



Functional Safety #1: Determining the SIL and CAT of a Transport Braking System

Presented by 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

The Requirement



SAFETY ALERT

Maintenance of Safety Critical Systems - Braking, Steering & Warning Systems

3. All safety critical systems have been assessed and the appropriate integrity level applied in accordance with AS 4024, AS 62061, AS 61508 or other similar standards.
4. A Failure Modes and Effects Analysis (FMEA) or other similar risk assessment method has been carried out to confirm the integrity of all safety critical systems.



The Standards

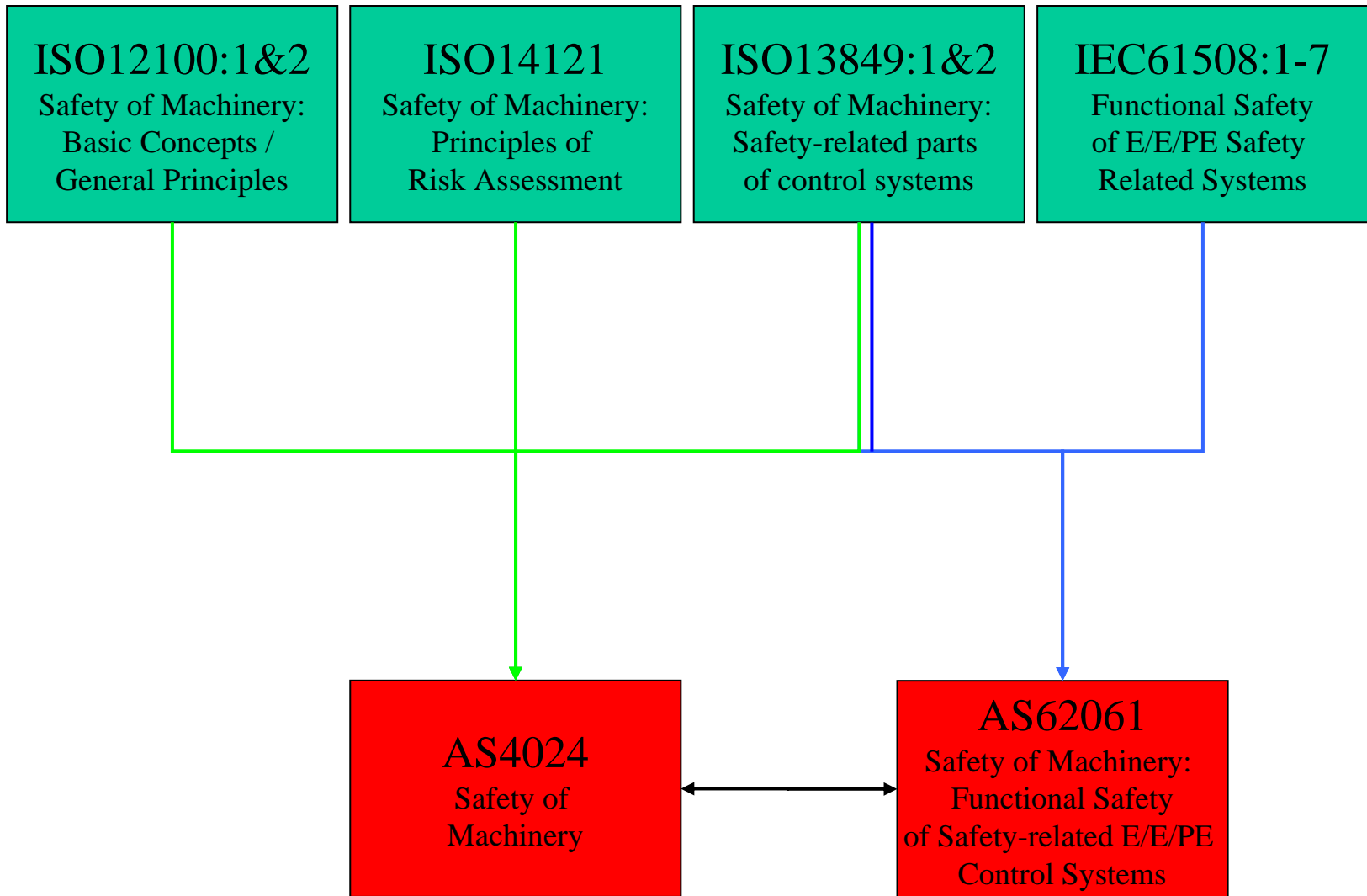
AS4024-2006 Safety of Machinery

- 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.

The Standards



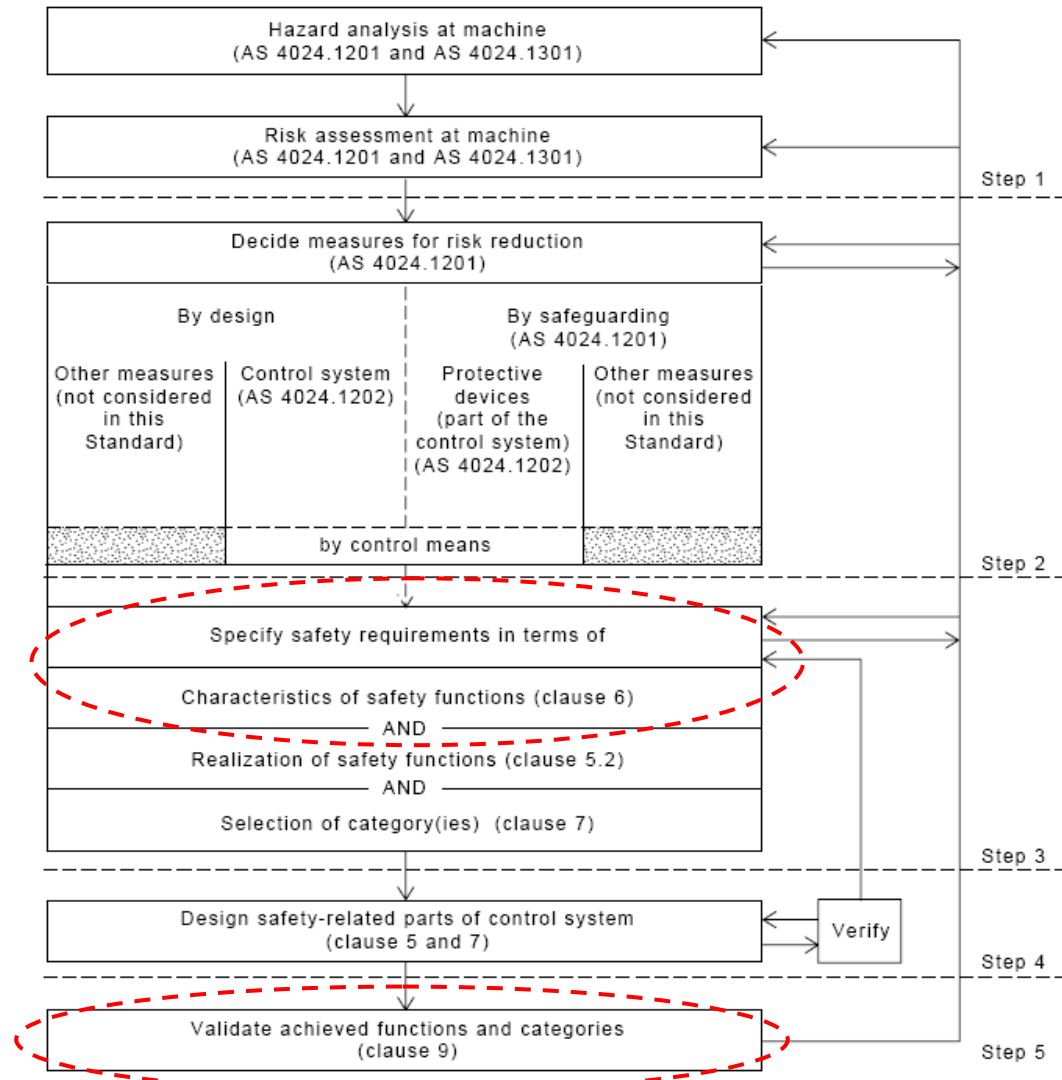
Key Similarities

- 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.

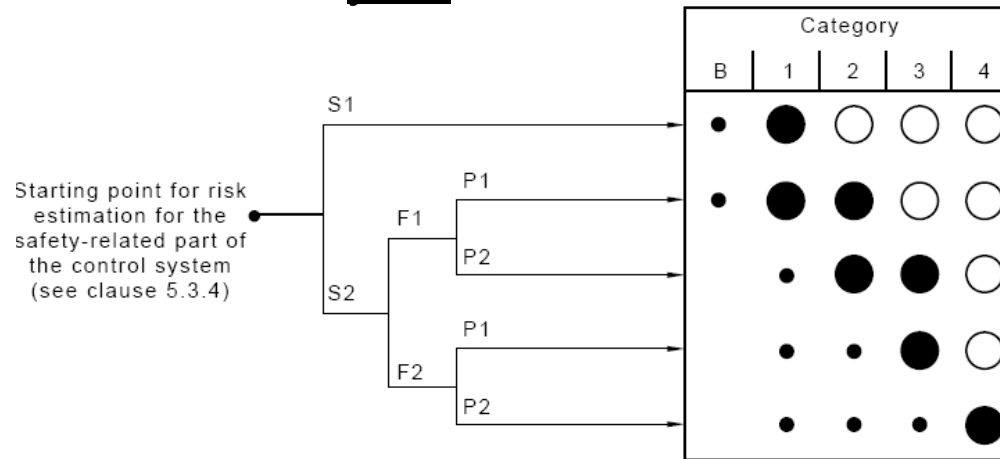
AS4024 Process



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

See AS4024.1501, Clause 7.

Category (see Note 1)	Summary requirements
B (see Clause 7.2.1)	Safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.
1 (see Clause 7.2.2)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.
2 (see Clause 7.2.3)	Requirements of B and the use of well tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.
3 (see Clause 7.2.4)	Requirements of B and the use of well tried safety principles shall apply. Safety-related parts shall be designed so that— a single fault in any of these parts does not lead to loss of the safety function; and whenever reasonably practicable the single fault is detected.
4 (see Clause 7.2.5)	Requirements of B and the use of well tried safety principles shall apply. Safety-related parts shall be designed so that— A single fault in any of these parts does not lead to loss of the safety function, and The single fault is detected at or before the next demand upon the safety function. If this not possible, then an accumulation of faults shall not lead to loss of the safety function.

AS4024 - Step 1

Identify Hazards & Assess Risk

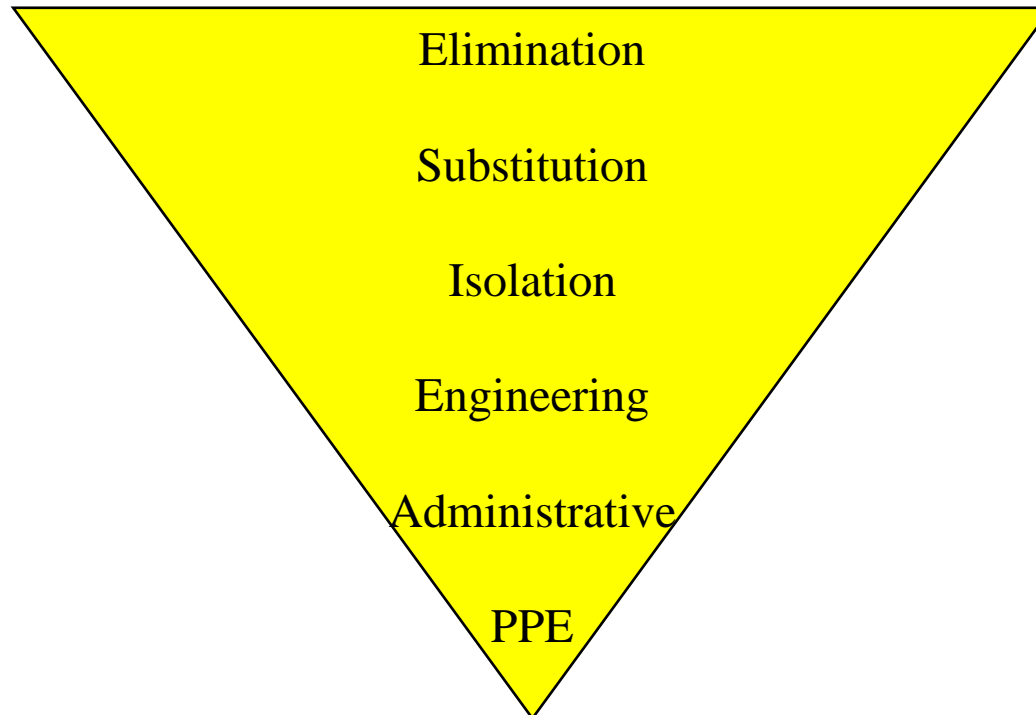
Hazard: Brake failure

Risk : Conceivable Consequence = 1 x Fatality
 Likelihood (per vehicle)= 'Very Unlikely'
 Risk = 'High'

	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

AS4024 - Step 2

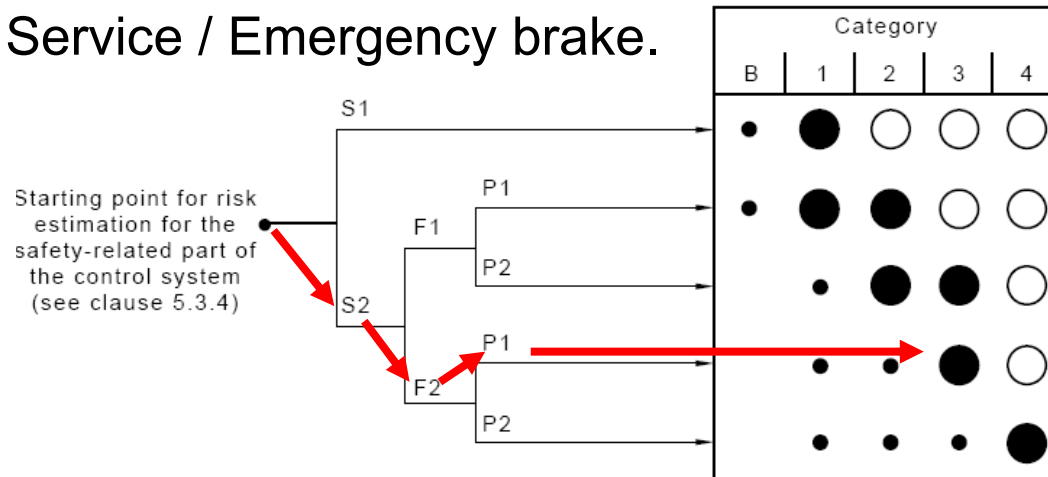
Decide Measures for Risk Reduction



- Service Brake (to be reliable as possible to avoid the hazard),
- Emergency Brake (if normal brake fails – but, part of same circuit),
- Retarder (to control speed),
- Driver training – emergency actions,
- Procedures,
- Etc...

AS4024 - Step 3

Specify Safety Requirements Service / Emergency brake.



CAT3

LEGEND:

S Severity of injury

S1 = Slight (normally reversible) injury

S2 = Serious (normally irreversible) injury, including death

← risk assessment

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

← most exposed person – the driver

P Possibility of avoiding the hazard

P1 = Possible under specific conditions

P2 = Nearly impossible

← other methods of stopping to be incorporated

Selection of categories B, 1 to 4

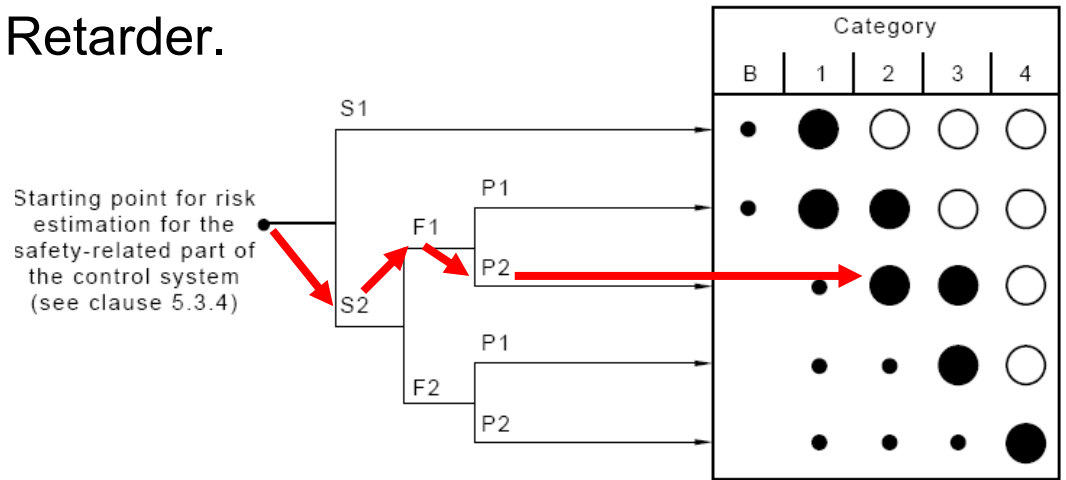
● = Preferred categories for reference points (see clause 5.2)

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

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

AS4024 - Step 3

Specify Safety Requirements Retarder.



CAT2/3

LEGEND:

S Severity of injury
 S1 = Slight (normally reversible) injury
 S2 = Serious (normally irreversible) injury, including death

← risk assessment

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

← hazard arises when normal brakes fail

P Possibility of avoiding the hazard
 P1 = Possible under specific conditions
 P2 = Nearly impossible

← other methods of stopping have failed

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 - Step 3

Specify Safety Requirements

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 Process

- “**Functional Safety**”: that part of overall safety that depends on a process / machinery and its control system and any safety-related systems operating correctly in response to their inputs.
- “**Safety-related System**” (SRS): is any system / equipment which maintains a process / machinery in a safe state or puts a process / machinery into a safe state in the event of a specific hazard occurring.
- “**Safety Integrity Level**”: or “SIL”, is a discrete number (1,2,3 or 4) representing a numerical target on the reliability performance of a safety function.

AS/IEC61508 Process

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)

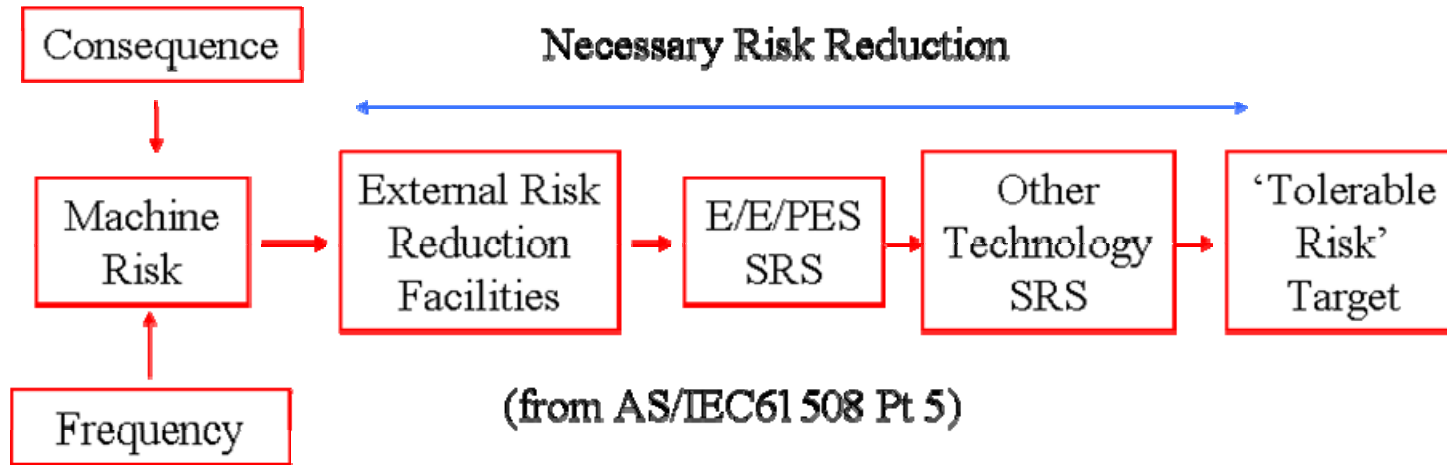
- 6-8. Plan
- 9-11. Design
12. Install & Commission
13. Validate

OPERATION

(Phases 14 to 16)

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

SIL Levels



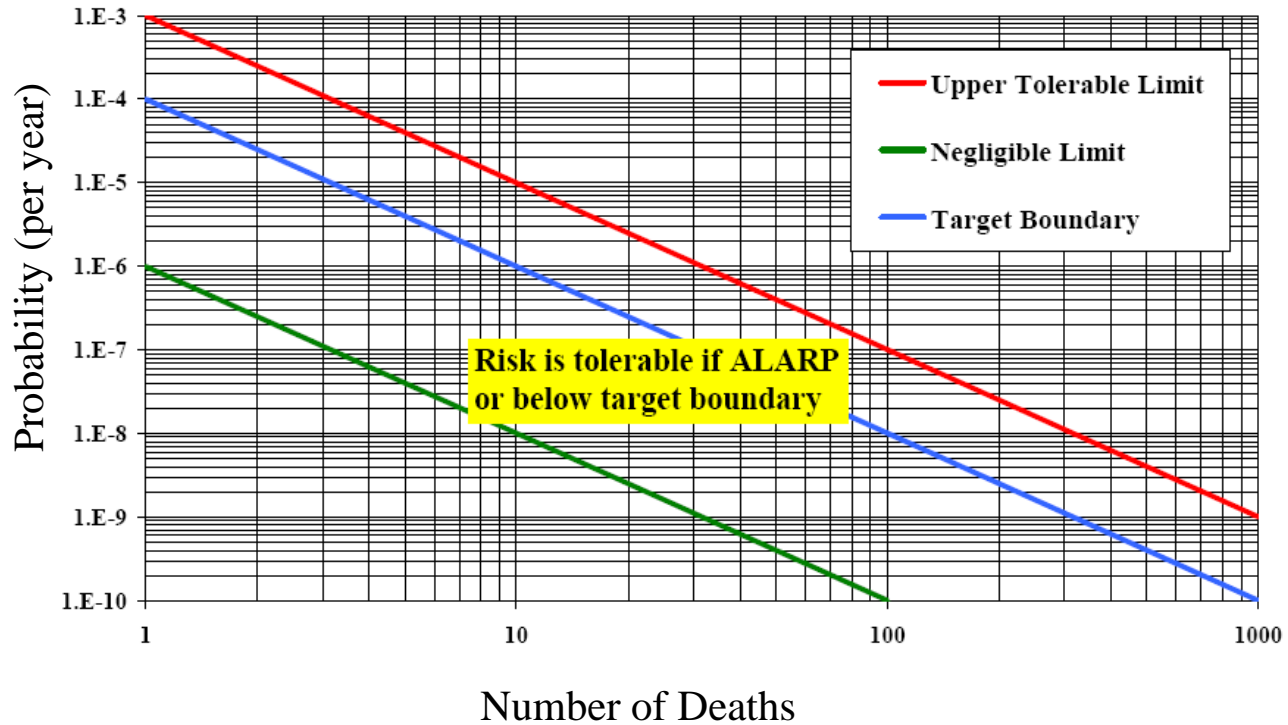
- A risk may be reduced by one or more ‘Layers of Protection’, eg. access restriction, control system trips, barriers, mechanical protection devices.

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

- “Tolerable risk” must be decided.

Tolerable Risk – Society

Eg. proposed quantitative safety criteria for new technological developments in EU countries.



Tolerable Risk - Industry

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

	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	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.

AS/IEC61508 and Design

Depending on the SIL allocated, there are specific requirements for:

Safety System Reliability

- Probability of Failure on Demand (PFD), or
- Probability of Dangerous Failure Per Hour (PFH),

Architecture (configuration)

- Hardware Fault Tolerance (eg. redundancy, single points of failure), and
- Safe Failure Fraction (ie. % of failures that are not dangerous and undetected)

Measures and Techniques to Avoid Systematic Failures

1. Hardware, and
2. Software.

Safety System Reliability

“High Demand” Mode

The frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof test frequency.

<u>SIL</u>	<u>Probability of Dangerous Failure per Hour (PFH)</u>
4	$PFH < 10^{-08}$
3	$10^{-08} \leq PFH < 10^{-07}$
2	$10^{-07} \leq PFH < 10^{-06}$
1	$10^{-06} \leq PFH < 10^{-05}$

“Low Demand” Mode

The frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.

<u>SIL</u>	<u>Probability of Failure on Demand (PFD)</u>
4	$PFD < 10^{-04}$
3	$10^{-04} \leq PFD < 10^{-03}$
2	$10^{-03} \leq PFD < 10^{-02}$
1	$10^{-02} \leq PFD < 10^{-01}$

AS/IEC61508 - Step 3

Risk Analysis

Hazard: Brake failure

Risk : Conceivable Consequence = 1 x Fatality

Likelihood (per vehicle)= 'Very Unlikely' (up to 0.01 / yr)

Risk = 'High'

	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

AS/IEC61508 - Step 4

Overall Safety Requirements

Likelihood (per vehicle)= 'Very Unlikely' (<0.01 / yr)

Tolerable Risk Frequency for single fatality: assume <0.00001 / yr

Necessary Risk Reduction to be achieved by all **independent** risk reduction measures, acting together:

$$= \frac{\text{Actual Frequency of Unwanted Consequence}}{\text{Tolerable Frequency of Unwanted Consequence}}$$

$$= 0.01 / 0.00001$$

$$= \underline{\mathbf{1000 \text{ times}}}$$

AS/IEC61508 - Step 5

Allocate Safety Requirements – Identify Measures

Necessary Risk Reduction to be achieved by all **independent** risk reduction measures, acting together: **1000 times**

- Service Brake (to be reliable as possible to avoid the hazard,
- Emergency Brake (if normal brake fails – part of same circuit),
- Retarder (to control speed),
- Driver training – emergency actions,
- Procedures.

Risk Reduction to be achieved by each measure is determined by a **Layer of Protection Analysis (LOPA)**.

AS/IEC61508 - Step 5

Allocate Safety Requirements – Service / Emergency Braking System

Initiating Event	Layer 1	Hazard Event	
<i>Driver Uses Vehicle Brakes</i>	<i>Service / Emergency Brakes</i>	<i>Failure of Normal Braking System</i>	
Event Frequency (per hr) = <u>40.0</u> (per yr) = <u>350400</u>		Event Frequency (per hr) = <u>1.142E-06</u> (per yr) = <u>1.000E-02</u>	
Demand Mode (Layer 1) = HIGH DEMAND		Demand Mode (Layers 2,3,4,5) = LOW DEMAND	
Tolerable Accident Frequency (per yr) = <u>1.000E-05</u> (per hr) = <u>1.142E-09</u>		Tolerable? No	
Necessary Risk Reduction = <u>3.504E+10</u>		Necessary Risk Reduction = <u>1000.0</u>	
	Risk Reduction Factor = <u>3.504E+07</u>		
	Probability of Failure (per Hour) = <u>2.854E-08</u>		
	SRS? = Yes		
	SIL Required = SIL3		

AS/IEC61508 - Step 5

Allocate Safety Requirements – Other Measures

Hazard Event		Layer 2		Layer 3		Accident Event	
<i>Failure of Normal Braking System</i>		Retarder		Trained Driver Able to Take Evasive Action		<i>Vehicle Accident and Fatality</i>	
Event Frequency (per hr)	<u>1.142E-06</u>					Accident Frequency (per hr) =	<u>1.142E-09</u>
(per yr)	<u>1.000E-02</u>					Tolerable Accident Frequency (per hr) =	<u>1.142E-09</u>
Demand Mode (Layers 2,3,4,5)=	LOW DEMAND					Risk Reduction Achieved =	<u>3.504E+10</u>
Tolerable?	No					Necessary Risk Reduction =	<u>3.504E+10</u>
Necessary Risk Reduction =	<u>1000.0</u>					% of Necessary Risk Reduction Achieved =	<u>100%</u>
		Risk Reduction Factor	500	Risk Reduction Factor	2		
		Probability of Failure (on Demand) =	<u>2.000E-03</u>	Probability of Failure (on Demand) =	<u>5.000E-01</u>		
		SRS? =	Yes	SRS? =	No		
		SIL Required =	<u>SIL2</u>	SIL Required =	<u>N/A</u>	OVERALL RISK REDUCTION IS SUFFICIENT	

Summary of Findings

System	CAT	SIL
Service / Emergency Brake	CAT3	SIL3 (high demand) PFH < 0.0000001
Retarder	CAT2/3	SIL2 (low demand) PFD < 0.01

Re-cap: CAT V's SIL

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

Next.....

3. All safety critical systems have been assessed and the appropriate integrity level applied in accordance with AS 4024, AS 62061, AS 61508 or other similar standards.
4. A Failure Modes and Effects Analysis (FMEA) or other similar risk assessment method has been carried out to confirm the integrity of all safety critical systems.

Functional Safety #2:

Verifying a SIL for a Transport Braking System.

Functional Safety #3:

Verifying a CAT for a Transport Braking System