



***Designing Safety Systems:
AS4024 V s AS/IEC61508
SIL Allocation***

The Requirement



NSW DEPARTMENT OF
PRIMARY INDUSTRIES

SAFETY ALERT

**Dangerous Unplanned Movements
Shuttle Cars and Continuous Miners**

RECOMMENDATIONS

All mines need to review mobile machinery design to establish that the safety-related functions and safety-related electrical control systems are adequately designed. The following points should be considered in that review:

General:

- Involving the machinery designer,
- Involving the machinery manufacturer,
- The use of AS61508, IEC62061, AS4024 as appropriate (the particular standard used depends on the complexity of the machinery and associated safety-related electrical control systems), and
- The use of AS/NZS4871 and AS60204 as appropriate.

The Standards

AS4024-2006 Safety of Machinery

This standard sets an overall framework and provides guidance to enable designers to produce machinery that is safe for its intended use. Parts 1501 & 1502 cover the Design of Safety-related parts of Control Systems .

AS/IEC61508 Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems.

This standard sets requirements for safety-related systems comprised of Electrical and/or Electronic and/or Programmable Electronic (E/E/PE) components. AS/IEC61508 can be used directly, but there are now application and sector standards available.

AS/IEC61511 for process plants,

AS/IEC62061 for industrial machinery.

Background to the Standards

Safety Systems

ISO12100:1&2
Safety of Machinery:
Basic Concepts /
General Principles

ISO14121
Safety of Machinery:
Principles of
Risk Assessment

ISO13849:1&2
Safety of Machinery:
Safety-related parts
of control systems

IEC61508:1-7
Functional Safety
of E/E/PE Safety
Related Systems

AS4024
Safety of
Machinery

AS62061
Safety of Machinery:
Functional Safety
of Safety-related E/E/PE
Control Systems

Key Similarities

Many pages !

AS4024 has 26 parts and 665 pages.

AS/IEC61508 has 7 parts and 365 pages (but AS62061 is only 90 pages).

Follow a risk-based approach to determining the requirements of safety functions.

Processes are consistent with overall risk management approach of AS/NZS4360:2004 and MDG1010.

Takes a holistic view of risk controls. ie. all elements contributing to the reduction of risk are considered.

Use a classification scheme for representing and specifying the integrity requirements of safety functions.

AS4024: CAT B, 1, 2, 3 & 4.

AS/IEC61508: SIL 1, 2, 3 & 4.

Key Differences

Life-cycle Scope and Steps

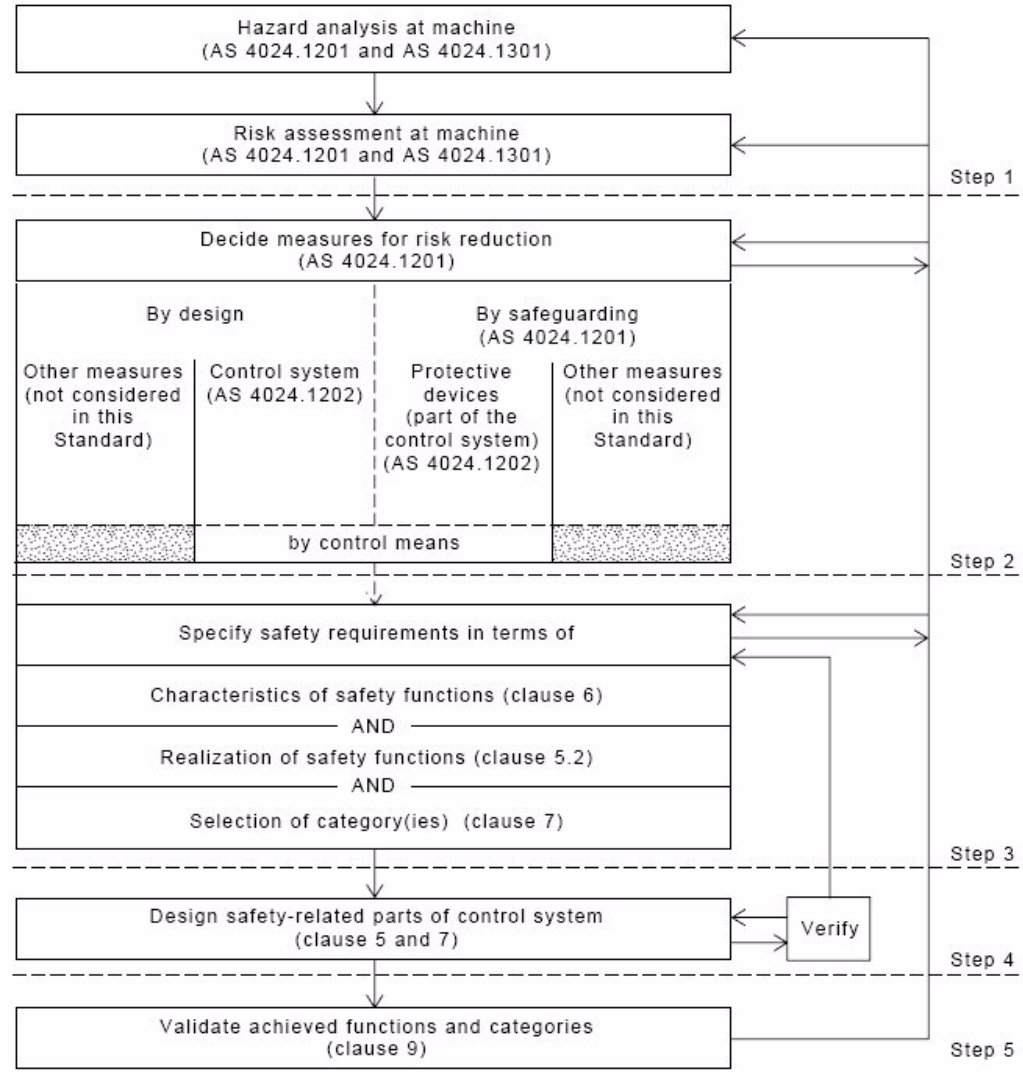
AS4024 Part 1501: 5-steps from initial risk assessment to design validation.

AS/IEC61508: 16 steps from system concept to decommissioning.

Allocating CAT and SIL levels.

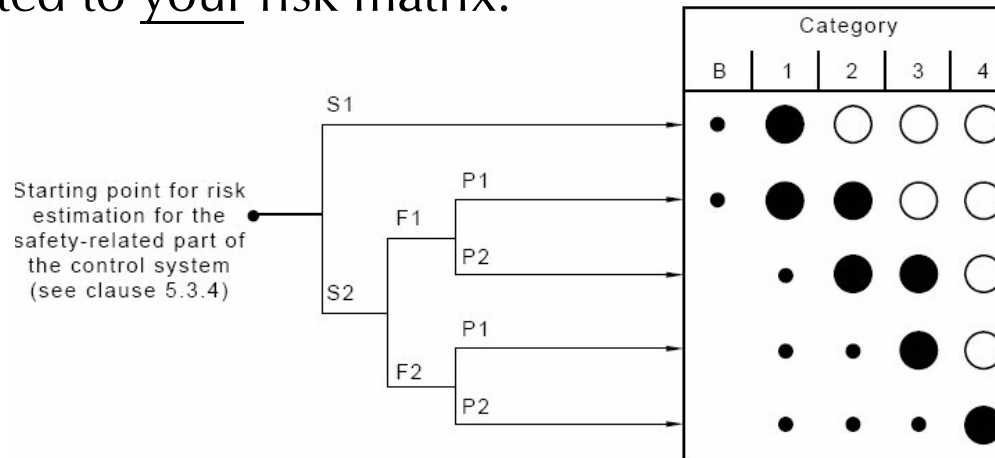
Design Implementation, Documentation and Verification.

AS4024 Process



CAT Levels (AS4024.1501 App C)

The CAT level allocated to a safety function is based on a 3-parameter risk graph method which is not necessarily correlated to your risk matrix.



LEGEND:

S Severity of injury

S1 = Slight (normally reversible) injury

S2 = Serious (normally irreversible) injury, including death

F Frequency and/or duration of exposure to the hazard

F1 = Seldom to quite often, and/or short exposure time

F2 = Frequent to continuous and/or long exposure time

P Possibility of avoiding the hazard

P1 = Possible under specific conditions

P2 = Nearly impossible

Selection of categories B, 1 to 4

● = Preferred categories for reference points (see clause 5.2)

● = Possible categories which may require additional measures (see paragraph C1)

○ = Measures which can be over-dimensioned for the relevant risk

AS4024 & Design

Proscriptive physical requirements see AS4024.1501, Clause 7.

Category 3

*The requirements of **Category B**, the use of **well-tried safety principles** and the following requirements shall apply:*

*(a) Safety-related parts of control systems to Category 3 requirements shall be designed so that **a single fault in any of these parts does not lead to loss of the safety function.***

(b) Common-mode faults shall be taken into account when the probability of such a fault occurring is significant.

*(c) Whenever reasonably practicable, **the single fault shall be detected at or before the next demand upon the safety function.***

Category 3 system behaviour allows that:

(i) when a single fault occurs, the safety function is always performed;

(ii) some but not all faults will be detected; and

(iii) accumulation of undetected faults can lead to loss of the safety function.

AS/IEC61508 Safety Life-cycle

PRE-DESIGN

(Phases 1 to 5)

1. Concept
2. Scope
3. Risk Analysis
4. Overall safety requirements
5. Allocate safety requirements

DESIGN AND INSTALLATION

(Phases 6 to 13)

- 6-8. Plan
- 9-11. Design
12. Install & Commission
13. Validate

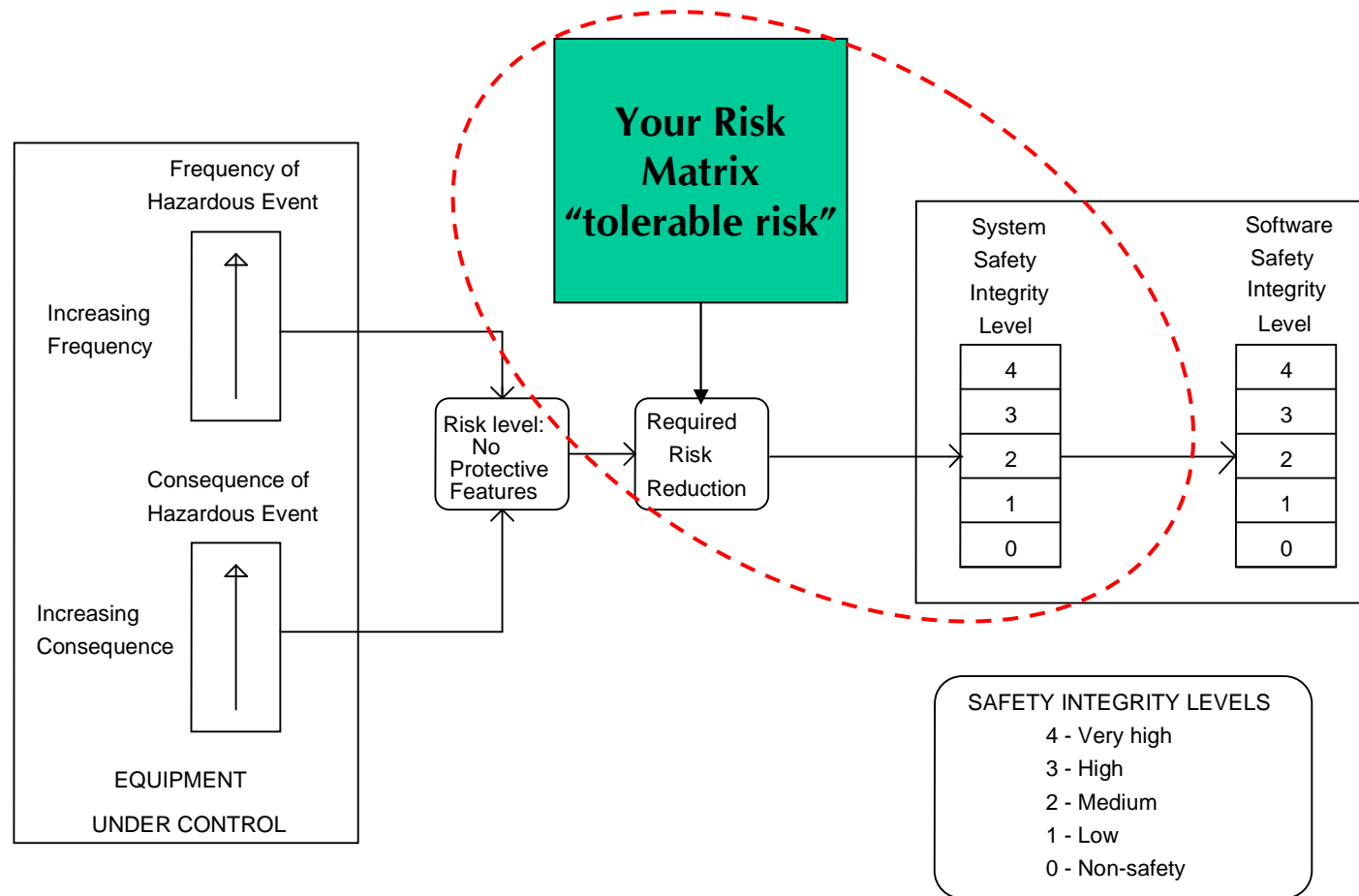
OPERATION

(Phases 14 to 16)

14. Operate & Maintain
15. Modify & Retrofit
16. Decommission

Principle of SIL Allocation

The SIL allocated to a safety function is based on a determination of the risk reduction needed to achieve “tolerable risk” in terms of your Risk Matrix.



Risk Matrix Calibration

Eg. Risk Matrix from MDG1010, Figure A.9.2)

	1 x Medically Treatable Injury (MTI)	1 x Compensible Injury (CI) or 10 x MTI's	10 x CI's	1 x Permanent Disablement (PD)	1 x Fatality	10 x Fatalities
Frequent: ≥ 1 per year	Medium	High	Very High	Severe	Severe	Severe
Possible: < 1 per year (but ≥ 0.1 per year)	Medium/Low	Medium	High	Very High	Severe	Severe
Unlikely: < 0.1 per year (but ≥ 0.01 per year)	Low	Medium/Low	Medium	High	Very High	Severe
Very Unlikely: < 0.01 per year (but ≥ 0.001 per year)	Low	Low	Medium/Low	Medium	High	Very High
Barely Credible: < 0.001 per year (but ≥ 0.0001 per yr)	Low	Low	Low	Medium/Low	Medium	High

Risk Matrix Calibration

First – Establish Your Risk Tolerance

	1 x Medically Treatable Injury (MTI)	1 x Compensible Injury (CI) or 10 x MTI's	10 x CI's	1 x Permanent Disablement (PD)	1 x Fatality	10 x Fatalities
Frequent: ≥ 1 per year	Medium	High	Very High	Severe	Severe	Severe
Possible: < 1 per year (but ≥ 0.1 per year)	Medium/Low	Medium	High	Very High	Severe	Severe
Unlikely: < 0.1 per year (but ≥ 0.01 per year)	Low	Medium/Low	Medium	High	Very High	Severe
Very Unlikely: < 0.01 per year (but ≥ 0.001 per year)	Low	Low	Medium/Low	Medium	High	Very High
Barely Credible: < 0.001 per year (but ≥ 0.0001 per yr)	Low	Low	Low	Medium/Low	Medium	High
				Low	Medium/Low	Medium
					Low	Medium/Low
						Low

Multiple (10) Fatalities	< 0.000001 / yr
1 x Fatality	< 0.00001 / yr
1 x PD	< 0.0001 / yr
10 x CI's	< 0.001 / yr
1 x CI or 10 x MTI's	< 0.01 / yr
1 x MTI	< 0.1 / yr

Tolerable limit should be determined via your own definitions.

Risk Matrix Calibration

- Then, make the cells just below the 'tolerable risk' level equal to 1.
- Determine Risk Reduction Factors (RRF) for each cell in the risk matrix.
- Here, each vertical or horizontal step in the risk matrix is equivalent to an RRF = 10.

	1 x Medically Treatable Injury (MTI)	1 x Compensable Injury (CI) or 10 x MTI's	10 x CI's	1 x Permanent Disablement (PD)	1 x Fatality	10 x Fatalities
Frequent: ≥ 1 per year	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)	Severe (10,000,000)
Possible: < 1 per year (but ≥ 0.1 per year)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)
Unlikely: < 0.1 per year (but ≥ 0.01 per year)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)
Very Unlikely: < 0.01 per year (but ≥ 0.001 per year)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)
Barely Credible: < 0.001 per year (but ≥ 0.0001 per yr)	Low (0.01)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)
				Low (1)	Medium/Low (10)	Medium (100)
					Low (1)	Medium/Low (10)
						Low (1)

SIL Allocation

Identify and Assess risk

Eg. Overpressure of hydraulic cylinder & rupture

Conceivable Consequence = 1 x Fatality

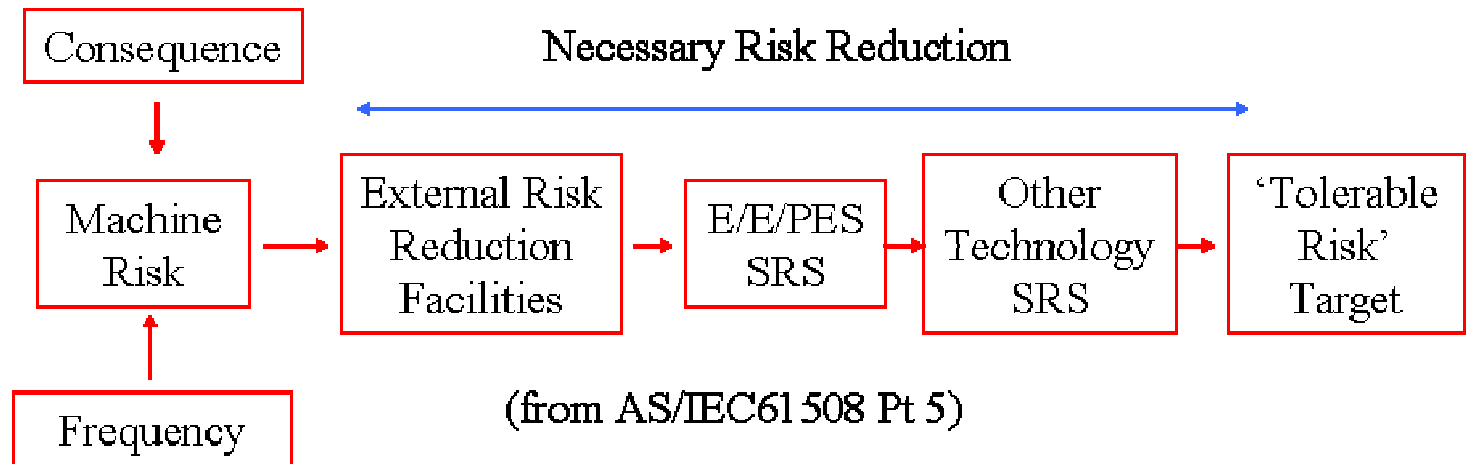
Likelihood (with no protective features) = 'Unlikely'

Risk = 'Very High' (necessary RRF = 10,000)

	1 x Medically Treatable Injury (MTI)	1 x Compensible Injury (CI) or 10 x MTI's	10 x CI's	1 x Permanent Disablement (PD)	1 x Fatality	10 x Fatalities
Frequent: ≥1 per year	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)	Severe (10,000,000)
Possible: < 1 per year (but ≥ 0.1 per year)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)	Severe (1,000,000)
Unlikely: < 0.1 per year (but ≥ 0.01 per year)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)	Severe (100,000)
Very Unlikely: < 0.01 per year (but ≥ 0.001 per year)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)	Very High (10,000)
Barely Credible: < 0.001 per year (but ≥ 0.0001 per yr)	Low (0.01)	Low (0.1)	Low (1)	Medium/Low (10)	Medium (100)	High (1,000)
				Low (1)	Medium/Low (10)	Medium (100)
					Low (1)	Medium/Low (10)
						Low (1)

Layers of Protection

Determine Overall Safety Requirement



A risk may be reduced by one or more 'Layers of Protection', eg. access restriction, control system trips, barriers, mechanical protection devices.

Where an electrical/electronic/programmable electronic system is used as a protective layer, this results in a SIL being allocated to that system.

Layers of Protection Analysis (LOPA)

Initiating Event	Layer 1 Hydraulic Overpressure Machine Trip Operates	Layer 2 Pressure Relief Valve / Plug Activates	Layer 3 Persons Not Present in the Hazardous Area	Layer 4 Persons in Hazardous Zone Avoid Hazardous Energy Release	Fatality Frequency
					0.00001 / yr
			Probability of Failure = 10%	Probability of Failure = 100%	Total RRF = 10,000
		Probability of Failure = 10%	RRF = 10	RRF = 1	
	Hydraulic Overpressure Hazard Frequency = 0.1 / year	Probability of Failure = 1% RRF = 100	RRF = 10		

An electrical/electronic/programmable electronic system is proposed to be used as a protective layer for:

- Layer 1 (the trip).

SIL Allocation

- Layer 1 (the trip).

Probability of Failure = 1% (RRF = 100)

Equates to SIL 2

Also to be considered:

- Layer 2 (the mechanical pressure relief device)

Probability of Failure = 10% (RRF = 10)

Equates to SIL 1, but this is not normally specified for mechanical devices.

Use AS4024 Part 1501 (ISO13849-1) for guidance.

AS62061, Table 6 equates SIL to CAT levels.

AS/IEC61508 & Design

General requirements on performance, design techniques and activities that shall/should be undertaken (see IEC61508 Parts 2 & 3 & 6):

Basically, safety functions must be designed to target a combination of “performance” criteria:

1. Reliability
 - Probability of Failure on Demand (low demand systems),
 - Probability of a Dangerous Failure (high demand systems).
2. Fault Tolerance (eg. redundancy)
3. Fail-safe (failures not “dangerous and undetected”)

Comparison

- AS4024
 - CAT allocation not necessarily based on your risk matrix,
 - more proscriptive (ie. less flexible) on design features,
 - relies on the use of “well-tried” components and practices,
 - less onerous on the reliability analysis, documentation and verification aspects.
- AS/IEC61508
 - SIL allocation based on your risk matrix,
 - more flexible on physical design implementation,
 - relies on setting performance measures and design practices,
 - very onerous on the documentation, verification and reliability analysis aspects.

Contact

Marcus Punch
Hatch Associates Pty Ltd. (Newcastle)

7 Warabrook Bld Warabrook NSW 2304
PO Box 5000, Hunter Mail Centre NSW 2310

Phone : +61 (0)2 4968 6879

Fax: +61 (0)2 4968 6800

Mobile +61 (0)434 603720

Email : mpunch@hatch.com.au