



Centennial Angus Place



Functional Safety Design of a Long-wall Remote Isolation System

Presented by: Marcus Punch
Hatch Associates Pty. Ltd. (Newcastle)
Mobile: +61 (0)434 603720
Email : mpunch@hatch.com.au

David Boyling
Centennial Coal Pty. Ltd. (Angus Place Colliery)
Phone: +61 (0)2 63548790
Email: dave.boyling@centennialcoal.com.au

Background

- Angus Place Colliery is situated in the Blue Mountains close to our markets - Mount Piper Power Station and Wallerawang Power Station.
- The Colliery has produced up to 3.2 million tonnes per annum by Long-wall extraction.
- The Long-wall mining System incorporates many control functions, which include Communications, Lockout and Remote Isolation.
- The Remote Isolation System will be our focus today.

Video Clip



Background

- The natural progression was to embrace the “Functional Safety” approach and incorporate the iMac supervisory controller which is already installed on our conveyors.
- This was the driving factor to develop a Remote Isolation, Communications and Control System that could be considered for Functional Safety assessment to a pre-determined Safety integrity Level.
- The process also had to comply with the Angus Place Electrical Engineering Management Plan and the Angus Place OH&S Management Plan.

Context

The following aspects (among others) of the ***NSW Coal Mine Health and Safety Regulation 2006*** apply to the design, operation and maintenance of the Long-wall Remote Isolation System. These clauses imply that a ‘functional safety’ approach is required. See also Legislative Update ***LU07-05***.

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 electrical safeguards for electrical and non-electrical hazards, with a ***probability of failure appropriate to the degree of risk*** posed by the hazard.

Design Considerations

- Versatility.
- Project planning and delivery timing factors.
- Factory Acceptance Testing.
- Software interaction.
- Redundancy.
- Voting.
- Hard-wired output interrupts.
- Safety-critical circuits.

Design Considerations

- Contactor monitoring.
- Complementary Monitoring.
- Number of operations.
- Circuit breaker's spring energy.
- Voltage Monitoring.
- Interface Cable condition monitoring.
- Component Change out.
- Safety Life Cycle approach and use of AS61508, AS62061, AS4024
- Failure Mode Effects Analysis.

Steps Taken: Specification → Design

- Develop a Functional Safety Plan.
- Machine Hazard identification.
- Identify Risk Controls & Safety Related Control Functions (SRCF).
- Determine functionality and safety requirements of the SRCF's.
- Safety Requirements Specification.
- Design Safety Related Electronic Control Systems (SRECS).
- Verification - calculate the reliability of each SRCF.
- Determine the Safety Integrity Level (SIL) claim for each SRCF.

Steps Taken: Design → Operations

- Document the Safety Related Electronic Control Systems (SRECS) design.
- Implementation of the SRECS.
- Validation.
- Operations and Maintenance.
- Component change out control and monitoring.
- Standard work procedures for Remote Isolation to limit any exposure.
- Maintenance program to ensure reliability and to maintain SIL rating.

Reference Information

- Reliability information for the Circuit Breaker and Contactors was collected from Japan.
- Safety Relay reliability information was collected both from Germany and the USA.
- Other ancillary components reliability information source from general references.
- iMac reliability information supplied by Ampcontrol.
- Continuity relay reliability information supplied by ATF Mining (Ampcontrol).
- Standards: AS62061, AS61508, AS4871 and AS4024.
- Amponrol iMac and Voice Communication Manuals.
- Connell Hatch Machinery Functional Safety Lifecycle Process Plan.

Outcomes

- Remote Isolation System proven to SIL2.
- Safe and User-friendly system.
- Easily maintained to assure Functional Safety within the guidelines.
- Valuable information on Function Safety validation.
- Good understanding on how to achieve Functional Safety in Design.
- Equipment Safety Life Cycle including a Safety File.
- Conform to New Management Systems and OH&S Regulations.
- Excellent working relationship with Ampcontrol and ATF Mining.
- Excellent working relationship with Marcus Punch. (Connell Hatch).

Key Assumptions

Prior to the Functional Safety work, the team established the following assumptions:

- The expected consequence of an unplanned movement of the Long-wall machinery during a clearing operation would be a **single fatality**, consistent with the initial risk assessment.
- The 'tolerable frequency' for a single fatality event was assumed to be:

10^{-5} / yr, or **$\sim 1.14 \times 10^{-9}$ / hr**.

- Why? See the next few slides.

Tolerable Risk – Industry Perspective

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
		< 0.0001 per year		Low	Medium/Low	Medium
			< 0.00001 per year		Low	Medium/Low
				< 0.000001 per year		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 Risk – Historical

Derivative
FINAL REPORT TO QUEENSLAND
RESOURCES COUNCIL ON UNDERLYING
CAUSES OF FATALITIES AND SIGNIFICANT
INJURIES IN THE AUSTRALIAN MINING
INDUSTRY.

Prepared by the
Minerals Industry Safety and Health Centre
Sustainable Minerals Institute
University of Queensland

4 March 2005

Page 11- “Safe” industry should be about 0.005 fatalities / million man-hours, or a factor of ten lower than currently reported in the mining industry.

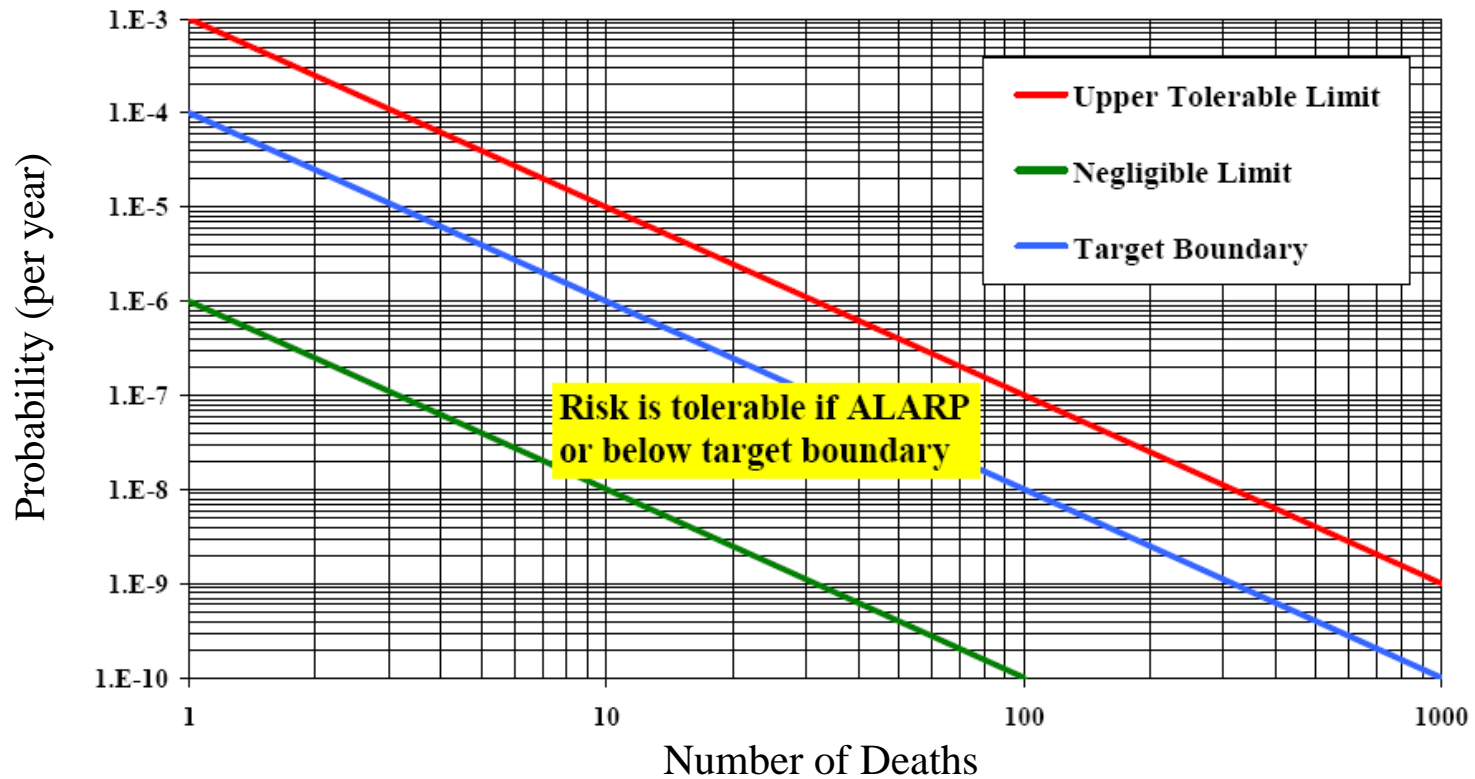
That is:

- For a mine with a 100 person workforce constantly on-site, this roughly equates to 1 fatality per 1000 yrs for the site, covering all hazards.
- Setting a tolerable risk frequency of 10^{-5} / yr for each fatal hazard provides average coverage for each worker for ~100 life-threatening hazards.

NB: the concept of “safe” is not fixed.

Tolerable Risk – Societal Perspective

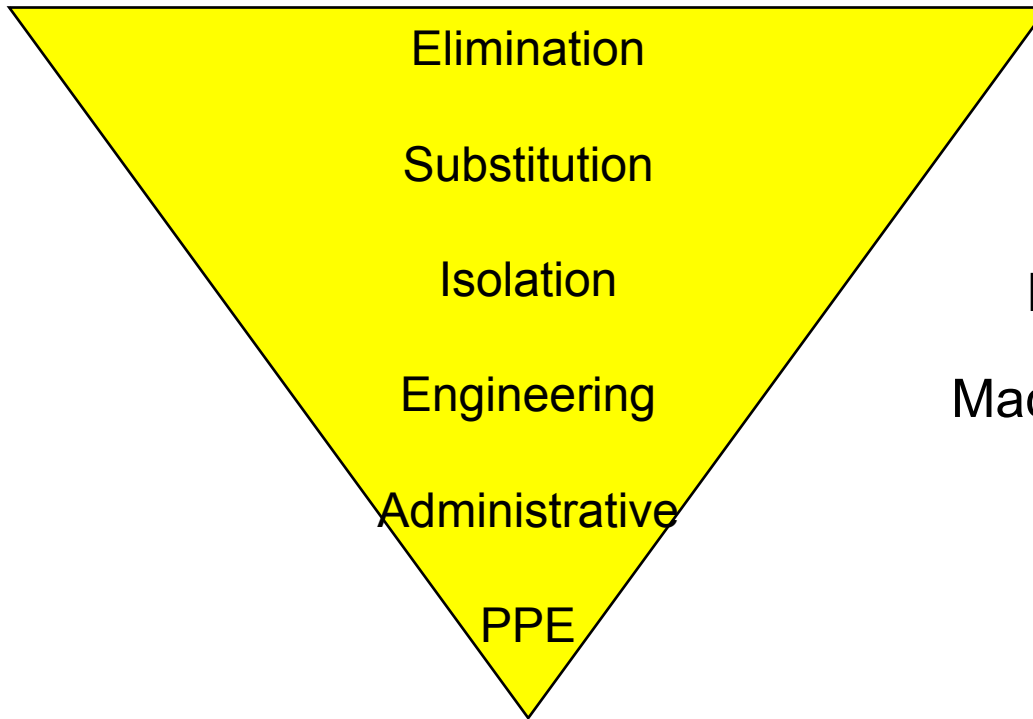
- Proposed quantitative safety criteria for new technological developments in EU countries.
- Adopted by UK HSE.



Key Assumptions

- The expected demand rate on the remote isolation system was expected to be up to **3 times per day**, or 0.125 demands per hour. Failure of the remote isolation system when in use creates the potential for a fatal accident.
- Discussions suggested that the frequency of demand is variable and may potentially increase factor of 2 for periods of time. The overall risk reduction should therefore take this possibility into account.

Risk Reduction Measures



Hazardous Situation:
Need to clear debris



Remote Isolation System



Machine Monitoring & Alarms



Rules & Procedures



Accident: Unplanned movement with fatality whilst clearing debris.



Layers of Protection Analysis

Safety Systems

Initiating Event		Layer 1	Intermediate Event	
<i>Process Disruption - Remote Isolation System Required.</i>		Remote Isolation System.	<i>Failure of Remote Isolation</i>	
Event Frequency (per hr) =	0.1250	Remote isolation is demanded by an operator. The IMAC system opens its control relay (normal stop) which opens the drive contactors at each drive via a safety relay. This is followed by the iMAC opening an aux. relay (remote isolation command) which trips	Event Frequency (per hr)	2.500E-08
Demand Mode (Layer 1)=	HIGH DEMAND		Demand Mode (Layers 2,3,4,5)=	LOW DEMAND
Tolerable Event Frequency (per hr) =	1.142E-09		Tolerable?	No
Necessary Risk Reduction =	1.095E+08			
		Risk Reduction Factor		5.000E+06
		Probability of Failure (per Hour) =		2.000E-07
		E/E/PE SRS? =		Yes
		SIL Required =		SIL2

Layers of Protection Analysis

Intermediate Event		Layer 2		Layer 3		Hazard Event	
<i>Failure of Remote Isolation</i>		DI8 detects incorrect feedback on contacts and voltages after isolation granted and triggers voice message.		Operator has followed rules for access and egress from hazardous area and is able to safely extricate themselves.		<i>Unplanned Movement & Fatality</i>	
Event Frequency (per hr)	2.500E-08	Monitors 3.3kV MCB complimentary contacts, every drive contactor complimentary contacts and monitors full voltage on NVR on load side of MCB. This system is independent of the RI system.		Human reliability thought to be better than 90%. Training and procedures deal with what can be done during remote isolation. There are multiple levels of supervision and responsibility. High levels of safety consciousness. This should be subject to continuous monitoring.		Event Frequency (per hr) =	2.778E-10
Demand Mode (Layers 2,3,4,5)=	LOW DEMAND					Tolerable Event Frequency (per hr) =	1.142E-09
Tolerable?	No					Risk Reduction Achieved =	4.500E+08
						Necessary Risk Reduction =	1.095E+08
				% of Necessary Risk Reduction Achieved =	411%		
		Risk Reduction Factor	9	Risk Reduction Factor	10		
		Probability of Failure (on Demand) =	1.111E-01	Probability of Failure (on Demand) =	1.000E-01		
		E/E/PE SRS? =	Yes	E/E/PE SRS? =	No		
		SIL Required =	<u>SIL0</u>	SIL Required =	<u>N/A</u>	OVERALL RISK REDUCTION IS SUFFICIENT	

Risk Reduction Achieved = 4.5×10^8

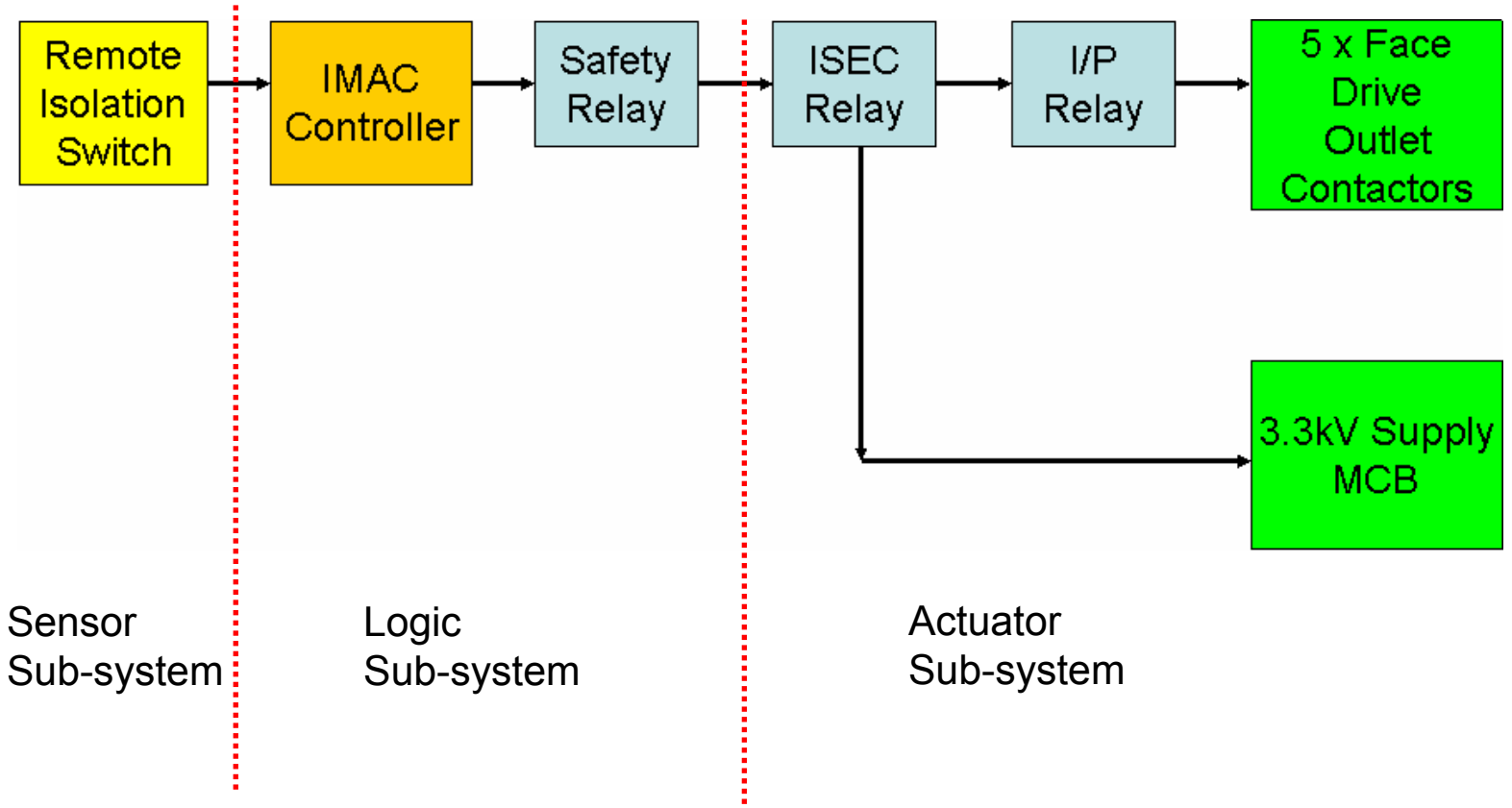
Necessary Risk Reduction = 2.19×10^8
 (incl. 2x factor for increased usage)

AS/IEC61508 and Design

Things to be demonstrated:

1. Reliability meets SIL2
 - Probability of Dangerous Failure per Hour $< 10^{-6}$.
2. Architectural requirements met for SIL2.
 - Hardware Fault Tolerance (eg. redundancy, single points of failure),
 - Safe Failure Fraction (ie. % of failures that are not dangerous and undetected)
3. Systematic failure avoidance in hardware and software design.
 - Hardware, and
 - Software.

Remote Isolation System Design



Failure Modes, Effects and Diagnostics Analysis (FMEDA)

iMAC controller : Using manufacturer failure modes and failure rates.

Table 2 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
iMAC Controller and EOL module	333 FIT	894 FIT	0 FIT	37 FIT	97.1%

λ_{du} → ie. Probability of Dangerous Failure Per Hour is 37×10^{-9} , or 3.7×10^{-8}

SFF → this means that 97.1% of failures will be safe or dangerous-detected.

ie. 2.9% of failures will be dangerous- undetected.

Failure Modes, Effects and Diagnostics Analysis (FMEDA)

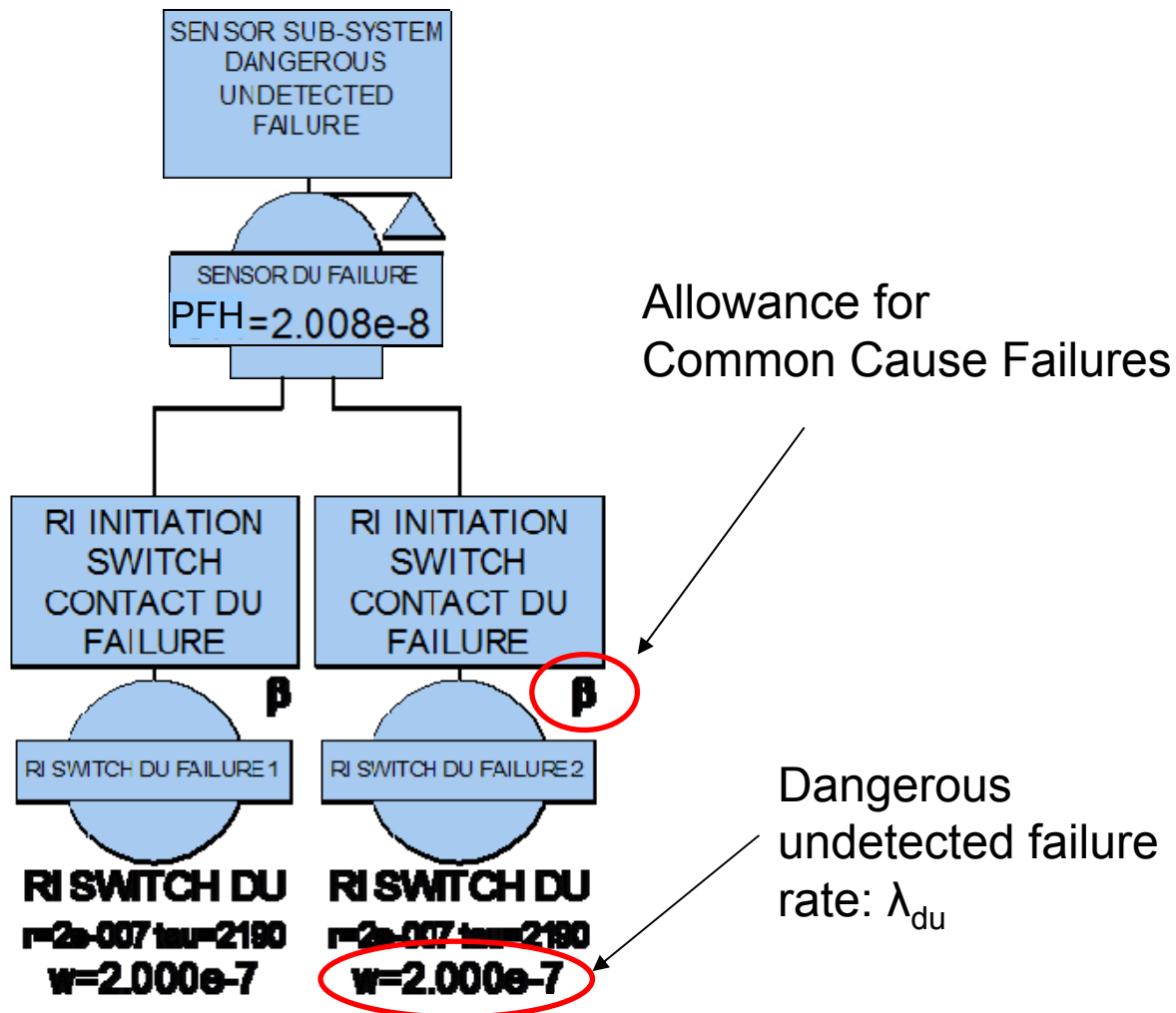
Switch: Using *STF38-A98445 Reliability Data for Control & Safety Systems*

Component / Device Name	Component Description	Total Failure Rate of Component (per hr)	Failure Mode	Failure Mode Apportionment of Failure Rate	Effective Failure Mode Failure Rate
Remote Isolation Switch (single contact set)	Dual pole contact switch	1.10E-06	Dangerous Detected	9%	1.00E-07
Total failure rate and apportionments based STF38-A98445 Reliability Data for Control and Safety Systems, page 67.			Dangerous Undetected	18%	2.00E-07
Total failure rate is consistent with failure rate provided for switches in similar environments in MIL-HDBK-217F, Annex A.			Safe Detected	18%	2.00E-07
			Safe Undetected	55%	6.00E-07

Results of FMEDA:

	1.10E-06	/ hr
λ_s	8.00E-07	/ hr
λ_d	3.00E-07	/ hr
λ_{su}	6.00E-07	/ hr
λ_{sd}	2.00E-07	/ hr
λ_{du}	2.00E-07	/ hr
dd	1.00E-07	/ hr
% Safe Failures	73%	
% Dangerous Failures	27%	
DC _s	25%	
DC _d	33%	
SFF	82%	

Sub-system Reliability Analysis



Architecture Analysis

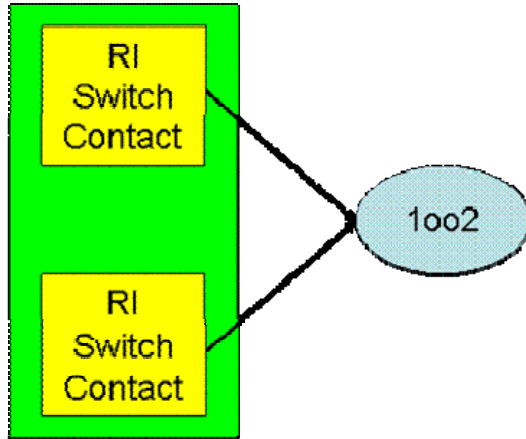


Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

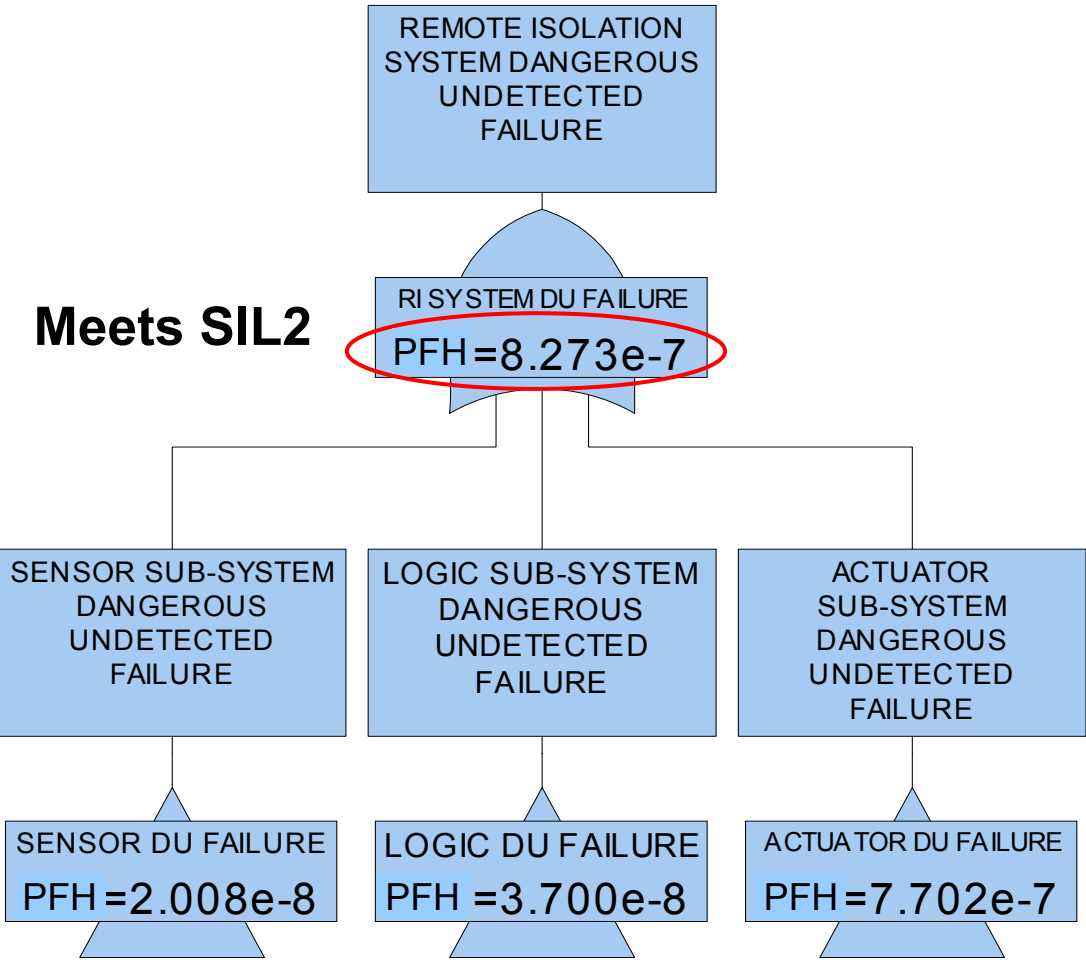
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
 NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.
 NOTE 3 See annex C for details of how to calculate safe failure fraction.

Architectural Analysis

Sub-system type = A
 HWFT = 1
 SFF = 82% (see FMEDA)

Therefore, by Table 2 of AS/IEC61508-2
 SIL Claim Limit (SILCL) = SIL3

System Reliability Analysis



Systematic Failure Avoidance

Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences

Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
Measures against voltage breakdown, voltage variations, overvoltage, low voltage	A.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Separation of electrical energy lines from information lines (see note 4)	A.11.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Increase of interference immunity	A.11.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	HR mandatory	HR mandatory	HR mandatory	HR mandatory
Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
Failure detection by on-line monitoring (see note 5)	A.1.1	R low	R low	R medium	R high
Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
Code protection	A.6.2	R low	R low	R medium	R high
Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
Diverse hardware (see note 6)	B.1.4	– low	– low	– medium	R high
Software architecture	7.4.3 of IEC 61508-3	See table A.2 of IEC 61508-3			

Reference: AS61508 Parts 2 & 3

Conclusion

- The Longwall Remote Isolation and Control System has been extremely reliable since the introduction due to the extensive “Factory Acceptance Testing and Simulation” conducted by Angus Place Colliery and ATF Mining.
- Angus Place will be re-assessing our systems already installed and working to lift the bar and achieve higher Safety Integrity Levels.
- Other Safety Systems that are currently under review include:
 1. Drift Winder System which will include fail safe communications and Remote Isolation.
 2. Conveyor System upgrade project.
 3. Long-wall face Chock Control System - Functional Safety Assessment to be carried out with the OEM.