Pike River Mine disaster (New Zealand)

“We are not an unsafe mine. However, an unsafe condition occurred, otherwise something wouldn’t have happened”

Pike River Coal chief executive Peter Whittall
(The Australian, November 23, 2010)

The accident began 19 Nov. 2010. Two explosions occurred (19 & 24 Nov.), killing 29 people trapped underground. A third and fourth explosion occurred on 26 Nov. and 28 Nov.
Safety management must prevent/protect against the KNOWN as well as the UNKNOWN.
Safety management requires THINKING about how accidents can HAPPEN.
The common understanding of safety implies a distinction between:

- **A normal state** where everything works as it should and where the outcomes/products are acceptable (positive or as intended).
- **A failed state** where normal operations are disrupted or impossible, and where the outcomes/products are unacceptable (negative or not as intended).

The purpose of safety (management) is to **maintain** a normal state by preventing disruptions or disturbances.

Safety efforts are normally driven by what has happened in the past, and are therefore **reactive**.

The level of safety is measured by the **absence** of negative outcomes.
Safety = (1 - Risk)

“By 2020 a new safety paradigm will have been widely adopted in European industry. Safety is seen as a key factor for successful business and an inherent element of business performance. As a result, industrial safety performance will have progressively and measurably improved in terms of reduction of
- reportable accidents at work,
- occupational diseases,
- environmental incidents and
- accident-related production losses.

It is expected that an ‘incident elimination’ culture will develop where safety is embedded in design, maintenance, operation and management at all levels in enterprises. This will be identifiable as an output from this Technology Platform meeting its quantified objectives.”
Safety measured by accident/incidents

“Safety is a dynamic non-event”
(Karl Weick)

But how can a non-event be measured or observed?

European Technology Platform on Industrial Safety (ETPIS) milestones:
- 25% reduction in accidents by 2020
- Programmes in place by 2020 to continue accident reduction at a rate of > 5% per year.
Theory W: Traditional safety perspective

Things go right because:

- **Systems** are well designed and scrupulously maintained,
- **Designers** can foresee and anticipate every contingency.
- **Procedures** are complete and correct
- **People** *behave* as they are expected to – as they are taught.

Humans are a liability and performance variability is a threat.
The purpose of design is to **constrain** variability, in order to prevent adverse outcomes.

The purpose of risk assessment is to identify *in a systematic manner* how adverse outcomes (= severe accidents) may be brought about.

Common assumptions

- Accidents are due to **failures or malfunctions** of components (*“human errors”*), equipment malfunctions.
- Risks can be represented by **linear combinations** or **chains of failures or malfunctions**. Example: Event tree - fault tree
Theory W: Safety by constraint

Function \rightarrow \text{Success (accident free)}

Non-compliance \rightarrow \text{Malfunction (root cause)}

- slow drift,
- abrupt transition

Failure \rightarrow \text{Failure (accidents, incidents)}
Theory W: Safety by constraint

Barriers, regulations, procedures, standardization, elimination

Non-compliance
slow drift, abrupt transition

Function

Malfunction
(root cause)

Success
(accident free)

Failure
(accidents, incidents)

Individual, team, organisation
(sharp end, blunt end)

Safety is achieved by constraining performance

Individual, team, organisation
(sharp end, blunt end)
Accidents are caused by people, due to carelessness, inexperience, and/or wrong attitudes.

Technology and materials are imperfect so failures are inevitable.

Organisations are complex but brittle with limited memory and unclear distribution of authority.
Work-as-done: The non-compliance view

**Unintentional**

Unintentional Understanding failure – when people have a different understanding of what the procedure is and what they have to do.

Unintentional Awareness failure – when people are not aware of the existence of a rule or procedure and therefore operate with any reference to it.

**Intentional**

Situational non-compliance – when the situation makes it impossible to do the job and be compliant, e.g., because of insufficient time or resources.

Optimizing non-compliance for company benefit – individuals take short-cuts believing that this will achieve what they believe the company, and their superiors, really want;

Optimizing non-compliance for personal benefit – short-cuts taken to achieve purely personal goals;

Exceptional non-compliance – deviations from the official procedures that may be difficult to follow under specific, and usually novel, circumstances.
Range of event outcomes

Neutral

Everyday events
(things that go right)

Very high
Probability

Range of event outcomes

Serendipity

Good luck

Incidents

Near misses

Mishaps

Disasters

Very low

Positive

Very high
Negative
Range of event outcomes

Very low

Serendipity

Good luck

Everyday events (things that go right)

Accidents

Incidents

Near misses

Mishaps

Disasters

Very high

Negative

Neutral

Positive

Probability

Probability

Range of event outcomes
Why only look at what goes wrong?

Safety = Reduced number of adverse events.

Focus is on what goes wrong. Look for failures and malfunctions. Try to eliminate causes and improve barriers.

Safety and core business compete for resources. Learning only uses a fraction of the data available.

Safety = Ability to succeed under varying conditions.

Focus is on what goes right. Use that to understand everyday performance, to do better and to be safer.

Safety and core business help each other. Learning uses most of the data available.

$$10^{-4} := 1 \text{ failure in 10,000 events}$$

$$1 - 10^{-4} := 9.999 \text{ non-failures in 10,000 events}$$

Safety = Ability to succeed under varying conditions.
Tractable and intractable systems

- **Tractable**
  - Easy
  - Simple
  - Low
  - Low rate of change (variability)

- **Intractable**
  - Difficult
  - Elaborate
  - High
  - High rate of change (variability)

**Descriptions**
Performance variability is necessary

Most socio-technical systems are intractable. Conditions of work are therefore underspecified.

Resources (time, manpower, materials, information, etc.) may be limited or unavailable

People (individually and collectively) must adjust what they do to match the conditions.

For the very same reasons, the adjustments will always be approximate.

Acceptable outcomes

The approximate adjustments are the reason why everyday work is safe and effective.

Unacceptable outcomes

But the approximate adjustments are also the reason why things sometimes go wrong.
Theory Z: Revised safety perspective

Things go right because people:

- Learn to **overcome** design flaws and functional glitches
- Adjust their performance to meet demands
- Interpret and **apply** procedures to match conditions
- Can **detect** and **correct** when things go wrong

Increasing complicacy have made modern technological systems **intractable**, hence **underspecified**.

Humans are therefore an **asset** without which the proper functioning of modern technological systems would be impossible.

Revised assumptions

- Accidents are due to **unexpected combinations** of actions rather than action failures. Example: **ETTO**.
- Risks can be represented by **dynamic coincidences** of performance variability. Example: **Functional Resonance**.
Theory Z: Safety by management

Physiological factors
Psychological factors
Social factors
Organisational factors
Contextual factors
External factors

Success (no accidents or incidents)

Performance variability is needed for everyday functioning (successes)

Failures cannot be prevented by eliminating performance variability

Everyday performance (variability)

“Amplify”

Failure (accidents, incidents)

“Dampen”

Individual, team, organisation (sharp end, blunt end)

Safety is achieved by managing unwanted combinations of performance variability without adversely affecting successes
Efficiency-Thoroughness Trade-Off

Thoroughness: Time to think
Recognising situation.
Choosing and planning.

If thoroughness dominates, there may be too little time to carry out the actions.

Neglect pending actions
Miss new events

Efficiency: Time to do
Implementing plans.
Executing actions.

If efficiency dominates, actions may be badly prepared or wrong

Miss pre-conditions
Look for expected results
The ETTO principle

The ETTO principle describes the fact that people (and organisations) as part of their activities practically always must make a trade-off between the resources (time and effort) they spend on preparing an activity and the resources (time, effort and materials) they spend on doing it.

ETTOing favours efficiency over thoroughness if throughput and output are the dominant concerns, and thoroughness over efficiency if safety and quality are the dominant concerns.

It follows from the ETTO principle that it is impossible to maximise efficiency and thoroughness at the same time. Nor can an activity expect to succeed, if there is not a minimum of either.
# Work-as-done: The ETTO view

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Avoid</th>
<th>Maintain-establish</th>
<th>Compensate for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Waste of time</td>
<td>Time buffer</td>
<td>Inadequate timing</td>
</tr>
<tr>
<td>Human effort</td>
<td>Waste of effort</td>
<td>Spare effort / work capacity</td>
<td>Manpower shortage</td>
</tr>
<tr>
<td>Workplace (HF)</td>
<td>Inadequate work conditions</td>
<td>Workable conditions</td>
<td>HMS deficiencies</td>
</tr>
<tr>
<td>Workload /stress</td>
<td>Work overload</td>
<td>Manageable workload</td>
<td>Overload (underload)</td>
</tr>
<tr>
<td>Materials / resources</td>
<td>Waste of material &amp; resources</td>
<td>Buffer of material / resources</td>
<td>Unavailability / inaccessibility</td>
</tr>
<tr>
<td>Equipment / tools</td>
<td>Improper use</td>
<td>Workable equipment / tools</td>
<td>Unavailability of tools</td>
</tr>
<tr>
<td>Finance (cost)</td>
<td>Waste of money</td>
<td>Financial buffer</td>
<td>Excessive cost</td>
</tr>
<tr>
<td>Data</td>
<td>Data overload</td>
<td>Data buffer</td>
<td>Missing data</td>
</tr>
</tbody>
</table>
From the negative to the positive

Negative outcomes are caused by failures and malfunctions.

All outcomes (positive and negative) are due to performance variability.

Safety = Reduced number of adverse events.

Eliminate failures and malfunctions as far as possible.

Safety = Ability to respond when something fails.

Improve ability to respond to adverse events.

Safety = Ability to succeed under varying conditions.

Improve resilience.
The resilient organisation

Resilience is the intrinsic ability of an organisation to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

In order to be resilient, the organisation must have four basic abilities.

- **Learn from past events**, understand correctly what happened and why
- **Factual** Monitor short-term developments and threats; revise risk models
- **Critical** Anticipate long-term threats and opportunities
- **Potential** Respond to regular and irregular conditions in an effective, flexible manner,
- **Actual**
# Complexity, intractability, and safety

<table>
<thead>
<tr>
<th>Traditional safety management</th>
<th>Resilience engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems are tractable and performance conditions can be completely specified.</td>
<td>Systems are intractable and performance conditions are always underspecified.</td>
</tr>
<tr>
<td>Most, if not all, adverse events can be attributed to a breakdown or malfunctioning of components.</td>
<td>Some adverse events can be attributed to component malfunctions, but others arise from unexpected combinations of variability of everyday performance.</td>
</tr>
<tr>
<td>Effective safety management can be based on accident tabulation and the calculation of failure probabilities.</td>
<td>Effective safety management is to cope with the complexity of the present and the future.</td>
</tr>
<tr>
<td>Re-engineering based on hindsight</td>
<td>Readiness based on foresight</td>
</tr>
</tbody>
</table>

© Erik Hollnagel, 2011
Engineering resilience

Solution: Enhance the abilities to respond, monitor, anticipate and learn.

The goal of resilience management is to increase the number of things that go right.

The goal of safety management is to reduce the number of things that go wrong.

Solution: Constrain performance by rules, procedures, barriers, and defences.
Conclusion: Two approaches to safety

Eliminate the negative (common safety approach)
Efforts to maintain or improve safety focus on what can go wrong and result in adverse outcomes. Many theories, models, and methods explain or predict how things can go wrong - with varying degrees of success. Some also propose solutions, focusing M, T, and O issues – also with varying degrees of success.

Accentuate the positive (resilience engineering)
In resilience engineering, efforts to maintain or improve safety focus on what goes right, as well as on what should have gone right. Theories, models, and methods to describe how things go right, but sometimes fail, and how humans and organisations cope with internal and external intractability and unpredictability.
Thank you for your attention