EMESRT Workshop
23rd – 25th September 2014

Legislative, Functional Safety, Risk Management & Controls Optimisation Contexts for Mine Collision Avoidance Systems

Presented by
Marcus Punch
FSExpert (TÜV Rheinland)
CPEng, NPER, RPEQ

Marcus Punch Pty. Ltd
Risk and Reliability

Mobile: +61 (0)432168849
Email: marcus@marcuspunch.com
Web: www.marcuspunch.com

Setting the Scene – The Pizza Party

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Australian / New Zealand Legislative Context

Primary Duty of Care – 'SFAIRP'

Model WH&S Act 2011

Clause 19 Primary duty of care

(1) A person conducting a business or undertaking must ensure, **so far as is reasonably practicable**, the health and safety of:

(a) workers engaged, or caused to be engaged by the person; and

(b) workers whose activities in carrying out work are influenced or directed by the person, while the workers are at work in the business or undertaking.

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Primary Duty of Care – 'SFAIRP'

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Model WH&S Act 2011 Part 2 Division 2 Clauses 22-26 (design , manufacture, import, supply, install / construct / commission)

Clause 22 Duties of persons conducting businesses or undertakings that design plant, substances or structures

(2) The designer must ensure, **so far as is reasonably practicable**, that the plant, substance or structure is designed to be without risks to the health or safety of persons:

(3) The designer must carry out, or arrange the carrying out of, any calculations, analysis, testing and examination that may be necessary for the performance of the duty imposed by subsection (2).

(4) The designer must give adequate information to each person who is provided with the design ….

What is 'Reasonably Practicable'?

Marcus Punch Pty. Ltd. Risk and Reliability
www.marcuspunch.com
0432168849

Model WH&S Act 2011 Clause 18

What Is Reasonably Practicable

That which is, or was at a particular time, reasonably able to be done in relation to ensuring health and safety, taking into account and weighing up all relevant matters including:

(a) the **likelihood** of the hazard or the risk concerned occurring.

(b) the **degree of harm** that might result from the hazard or the risk.

(c) what the person concerned **knows, or ought reasonably to know**, about: (i) the hazard or the risk, and (ii) ways of eliminating or minimising the risk.

(d) the **availability and suitability** of ways to eliminate or minimise the risk,

(e) **after** assessing the extent of the risk and the available ways of eliminating or minimising the risk, the **cost associated** with available ways of eliminating or minimising the risk, including whether the cost is **grossly disproportionate** to the risk.

What is 'Reasonably Practicable'?

- An objective test usually applied <u>after</u> the fact.
- A duty-holder must meet the standard of behaviour expected of a **reasonable person** in the duty-holder's position and who is required to comply with the same duty.
- There are two elements:

  what can be done - what is possible, given the circumstances.

  whether it is *reasonable,* *in the circumstances* to do all that is possible.

- This means that **what can be done should be done** unless it is reasonable in the circumstances to do something less (see the **Safe Work Australia Interpretive Guideline**).

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Post-accident: The objective test.

Marcus Punch Pty. Ltd. www.marcuspunch.com
Risk and Reliability 0432168849

Question posed to the expert witness:

- **What would be the minimum requirement have been to make the system of work safer?**

That is:

- What ***you thought*** the likelihood of the event (and therefore its 'risk') was before the accident is largely irrelevant after it happens.
- What **you *knew***, and how ***you responded*** is not relevant either.
- What is more important is:
  - What a reasonable person would have **known**, and
  - What a reasonable person would have **done** in response to the hazard.
- If a **standard / guide / code or expert witness** testimony indicates that more could have been done, then you may not have met the test of reasonably practicable.

A Few Words on Cost.....

From the Safe Work Australia Interpretive Guideline:

- If the degree of harm is **significant** (eg. death or serious injury is at least moderately likely) it is likely that the cost of available and suitable safeguards would **never be so disproportionate** as to justify a decision not to implement them.
- If the degree of harm is significant and you cannot afford to implement an available and suitable safeguard, **you should not engage in the activity** that gives rise to that hazard or risk.
- Cheaper options may be used where the costlier option is grossly disproportionate to the risk, but only if the cost is high and the **likelihood or degree of harm is low** (eg. a slight chance of minor cuts or strains).
- And again, if it is an available and suitable safeguard, **capacity to pay is not relevant**, especially if the degree of harm is significant.

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Cost / Benefit Analysis (CBA)

Marcus Punch Pty. Ltd.
Risk and Reliability
0432168849
www.marcuspunch.com

- The Proposal: Collision avoidance system
- The Cost: 30 trucks x $50,000 per truck = $1,500,000
- The Benefit: Annual likelihood of collision (and serious injury) predicted to be reduced from 1% (0.01) to 0.1% (0.001). Financial effect of an accident is $15,000,000.
- Calculation:
- Financial costs = $1,500,000
- Expected financial benefits (over the 20 year life of the installation)

  = $15,000,000 x (0.01-0.001) x 20 = $2,700,000

- Financial Cost / Benefit Ratio (CBR)

  = 1,500,000 / 2,700,000 = 0.55

  If CBR is greater than 1, the costs exceed the benefits.

  If CBR is less than 1, the benefits exceed the costs.

Should the proposal go ahead?

Do we need prescriptive regulations?

- Interpretation of Clause 19 of the Model WH&S Act would indicate that CA systems would effectively be 'mandatory' anyway because in many foreseeable collision scenarios they are known, available and suitable and can prevent significant harm from occurring.
- However, there is no requirement to take a systematic risk assessment approach to hazards which fall outside of the hazards specifically addressed in the Model Regulations.
- Therefore, there is no requirement to systematically assess collision hazards.
- But there is a requirement to implement CA systems if they are known, available and suitable for a particular foreseeable hazard.
- This is patently stupid! See Johnston and page 94.
- **ie. there is no need to mandate collision avoidance systems – just amend the Model Regulation to require systematic risk assessment of all hazards.**

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

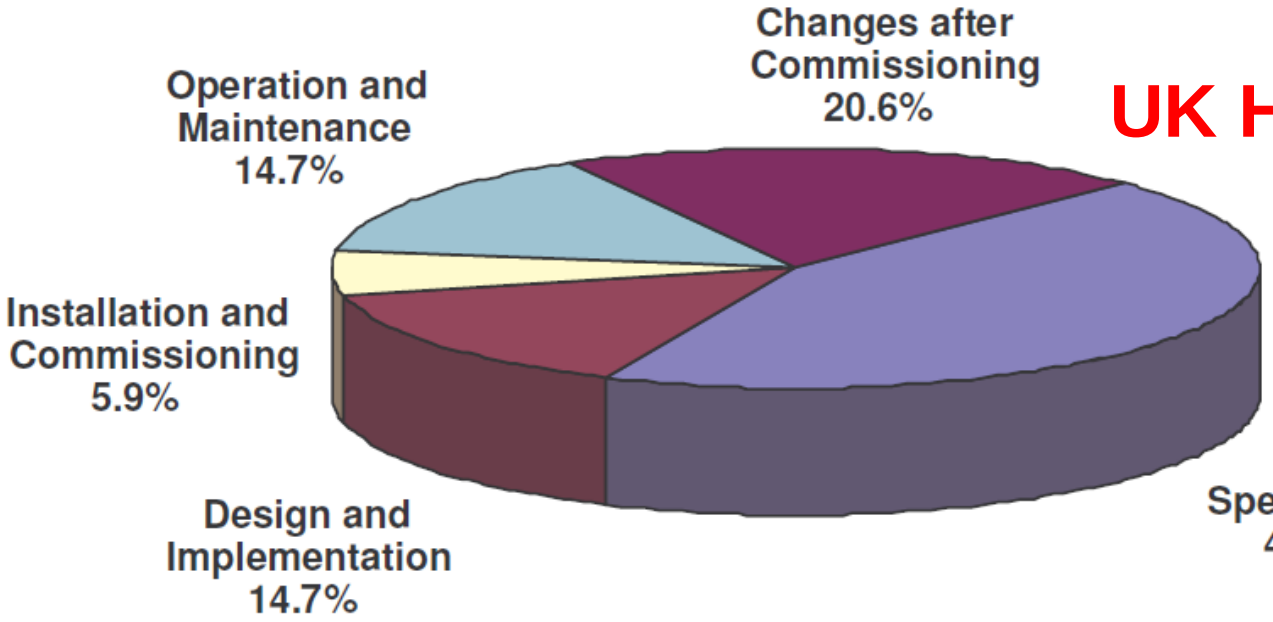
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Functional Safety & Risk Management Context

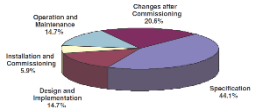
Why the Fuss?

"Our ability to understand and manage the complexities of PE-based systems have not kept pace with the technology's utilization. As a result, PE-related incidents causing mission failures, harm to the environment, injuries, and fatalities have occurred."

Source: *"A Complexity Assessment Methodology for Programmable Electronic (PE) Mining Systems", John J. Sammarco, P.E.; National Institute for Occupational Safety and Health (NIOSH); Pittsburgh, Pennsylvania. 2002.*



UK H&SE Study



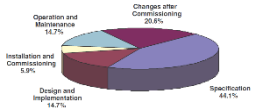
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

What is 'Functional Safety'?

Correct operation in response to inputs.

*"Functional safety is that part of the overall safety relating to the EUC (equipment under control) and the EUC control system, **which depends on the correct functioning** of the electrical, electronic and programmable electronic (E/E/PE) Safety-related systems (SRS) and other risk reduction measures."*

See AS61508, Part 4.



Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

What is a ‘Safety-related System’?

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

1. Achieves or maintains a safe state.

2. Failure can result in an immediate increase in risk.

Would the presence of a proximity detection / collision avoidance system lead an operator to rely upon it (in full or in part) to ‘maintain’ a safe state?

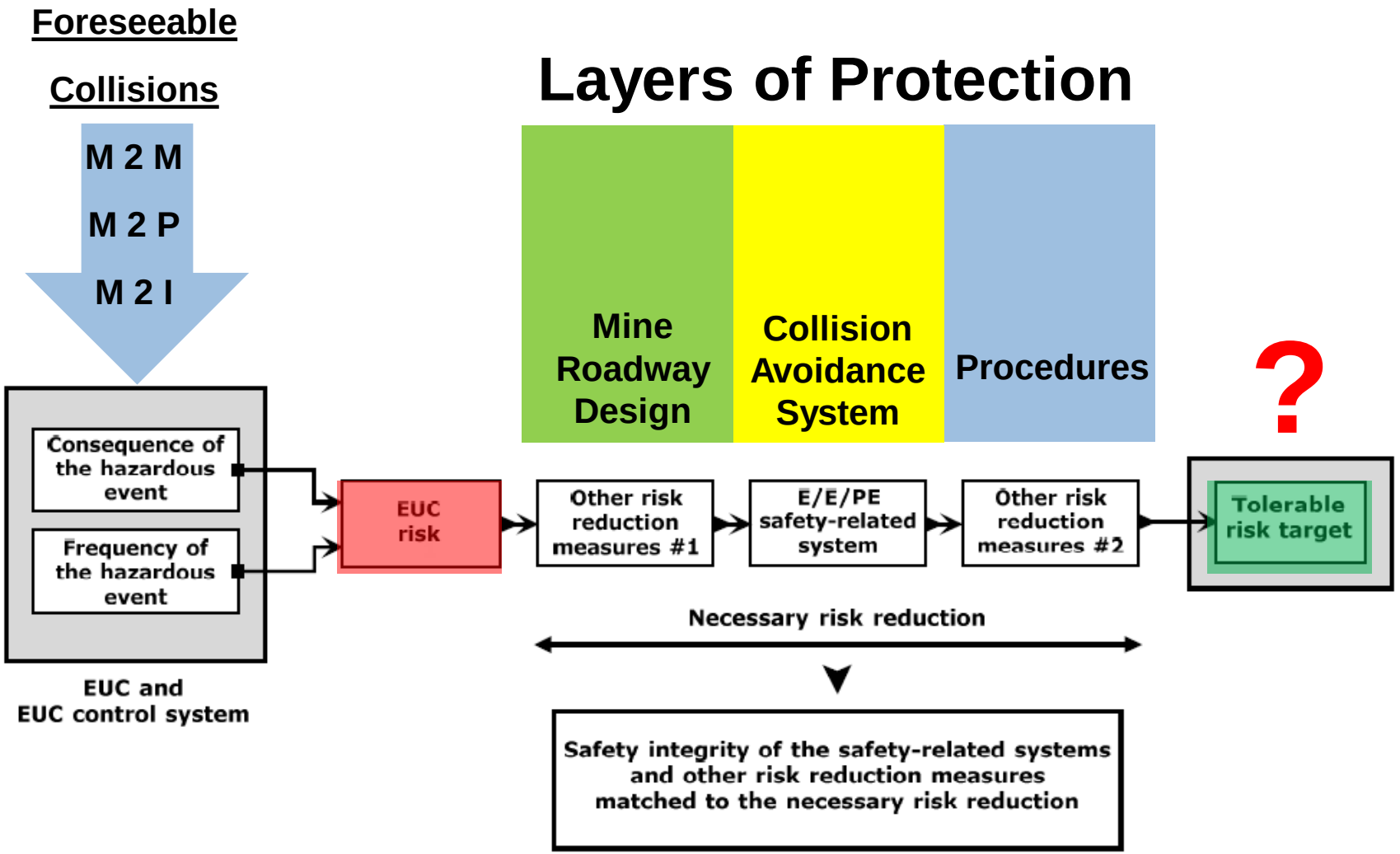
What is 'Safety Integrity'?

Probability of satisfactory performance .....a number!

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

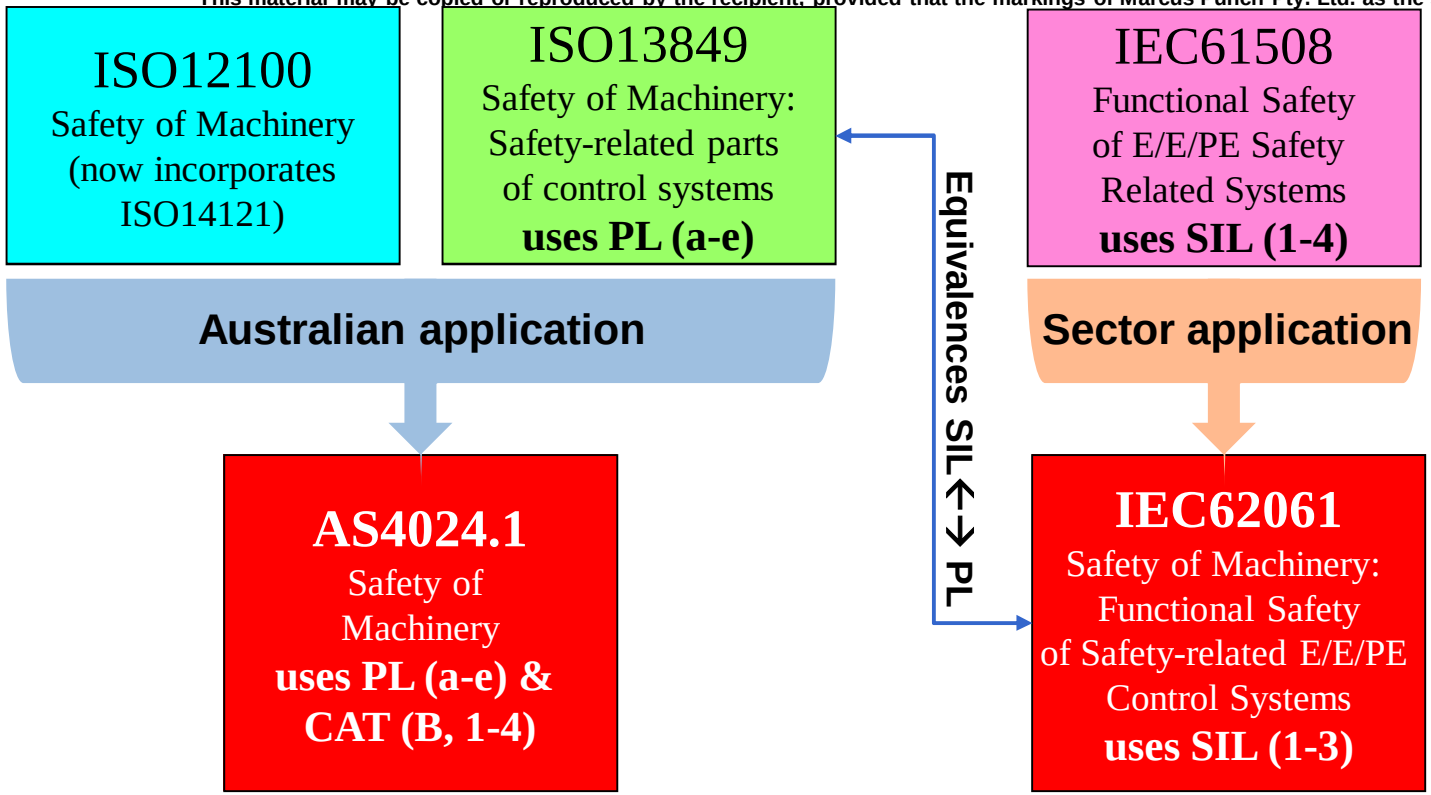
AS61508 Risk Reduction Process

Marcus Punch Pty. Ltd. www.marcuspunch.com 0432168849
Risk and Reliability



The SIL allocated to an E/E/PE safety-related system is based on the risk reduction required by that layer after accounting for the EUC risk, the tolerable risk target and the risk reduction required of the other layers of protection.

Safety Integrity Target Measures



AS4024.1501&1502 (2006) retains CAT as the safety integrity target measure, per 1990's versions of EN954-1&2 and ISO13849-1&2.

IEC62061 (2005) adopted as AS61508 (2006) in Australia.

ISO13849-1 (2008) has been adopted as AS4024.1503 (2014) allowing the use of PL as an alternative to CAT in Australia.

IEC62061 was updated in 2012.

Marcus Punch Pty. Ltd. *Risk and Reliability* *0432168849* *www.marcuspunch.com*

Reasonably Practicable V's Tolerable Risk

- A PCBU must ensure, **so far as is reasonably practicable**, the health and safety of workers (Model WH&S 2011, Clause 19).
- The concept of 'Reasonably Practicable' is primarily concerned with ensuring that all **known, available and suitable** safeguards to eliminate or reduce risk have been implemented.
- **'Tolerable risk' is not relevant in law.**
- Just because a 'tolerable' level of risk is demonstrated / achieved, does not mean that the test of 'SFAIRP' has been met.
- However, the SFAIRP approach does not provide a mechanism for engineering decision-making about the appropriate level of integrity / strength / reliability to be designed into the selected safeguards.

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Reconciling the Approaches – SFAIRP First !

- Try to **eliminate** the hazard first.
- Then use the **hierarchy of risk controls**.
- Ensure that all **known, available and suitable controls** are considered and the most effective are chosen.
- If the **potential for harm is significant** then all known, available and suitable controls should be used, or stop the activity giving rise to the risk.
- Check that the **SFAIRP test** would be met before using the 'tolerable risk' approach to determine the SIL/PL requirements.
- Is the chosen 'tolerable risk' **target reasonable** and justifiable?
- Is it 'reasonably practicable' to drive the 'residual risk' **even lower**?
- Consider what level of safety integrity would be reasonably practicable for the **designer** to achieve?
- Consider any SIL requirements of **regulations, codes of practice and standards.**

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

MINE: Hazard and Risk Analysis

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Proximity detection / collision avoidance is no ‘silver bullet’.

The following collision hazards are ones where risk ‘elimination’ or ‘substitution’ may be an option:

Manned dozer falls into coal valve.

- Option 1 (Prevention): Collision avoidance, but at SIL3.
- Option 2 (Substitution): Remote control dozer.

MINE: Hazard and Risk Analysis

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Proximity detection / collision avoidance is no 'silver bullet'.

HV / HV head-head collision (drive-by opposite directions).

- Option 1 (Prevention): Collision avoidance, but at SIL2.
- Option 2 (Substitution): One-way or divided traffic flows on mine roads used by heavy vehicles.

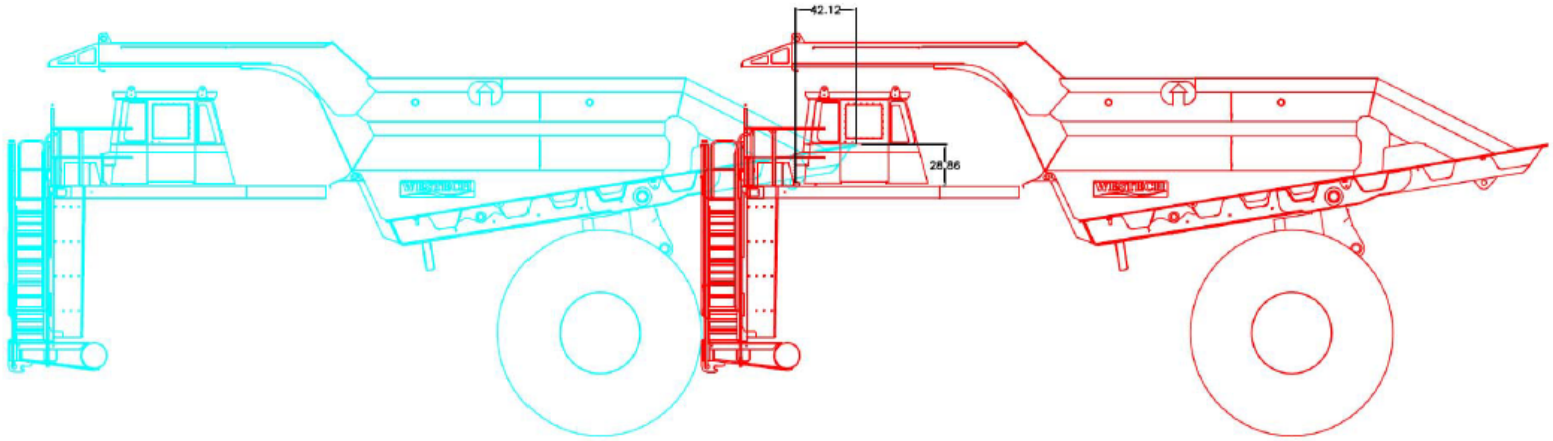
MINE: Hazard and Risk Analysis

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Proximity detection / collision avoidance is no ‘silver bullet’.

HV / HV head-tail collision (reversing / rear-ender).

- Option 1 (Prevention): Collision avoidance, but at SIL2.
- Option 2 (Prevention): Re-design truck (or don’ t buy that model) to prevent nose-to-tail collisions crushing a driver’s cabin.



MINE: Safety Requirements Allocation

Defines the overall safety function requirements based on the results of the hazard and risk analysis:

- Defines the intent of the safety functions

eg. Detects proximity of / prevents collision of …..

- Target safety integrity requirements for the safety functions in terms of:

eg. Probability of Failure on Demand (PFD), or

Probability of Dangerous Failure per Hour (PFH).

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

MINE: Safety Requirements Specification

- The Safety Requirements Specification (SRS) is the key interface between ‘analysis’ and ‘realisation’ stages.
- A supplier’s assertion that they do not need to comply with AS61508 / AS4024 / AS62061 / ISO13849 can be avoided if the contract requires compliance and payment is linked to successful delivery.
- The Safety Requirements Specification (SRS) should therefore be a core part of the Statement of Work (SOW) and the contract of supply. See AS62061 Clause 5 or ISO13849 Clause 5 or AS61508.1 Clause 7.10.
- Put the SRS in your tender package, and get the vendors to respond to it.
- Simply stating: “...the supplier shall comply with AS61508”, or words to that effect, is not enough – and is, in fact, meaningless.

Ask yourself if this happens at your site / project.

Marcus Punch Pty. Ltd. www.marcuspunch.com 0432168849
Risk and Reliability

SUPPLIERS: Information

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

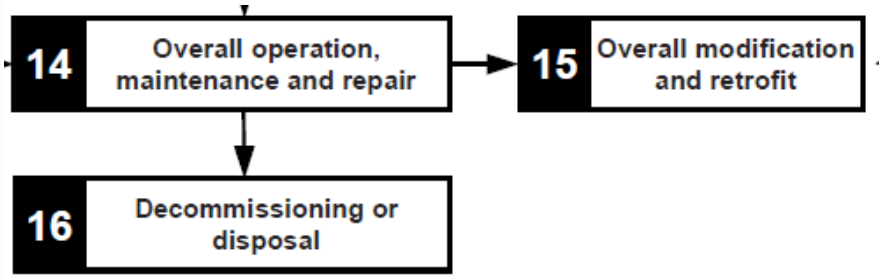
- Designers, manufacturer's and suppliers should be expected to produce information sufficient to allow independent verification that the safety requirements have been met within their scope of supply, and for future lifecycle management.
- This is consistent with the designer / manufacturer / supplier PCBU primary duties in the WH&S Act.
- **AS61508-2:2010 Clause 7.4.9.7, Note 2:**

  " There may be commercial or legal restrictions on the availability of evidence. These restrictions are outside the scope of this standard. If such restrictions deny the functional safety assessment adequate access to the evidence, **then the element is not suitable for use in E/E/PE safety-related systems**".

Ask the suppliers if they have this information available now.

Ask the suppliers if they will provide access to the evidence.

MINE: Operational Phases



Can you demonstrate that you maintain / test / analyse your protective systems correctly?

Can you demonstrate that you are in control of your modification process?

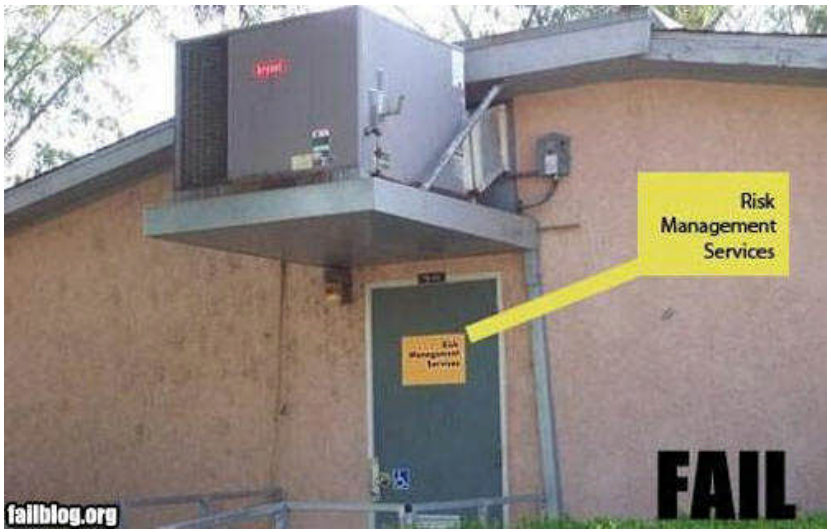
The keys to success:

1. **Competence** of operators / maintainers / engineers.
2. **Compliance** to operating / maintenance / engineering requirements.
3. **Control** of operating / maintenance / engineering changes.
4. **Vigilence** and prompt action by all.

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Controls Optimisation Context



What is a control…….?

AS/NZS ISO31000-2009:

Control: "Measure that is modifying risk".

Risk: "Effect of uncertainty on objectives".

Control: "Measure that is modifying the effect of uncertainty on objectives".

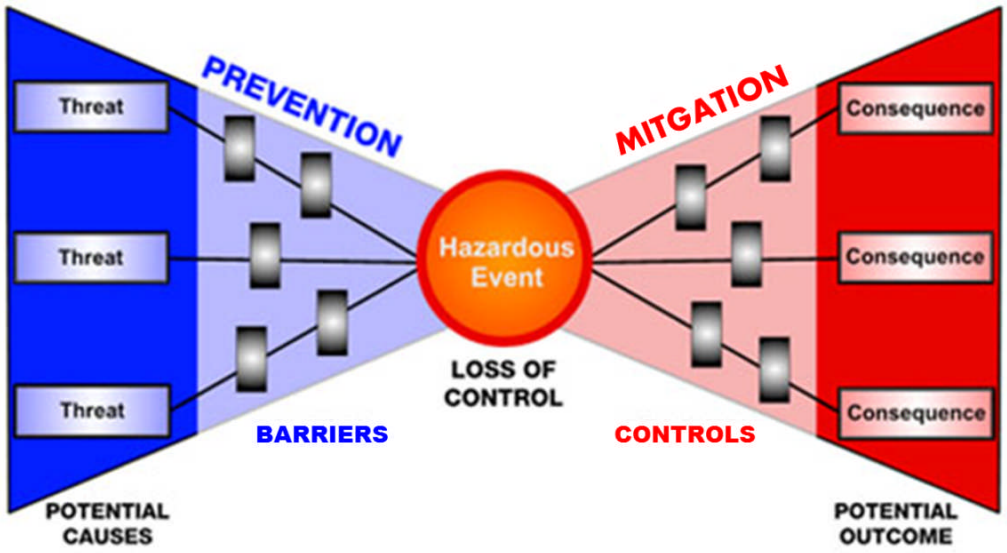
Shortcomings:

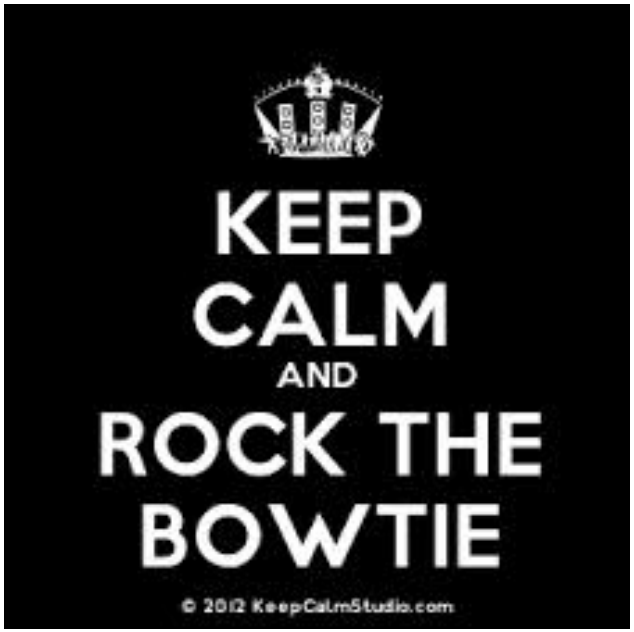
- Risk-centric.
- Too broad – to accommodate the financial sector.
- User-unfriendly?
- Vague?
- No recognition of how controls act on accident sequences.
- No recognition of when controls act in the sequence.
- No recognition of the relationship between causes, controls and consequences.

Marcus Punch Pty. Ltd. Risk and Reliability
www.marcuspunch.com 0432168849

What is a control…….?

A “bow-tie” or similar diagram used by safety barrier models usually shows the cause-control-consequence relationships and the general event sequence for any given unwanted event or accident.





Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

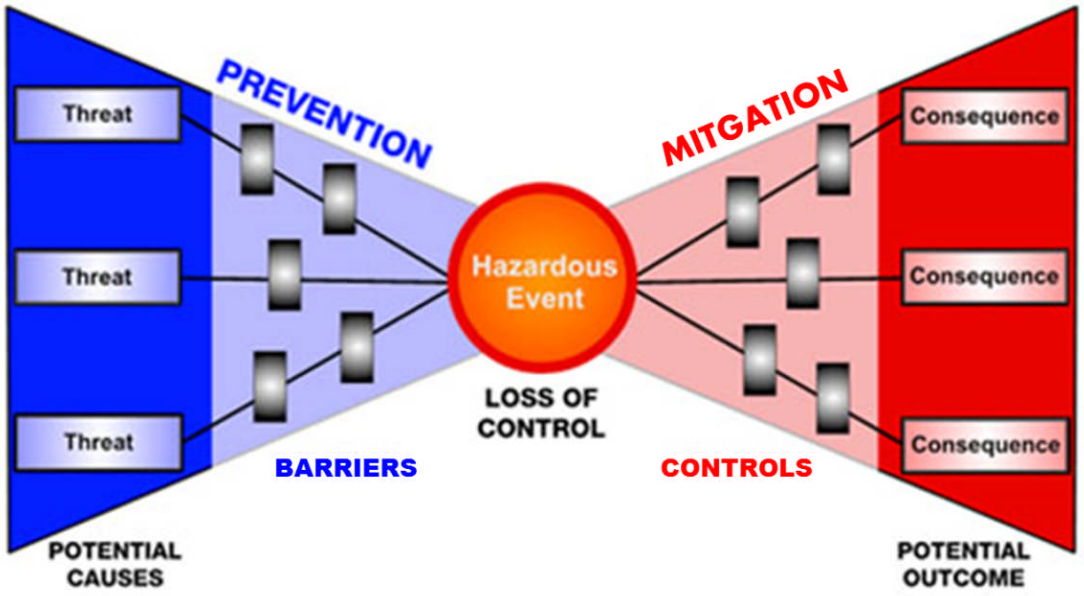
What is a control…….?

- The function of controls is to stop the accident sequence (ie. arrest it), or to deviate its propagation to a less severe consequence (ie. deflect it).

Control: "arrests or deflects an accident event sequence".

arrest: stop, catch, seize and hold.

deflect: turn aside, bend or deviate.



Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

What is a control…….?

- A tangible / physical object or system, which of itself, arrests/deflects an unwanted event.

  - May be passive (eg. bund) or active (eg. gas monitoring).
  - May be automatically operated (eg. inter-trip) or rely upon a human act to operate (eg. push an emergency-shut-down button).
  - May include software (eg. within a PLC).

  eg. fire suppression system, roof-bolts, collision avoidance system, emergency shut-down system, transformer bunding, redundant braking system, pressure relief valve, earthing.

Marcus Punch Pty. Ltd. *Risk and Reliability* *www.marcuspunch.com* *0432168849*

What is a control…….?

- A human act (eg. behaviour or response to stimuli), which of itself, arrests/deflects an unwanted event.
  - May be derived from the contents of a procedure, training or experience about what is expected of a person in a given situation.
  - Can often be described using a verb / noun pair.

eg. obey speed restrictions, isolate electrical supply, apply emergency brake, wear safety glasses, drink water.

Marcus Punch Pty. Ltd. *Risk and Reliability* *www.marcuspunch.com* *0432168849*

What is a control…….?

- A control is often supported by things which help assure its reliability, potency, robustness etc…, but sometimes these things are mistaken as being controls too.
- But, of themselves, they do not arrest/deflect an unwanted event.

eg. competency assessment.

eg. a brake inspection.

eg. common-sense.

eg. a procedure.

eg. a prayer ?.

Marcus Punch Pty. Ltd. *Risk and Reliability* *www.marcuspunch.com* *0432168849*

What is control effectiveness…….?

It is suggested that the most effective controls are:

- Pro-active (or Preventive) – they prevent the point of 'loss of control' (the unwanted event), rather than control or mitigate the consequences of the unwanted event after it has occurred.
- Potent (ie. efficacy) - are technically capable of arresting or deflecting the accident sequence.
- Reliable – have a high probability of successfully performing their function when required.
- Responsive – operate within sufficient time to arrest or deflect the accident sequence.
- Robust – are able to cope with changes to their operating environment.
- Realistic – are cost effective / utilitarian, resource efficient and simple with ease of legacy.

Marcus Punch Pty. Ltd. *Risk and Reliability* *www.marcuspunch.com* *0432168849*

What is control effectiveness…….?

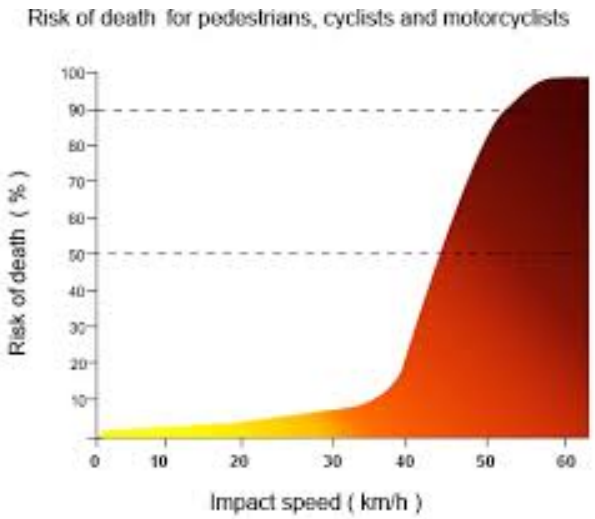
AS/NZS ISO31000-2009:

- Risk treatment (ie. controls) can create new risks or modify existing risks.
- Controls may not always exert the intended or assumed modifying effect.
- Risk treatment can itself introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures.

Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

What is a control effectiveness…….?

- Is evidence-based, specifiable, measureable and auditable.



Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Questions…….?

Functional Safety -

- Standards Australia, AS61508.0 – Functional Safety and AS61508, (10-page basic overview of the standard).
- Marcus Punch, ***Functional Safety for the Mining & Machinery-based Industries – An integrated framework using AS(IEC)61508, AS(IEC)62061, AS(IEC)61511, ISO13849 and AS4024****.1, 2nd Edition,* ISBN 978-0-9807660-2-8.

Tolerable Risk and SFAIRP -

- Safe Work Australia, *Interpretive Guideline - The Meaning of Reasonably Practicable.*
- Johnstone & Tooma, *Work Health & Safety Regulation in Australia – The Model Act*.
- UK H&SE, *Reducing Risks, Protecting People (R2P2)* - HSE's Decision-making Process, ISBN 0-7176 2151-0.

Marcus Punch Pty. Ltd. www.marcuspunch.com 0432168849
Risk and Reliability