



Powered winding systems: Experiences and practical tips when seeking plant registration

Presentation to Electrical Engineering Safety
Conference, Penrith 14-15 Nov 2007

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



- Human failures
- Equipment failures - modes - data sources
- FMEA
- Assessing risk. What is unacceptable risk?
- Safety functions of winder
- Determining SIL or Category. Which is preferred?
- Problems with pre-packaged computer programs
- Making safety file traceable and logical
- Older equipment - eg Goninan unit on dolly car
- Be careful with PLC's
- How to deal with mechanical components

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



At the end of this presentation:

- A few terms and concepts demystified
- Know how to ask the right questions
- More confident when dealing with risk and reliability experts
- Know the limitations
- Recognise that data is imperfect. How much buffer do we have?

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Background

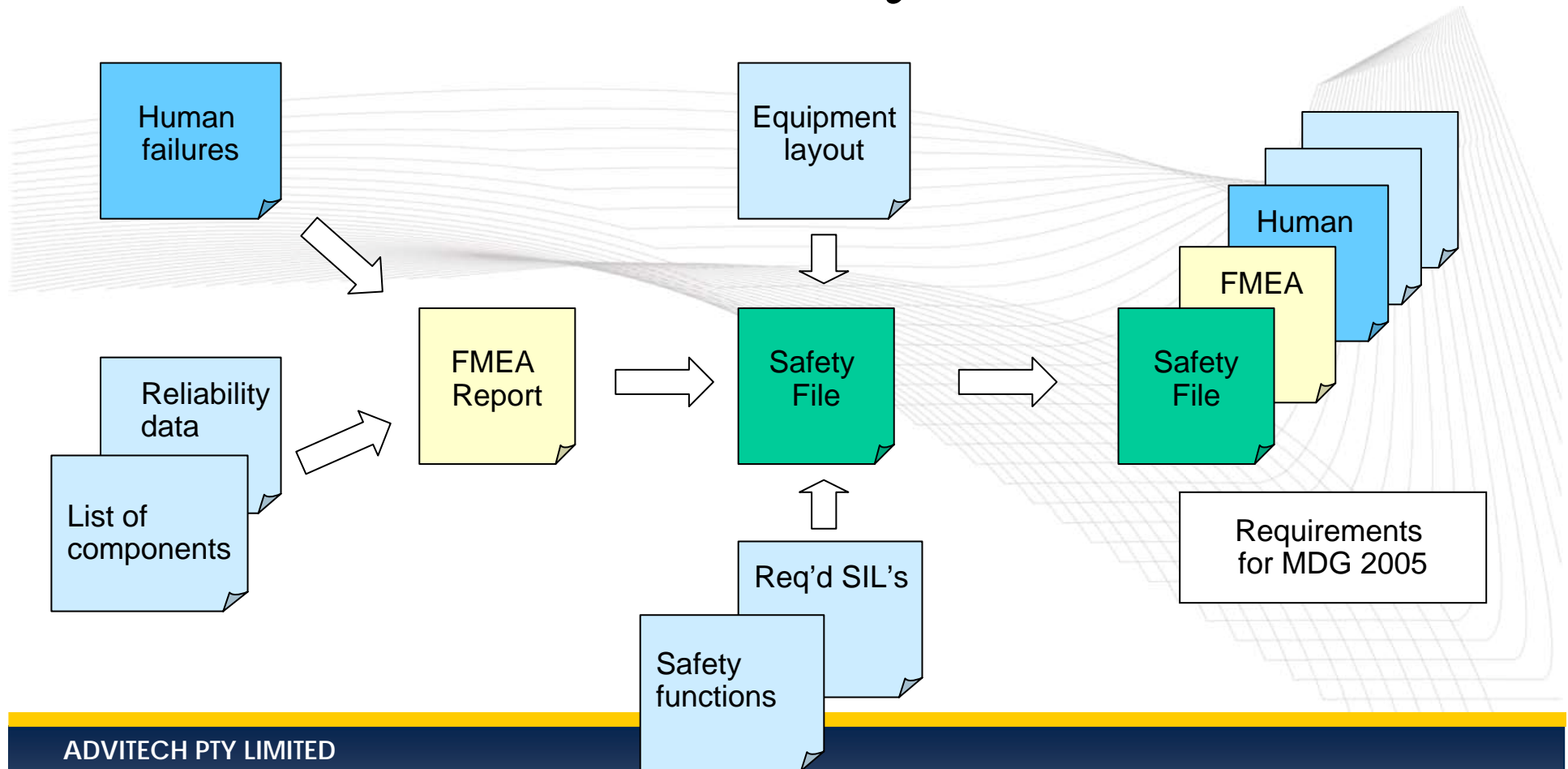
- DPI's Special Projects Program for high risk plant
- Plant registration under latest coal regulations - transitional periods
- Draft regulation for general mining (metalliferous, etc)
- Engineering management plans - control system safeguards as per international standards

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Key element of MDG 2005: The Safety File



ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Human failures

- Consider normal, maintenance and abnormal operating modes for winder
- Apply human error prompt words, eg
 - Slip (right intentions - wrong action)
 - Lapse (forgetful, inattentive - wrong action)
 - Rule-based mistake (right information, wrong action)
 - Rule-based mistake (rules incomplete/ambiguous/wrong)
 - Mistake (new situation - no information - wrong decision)
 - Routine violation (“Everybody does it this way”)
 - One-off violation (various reasons)
 - Deliberate malicious violation (sabotage)
- Aim to have system able to tolerate most of these actions

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA

Ph +61 2 4961 6544 Fax +61 2 4969 3530

mail@advitech.com.au www.advitech.com.au

Equipment failures and FMEA

- List the components used
- Show modes of failure (stuck open, stuck closed, etc)
 - AS 62061 has useful list of devices and failure modes
- Which failures are dangerous?
- At what rate do failures occur?
- Problems in using supplier data
- Adjust for operating conditions, eg increase the published rate if used in harsh environments

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



What is unacceptable risk?

- Lawyer's view of safety: Freedom from risk
- MDG 2005 view: Freedom from unacceptable risk
- ALARP (As Low as Reasonably Practicable): Risk reduction is no longer commensurate with outlay
- Comparative risk: Significantly lower than industry average, particularly if upgrading the equipment
- Can use published long-term fatality rates for Australian and US coalmining
- May be difficult to find fatality rates for particular activities

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Safety functions

Three identified:

- Bringing winder drum (and hopefully dolly car) to a halt upon command
- Bringing dolly car to a halt using on-board systems (eg in event of rope detachment/breakage)
- Removing control power from winder if ultimate over travel is exceeded

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Examples

- Emergency stop button at pit bottom pressed (sensor)
- Sends signal to control system in winder house to stop motor and apply brakes (logic solver)
- Winder mechanical system applies brakes and brings drum to a halt (final element)

- Dolly car sensor (over speed) sends signal to on-board logic solver (eg Goninan unit) to activate different final element (dumps pressure, sets friction pads onto rails)

- Ultimate over travel activates different final element (removes control power)

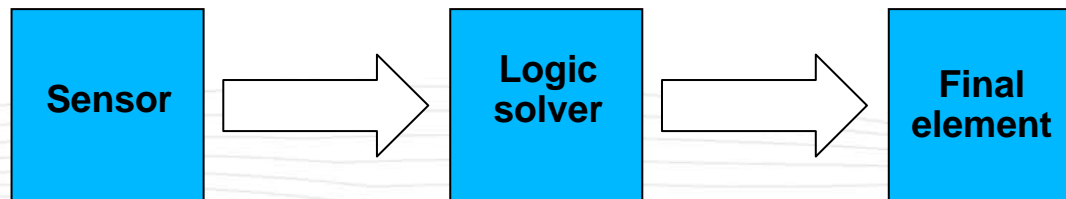
ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Safety systems

- Three different sets of safety systems



- Each needs to be analysed separately
- Need to consider reliability (probability of failure on demand) of sensor, logic solver and final element for each of the three safety functions in turn
- More than just electrical systems involved
- Requires reliability assessment for brakes, springs, friction pads, hydraulic components, etc

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Determining SIL or Category: Which is preferred?

- Advitech's preference is to use SIL (and hence AS 61508) everywhere, even if no programmable electronics involved
- Have successfully applied SIL concept to purely relay-based control systems and mechanical components
- SIL concept provides a logical, traceable path through "proof of safety" in the Safety File
- Risk graphs for both systems quite similar - can apply approximate equivalence using AS 62061

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



Determining SIL / Category

- Break out the safety functions into more detail as required
- Follow the simple instructions in the respective standards to determine the SIL or Category needed to achieve acceptable safety
- Use several determination methods as a cross check
- Decide whether non-safety related controls can provide any improvement
- Use the determined SIL or Category as the specification for the function (ie specifies what the safety system needs to achieve)

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

Problems with pre-packaged computer programs

a)
$$\left(\frac{\pi \cdot D_1 \cdot h}{2}\right) \cdot \left(\text{SQRT}\left(1 + \frac{D_1^2}{4 \cdot h^2}\right)\right) + \left(\frac{\pi \cdot D_1^2}{4}\right)$$

b)
$$\frac{\pi \cdot D \cdot h}{2} \cdot \sqrt{1 + \frac{D^2}{4h^2} + \frac{\pi D^2}{4}}$$

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

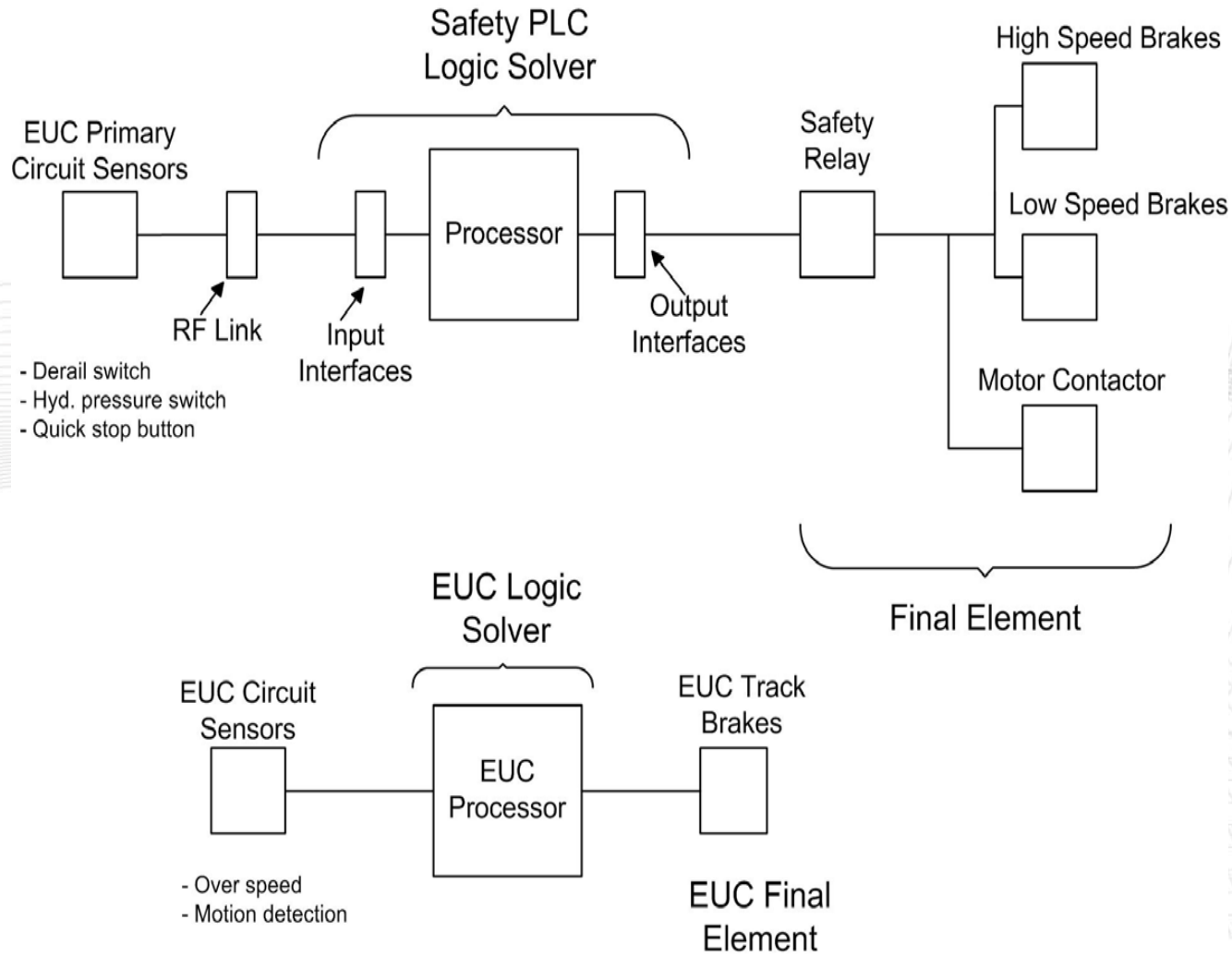


Making Safety File traceable and logical

- Use simple diagrams to show the equipment layout and sequence

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

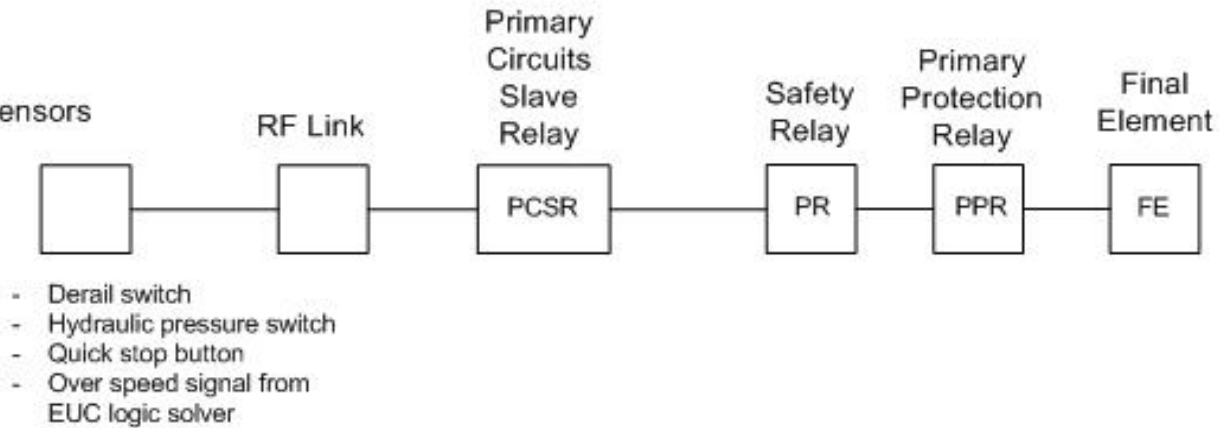




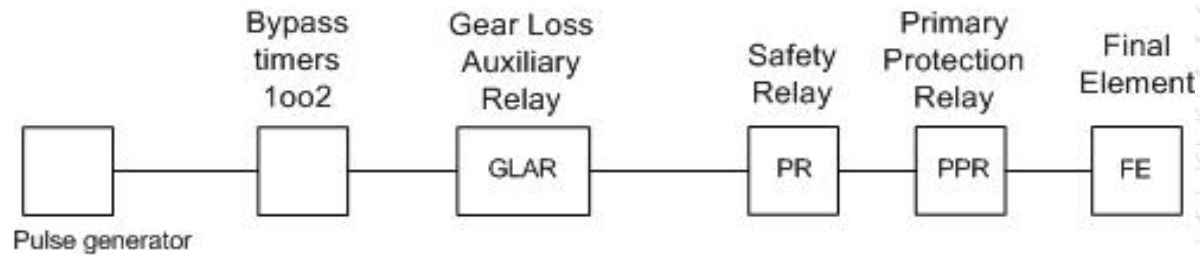
1. E-Stops



2. EUC sensors



3. Gear loss



ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA

Ph +61 2 4961 6544 Fax +61 2 4969 3530

mail@advitech.com.au www.advitech.com.au

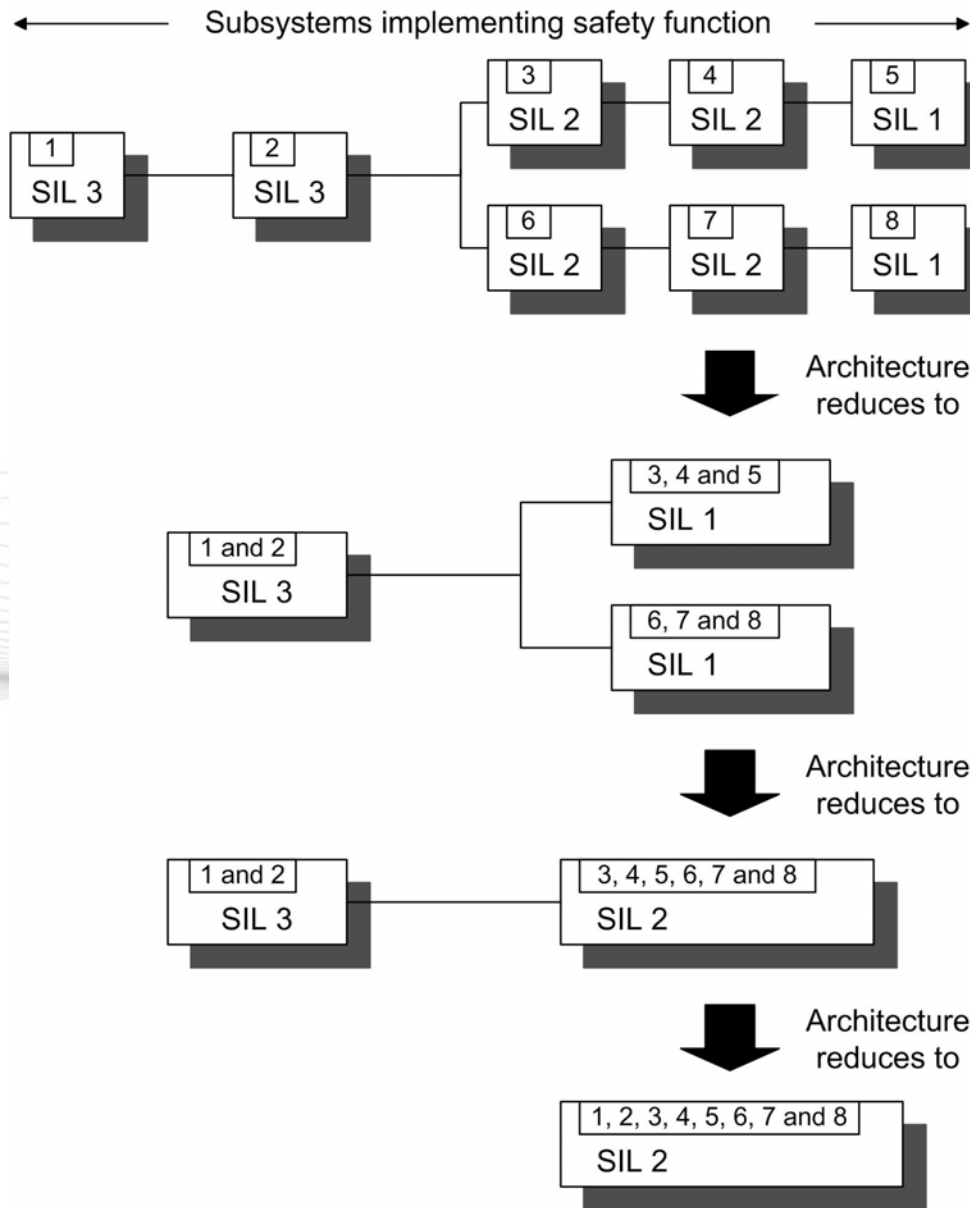


Making Safety File traceable and logical

- Use simple diagrams to show how subsystems are combined to reach an overall system SIL claim
- Keep any computer calculations in the background. Display the logic fully, so that it may be traced at a later date if needed

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

Example calculation - E-stop button subsystem:

- $\lambda = 2$ failures per million hours or 2×10^{-6} failures per hour
- Proportion of dangerous failures = 20%
- $\lambda_D = \lambda \times \text{Proportion dangerous} = 0.4 \times 10^{-6}$ per hour
- $T_i =$ One week or 170 hours

Average Probability of Failure on Demand

$$\begin{aligned} \text{PFD}_{Av} &= \lambda_D \times T_i/2 \\ &= 0.4 \times 10^{-6} \times 170/2 \\ &= 3.4 \times 10^{-5} \end{aligned}$$

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

Dealing with older equipment

- Some items (eg Goninan unit) considerably pre-date modern standards
- Based on current information, have not been able to fully demonstrate reliability using SIL concepts
- Partial calculations used, including Probability of Failure on Demand (meets SIL targets here, but fails other tests)

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

Be careful with PLC's

- Simple, cheap, functional, versatile
- Very commonly used for control functions
- But not reliable - not suited for safety-critical applications
- With powered winding systems, “PLC's” sometimes used for combined control and safety functions
- Such “PLC's” are not the standard type - instead they incorporate redundant systems, internal diagnostics and the like. Sometimes called Safety PLC's.
- More expensive, but bring considerable advantages.

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



How to deal with mechanical components

- Treat like any other component - determine failure modes; which ones are dangerous; failure rates
- Examples: Directional control valves, pistons, caliper springs, friction pads, discs, shaft attachments, etc
- Tip: Failures of certain components such as levers, hinge pins and the like may be excluded, on the grounds that their rate of failure is low compared with other items. Standards offer guidance on this.

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

How much buffer do we have?

- If using SIL concepts, calculated probabilities of failure are compared to target bands for the desired SIL
- If just inside the band, then buffer or margin against questionable input data is low
- Expect data to be questionable. Aim for calculated probabilities to be well inside band, with buffer of perhaps a factor of five or more.

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au

- Start with operating modes, looking for human failures that might suggest design changes
- List the components. Gather data for FMEA. Be careful with supplier data.
- Use FMEA data as input to Safety File. Use a traceable, logical approach.
- Analyse reliability of full function - right to mechanical final element
- Consider using SIL concepts - may well be easier than Categories
- Estimate the buffer in hand. Expect input data to be incomplete or questionable.

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au



End

- Thank you for your interest and attention
- Questions please!

ADVITECH PTY LIMITED

1 Elizabeth Street, Tighes Hill NSW AUSTRALIA
Ph +61 2 4961 6544 Fax +61 2 4969 3530
mail@advitech.com.au www.advitech.com.au