Safety in Mining and Processing Operations
Mr. Chris Leahy,
NHP – Product Manager - Safety
Electrical Engineer supporting NHP safety products
across a broad range of industries

Mr. Peter Kroon,
Principle Engineer - Sage Automation
TUV Certified Functional Safety Engineer, with 20 years of experience in the design and construction of various disciplines of engineering
Topics
- Operation of the Mining Safety and Health Acts
- Achieving your obligations
- Applicable industry Standards for “Mining”
- Control and Management of Risk
- Risk reduction strategies
- What are Categories, Performance Levels and Safety Integrity Levels?
• Mining industry
  – Coal Mining
  – Mining and Quarrying
  – Processing Operations
  – Conveyors

• The "Mining" Safety and Health Act ‘s set out the laws about the health and safety requirements affecting “Mines” in Queensland. You need to be familiar with the Act in order to understand your obligations and safety requirements
• Safety within the Queensland “Mining” industry is regulated by 5 key pieces of legislation
  – Coal Mining Safety and Health Act 1999
  – Coal Mining Safety and Health Regulation 2001
  – Mining and Quarrying Safety and Health Act 1999
  – Mining and Quarrying Safety and Health Regulation 2001
• The Workplace Health and Safety Act 1995
  – Does not apply to Coal Mining or Mining and Quarrying Safety
  – However, obligation is imposed under Part 3 of WHS ACT on
    • Clients
    • Project Managers
    • Principle Contractors
    • A mine under a regulation where the M&Q ACT has declared it does not apply
• Who do the ACT’s apply to:
  – A person who, or everyone who may effect the safety or health of persons
    • At a “Mine”
    • As a result of “Mining operations”
      – Holder
      – Operator
      – Contractor
      – etc
How are the objectives achieved?

- Objectives of the ACT’s
  - To protect the safety and health of persons
  - To require the risk of injury or illness be at an acceptable level
  - To provide a way of monitoring the effectiveness

- The objectives of this ACT are to be achieved by
  - Making regulations and recognised standards for the “mining” industry to require and promote risk management and control
What is the difference between a “Coal Mine” and “Mining and Quarrying”?

<table>
<thead>
<tr>
<th>Coal Mining</th>
<th>Mining and Quarrying</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploring for, wining and treating coal, including disposal of waste</td>
<td>Mining - Exploring for, wining, or wining and treating, minerals or hard rock</td>
</tr>
<tr>
<td>Quarry – a place on land where hard rock is excavated</td>
<td>On site activities</td>
</tr>
<tr>
<td>standard work instruction</td>
<td>Operations</td>
</tr>
<tr>
<td>Principle Hazard – multiple fatalities</td>
<td>Not specified</td>
</tr>
<tr>
<td>Standards</td>
<td>Guidelines</td>
</tr>
</tbody>
</table>
• What is an acceptable level of risk from operations?
  – Within acceptable limits
  – As low as reasonably achievable

• Regard must be given to
  – The likelihood of injury or illness
  – The severity of the injury or illness
How can I discharge my obligation and create a “Defence”?

- If a regulation prescribes a way of achieving an acceptable level risk
- If a regulation prohibits exposure to a risk
- If a recognised Standard/Guideline states a way of achieving an acceptable level of risk
- The obligation is discharged providing the above points are adopted and followed in the stated way
What’s after the ACT?

• **What you must do?**
  
  – Fulfill your obligations under the “Mining” Safety and Health Act’s.
  
  – If a *regulation* exists for specific risks, you **must** do what the *Regulation* says to prevent or minimise the impact of the risk.
  
  – If there is a *Code of Practice* – for specific risks you **must** either:
    
    • do what the Code says; or
    
    • adopt and follow another way that gives the same level of protection against the risk; **and** ensure you take reasonable precautions and exercise proper diligence.
• What are Regulations?

– Regulations will either prohibit exposure to a risk or prescribe ways to prevent or minimise exposure to a risk.

“The emergency stopping systems and safety alarms at the mine remain effective if there is a fault or failure in a system”

– Mining and Quarrying Safety and Health Regulation 2001 Chap 2 Part 4 – 24 Automatic Control
What if a Specific Regulation does not exist?

- “Mining” Safety and Health Regulation 2001
  - Risk Management Process
  - Electrical
  - Emergencies
  - Dredging
  - Hazardous substances and dangerous goods
  - Explosives and blasting
  - Fitness
  - Winding operations
  - Ventilation
• What are Codes of Practice?
  • Industry codes of practice provide practical guidance and advice on how to achieve the standard required by the Act and regulation.

  “A guard is a device to provide a physical or other barrier which prevents or controls access to dangerous areas of plant.

Guards should:
(a) Be designed to eliminate or reduce risk
(b) Be designed to prevent by-passing or disabling
• Codes of Practice for Queensland
  – Risk Management Code of Practice 2007
    • Clearly defines the Risk Management Process that obligation holders under the ACT are accountable to
  – Plant Code of Practice 2005
    • Machinery, equipment, implement and tool
    • Personal protective equipment
    • A component of plant and a fitting, connection, accessory or adjunct to plant.

• What are Guidelines?
  – Guidelines raise awareness of a range of hazards associated with, in this case, common machinery and plant. Practical advice is provided in relation to methods that can be used to safeguard machinery and plant

• Similar to Codes of Practice and note that they should be read in conjunction with.
• Guidelines for Queensland
  – Guide to Safeguarding Common Machinery and Plant
    • Workplace Health and Safety Queensland
What is the simple connection between the ACT’s, the Regs, the COP and the Guidelines?

– The Act discharges the persons obligations providing they follow a recognised Regulation, COP or Guideline

– The Act calls for effective Risk Management Processes

  • Risk Management Code of Practice 2007
  • Guide to Safeguarding Common Machinery and Plant
– Under the M&Q Safety and Health Regulation 2001

• Chapter 2 Part 2 Div 8/2 (c)

• The site senior executive must ensure hazard controls used to reduce risk in the mine’s work and local environments are appropriate having regard to the following -

  – (c) other reasonably available relevant information and data from, and practices in, other industries and mining operations
Risk Management Processes

• What are Risk Management Processes?
  – A process divided into 5 steps
    • Identify Hazards
    • Assess risks that may result because of the hazard
    • Decide on appropriate control measures to minimise risk
    • Implement the chosen control measures
    • Monitor and review the effectiveness of the chosen controls

We will review this further in the AS4024
• Where do the Standards fit?
  – Within the Codes of Practice and the Guidelines reference is made directly to:
    • AS 4024 – Safety of Machinery
    • AS1755 – Conveyors
    • AS61508 – Functional Safety – Safety Related Systems
  – The Standards provide technical guidance in achieving the your obligations
• When can I use a Standard
  – In General
    • When it is recognised
    • States ways to achieve an acceptable level of risk to persons arising out of “Mining” operations
  – In Proceedings
    • When there is a contravention of an obligation
    • The Standard is about achieving an acceptable level of risk
Value of Standards

How do standards add value??

• Developed by industry for industry
• Supplement our experience
• Provide benchmark, aid in defence or used as evidence
• Challenge our views
• Challenge long standing practices
Summary

• Standards assist in creating a defensible argument
• LOTO – an approved and documented solution to creating a safe situation
• Hierarchy
• Administrative control
• AS4024 increases machine availability
Industry Standards
• AS 60204.1 Safety of Machinery – Electrical equipment of machines
  – Sets out electrical requirements
    • Isolation
    • Protection against electric shock
    • Protection of equipment
    • Earthing
    • Push-buttons
    • Conductor colors within the machine
• Stop functions
  – There are three categories of stop functions
    • Stop Cat 0: stopping by immediate removal of power to the machine actuators
    • Stop Cat 1: a controlled stop and then removal of power
    • Stop Cat 2: a controlled stop with power left available to the machine actuators
• Is referenced for electrical requirements within the AS 4024.1 series
• Suspension of safety function
  – During machine setting or maintenance protection shall be ensured by:
    • Initiation of operation by a hold to run device
    • A portable control station with an Estop device
    • Limitation of the speed
    • Limitation of the range of motion
• Safety functions and/or protective measures (e.g., interlocks) shall be provided for safe operation
  – Start operation
  – Stop function
  – Emergency stop
    • Types, color and locations
  – Control functions
    • Hold to run
    • Two hand control
    • Interlocks
Machine Safety
&
Australian Standards
AS4024

Presenter
Peter Kroon
Principal Engineer, Sage Automation
• Presentation Objectives

- Present overview of Australian standard AS4024
- Discuss its relevance to the mining industry
- Outline its content
- Present some of its key concepts
• Structure of AS 4024 series

- It comprises of 3 parts:
  - Part 1: 1000 series General Principles
  - Part 2: 2000 series Optional standards
    - Eg. 2 hand control, safety distances and safe positioning, etc
    - Eg industrial robots, power presses, milling machines, etc
AS4024.1-2006

- Includes the 1000 series
- 26 parts
- All based on European (EN) or international standards (ISO)
- Modified where required to suit Australia’s stringent safety practices
Structure AS4024.1-2006

- 1100 Series Terminology
- 1200 Series General principals
- 1300 Series Risk assessment
- 1400 Series Ergonomic principals
- 1500 Series Design of safety related parts of control sys.
- 1600 Series Design of controls, interlocks and guarding
- 1700 Series Human body measurements
- 1800 Series Safety distances and safety gaps
- 1900 Series Display controls, actuators and signals Indication, marking and actuation
AS4024.1201 Risk Reduction Process

AS4024.1201 Risk reduction process from the point of view of the designer
Hazard analysis & Risk Assessment at machine

Decide measures for risk reduction
- By design
- By safeguarding
  - Other measures
  - Control system
  - Protective devices
  - Other measures

Specify safety requirements in terms of
- Characteristics of safety functions
- Realisation of safety functions
- Selection of categories

Design SRCS

Validation

Risk Assessment

Risk controls

Specify requirements

Design

Validate
1300 series - Risk Assessment

• Provides guidance on
  – Risk assessment process
  – Risk assessment techniques for machinery
  – Potential hazards
  – Risk definition as it relates to ‘Safety of Machinery’
  – Risk estimation
  – Risk evaluation
Iterative Risk Assessment Process Flowchart

Start

- Determination of limits of the machinery
- Hazard Identification
- Risk Estimation
- Risk Evaluation

- Is the machinery Safe?

- Risk Reduction

Risk Analysis

Risk Assessment

End
• **Limits of machinery**
  - The phases of the machinery life
  - The intended use
    - Inc. correct operation and consequence of foreseeable misuse and malfunction
  - **Foreseeable uses of the machinery**
    - Inc industrial, non industrial, sex, age, dominant hand usage and limiting physical abilities (hearing impairment, size, strength, etc)
  - Anticipated level of training, experience and abilities
  - Consider exposure of other persons
Risk Assessment

- Hazard Identification

Critical step

Hazards not identified are not evaluated and not managed
• Hazard Identification
  - Consideration should be given to
  - Energy sources such as electrical, mechanical gravity, etc, inc. stored energy
  - Emissions, inc noise, radiation, dust
  - Static hazards
    - List of potential hazards – (AS 4024.1301 Appendix B)
    - Methods to use for this process – “What-If” Method, DELPHI technique, etc (AS 4024.1301 Appendix A)
Hazard Identification

Hazard
- Crushing hazard
Elements of risk as presented in AS4024.1301-2006 Figure 2

\[
\text{Risk} = \text{Severity} \& \text{Probability of Occurrence of that harm}
\]

- Risk related to the considered hazard
- Severity is a function of the possible harm for the considered hazard
- Probability of occurrence of hazardous event
- Frequency and duration of exposure
- Possibility to avoid or limit harm
• Risk Evaluation
  - For each hazard the risk needs to be evaluated
  - Provides a definition of achievement of risk reduction
  - Additional controls need to be assessed
Risk Reduction

- Control the Risk
  - Eliminate risk
  - If not possible to eliminate
    - Substitute with lesser hazard
    - Control risk of hazard by engineering
    - Isolation from hazard
  - If above not possible or extra risk reduction required
    - Administrative controls
    - Personal protective equipment
Guarding Hierarchy

- Permanent fixed guard
  - No access to danger area during normal operation, cleaning, maintenance, etc.

- Interlocked guard
  - Where access is required during normal operation

- Fixed guard, only when first two options are not practicable

- Presence sensing systems, only when the first three options are not practicable
  - Safety Mats, light curtains, etc.
Categories

- Relates to safety related control systems
- Independent of energy used e.g. electrical, fluid power, mechanical
- Defines five categories with increasing integrity
  - Tolerance to faults and diagnostic ability
- Specifies the behavior of safety related parts of the system in normal operation and under fault conditions
Category Selection tool

S1 – Slight
S2 – Serious

F1 – Seldom / short
F2 – Frequent / long

P1 – Possible under specific conditions
P2 – Scarcely possible

Possible selection of categories for safety related parts of control systems
Reproduced from AS4024.1501-2006 Figure C1

Starting point for risk estimation for the safety-related part of the control system

Selection of categories B, 1 to 4
● = Preferred categories for reference points
● = Possible categories which may require additional controls
○ = Measures which can be over-dimensioned for the relevant risk
Category B

- Basic safety principles apply
- Withstand expected operating stress
- Influence of processed material
- Other relevant external influences eg vibration

- Essentially just good engineering
• Category B – Fault handling behaviour

- A single fault may result in the loss of the safety function.
- Detection of the fault is not required
Category B - Normal operation
Category B – Guard Switch Fault

Diagram showing a guard switch fault with a switch labeled 'Stop' and a motor labeled 'M'. The diagram includes a control panel with buttons labeled 'Stop' and 'Start'.
Category B – Contactor Fault

Diagram showing a circuit with a guard switch, start and stop buttons, and a motor labeled 'M'.
Category 1

- Requirements of category B
- Well-tried components
  - Guidance provided in 4024.1502
- Well-tried safety principles
  - Avoidance of fault e.g. segregation to avoid short circuit
  - Over dimensioning and underrating
  - Orientation if fault mode
• Category 1 – Fault handling behaviour
  ▪ A single fault may result in the loss of the safety function.
  ▪ Probability of failure lower than Cat B
  ▪ Detection of the fault is not required
Category 1 – Contactor Fault
Category 2

- Requirements of category B
- Safety function checked as suitable interval
  - Manual or automatic initiation
  - Control system to detect fault
- In event of fault generate an output which
  - Initiate a safe state
  - Where not possible, provide a warning of the hazard
  - Orientation if fault mode
• Category 2 – Fault handling behaviour

- A single fault may result in the loss of the safety function between checks.
- Detection of the fault is required
Category 2 – Typical example
Category 2 – Logic Solver

Diagram showing a logic solver connected to a motor with components such as switches (Sw1, Sw2), a warning indicator, and a reset button.
Category 2 – Warning
Category 2 – Normal operation
Category 2 – Guard Switch Fault
Category 2 – Contactor Fault

Diagram showing a contactor fault with connections to a logic solver, warning indicator, motor, and reset function.
Category 3

- Requirements of category B
- Single fault shall **not** lead to a loss of the safety function
- Common mode faults shall be taken into account
- Whenever reasonably practicable faults shall be detected at or before next demand of the safety function
• Category 3 – Fault handling behaviour

- A single fault shall not lead to the loss of the safety function.
- Detection of the fault is required, where reasonably practicable
- Accumulation of faults may lead to a loss of the safety function
Category 3 – Typical example
Category 3 – Logic solver
Category 3 – Normal Operation
Category 3 – Guard Switch Fault
Category 4

- Requirements of category B
- Single fault shall **not** lead to a loss of the safety function
- Faults shall be detected at or before next demand of the safety function
- If not possible and accumulation of faults shall not lead to a loss of the safety function
- Common mode faults shall be taken into account
• Category 4 – Fault handling behaviour
  - When faults occur, the safety function is always performed.
  - Faults will be detected in time to prevent the loss of the safety function.
Category 4 – Contactor Fault
Validation

- Determine the level of conformity of the safety related part of the control system with the specification
- Combination of test and analysis
- Validation demonstrates
  - Specified safety functions implemented
  - All requirements of specified category are met
  - Compliance with dimensioning and environmental parameters
  - Assumptions have been assessed
Documentation should demonstrate the procedures used and results achieved for the following:

- Machine specifications, limits, intended use, etc
- Hazards identified
- Information used in preparation of the risk assessment
- Safety measures used to eliminate risk or reduce risk
- Residual risk
- Result of final risk evaluation
Guarding

- Safety Distances
  - Provide guidance on guard clearances based on
    - Height of guard
    - Height of hazard
    - Size of aperture in guarding
<table>
<thead>
<tr>
<th>Height of danger zone, ((a)) (see Note 3)</th>
<th>Height of protective structure, ((b)) (see Note 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>2700</td>
<td>—</td>
</tr>
<tr>
<td>2600</td>
<td>900</td>
</tr>
<tr>
<td>2400</td>
<td>1100</td>
</tr>
<tr>
<td>2200</td>
<td>1300</td>
</tr>
<tr>
<td>2000</td>
<td>1400</td>
</tr>
<tr>
<td>1800</td>
<td>1500</td>
</tr>
<tr>
<td>1600</td>
<td>1500</td>
</tr>
<tr>
<td>1400</td>
<td>1500</td>
</tr>
<tr>
<td>1200</td>
<td>1500</td>
</tr>
<tr>
<td>1000</td>
<td>1500</td>
</tr>
<tr>
<td>800</td>
<td>1500</td>
</tr>
<tr>
<td>600</td>
<td>1400</td>
</tr>
<tr>
<td>400</td>
<td>1400</td>
</tr>
<tr>
<td>200</td>
<td>1200</td>
</tr>
<tr>
<td>0</td>
<td>1100</td>
</tr>
</tbody>
</table>

**NOTES:**

1. Protective structures less than 1000 mm in height are not included because they do not sufficiently restrict movement of the body, or toppling over the structure.
2. Protective structures lower than 1600 mm should not be used without additional safety measures.
3. For danger zones above 2700 mm, refer to Clause 5.2.
Safe Distance

<table>
<thead>
<tr>
<th>Height of danger zone, (a)</th>
<th>Height of prototype (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>1200</td>
</tr>
<tr>
<td>1400</td>
<td>1400</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Height of prototype (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
</tr>
<tr>
<td>1200</td>
</tr>
<tr>
<td>1400</td>
</tr>
<tr>
<td>1600</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Horizontal</th>
</tr>
</thead>
<tbody>
<tr>
<td>2700</td>
</tr>
<tr>
<td>2600</td>
</tr>
<tr>
<td>2400</td>
</tr>
<tr>
<td>2200</td>
</tr>
<tr>
<td>2000</td>
</tr>
<tr>
<td>1800</td>
</tr>
<tr>
<td>1600</td>
</tr>
<tr>
<td>1400</td>
</tr>
<tr>
<td>1200</td>
</tr>
<tr>
<td>1000</td>
</tr>
<tr>
<td>Part of body</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Finger tip</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Finger up to knuckle joint or hand</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Arm up to junction with shoulder</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** If the length of the slot opening is less than or equal to 65 mm, the thumb will act as a stop and the safety distance can be reduced to 200 mm.
### AS4024.1801 Table 4

<table>
<thead>
<tr>
<th>Opening</th>
<th>Slot</th>
<th>Square</th>
<th>Round</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &lt; e ≤ 30</td>
<td>≥ 850 (see note)</td>
<td>≥ 120</td>
<td>≥ 120</td>
</tr>
<tr>
<td>30 &lt; e ≤ 40</td>
<td>≥ 850</td>
<td>≥ 200</td>
<td>≥ 120</td>
</tr>
<tr>
<td>40 &lt; e ≤ 120</td>
<td>≥ 850</td>
<td>≥ 850</td>
<td>≥ 850</td>
</tr>
</tbody>
</table>

**NOTE:** If the length of the slot opening is less than or equal to 65 mm, the thumb will act as a stop and the safety distance can be reduced to 200 mm.
Machine Safety
&
Australian Standards
ISO13849
• Presentation Objectives
  - Present overview of ISO 13849
  - Outline its content
  - Outline significant differences to AS4024
• Structure of ISO13849

- It comprises of 2 parts:
- Part 1: General Principles of Design
- Part 2: Validation
Risk assessment / risk reduction

START

Determination of the limits of the machinery

Risk assessment carried out in accordance with ISO14121 (AS4024:1301)

Yes

Has the risk been adequately reduced?

Risk reduction process for the hazard:
1 by intrinsic design,
2 by safeguards,
3 by information for use

No

Has the risk been adequately reduced?

Yes

Iterative process of the design of safety-related parts of the control system

No

The protective measure selected depend on a control system

END
Iterative design process

1. Identify the safety functions to be performed by SRP/CSs.
2. For each safety function specify the required characteristics.
3. Determine the required performance level PLr.
4. Design and technical realisation of the safety function: Identify the safety-related parts which carry out the safety function.

Evaluate the performance level PL:
- category
- MTTFed
- DC
- CCF
- if existing: software of the above safety-related parts.

Verification of PL:
- For the safety function: is PL ≥ PLr

Validation:
- Are all requirements met?
  - Yes
  - No

Have all safety function been analysed?
- Yes
- To Figure 1
Risk graph for determining required PLr

Start

S1

F1

P1

a

S2

F2

P2

b

P1

c

P2

d

P1

e

F2

P2

High contribution to risk reduction

Low contribution to risk reduction
Performance Levels

- Five level increasing integrity requirements
- Structure
- Behaviour of the safety function under fault condition(s)
- MTTFd Value for single components (low, medium, high)
- Common Cause Failure CCF (Pass, Fail)
- Diagnostic Coverage DC (none, low, medium, high)
- Safety Related Software
- Systematic failure
Structure for Category B

\[ I \xrightarrow{i_m} L1 \xrightarrow{i_m} O \]

- \( i_m \) Interconnecting Means
- \( I \) Input device, e.g. sensor
- \( L \) Input device, e.g. sensor
- \( O \) Output device, e.g. Main Contactor
Structure for Category 4

\[ i_m \quad \text{Interconnecting Means} \]
\[ c \quad \text{Cross monitoring} \]
\[ I1, I2 \quad \text{Input device, e.g. sensor} \]
\[ L1, L2 \quad \text{Input device, e.g. sensor} \]
\[ m \quad \text{Monitoring} \]
\[ O1, O2 \quad \text{Output device, e.g. Main Contactor} \]
Category 4 Requirements

- Requirements of Category B, well Tried Safety Principles
- A single fault does not lead to the loss of a safety function
- Single fault shall be detected at or prior to the next demand of the safety function
- If not possible then accumulation of faults shall not lead to a loss of the safety function
- DCavg shall be high
- MTTFd of each redundant channel shall be high
- Pass common cause failure (CCF) test
### Denotation each Channel

<table>
<thead>
<tr>
<th>Denotation each Channel</th>
<th>Range of each channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>3 years ≤ MTTFd &lt; 10 years</td>
</tr>
<tr>
<td>Medium</td>
<td>10 years ≤ MTTFd &lt; 30 years</td>
</tr>
<tr>
<td>High</td>
<td>30 years ≤ MTTFd</td>
</tr>
<tr>
<td>Denotation</td>
<td>Range</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>None</td>
<td>DC&lt;60%</td>
</tr>
<tr>
<td>Low</td>
<td>60% ≤ DC &lt;90%</td>
</tr>
<tr>
<td>Medium</td>
<td>90% ≤ DC &lt;99%</td>
</tr>
<tr>
<td>High</td>
<td>99% ≤ DC</td>
</tr>
<tr>
<td>No.</td>
<td>Range</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Separation / Segregation</td>
</tr>
<tr>
<td>2</td>
<td>Diversity</td>
</tr>
<tr>
<td>3</td>
<td>Design/application/experience</td>
</tr>
<tr>
<td>4</td>
<td>Assessment /analysis</td>
</tr>
<tr>
<td>5</td>
<td>Competence /training</td>
</tr>
<tr>
<td>6</td>
<td>Environmental</td>
</tr>
</tbody>
</table>

Need ≥ 65 to meet requirements
**Simplified procedure for evaluating PL**

<table>
<thead>
<tr>
<th>Category</th>
<th>B</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>3</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCavg</td>
<td>None</td>
<td>None</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>MTTFd of each channel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>a</td>
<td>Not covered</td>
<td>a</td>
<td>b</td>
<td>b</td>
<td>c</td>
<td>Not covered</td>
</tr>
<tr>
<td>Medium</td>
<td>b</td>
<td>Not covered</td>
<td>b</td>
<td>c</td>
<td>c</td>
<td>d</td>
<td>Not covered</td>
</tr>
<tr>
<td>High</td>
<td>Not covered</td>
<td>c</td>
<td>c</td>
<td>d</td>
<td>d</td>
<td>d</td>
<td>e</td>
</tr>
</tbody>
</table>
Machine Safety
&
Australian Standards
AS61508

Presenter

Peter Kroon
Principal Engineer, Sage Automation
• Presentation Objectives
  ▪ Present overview of AS61508
  ▪ Outline its content
  ▪ Detail some key concepts
• Structure of AS61508
  - It comprises of 7 parts:
    - Part 1: General Requirements
    - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
    - Part 3: Software requirements
    - Part 4: Definitions and abbreviations
• Structure of AS61508 cont.
  ▪ Part 5: Examples of methods for the determination of safety integrity levels
  ▪ Part 6: Guidelines on the application of AS61508.2 and AS61508.3
  ▪ Part 7: Overview of techniques and measures
61508 lifecycle - Conceptualisation

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation
61508 lifecycle - Realisation

- 10: Safety related systems: other technology
- 11: External risk reduction facilities
- 12: Overall installation and commissioning
- 13: Overall safety validation
61508 lifecycle – Realisation Software

9.1 Software safety requirements specification
- 9.1.1 Safety functions requirements specification
- 9.1.2 Safety integrity requirements specification

9.2 Software safety validation planning

9.3 Software Design and development

9.4 PE integration (hardware/software)

9.5 Software operation and maintenance procedures

9.6 Software safety validation

Overall operation, maintenance and repair
61508 lifecycle – Operation & Maintainence

14. Overall operation, maintenance and repair

15. Overall modification and retrofit

16. Decommissioning or disposal
61508 Risk reduction

- Residual Risk
- Tolerable Risk
- EUC Risk

Necessary risk reduction

- Partial risk covered by other technology safety related systems
- Partial risk covered by E/E/PE safety-related systems
- Partial risk covered by external risk reduction facilities

Actual risk reduction

Risk reduction achieved by all safety related Systems and external risk reduction facilities
Target failure measures low demand

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Low demand of operation (Average probability of failure to perform its design function on demand)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} ) to ( &lt; 10^{-4} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} ) to ( &lt; 10^{-3} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} ) to ( &lt; 10^{-3} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} ) to ( &lt; 10^{-1} )</td>
</tr>
<tr>
<td>Safety integrity level</td>
<td>High demand or continuous mode of operation (Probability of a dangerous failure per hour)</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 10^{-9}$ to $&lt; 10^{-8}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
</tbody>
</table>
## Architectural constraints - type B

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60%</td>
<td>Not allowed</td>
</tr>
<tr>
<td>60% - &lt; 90%</td>
<td>SIL 1</td>
</tr>
<tr>
<td>90% - &lt; 99%</td>
<td>SIL 2</td>
</tr>
<tr>
<td>≥ 99%</td>
<td>SIL 3</td>
</tr>
<tr>
<td></td>
<td>SIL 4</td>
</tr>
</tbody>
</table>

- SIL: Safety Integrity Level
## Minimum level of Independence

<table>
<thead>
<tr>
<th>Minimum level of Independence</th>
<th>Safety integrity level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Independent person</td>
<td>HR</td>
</tr>
<tr>
<td>Independent department</td>
<td>-</td>
</tr>
<tr>
<td>Independent organisation</td>
<td>-</td>
</tr>
</tbody>
</table>
61508 Software development lifecycle

- E/E/PES safety requirements specification
- Software safety requirements specification
- Software architecture
- Integration testing (components, subsystems, and programmable electronics)
- Validation testing
- Validation
- Validated Software
- Module design
- Module testing
- Coding

Output

Verification
Machine Safety
&
Australian Standards
AS62061

Presenter
Peter Kroon
Principal Engineer, Sage Automation
• Presentation Objectives

- Present overview of AS62061
- Outline its content
- Detail some key concepts
• Structure of AS62061
  - It comprises of 1 part:
  - Daughter standard of AS61508
  - Sector standard for machine guarding
Risk Estimation – AS 62061 Method

- **Severity of outcome**

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Severity (Se)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irreversible: death, losing an eye or limb</td>
<td>4</td>
</tr>
<tr>
<td>Irreversible: broken limb, losing a finger</td>
<td>3</td>
</tr>
<tr>
<td>Reversible: requiring medical attention</td>
<td>2</td>
</tr>
<tr>
<td>Reversible: requiring first aid</td>
<td>1</td>
</tr>
</tbody>
</table>
**Risk Estimation – AS 62061 Method**

- **Frequency and duration**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Fr when Duration &gt; 10min</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 1h</td>
<td>5</td>
</tr>
<tr>
<td>&gt; 1h to &lt;= 1 day</td>
<td>5</td>
</tr>
<tr>
<td>&gt; 1 day to &lt;= 2 weeks</td>
<td>4</td>
</tr>
<tr>
<td>&gt; 2 weeks to &lt;= 1 year</td>
<td>3</td>
</tr>
<tr>
<td>&gt; 1 year</td>
<td>2</td>
</tr>
</tbody>
</table>

- If frequency is less than 10min then drop to the next lower Fr value, except when frequency is <= to 1h.
**Risk Estimation – AS 62061 Method**

- Probability of event occurring

<table>
<thead>
<tr>
<th>Probability of occurrence</th>
<th>Probability (Pr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>5</td>
</tr>
<tr>
<td>Likely</td>
<td>4</td>
</tr>
<tr>
<td>Possible</td>
<td>3</td>
</tr>
<tr>
<td>Rarely</td>
<td>2</td>
</tr>
<tr>
<td>Negligible</td>
<td>1</td>
</tr>
</tbody>
</table>
Risk Estimation – AS 62061 Method

- Possibility of avoidance

<table>
<thead>
<tr>
<th>Possibility</th>
<th>Av</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impossible</td>
<td>5</td>
</tr>
<tr>
<td>Rarely</td>
<td>3</td>
</tr>
<tr>
<td>Probable</td>
<td>1</td>
</tr>
</tbody>
</table>
## Risk Estimation Model

<table>
<thead>
<tr>
<th>Severity (Se)</th>
<th>Class (Cl)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3-4</td>
</tr>
<tr>
<td>4</td>
<td>SIL 2</td>
</tr>
<tr>
<td>3</td>
<td>(OM)</td>
</tr>
<tr>
<td>2</td>
<td>(OM)</td>
</tr>
<tr>
<td>1</td>
<td>(OM)</td>
</tr>
</tbody>
</table>

Cl = Fr + Av + Pr
## Risk Estimation Models

<table>
<thead>
<tr>
<th>Severity (Se)</th>
<th>Class (Cl)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3-4</td>
<td>5-7</td>
<td>8-10</td>
<td>11-13</td>
<td>14-15</td>
</tr>
<tr>
<td>4</td>
<td>&lt;=16</td>
<td>&lt;=28</td>
<td>&lt;=40</td>
<td>&lt;=52</td>
<td>&lt;=60</td>
</tr>
<tr>
<td>3</td>
<td>&lt;=12</td>
<td>&lt;=21</td>
<td>&lt;=30</td>
<td>&lt;=39</td>
<td>&lt;=45</td>
</tr>
<tr>
<td>2</td>
<td>&lt;=8</td>
<td>&lt;=14</td>
<td>&lt;=20</td>
<td>&lt;=26</td>
<td>&lt;=30</td>
</tr>
<tr>
<td>1</td>
<td>&lt;=4</td>
<td>&lt;=7</td>
<td>&lt;=10</td>
<td>&lt;=13</td>
<td>&lt;=15</td>
</tr>
</tbody>
</table>

\[ \text{Cl} = \text{Fr} + \text{Av} + \text{Pr} \]
AS 1755 – Conveyor Safety Requirements
- Used as the primary reference for conveyor safety in Australia
  - Referenced in the Plant Code of Practice 2005 (QLD)
  - Referenced in the QLD Guide to Safeguarding common Machinery & Plant
  - Prescribed Standard in SA Quarry and Mining Safety Handbook
  - etc…
General Design and Construction Requirements

- Design & construct consistent with AS 4024 requirements
- Design for expected loading and forces
- Safe stopping
  - Stop in “shortest” practicable time
  - Remain stopped until energy is restored
- Take-ups
  - All take-up components that move during operation must be guarded
- Must provide access to the conveyor and its controls
- Clearance under the conveyor when it crosses a walkway must be at least 2.1m
- Clearance of 600mm must exist in working areas along the conveyor
- Sufficient clearance should be provided to allow any spillage to fall clear
- Devices should be manually operated and manually reset

- Placement
  - If conveyor is less than 2.5m in length and less than 2.5m above the walkway → Single device in middle of conveyor
  - If conveyor greater than 2.5m in length and less than 2.5m above the walkway → Device at head, tail, drive and intervals not exceeding 30m
  - If conveyor above 2.5m from the walkway → Devices at intervals not exceeding 100m
  - Devices at places where conveyor can be started and at permanent work stations
- Breaking, slackening or removal of wire shall be detected
- Force required to activate shall not exceed 70N with less then 300mm of movement, if force applied:
  - At right angles to wire axis
  - Midway between supports
- Force required to activate shall not exceed 230N along axis of wire
- Switch should be activated when wire pulled in any direction
Pullwire Requirements

(a) Incorrect

Correct for tension systems
Incorrect for non-tensioned systems
Wire shall be:
- External to vertical line of nip/shear point
- Within 1m of nip/shear point
- At least 900mm from the floor
- Not more than 1500mm from the floor
Pullwire Placement

(a) Preferred location

(b) Location when nip points higher than 1500 mm
- Designed and located according to AS 4024
- Guards should protect these common hazards
  - Shear and nip points
  - Rotating parts
  - Openings of hoppers and chutes
  - Falling material
Conveyor Guarding Examples
Conveyor Guarding Examples

- Underguard to protect walkway from falling material
- Sheet metal guard over passageway
- Railing
- Railing
????????

????????