ACARP Roadway Development Operator's Workshop

Roadway Automation – What are the Functional Safety Requirements?

Presented by

Marcus Punch
TÜV FSExpert (Machinery), ID:154/10

Marcus Punch Pty. Ltd
Risk and Reliability

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

Objectives

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

The objectives of this presentation are:

- To give an appreciation of the regulatory environment and the obligations on mines and manufacturers / designers / suppliers regarding functional safety.
- To provide guidance on how the functional safety approach may be undertaken when mine automation technologies are introduced.
- To explain why **mine automation is not a 'silver bullet'.** Whilst it removes or significantly decreases certain risks, it also introduces a range of entirely new risks that need to be systematically addressed.
- To share some lessons learned from underground mine automation projects in the metaliferous sector.

MINE: Requisite Standard of Care

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

NSW Coal Mine Health and Safety Regulation 2006, Clause 13:

Clause 13(1)(e)(v)…. to provide electrical safeguards for electrical and non-electrical hazards, with a probability of failure appropriate to the degree of risk posed by the hazard.

Clause 13(1)(f) (viii)…. to provide safeguards for mechanical plant and installations, with a probability of failure appropriate to the degree of risk posed by the hazard.

NSW DPI Legislation Update LU07-05 (CMH&SR2006)
Mandates the use of AS61508, AS62061 and/or AS4024 to fulfil these requirements.

SUPPLIERS: Requisite Standard of Care

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

NSW OH&S Act, Part II, Division 1, Clause 11:

- A person who designs, manufactures or supplies any plant or substance for use by people at work must

  (a) ensure that the plant or substance is safe and without risks to health when properly used, and

  (b) provide, or arrange for the provision of, adequate information about the plant or substance to the persons to whom it is supplied to ensure its safe use.

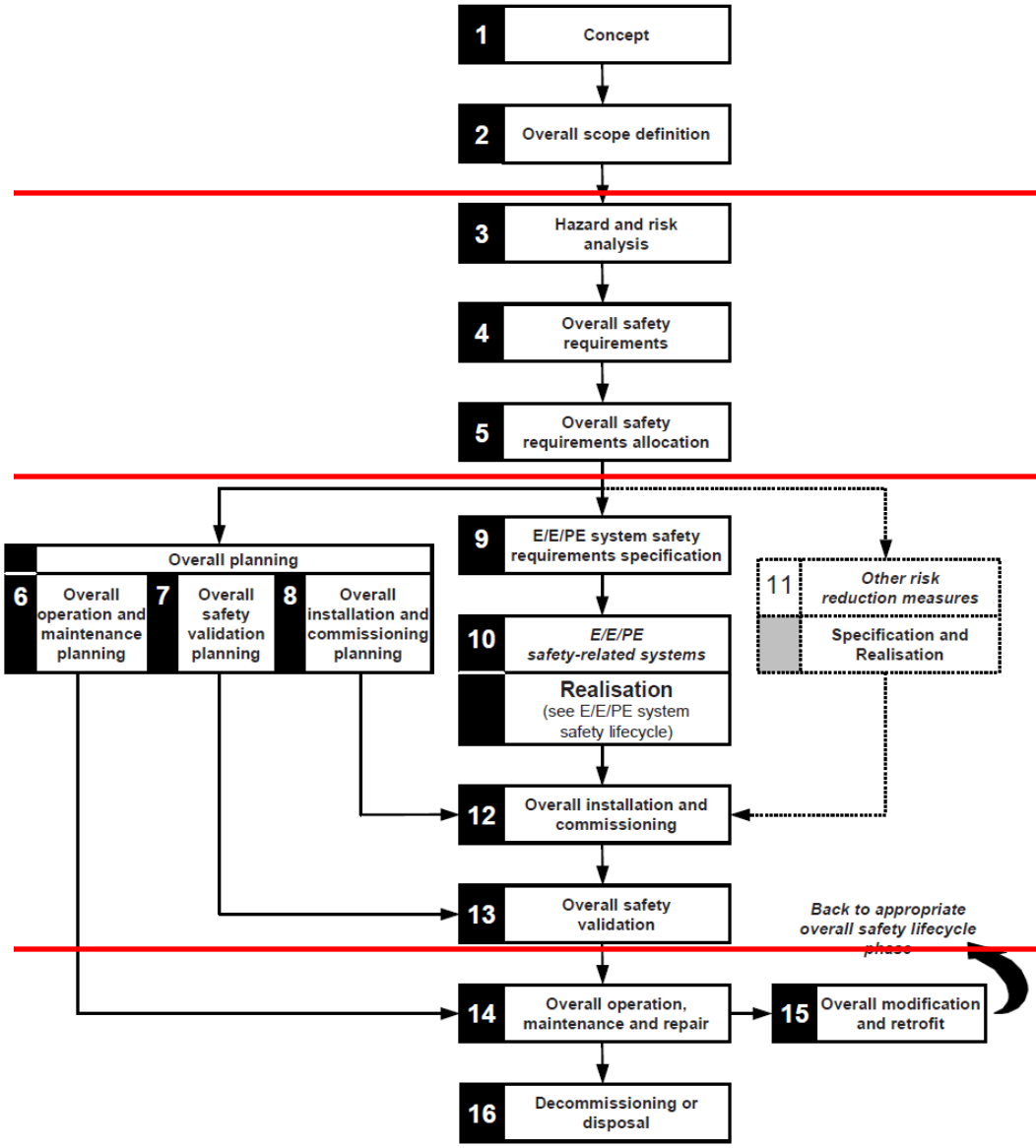
NSW OH&S Regulation, Chapter 5, Part 5.2, Division 2, Clause 99:

Importers of plant manufactured outside the State to ensure that manufacturer's responsibilities are met.

NOH&SC Safe Design Project 2001, page 17-18:

Standards, guidelines and codes of practice may be used as evidence of what a reasonable duty holder would do to comply with the legal obligation for which the document provides guidance.

AS61508:2011 - a Full Life-cycle Process !



Concept & Scope
MINE (1-2)

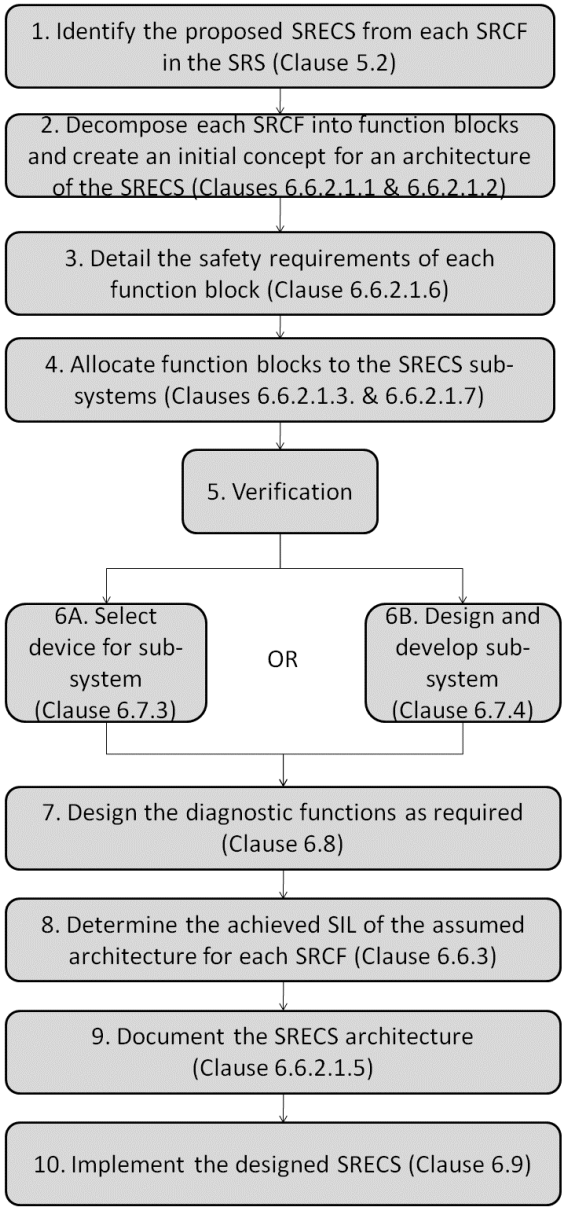
Analysis
MINE (3-5)

Realisation
SUPPLIER/S (10-12)
MINE (6-8, 9, 13)

Operation
MINE (14-16)

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

AS62061:2006: a Realisation Process

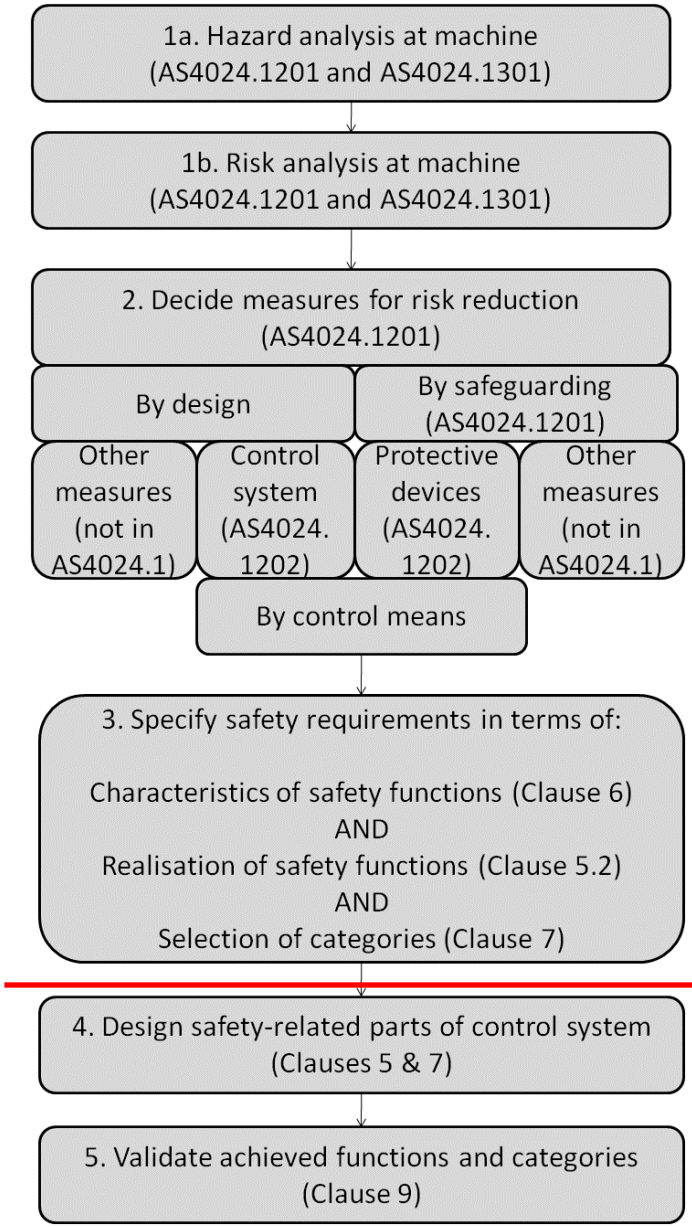


Realisation

SUPPLIER (1-10)

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

AS4024.1:2006: an Analysis & Realisation Process



Analysis

MINE (1-3)

Realisation

SUPPLIER/S (4-5)

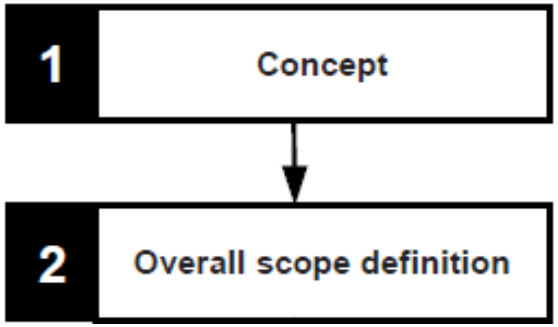
Marcus Punch Pty. Ltd.
Risk and Reliability
0432168849
www.marcuspunch.com

MINE: Concept and Scope Stage

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

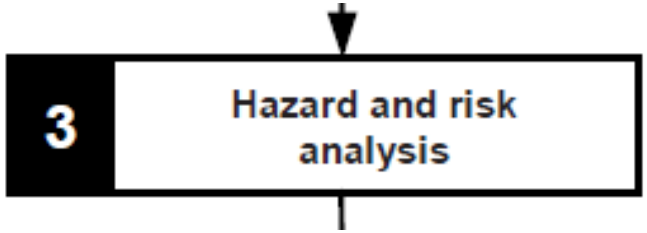
Develop a Functional Safety Management Plan (see AS62061 Clause 4)

1. Overall policy and strategy.
2. Safety lifecycle activities to be conducted.
3. Persons and organizations responsible.
4. Procedures for recording and maintaining information.
5. Overall strategy for software.
6. Strategy for engineering change management.
7. Establish the need for a verification plan.
8. Establish the need for a validation plan.



MINE: Hazard and Risk Analysis

- Systematically analyse the proposed operation, including all modes, sequences, mode changes, interfaces, prevailing conditions and human errors and consider all potentially dangerous scenarios and interactions.
- Use a 'well-tried' analysis technique such as HAZOP and assess the consequences and likelihood of each hazard.
- Use your standard risk assessment procedures but also refer to AS61508.1, MDG1010 / MDG1014, AS4024.1301 or ISO14121.
- Use the hierarchy of risk controls to determine the most effective and appropriate risk controls.
- Remember - hazard elimination / substitution trumps an engineered electronic protection system.



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

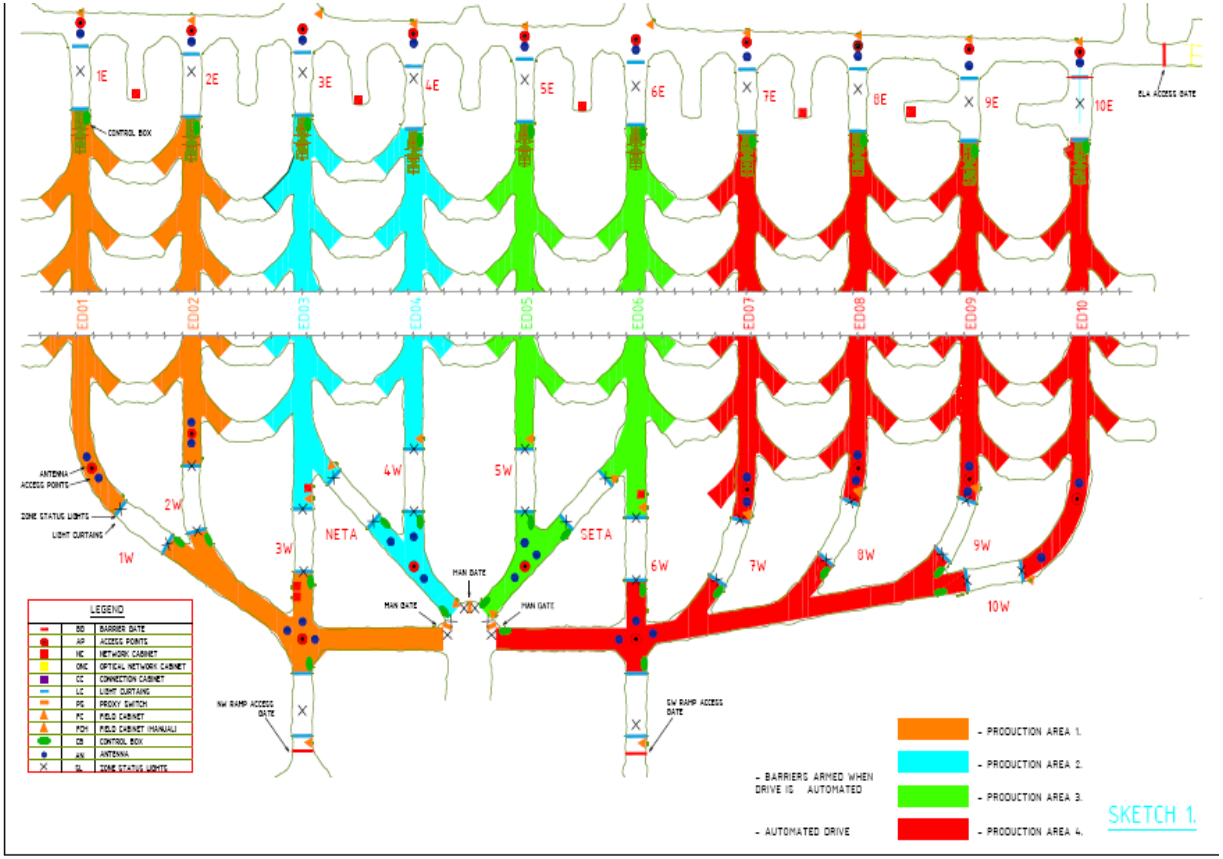
MINE: Hazard and Risk Analysis

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

A sample of hazards that were considered in U/G metaliferous projects.

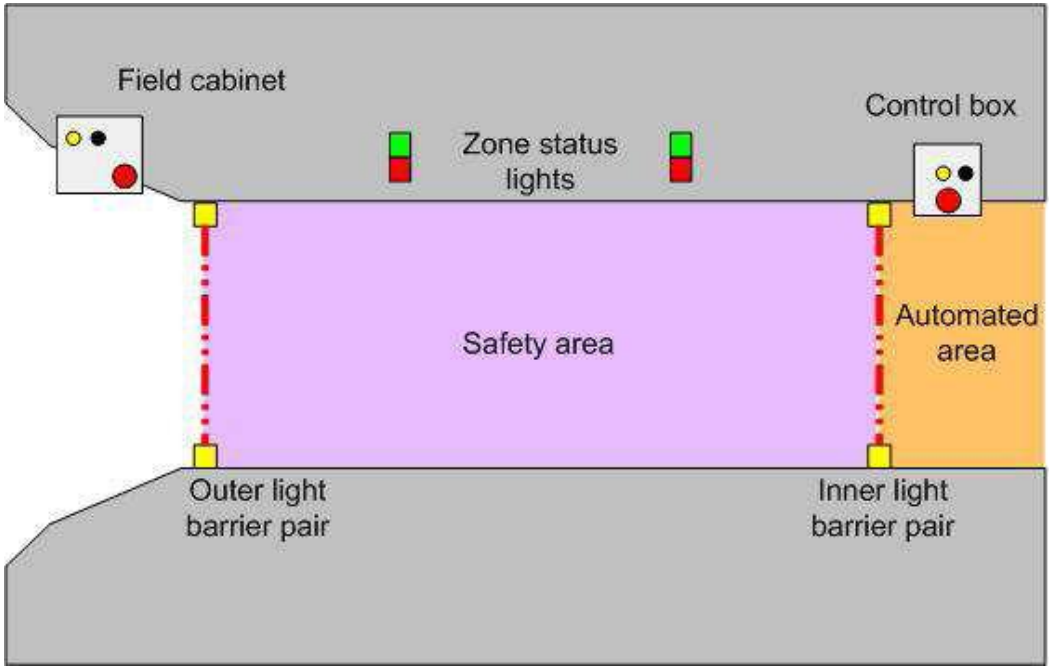
These could also apply to automation in underground coal mines.

- Person left in autonomous zone during initialisation.



MINE: Hazard and Risk Analysis

- Person enters autonomous zone (advertantly or inadvertantly).
- Mine incident (eg. fire) causing person to attempt escape through autonomous zone.

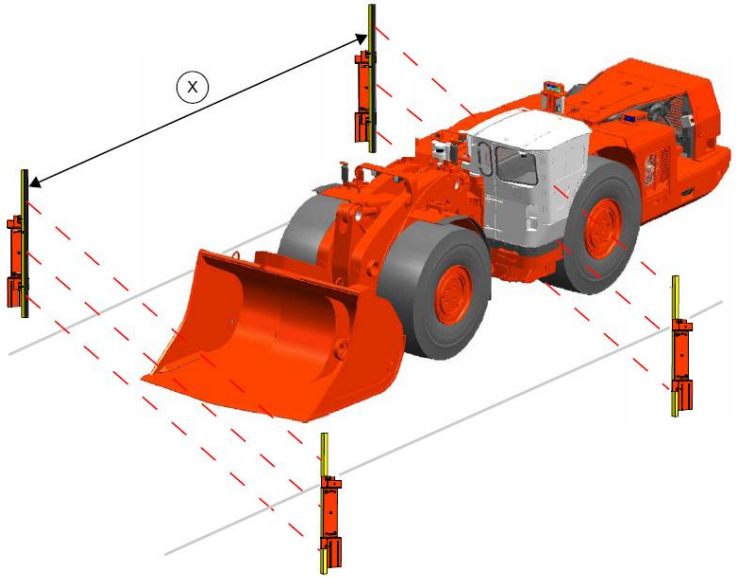


- Autonomous machine malfunctions and tries to leave autonomous zone.

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

MINE: Hazard and Risk Analysis

- Roadway / brakes / tyre condition - leads to increased braking distances (this affects ability to stop machines within automated zone).



- Production control system malfunction - collisions between autonomous machines.
- Unplanned movement during change-over from autonomous mode to manual mode.

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

MINE: Hazard and Risk Analysis

- Surface operator incapacitation / absence.
- Fatigue / boredom / human error.

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

MINE: Hazard and Risk Analysis

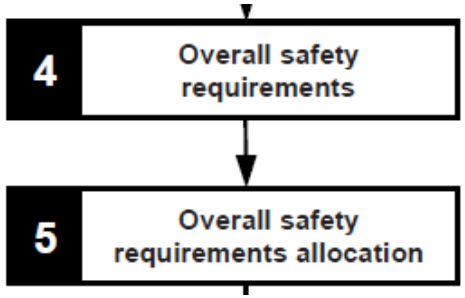
- Un-authorised or poorly controlled modifications .
- Loss of wireless communication with machines.
- Excessive safety system response time.
- Electromagnetic interference.
- Remote access / hacking.

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

MINE: Safety Requirements Allocation

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

- If possible attempt one of the 'quantitative' or semi-quantitative methods of SIL allocation, per AS61508-5. These methods include: Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and Layer of Protection Analysis (LOPA).
- **<u>Absolutely avoid</u> the temptation to skip this step and just specify everything as SIL2 etc.... SIL allocation is an opportunity for us to think more deeply about hazards and the sequence of events that leads to harm.**
- And always keep the following in mind:
  - What is my 'tolerable risk target'. Is it reasonable? How will I justify it?
  - Can I reasonably achieve a lower target for certain hazards?
  - The hierarchy of risk controls - is hazard elimination / substitution still possible?
  - Will risk be ALARP with safeguards in place?

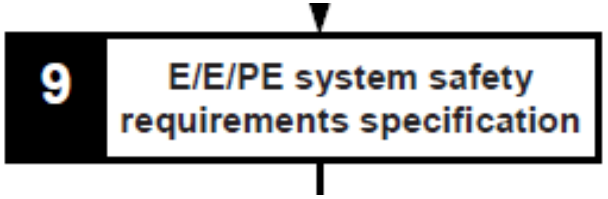


MINE: Safety Requirements Specification

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

- The Safety Requirements Specification (SRS) is the key interface between 'analysis' and 'realisation' stages.
- The specification should fundamentally address the following:

1. Functional requirements and safety integrity (ie. SIL) requirements for the electrical / electronic safety-related systems,
2. Functional requirements and safety integrity (ie. CAT) requirements for the 'other technology' (ie. mechanical, hydraulic, pneumatic, etc...) safety-related systems,
3. Information on the other risk reduction facilities to be used (eg. guards, exclusion zones, procedures, etc...)
4. See AS62061 Clause 5 for a checklist of what should be included in the specification.



MINE: Safety Requirements Specification

- Any argument or dispute arising from a supplier's assertion or opinion may that they do not need to comply with AS61508 / AS4024 / AS62061 can be avoided, if the contract requires compliance and the payment schedule is linked to successful delivery.

- The Safety Requirements Specification (SRS) should therefore be clear and unambiguous, referencing the key requirements of the standards and be a core part of the Statement of Work (SOW) and the contract of supply.

- Simply stating: "...the supplier shall comply with AS61508", or words to that effect, is not enough.

Ask the suppliers if they agree in principle that they are obliged to comply with the functional safety / machinery safety standards!

Ask them if they already have (or are in the process of) implementing a design approach based on one of the relevant standards!

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

MINE: Define the Safety Functions

SRCF Description
Light Curtain Stop
Surface Operator's Main Fast Stop
Communication Time-out Stop
Zone E-Stop
LHD Operator's Cabin Emergency Stop
Gate End Panel E-Stop

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

MINE: Define "Safe State"

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

With regard to the implementation of the safety system, a particular machine will be deemed to have achieved a "safe state" when the following are achieved:

1. Successful disconnection of the electrical power to the traction motors, and
2. Successful application of sufficient braking effort on all wheels such that the machine is brought to a halt within the affected autonomous zone and within fifteen (15) metres.

MINE: Define the Scope of the Safety Function

The functional and physical scope of each safety function, for the purposes of design, verification and validation will be taken to include all E/E/PE and “other technology” sub-systems and parts that will be instrumental to the achievement of the functional requirements.

The scope of each safety function shall include all sensors, logic , valves , data communication, wiring, piping and actuation elements, including the final elements (ie contactors, valves, hydraulic brakes etc) involved in the isolation of electrical or mechanical power.

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

MINE: Define the Need for Segregation

Where possible there should be physical and functional separation of safety-related systems and non-safety-related systems.

Any interfaces (hardware or software) between a safety-related system and a non-safety-related system shall be specified and designed according to AS61508.7 Clause B.1.3.

Interface testing, per AS61508.7 Clause C.5.3, shall be performed to confirm the achievement of the specified requirements during the validation of the safety-related systems.

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

MINE: Define the Functional Requirements

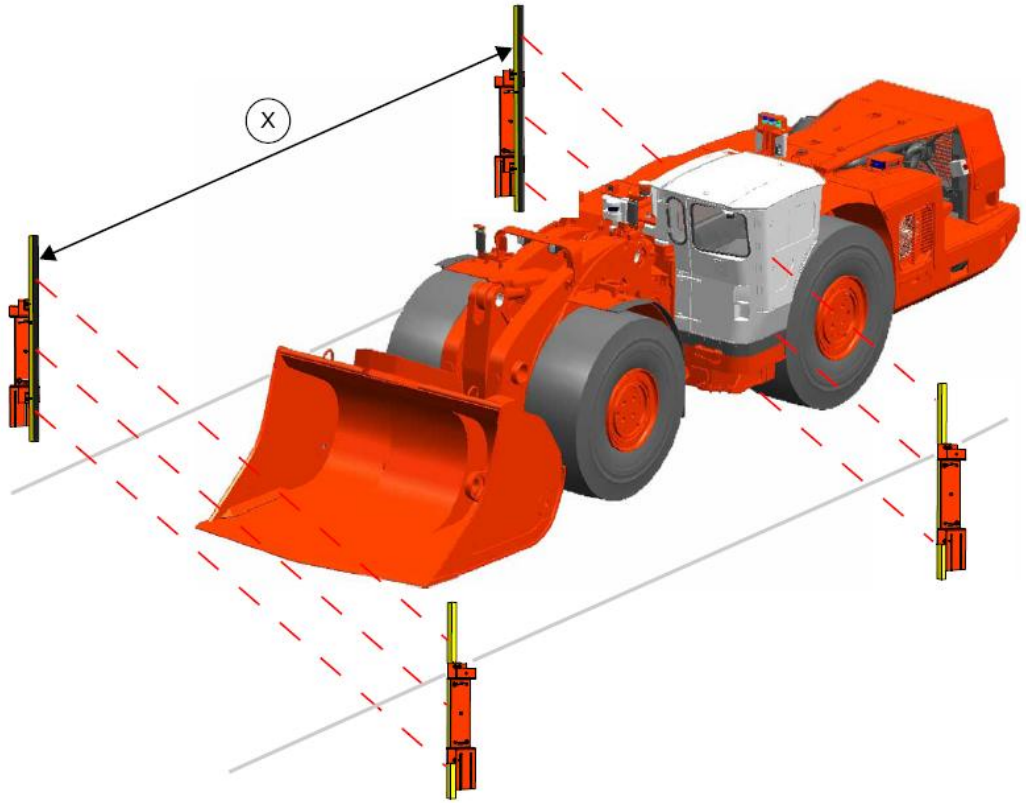
When a light curtain barrier is breached by a person or machine, a fast stop of the affected machine/s shall occur, via tripping of the traction motor power and application of braking on all wheels of the affected machine/s. The machine/s shall be brought to a halt within the autonomous zone and within fifteen (15) metres.

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

MINE: Define the Response Requirements

The response delay from sensing to actuation shall be less than 1000 milliseconds.

The machine/s shall be brought to a halt within the autonomous zone and within 15 metres.



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

MINE: Define the Safety Integrity Requirement

This safety function is to achieve a level of reliability in the range of SIL2 in low demand mode.

The Probability of Failure on Demand (PFD) of this safety function is not to exceed 0.01, but may exceed 0.001, according to AS61508.2.

Any non-electrical / electronic parts and configurations (eg. pneumatic, hydraulic, mechanical etc…) intended to be used to perform this safety function are to achieve the requirements of AS4024.1 for CAT 3.

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

MINE: A Significant Learning !

Consider specifying a target level of reliability (eg. failure rate or MTBF) or compliance to dependability standards for the machine guidance / control system and its software.

eg. IEC62628 Guidance on Aspects of Software Dependability

The more often the machine guidance / control system malfunctions, the greater the potential there is for attempted escape from the autonomous zone, and therefore demands on the safety systems.

And, since the safety systems also have finite probabilities of failure – the greater the potential for a machine to escape an autonomous zone and harm people.

Control system reliability also contributes to safety.

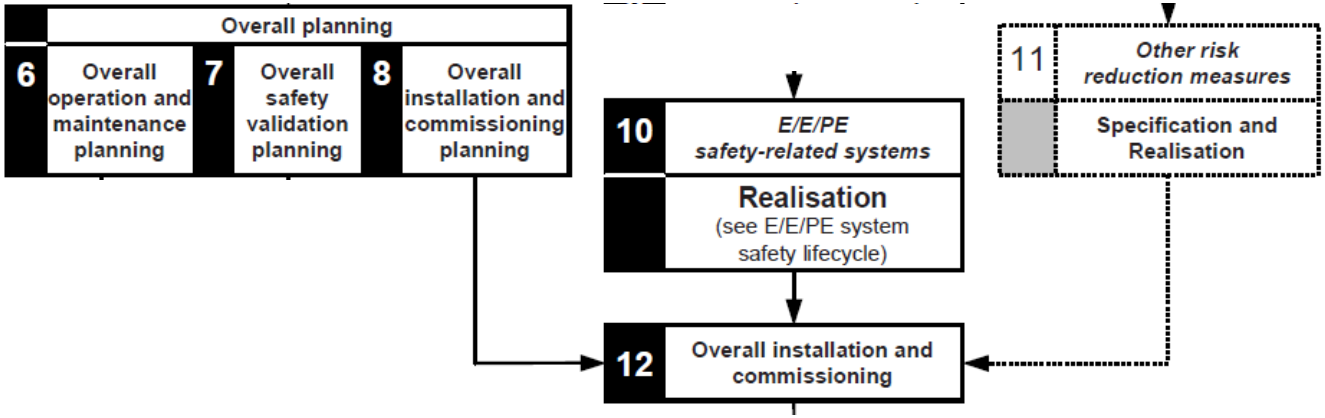
Marcus Punch Pty. Ltd.
Risk and Reliability
0432168849
www.marcuspunch.com

SUPPLIERS: The AS61508/AS62061 Approach

Under AS61508 and AS62061 the following fundamental aspects must be verified in order to substantiate a SIL claim for each safety function.

1. **Probability of Failure** (ie. a mathematical calculation)
2. **Architecture** (ie. fault tolerance, safe failure and complexity).
3. **Systematic Failure Avoidance and Control** (ie. design and development techniques and activities)

Ask the suppliers what SIL capability they claim for their product /s and how they can prove it to you!



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

SUPPLIERS: New Approaches

- AS61508:1999/2000 was superceded by AS61508:2011 in April 2011. This new standard is based on IEC61508:2010.
- Under AS61508:2011 there is now an alternative 'proven-in-use' approach for the verification of safety devices / systems with previous field use.
- Also keep an eye on draft AS standards and new international standards (eg. IEC, ISO) - a legal precedent exists concerning the status of international and draft Australian standards: see Engineers Australia March 2009 issue, pages 38-39.

eg. ISO13849 Machinery Safety - Safety-related Parts of Control Systems

ISO15998 Functional Safety of Earth-moving Equipment

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

MINE/SUPPLIER: The Relationship

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

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, such as:

1. Safety-related system architecture and detailed design,
2. PFD / PFH and SIL Claim Limit calculations, design FMEA and supporting data,
3. Evidence of compliance to systematic failure avoidance and control (for SIL) or equivalent (for CAT).
4. Documentation of Safety Lifecycle activities undertaken.
5. "Information for use" per AS62061 Clause 7.

All of this is consistent with the designer / manufacturer / supplier obligations under NSW OH&S Act, Part II, Division 1, Clause 11.

Ask the suppliers if they have this information available now!

MINE/SUPPLIER: The Relationship

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

AS61508-2:2011 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**".

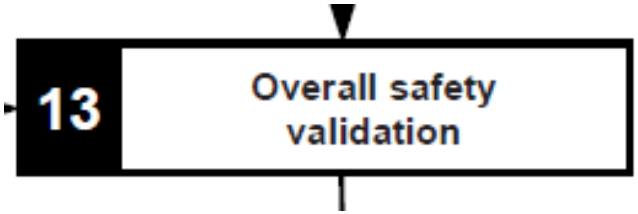
Ask the suppliers if they will provide access to all evidence of compliance!

MINE: Validation and Acceptance

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

A safety validation (Phase 13) should be conducted during / after commissioning to ensure that the requirements of the Safety Requirements Specification are met. (See AS62061 Clause 8):

1. Functional and proof-testing of the safety-related systems under the expected environmental conditions.
2. Fault-insertion testing – what happens if…?
3. Interference immunity testing.
4. Involvement of operational staff – increases their confidence in the protective systems.

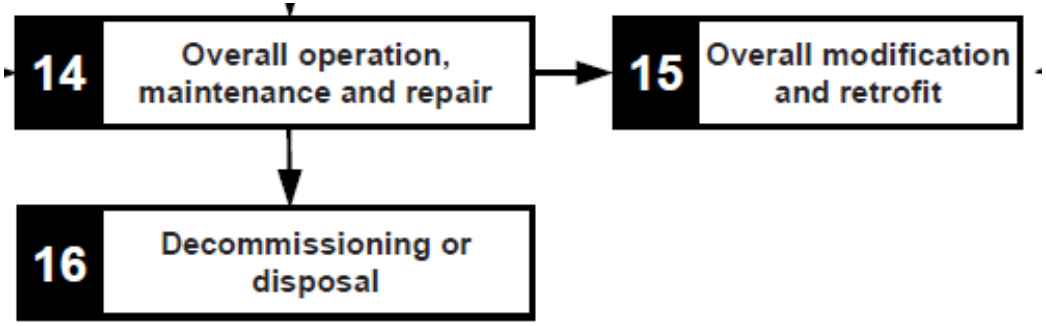


MINE: Operation

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

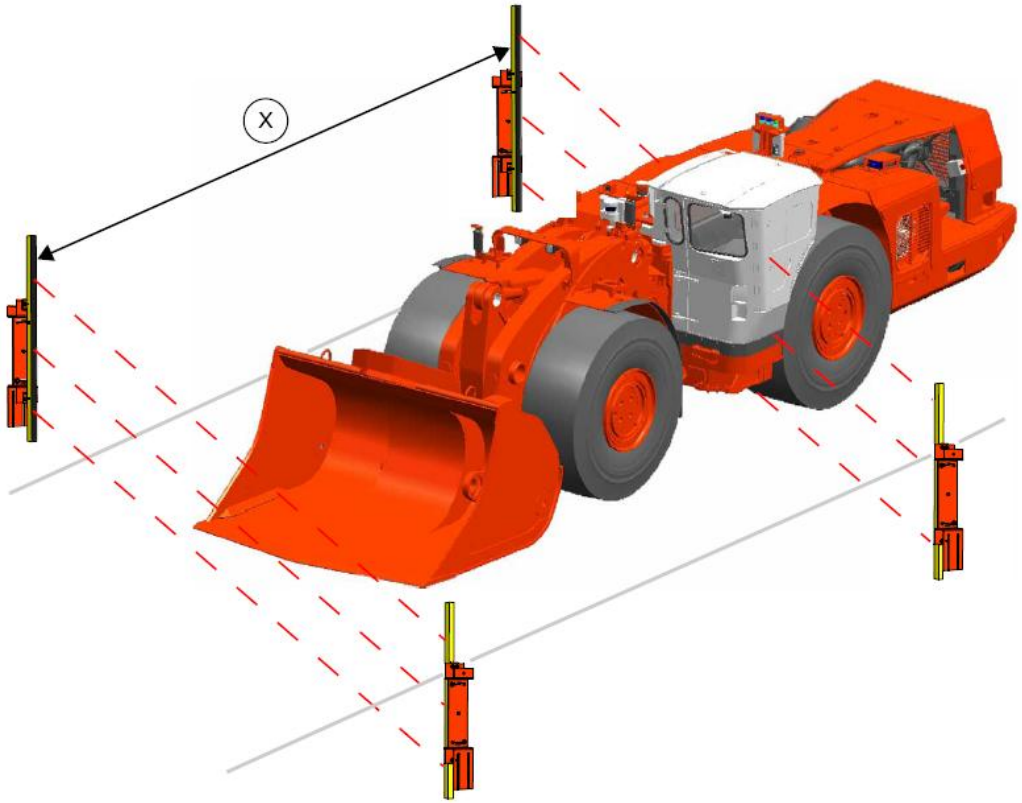
The key issues during operation and maintenance:

1. Operator / maintainer awareness, understanding and competence.
2. Compliance to maintenance requirements.
3. Control of engineering changes.



Thankyou for listening.....

safeguards .... with a probability of failure appropriate to the degree of risk posed by the hazard.



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