NSW Department of Trade & Investment
Electrical Engineering Safety Seminar
5th - 6th November 2014

When SIL2 Will Just Not Do !

Presented by
Marcus Punch
FSExpert (TÜV Rheinland), CPEng

Marcus Punch Pty. Ltd.
Risk and Reliability

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

Overview

- A retrospective overview of the use of the functional safety approach in mines since 2006.
- Focussing on three (3) common implementation pitfalls:

1. By-passing the process.
2. Inadequate specification of safety requirements.
3. When SIL2 will just not do.

- And briefly, two (2) knowledge / competence issues:

1. The root of all confusion.
2. The elephant in the training room.

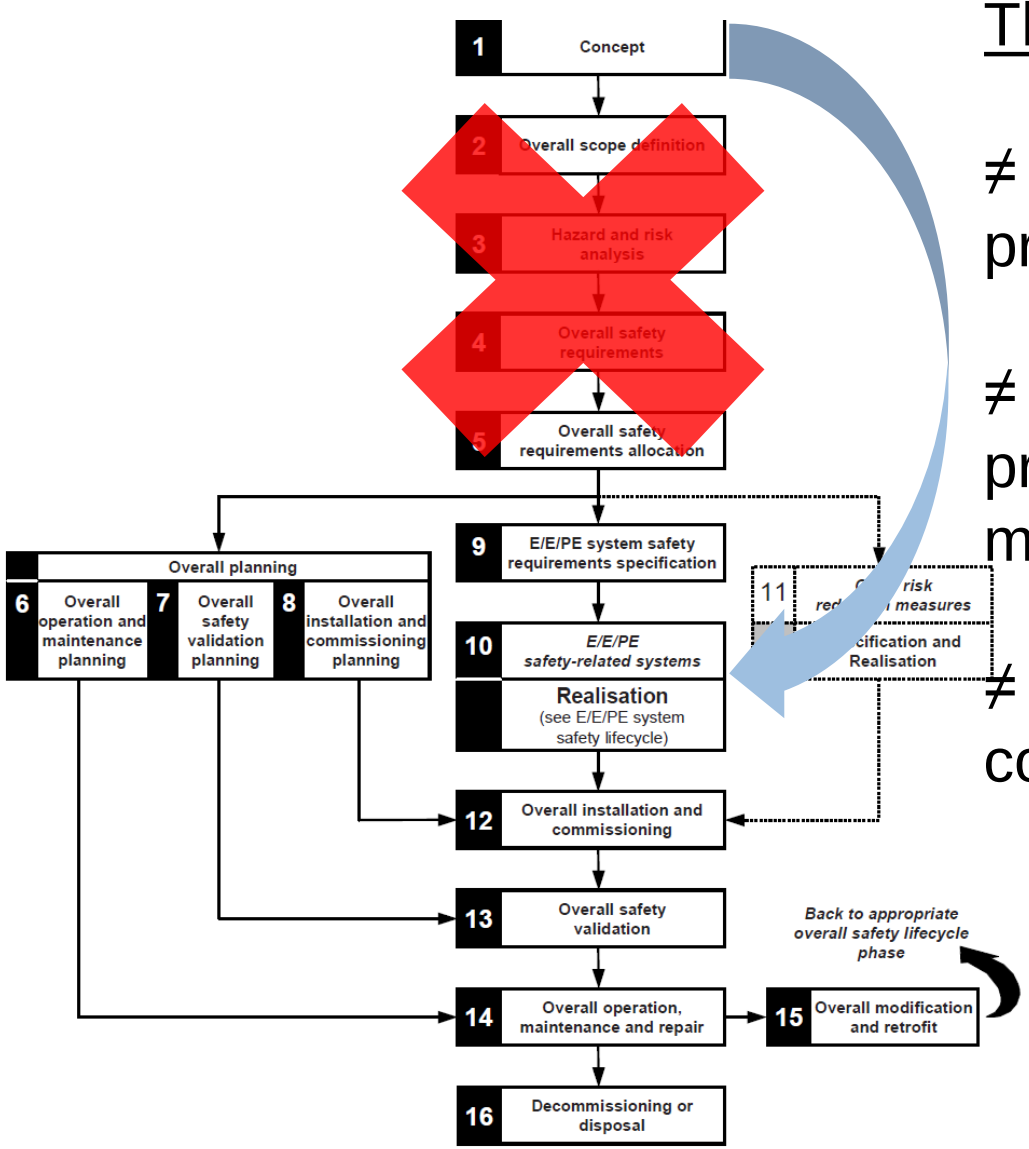
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

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

By-passing the Process

The Case of the Lost Opportunity

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



<u>The by-pass flick-pass:</u>

≠ The supplier shall provide a SIL2 E-Stop…

≠ The supplier shall provide a SIL2 machine…

≠ The supplier shall comply with AS61508...

The Case of the Lost Opportunity

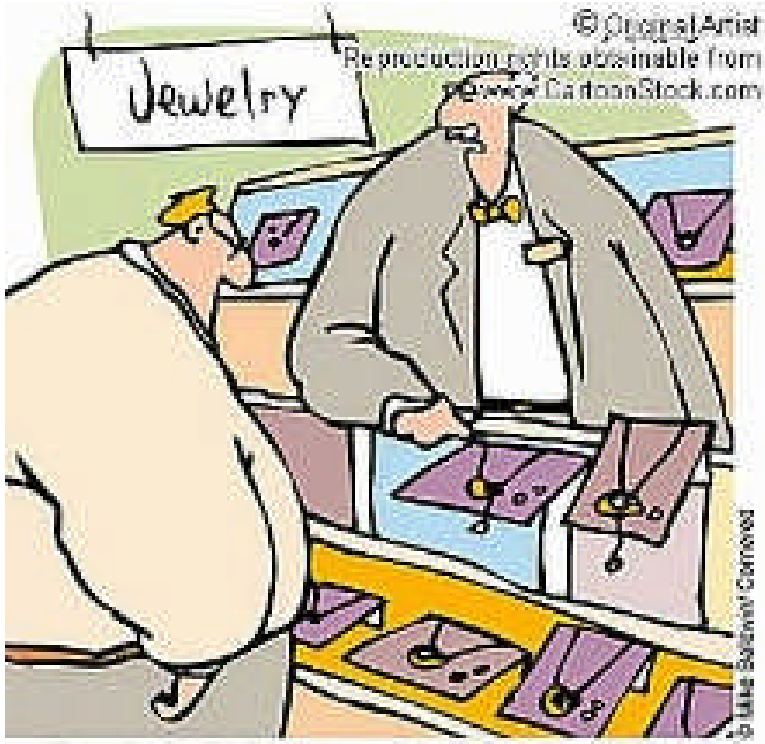
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

The upside:

- Less time / cost / effort / inconvenience.

The downside:

- Insufficient and / or ineffective risk controls selected.
- Inadequate specification of safety requirements.
- Supplier either ‘gold-plates’ the machine or makes a token effort, depending on their contract terms.
- Level of safety assurance is open to question.



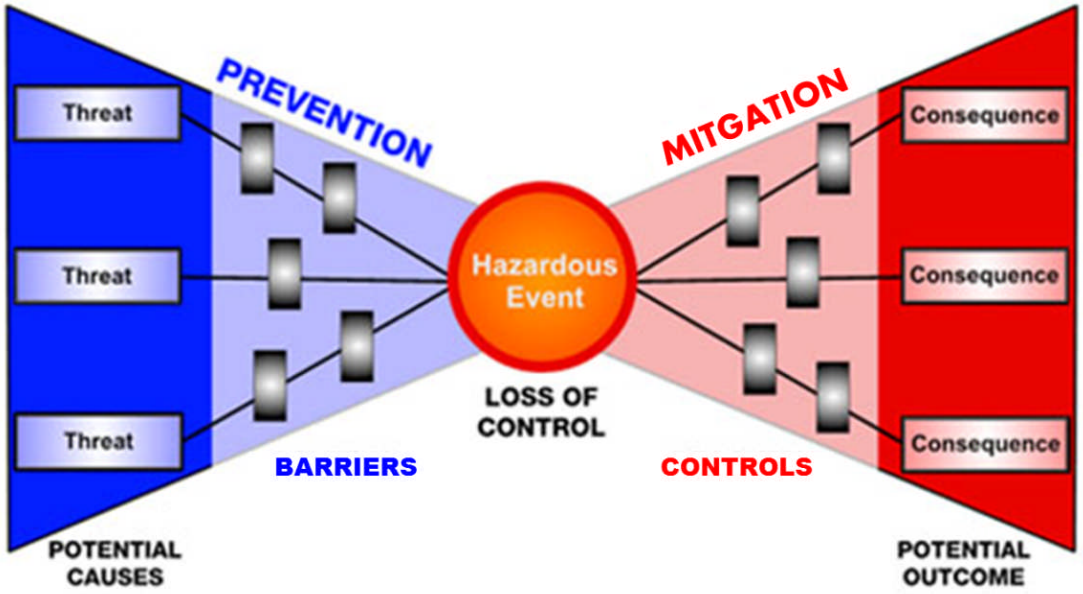
"Too pricey? Perhaps you wish to see something in macaroni and spray paint?"

The Case of an Ineffective Control…

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

What is a risk control…….?

- Think of the 'Bowtie'.



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

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

What is a risk control…….?

- A **tangible / physical object or system**, which **of itself**, arrests/deflects an unwanted event.
  - May be passive (eg. guarding) or active (eg. proximity detection).
  - May be automatically operated (eg. fire suppression) or rely upon a human act to operate (eg. emergency brake).
- 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 not a risk 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. training,
procedures.
competency assessment.
a maintenance task.
common-sense.
a prayer.

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

What is control effectiveness…2P4R ?

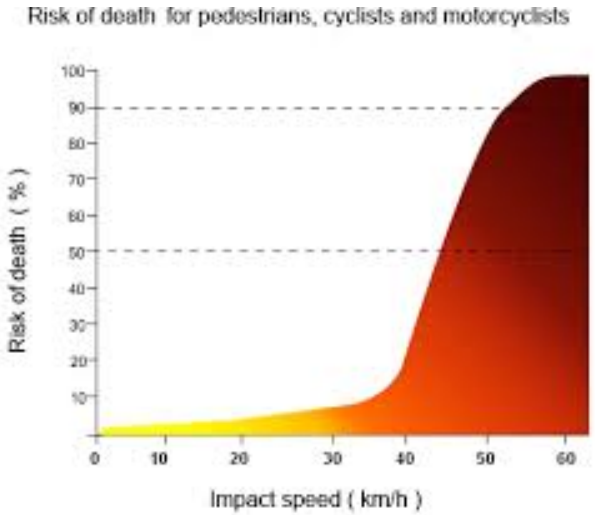
- **Pro-active** – prevent the unwanted event, rather than control the consequences.
- **Potent (ie. efficacy)** - technically capable of arresting or/ deflecting the accident sequence without imposing additional risk.
- **Responsive** – in place, or operates within sufficient time.
- **Robust** – can cope with changes to the operating environment.
- **Realistic** – value for money, simple, with ease of legacy.
- **Reliable** – high probability of successful operation.

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

What is control effectiveness…ESMA?

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

Evidence-based



Specifiable

Measureable

Auditable

But….back to those pesky E-Stops…

- NSW / QLD WH&S Regulation Cl.191.2.(c).

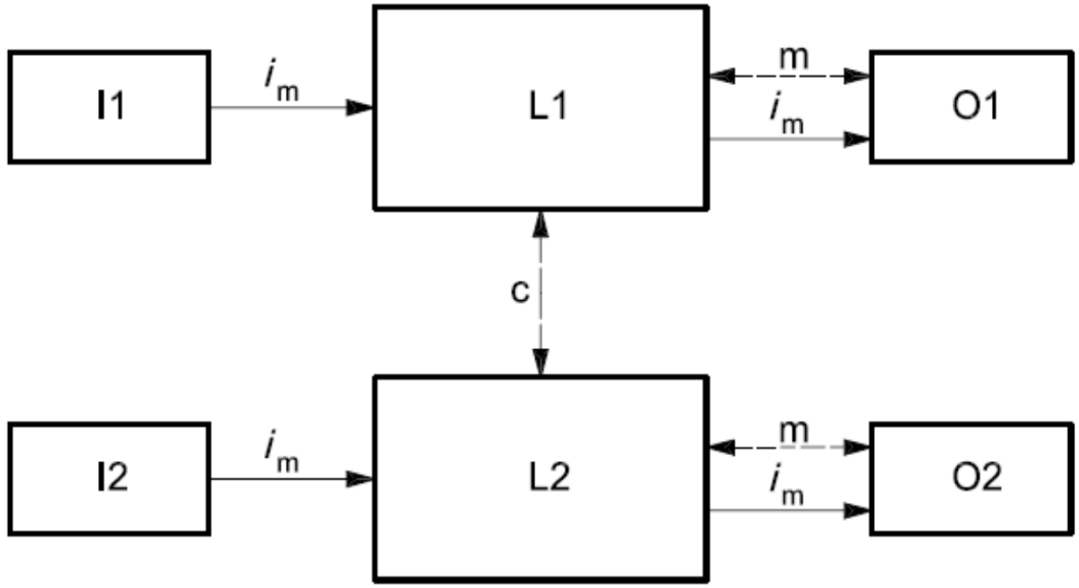
"…cannot be adversely affected by electrical or electronic circuit malfunction".

- Hierarchy: Act > Regulation > CoP > Standard > Guideline
- Must be complied with regardless of E-Stop effectiveness or SIL allocated.
- So far as is reasonably practicable?
- Effective use of scarce financial resources?

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

A Solution…..

- Determine if / when any E-Stop is an effective control.
- If it is, determine a SIL requirement for it - design for fault tolerance regardless of the SIL required.
- If not, design for fault tolerance anyway.

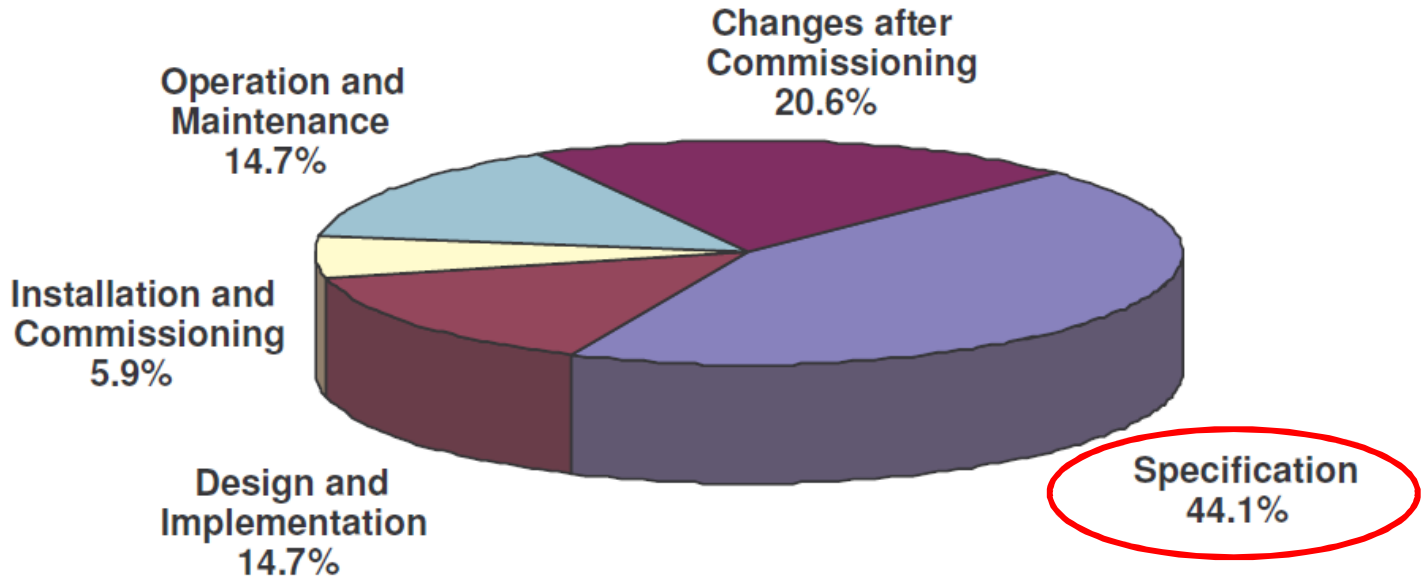


Refer ISO13849-1 Section 6.2.6 (now in AS4024.1503).

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

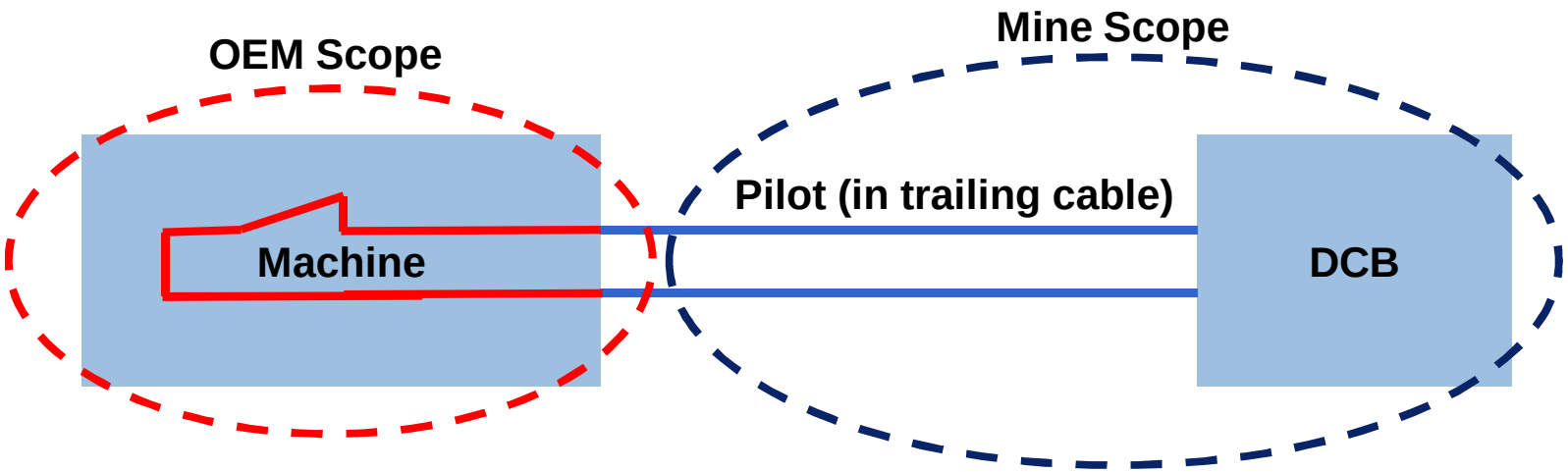
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

Inadequate Specification of Safety Requirements



The Case of the Pilot Circuit

- Safety functions utilising the pilot circuit of the machine require consideration of on-board and off-board parts.
- OEM → On-board parts (eg. pushbutton, etc…)
- Mine → Off-board parts (eg. cable, DCB, etc…).
- What happens if the mine passes responsibility to the OEM to meet a SIL but does nothing itself?



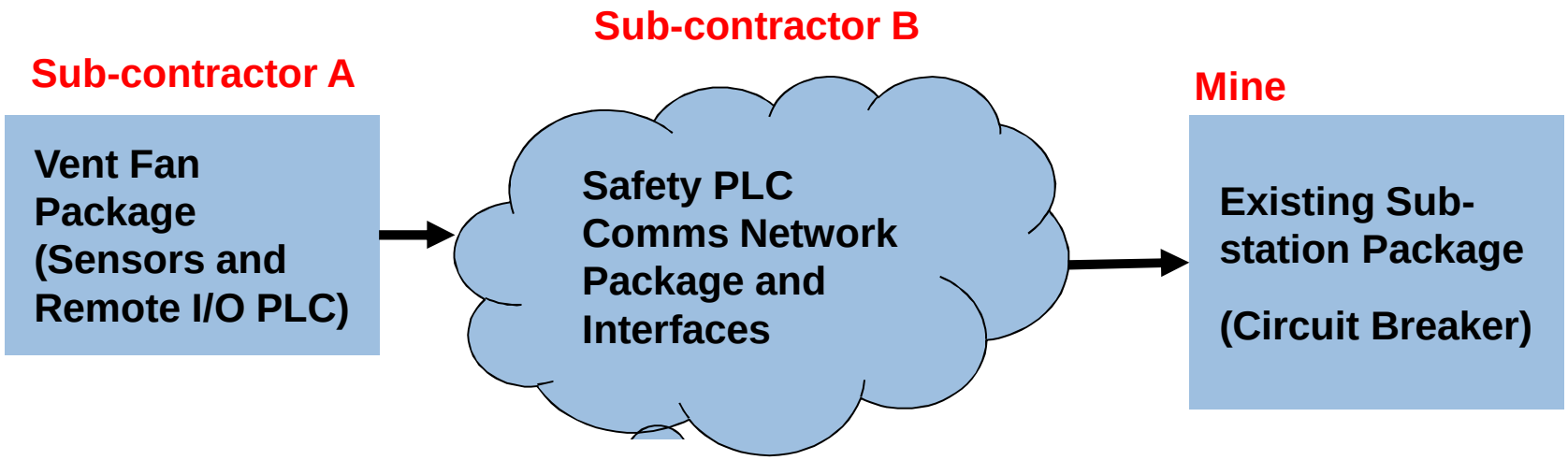
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

The Case of the Vent Fan Inter-trip

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

Someone needs to have overall control of system specification, verification and integration.

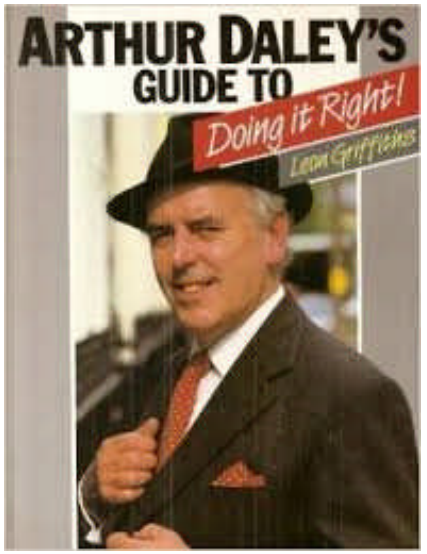
- Subcontractor A (less experienced) delivered SIL2 sensors and a SIL1 network interface.
- Sub-contractor B (experienced) delivered a SIL3 capable comms network, network and sub-station trip relay interfaces.
- The mine (inexperienced) used a legacy sub-station with a single shunt trip.



An Exception to the Rule…?

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

- Safety lifecycle problematic for high volume / commercial off-the-shelf (COTS) equipment. eg. mine haul truck.



- **User focussed compliance approach**
  - Requirements based on user's actual use and environment.
  - Risk-based approach – subjective.
  - OEM receives many user-based safety requirements specifications.
  - Does any customer or corporation have sufficient market power?
  - OEM can't / won't meet requirements → after-market mods?
- No easy answer but an **OEM-focussed compliance approach** for high volume / COTS would help. eg. car industry ADR's & ANCAP, EU Machinery Directive.

The Case of the OEM's Intended Use

- An OEM should analyse, specify safety requirements and design on the basis of reasonably foreseeable use and misuse.
- This should include functional safety requirements.
- Use AS62061 or ISO13849 (< 200 pages)

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

The Case of User's Actual Use

- The OEM's analysis, specification and design provides a baseline for further consideration by end-users.
- Confirm it meets the actual / intended user requirements.

- If not, modify the safety requirements.

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

When SIL2 will just not do!

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

Remote Isolation – The SIL2 Safety Catch….

NSW Mines Work Health and Safety Regulation 2014 (Public Consultation Draft), Clause 33:

(1)(m)…. that any electrical safeguards provided to control the risk from both electrical and non-electrical hazards have a safety integrity ***sufficient*** *for the level of risk being controlled,*

- People in the line of fire if remote isolation fails.

- Remote Isolation Systems need proper consideration – tasks, exposure of workers, other safeguards, ability to escape etc….

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

What is SIL2? Is it sufficient?

- Probability of Dangerous Failure Per Hour (PFH) < 0.000001.
- MTBF (dangerous) = 1 / PFH = 1,000,000 hrs = 114.2 yrs.
- If the life of mine (LoM) is 20 yrs, the likelihood of a dangerous failure at some time is up to **16%**
- A SIL2 Remote Isolation System **may** fail at some time during the life of a mine.
- What happens next? – Who is exposed? What other controls are in place – alarms, back-up trips etc…? Time to escape?
- Worst case: 16% LoM risk of death → tolerable, sufficient?

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

What SIL is “sufficient”?

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

- SIL1 up to 83% likelihood of dangerous failure in 20 yr LoM.
- SIL2 up to 16% likelihood of dangerous failure in 20 yr LoM.
- SIL3 up to 1.7% likelihood of dangerous failure in 20 yr LoM.
- SIL4 up to 0.2% likelihood of dangerous failure in 20yr LoM.

- **Is SIL3 sufficient, SIL4…?**
- **….Should we be using remote isolation?**
- **….How does this compare to the reliability of a human-based, manual isolation?**

But what SIL is a Person?

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

- Assume ~3 isolations per day.
- ie. ~1000 per yr or ~20,000 during 20yr LoM.
- How reliably is manual isolation performed?

- **What error rate is realistic for a human?**
- 1-in-10 → 2000 errors in 20yr LoM
- 1-in-100 → 200 errors in 20yr LoM
- 1-in-1,000 → 20 errors in 20yr LoM
- 1-in-10,000 → 2 errors in 20yr LoM
- 1-in-100,000 → 0.2 errors in 20yr LoM

But what SIL is a Person?

- Assume ~3 isolations per day, or ~1000 per yr.

- SIL1 → < 1-in-11,400, per isolation → <2 errors in LoM.
- SIL2 → < 1-in-114,000, per isolation → <0.2 errors in LoM
- SIL3 → <1-in-1,140,000, per isolation.
- SIL4 → <1-in-11,400,000, per isolation.

- **Even SIL1 is probably better than a human !**
- **….Does this mean that humans should not be doing manual isolations where a SIL-rated remote isolation system is known, available and suitable?**

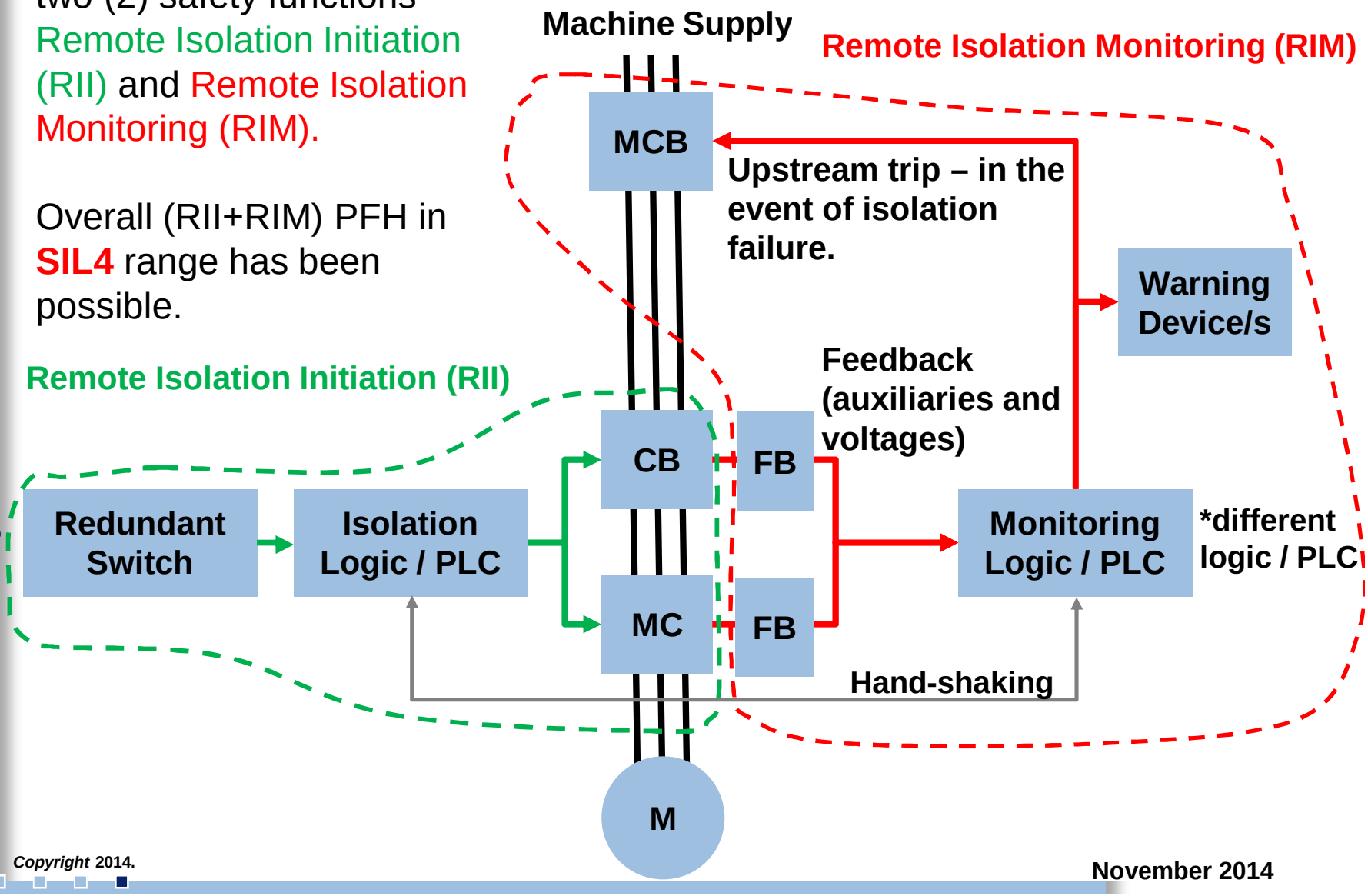
Marcus Punch Pty. Ltd.
Risk and Reliability
www.marcuspunch.com
0432168849

A 'Reasonably Practicable' Solution…..

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

Segregate the system into two (2) safety functions - Remote Isolation Initiation (RII) and Remote Isolation Monitoring (RIM).

Overall (RII+RIM) PFH in **SIL4** range has been possible.



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

The Root of All Confusion

The Rules Get Made By Those Who Turn Up!

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

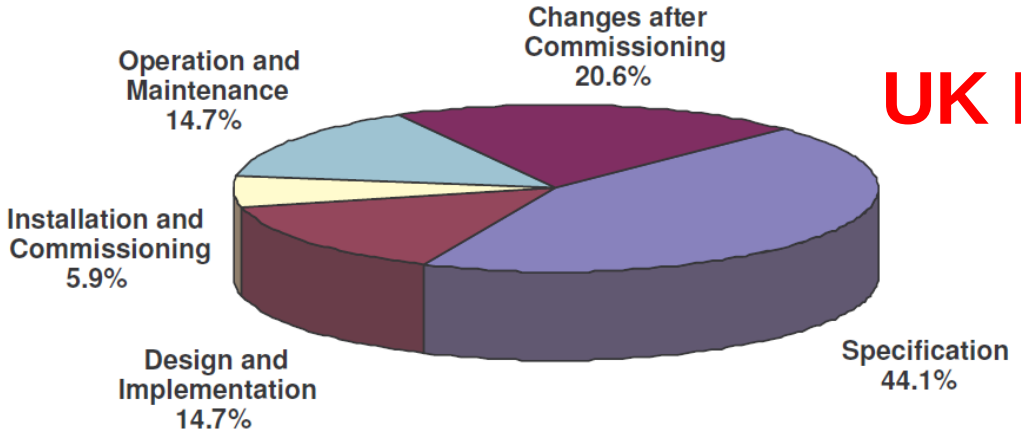
- AS61508 has 8 parts and ~600 pages !
- AS62061 has 1 part and ~100 pages !
- AS61511 has 3 parts and ~200 pages !
- ISO13849 has 2 parts and ~200 pages !
- AS4024.1 now has 27+ parts and ~900+ pages !
- **These numbers are increasing…..**

- Only AS61508 covers all lifecycle phases.
- Only ISO13849 covers all technologies.
- Numerous schemes for describing and determining safety integrity.
- Conflicting terms and definitions.
- Differing methods for designing, verification, documentation etc…

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

The Elephant in the Training Room

Nertney...Competent People...Safe Practices!



UK H&SE Study

- 58.8% incidents caused during engineer-dependent phases.
- 41.2% incidents caused during technician-dependent phases.
- Training and certification for FS Engineers, but not for technicians?
- Coming in 2015…Marcus Punch Pty. Ltd. in co-operation with TÜV Rheinland…FS Technician certification for the mining industry!

http://**www.tuvasi.com**/en/trainings-and-workshops/tuev-rheinland-functional-safety-program/tuev-rheinland-fs-technician/trainings/181-marcus-punch

ID: 999/99
FS Technician
TÜV Rheinland

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