting risk slowly increases, and every day, the potential for a disastrous failure looms closer...”

Many times in its history, there will be “no failure and no event”, but only if they heeded the warnings!

An analysis of the launches of all the shuttle missions after the event produced a graph which was almost damning: It showed that of all flights launched *above 65 degrees (Fahrenheit), 17% of theses had anomalies during launch. Of the flights launched below 65 degrees, 100% showed anomalies.*

On 28 January, NASA launched at 27 degrees.

But this graph was never drawn and an opportunity to avert the disaster was lost.

At Moura, a similar graph was never drawn, namely the ones mentioned above on the increases in CO and the ones on the so-called Graham's ratio, which had it been used in context with other information, it “may have tipped caution in the right direction”.

Further examples of the gradual acceptance of risks through a continuing belief in margin of error at Moura:

“Reliance on incubation period as primary determinant of likelihood of spontaneous combustion led to some false sense of security...and some complacency...”

“It was widely believed that a slow steady rise in CO production could not constitute a problem and that an exponential rise was required to indicate a heating ...”

“However none could recount the source of such impression...”

---

The belief in a margin of error is a result of all high-risk work environments. In organizations such as this, a “mindset” develops over time that risk can and should be conquered. In fact, the most fundamental purpose of organizations such as NASA, oil rigs and mining companies is to conquer risk. And they do that through a belief in their ability to achieve, a culture of “can do” and a belief in the redundancy of risk.

An organization that does not believe in the redundancy of risk will find it impossible to continue as a business. And therein is the irony – what makes us successful as a mining company is also our undoing, our weakness.

Into the unknown: risk secrecy

Donald Rumsfeld has introduced us the notion of “not knowing what we don’t know” (he didn’t really, he just made it famous) but in the world of organizational culture, it is a reality with potentially disastrous consequences.

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

It was later revealed that, on the eve of the Challenger launch, the higher levels of NASA were not informed of the initial 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 that communication problems existed (heard that before?) and, because the engineers failed to express their doubts about the issues surrounding the launch, it was concluded that the lower levels of management had deliberately withheld information flowing to the senior levels.

Was it just a question of deliberate withholding of information, something that can be described as human, and therefore both understandable and punishable? Or, on the other hand, was it something senior management could be blamed for, if it was their autocratic, aggressive behavior that led to the suppression of communication or to the faulty communication systems?

The answer, as always, is not that simple.

‘Secrecy’ is built into the very structure and fabric of organizations.

The division of labor between sub-units, levels of management, geographic location and so on, actively segregates knowledge about tasks and goals. Specialization further inhibits this knowledge. The functional focus of

---

organizations (production, engineering etc) is such that almost every organization has departments at loggerheads. Communication systems in most modern organizations have grown so complex that *more* communication frequently results in *less* knowledge. Secrecy in organizations is on the increase.

Top people do not get all the information churning around in their organizations. In fact they get very little - by design and by necessity. The sheer quantities of information, especially in our electronic age, are such that we cannot make sense of it all unless it is severely edited.

Decision-makers have to rely on "signals" developed based on experience. The bulk of the information remains unknown to them.

Secrecy also develops as a result of weak signals. Often in organizations warnings about any course of action are many and diverse. No activity, program or project is done with absolute certainty and risks are never completely understood and calculated.

Even if people overcome their reluctance to voice opinions about danger, risks or threats to an intended course of action, their signals be may simply too weak to be heard in the organization and they get lost in the static. For example, one engineer at NASA explicitly recommended that launches should be terminated until the problems with the O-ring failures were sorted out. This signal, although highly significant in hindsight and apparently indicating criminal inattention among those who should have heard it, was simply not heard! The signal was not given to anybody with sufficient authority to do anything about it.

### 7.1 Systematic censorship...

Adding to secrecy in the organization is the process of "systematic censorship", common to all organizations.

At every level of all organizations, a process of information censorship takes places continuously and at varying rates. It is a process over which management has no clear control.

There is a natural tendency at every level to withhold as much bad news as possible if it can be done unnoticed. Although this can lead to catastrophic consequences, it is essentially a very functional and necessary process in most organizations. It ensures that top levels are not overwhelmed by paperwork, that decisions are taken at the appropriate level of the organization, and that only critical exceptions are communicated to senior management.

One of the most reasons why "structural secrecy" has developed in mines internationally today is the untenable situation developing on the IR front. Strategically, we have modern approaches to people management sweeping through the industry, with a new and positive emphasis on the critical interfaces of management and supervisor-operators.

---

Against this we have an industrial relations arena where the battleground and the battle rules are antiquated, and where unions' have been unable to establish a new and modern role for themselves. It seems that the unions' most basic point of departure is still that the management is exploiting workers and they see their role as fundamentally that of protection. This outdated notion has no links with the reality of mines implementing benevolent, and very participative, management systems. The result is a high degree of emotional and philosophical conflict between the opponents. This, in turn, has profoundly increased secrecy at the lower organizational levels.

The unions, in their failure to adopt a flexible approach to modern organizational practices, may themselves be contributing to the very processes that foster a high-risk culture.

A high degree of job specialization is also contributing to the loss of information in organizations. The people occupying the many new specialist positions are experiencing great difficulty in sharing information amongst themselves. Add to this the tendency, at middle and senior management levels of organizations, for engineers to become managers and administrators, losing their hands-on engineering exposure and their day-to-day understanding of production and engineering processes. This may inhibit their ability to effectively understand, challenge or reject the technical information they receive from lower levels.

Another factor is the creation of highly specialized safety departments in many organizations from which managers must often accept information and interventions on face value. Most companies today operate some kind of safety and/or risk management system. These systems create blizzards (even cyclones!) of paperwork, terminology and jargon which managers have no option but to accept and visibly support.

This was the process typical of the NASA management structures.

Quite often - as happened with the O-ring - warning signals may be only weakly received in the organization and lost sight of. Combine these weak signals with the mixed signals that managers in the real world have to contend with, and you have, at the very least, a confused situation.

It is practically impossible for any management team to act on each of the multitude of signals that reach them. One reason for this is that the levels of probability of any of these possible events often fall in a range where it is physically impossible for managers to logically and rationally prioritise them.

An example of this was the NASA manager who was accused of neglect because he spent most of his time prior to the launch on the problems of the SRB's parachutes, instead of working on the O-ring problem. But, at that stage, the O-ring was regarded as a classified and acceptable risk, and the parachute problem (it continuously tore and had the potential to cause the large boosters to

---

fall back to earth unrestrained) was an acute, very urgent and very realistic problem to deal with - and he dealt with the problem with great commitment. The critical issue here is that the manager could not possibly make a rational judgment about 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 of that mine was, like all managements of mines all over the world, just dealing with urgent problems, reacting to signals, which they receive about the relative importance of these events. They could not possibly be expected to weight one risk against another, an make a "mathematically correct" decision. No one can do that.

Nor, sensibly, can mine managers' make similar judgments before the event - and be expected to make them logically. Yet in hindsight, it is all too easy to demonstrate that their failure to do so was neglectful and wrong.

On Piper Alpha, it was "regretfully evident" to the inquiry that "management failed in some very basic duties". Even a decision the manager of that oil rig 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 it was a decision in the interest of safety, in as much as NASA managers made similar decisions and also at Moura, where several decisions they made can only be seen as "in the interest of safety or as precautionary.

Yet in hindsight, these decisions appear flawed, but they were not. They were realistic decisions made at the time under realistic circumstances.

## 7.2 Systematic distortion...

A close relative of structural secrecy is the concept of "systematic distortion". At the same time systematic censorship in the organization reduces the information available to the top levels, unfavorable information - that is information that does not support the ambitions, goals, or survival needs of the organization - is also filtered out.

This unfavorable information is not lost by malicious intent, or purposeful concealment, or even just because of a reluctance to tell superiors things they do not want to hear. The information is lost because that is the way organizations tend to function: people deliberately seek out favorable information, often to the exclusion of negative information. The resulting distortions can have disastrous consequences.

A source of distortion which prevents risk experts and decision-makers from coming to grips with the likelihood of failure lies in the tricky area of "failure probabilities", also called "disqualification heuristic". In simple terms, if you hold a

---

conviction that, for example, it is safe to fly, or mining is a safe activity, you neglect contradictory information and focus selectively on confirming information.

Going back to the Challenger Disaster, you will recall that there was evidence that the probability of a disastrous failure of the shuttle varied from 1: 100,000 to 1:100 (there was even one estimate of 1:25!) The higher probabilities came from engineers and safety officers and the lower probabilities from NASA managers.

The engineers' estimates varied so markedly from the managers because they had access to a variety of tasks, calculations and risk reviews, information the managers did not have as readily available.

In mining, as in other organizations, the same inherent problem exists: It is easy to see how a "can do" culture can develop in organizations, especially in mining companies, where high production volumes continuously demand a high achievement culture.

Very few mining organizations have the internal structures, processes or units to foster or force self-criticism and critical self-review, but almost all of them are inherently focused on survival and therefore information distortion thrives. At some point, these intangible forces in the organization may become so powerful that, if the right physical conditions and deficiencies exist, a disaster becomes almost inevitable.

The organization that produces a disaster has not done so out of neglect, wrongdoing or criminal misconduct. Yet, so often our own inquiries into such events, even those that look at minor work accidents and incidents, fall prey to the "politics of blame". We need to put the blame somewhere but, in our hurry to do so, we generally fail to identify the real organizational and cultural causes and influences on such events.

We demand straightforward, simple answers, but the answers are seldom simple.

The heart and mind of organizations are beyond the control of individual managers, because mistakes are socially organised in a highly complex, unpredictable manner.

### 7.3 *Dynamic distortion...*

One of the most problematic sources of secrecy lays in the dynamics of safety goals and achievements. The well-intentioned statement of zero accident goals in the organization leads to a variety of unintended distortions at supervisory levels. The need for good news at the top of the organization becomes an invading force through all levels and each level performs increasing filtering and fudging (softening) of the information. The most filtering however happens underneath the supervisor or with the supervisor. Reluctance to report accident,

---

incidents, near-misses (bad news) inevitably leads to increasing degrees of risk secrecy.

Looking at this problem of risk secrecy at companies that experienced disasters, it is quite striking to notice how “well they performed on safety ” just prior to the disasters. There is a ‘thread’ running through all of the mine disasters in the modern era of the 1980’s, 1990’s and recently: Excellent safety performance as measured by lost time injury rates. Moura Mine, Northparkes Mine, Gretley Colliery, Beaconsfield Gold Mine and elsewhere, the West Ray Mine in Canada, Sago Coal in the USA and more recently the BP Texas City blast killing 14 people, when the Baker Report mentioned:

*“BP primarily used injury rates to measure process safety performance at its U.S. refineries before the Texas City accident, (but) did not understand or accept what this data indicated about the risk of a major accident or the overall performance of its process safety management systems.*

*BP’s executive management tracked the trends in BP’s personal safety metrics and they understood that BP’s performance in this regard was both better than industry averages and consistently improving. Based upon these trends, BP’s executive management believed that the focus on metrics such as OSHA recordables and the implementation of the Group-wide driving standard were largely successful.”*

At Moura, they were criticized by the inquiry because: “No one person or group of persons at any time had all the facts available to them on which to base their decisions”

In normal circumstances, at normal mines on a normal day, this is just normal. It is normal on any organization where complex processes exist and where decisions are being made at all levels of the organization, and where the fundamental aim is to conquer risk.

And many other communication issues appeared suspect or seriously flawed from the outside, such as the various reports on “benzene-type” smells underground that failed to raise concern, the assumptions made by several individuals at the mine, for example, the *assumption* that workers knew of the risk of spontaneous combustion on the day of the event, etc. All these issues point to another feature of the high risk organization, namely the *distortion of information*.

At Piper Alpha, the 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 naive, or even stupid, but there is a message in there: the information that reached him was simply distorted to the point that his only impression of it could be this one: that everything is all right. It was no different at NASA (e.g. what was reported to the NASA 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”

Our willingness to accept risk is a phenomenon that is often underestimated or not even taken account of at all. The factors which make it possible for us to accept risk - and the possibility of disastrous breakdowns - include:

- Risk assessment processes.
- The culture of production.
- A margin of error which develops misplaced confidence.
- Organizational pressures.
- The probability that an accident may happen to the individual are incomprehensibly small.
- Illusions of invulnerability that develop over time as a result of a "can do" culture.

## **8. The Social Organization of Mistakes**

The Challenger disaster, like all others happened because mistakes were made. It is however not a simple case of human error - the mistakes themselves were "socially" organised and systematically produced.

Disasters have systematic origins that transcend individuals, organizations, time and geography. Their source of disasters can be found in the routines and the taken-for-granted aspects of organizational life.

Those key questions about Challenger - why did they launch despite their knowledge of the O-ring deficiencies, and despite 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 Challenger disaster, or any other disaster. But combine these three factors, add to the mixture the right combination of circumstances, and mistakes will happen, some of them leading to disasters.

In looking for causes of disasters we need to shift our attention from the technical (such as the O-ring) 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, the biggest flaw 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 organizations are taken every day without resulting in disasters - but they do routinely result in mistakes. When disasters are analyzed after the event many of these routine decisions can be demonstrated to be rationally flawed and blame is cast on those making the mistakes. But decisions are taken within the context of an environment, a paradigm, and a culture in the organization. They cannot be divorced from that culture.

The problem is that our public inquiries do just that.

It can be argued that organizations suffering disasters generally suffer from failures of foresight, that these disasters had long incubation periods during which warning signals were ignored, rationalized or accepted as normal. And this is true. Organizations need mechanisms to counteract these organizational influences.

## **9. The Aftermath of Disasters**

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

Public inquiries, despite their unquestionable necessity, have a number of serious deficiencies and flaws which may erode their effectiveness.

There are a number of structural problems associated with public inquiries:

#### *Political Problems*

No inquiry is conducted in a vacuum, to be filled only with facts or truths. The process, and often many of the findings, is a political compromise of some degree - sometimes slight, sometimes significant.

#### *Terms of Reference*

Too often, the terms of reference of public inquiries are set too narrowly, or in an unbalanced way. Often an inquiry searches too deeply into some aspects of a disaster, and persistently ignores 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 guts" of organizations.

#### *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. training of staff, superiors, committees.

- 
- Authority - use of legislation to enforce rules.
  - Information:
    - Improve communication, 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 extremely detailed and voluminous nature. The other possibility is that organizations typically make only technical and communication mistakes - which is clearly not always the case.

### 9.2 About biting dogs and accident analyses in organizations...

There are many contributing factors behind each accident, yet accident investigations and analysis mainly focus on the immediate events, behaviors and hazards that surround the event.

The "muzzle" approach is often used to deal with accidents in industry. Accidents and incidents can be likened to aggressive dogs in the neighborhood. When a dog bites, it is caught, fitted with a muzzle ("muzzle": a new procedure, a machine guard, etc) and released. Every dog that bites gets a muzzle. 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")?

### 9.3 Developing "active foresight" from hindsight...

Accident analysis is essentially hindsight. It may sound contradictory, but the hindsight should be aimed at foresight, namely to prevent the same and 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 organizations.

---

The analysis that follows in the wake of a disaster or a fatal accident is often very extensive and extremely comprehensive. It includes lengthy official inquiries, analyses, recommendations, and weighty reports. It generally identifies the proximate causes of the accident and the causes of deaths (if any). It also often goes on to identify so-called "root causes", in other words the fundamental deficiencies in the organizations which produced the immediate triggers for the event.

Active foresight, on the other hand, goes further than this. More than one inquiry (examples are Piper Alpha, Kings Cross fire in London, etc) has attempted to take the additional step of analyzing the organization's culture and fundamental systems, to pinpoint deficiencies at these levels. This shows that there is a growing realization that disasters and accidents cannot satisfactorily be explained by direct and immediate cause analysis.

An in-depth approach like this is very sound because, as discussed at the beginning of this paper, 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 organization.

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.

#### *9.4 How can an organization develop foresight?*

The steps that an organization can take to develop "active foresight" are outlined in the following model. The model will, however, only work if the organization is able to come to grips with the dynamics of its own existence, and install processes to effectively measure those dynamics. More importantly however, it must interpret these measurements within the context of pro-active risk management.



---

The first step is to understand the various levels in the organization at which deficiencies can occur. These levels are:

- **Organizational** level (this includes management and supervision issues).
- **Systematic** levels of managerial and functional control and regulation (such as training, responsibility and authority).
- **Technical** levels (of plant, equipment and maintenance and production systems).
- **Operational** levels of execution of tasks (as prescribed by the systems, policies, regulations etc)

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

Deficiencies at any of these levels may interact and generate accidents. A superficial analysis will quickly 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 organizational deficiencies are seldom identified, and lie "dormant" in the organization 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 organizational level, the measurements are done by effective safety culture surveys; at the systems level, they are done by system audits; at the technical level, by risk assessments; and, at the organizational level, by behavior measurement and job safety analysis.

The analysis of accidents and incidents is a critical activity because it offers the organization 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.

---

### 9.5 Subjectivity of the analysis processes...

Accident analysis is often the only means an organization 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 analyze 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 inches or a few seconds. As a result of this, sadly, most of the time we do not analyze the root causes of minor incidents or accidents. This is largely because such an analysis is very complex and expensive.
- The inquiry is subjective. It may be presumptuous to say that an official disaster inquiry following proper legal channels, and even attended by the learned profession of lawyers and judges is subjective, but regrettably too often this is the truth. This is especially the case if there were several fatal accidents - where the tragic loss of life provides ready "proof" of serious deficiencies in the organization. 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 most other similar organizations in the industry, without necessarily resulting in disasters or even fatal accidents.
- An inquiry can only identify and investigate what is apparent in the organization at that particular point in time. This "snapshot" of organizational deficiencies may be totally off the mark for the organization over a period of time, even though it may be correct for the specific period being investigated. It may even be accurate without those particular "findings" being really connected to the incident itself! There are just no objective analytical tools available to make these statements categorically. Organizational dynamics are just too complex! Such inquiries do not - though they ought to - analyse trends and dynamics in the organization over a period of time.

However, public inquiries are almost without exception staffed with technical and managerial personnel. And technical and managerial personnel will focus on technical and managerial issues. Possibly, every enquiry should be required to draw upon the expertise of social scientists in this field, and should even be a member of such inquiries.

- 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 organization? Clearly not, but there may be nothing "more wrong" with this company than with the one next door where no disaster happened.

Quite often organizations 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. The model in *Figure 1* shows that organizations may simply react to incidents by putting new regulations in place and fail to do the proactive surveys, audits, assessments and analyses needed.

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

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

### *10.1 Getting to the real, root causes*

An objective system of root cause analysis is needed. There are a number of principles and procedures that will achieve this goal:

- 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, i.e. 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 organization must continuously review its overall safety approach to strike a balance between managing the physical working environment (ie. hazards, procedures and safety systems) and managing behavior at the coal face (getting people to comply with safety standards coaching, getting them to recognize dangers; to demonstrate commitment to safety); and improve their attitudes to safety as well as developing the necessary knowledge and skills.
  - The most important aspect, and the one most neglected by most organizations, 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' strategic audits and design. Implementing a major safety management system, a new training program or a new safety administration 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?

### 10.2 What else can organizations do?

The following can be regarded as the issues, which organizations should typically address:

- Select the right safety precautions - not just those known to be available or expedient.
- Supervise and monitor the processes, procedures, individuals, departments, etc.
- Keep working practices, procedures, rules and regulations up-to-date.
- Exchange and manage information between individuals, departments, and organizations.
- Train staff and update skills.
- Focus on, analyze and manage the "safety culture" of the organization. In other words, develop "foresight" or active imagination about potential safety problems in the organization.

---

Unfortunately, all organizations have a specific approach to safety, an approach which determines the way they analyze problems. This "specific approach to analysis" largely influences the outcome of the analysis. For example, if the organization's approach or model is a strongly technical-engineering one, the findings of accident analysis will be mostly technical.

The model presented in *Figure 1* is one of Total Risk Management. It is a model that proposes that risk should be managed at all levels of the organization:

### 10.3 Shocking the system...

At organizational levels, the most complex issues are involved. It is at this level that the "culture" of the organization exists (if it can be said to "exist" at all) and it is at this level that interventions are also the most difficult to make work. Ensuring that the culture of organization does not produce the social readiness for a disaster requires bold and comprehensive actions from management. Management has to allow the organization to be subjected to severe "shocks and criticisms", in order to break, and continually break, the growth of complacency.

Shocking our system (SOS) in an organization ensures not only that ineffective systems or procedures are eliminated, but also that a continuous state of readiness is promoted. Our modern trends of self-regulation in legislation and of internal safety staff becoming "facilitators or advisers" may have contributed to the high levels of complacency in organizations.

A warning: The implementations of some of the recommendations that follow 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. This must not become merely human-resources-department reading matter. Spreading bad news in the organization can be good management practice.
- Expect, elicit, demand and "facilitate" bad news reaching the top of organization. This is the most difficult part, because it must make open upward communication of mistakes possible.
- Subject the organization 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. Provide them with resources and opportunities to complete extensive and intensive reviews.
- Ensure that the organization develops the willingness and skill to review, criticize and continually re-engineer itself. This can be achieved by intra-group reviews and self-assessment, e.g. within departments or within work teams, or by inter-group or peer reviews.

- 
- Consciously focus on "re-engineering" the organization 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, standards and local standards and practices.
  - Review the role of safety staff in the organization 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 organizations have lost a critical resource and the ability to keep a high(er) level of internal alertness. In the real world many individuals only function effectively when commanded to act and when "policed" to comply. If it was really possible to achieve full commitment from all levels in organizations, it should have been possible in public communities as well, rendering traffic rules, like speed limits, superfluous.
  - There may be a intense obligation for employers and employer organizations 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" and the resistance to criticism within the management of organizations. The advent of broader management practices in the last two decades has created the ability and processes for positive cooperation between management and labor in most developed industries. However, serious concerns exist that unions are not allowing this to happen in order to protect ideological turf. The unions' future role is potentially that of expert mediator between management and labor, and not of protector of labor against an "exploitative management".

## **11. 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 as diligently and honestly as they see fit at that moment in time, and as they are permitted by the circumstances.

Combine this with honest mistakes, misplaced risk perceptions, widespread organizational failures and a touch of coincidence, and the risk of disaster increases exponentially. It may never happen. But on the day it does...

Right now, back at the mine, our employees are going about their tasks in exactly the ways described in this paper. And if one or more of our controls falter, such as happened with Vaal Reefs, Challenger, Piper Alpha and Moura, disaster will strike us too, a disaster that has been created over a period of time and is in the process of creation now - by us, by our organizations.

---

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? History shows that it is true.

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.

Organizations have very poor memories. Industries have no memory at all...

---

## 12. Bibliography

Catastrophe! When Man Loses Control. Bantam Books, New York, 1979.

Clinard, Marshall B Corporate Ethics and Crime: The Role of Middle Management. Beverley Hills, California, Sage, 1983

Cook, R.C. The Challenger Report: A Critical Analysis of the Report to the President by the President's Commission on the Space Shuttle Challenger Accident" 1986. Mimeograph.

Dala, S.R., Fowlkes, E.B. and Hoadley, B. "Risk Analysis and the Space Shuttle: Pre-Challenger Prediction of Failure". Journal of American Statistical Association 84 (1989): 945-57

Douglas, Mary. How Institutions Think. London: Routledge and Kegan Paul, 1987

Essre, James K. and Lindoerfer J.S. "Groupthink and the Space Shuttle Challenger Accident: Toward a Quantitative Case Analysis" Journal of Behavioral Decision-Making 2 (1989): 167-77

March J. and Simon H.A. "Managerial Perspectives on Risk and Risk-Taking". Management Science 33 (1987): 1404-18.

Martin, J Cultures in Organizations: Three Perspectives. New York: Oxford University Press, 1992.

McCurdy, H.E. "The Decay of NASA's Technical Culture" Space Policy (Nov 1989): 301-10.

Perrow, C. Complex Organizations. A Critical Essay. Random House New York, 1986

Perrow, C. Normal Accidents. Living with High-Risk Technologies. Basic Books, USA, 1984

Petroski, H. To Engineer is Human: The Role of Failure in Successful Design. New York: St Martins, 1985.

Pitzer, C.J. "An investigation into Safety Culture in the New South Wales Coal Mining Sector, January 1977, (Research paper accompanying a Submission by the New South Wales Minerals Council)

Report on an Accident at Moura No 2 Underground Mine by the Wardens Inquiry, Queensland, 1996.

Report of the Presidential Commission on the Space Shuttle Challenger Accident. The President's Commission, June 1986, U.S. Government Printing Office, United States of America.

Statistical Reports (various) from the Departments of Minerals and Energy of NSW, Queensland and Western Australia.

The Public Inquiry into the Piper Alpha Disaster, October 1990, United Kingdom.

Thygerson, A.L. Accidents and Disasters. Causes and Countermeasures. Prentice-Hall, Inc Englewood Cliffs, New Jersey, 1977.

Toft, B and Reynolds S, Learning from Disasters. A management approach. Butterworth-Heinemann, Oxford, UK, 1994