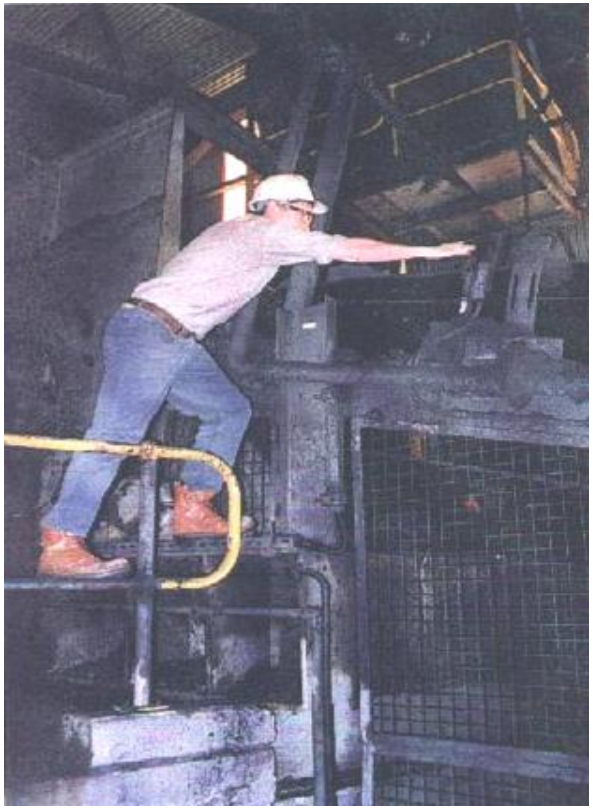
Case Study:

Safety in Design Process Development



Mike Hurd, representing…

ENGINEERING SYSTEMS MANAGEMENT

ElectraNet

ENGINEERS AUSTRALIA

SA Division

Engineered Safety

Special Interest Group

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Contact details

Engineering.Systems.Management@gmail.com

Mike Hurd

0432 858 958

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

This is what it is all about

Design-related issues contributed to **37%** fatalities studied (total 210 researched incidents) and **30%** of serious non-fatal injuries.

Half of all accidents in construction could have been prevented by designer intervention

Equipment designers of tools, plant and equipment could have reduced the risk in **60 of 100** accidents.

Statistics quoted from Australian and UK safety authorities

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

What is Safety in Design?

Practice / tool / technique	Used for….
Safety in Design	What will be the 'human-to-asset', and environment-to-asset interfaces, and how can we make them safer?
Systems Safety	Understand top-level concepts of operations & functional reqt's, identify the hazards and then the safety functions to control them
HAZOP studies per AS IEC 61882	Analysis of what happens when design are operated **outside its design intent**
SWIFT	Subjective what-if technique. Good for operator interactions with / into a system (less formal / faster than HAZOP)
FMEA per AS IEC 60812 (FMECA, FMEDA, process FMEA)	What if a component fails whilst operating within design intent? Analysis of predicted, random failure rates of new designs / mod's
QRA/ PRA & Bow-tie analysis; Event tree & Fault tree analyses	Typically: incident causation and consequence analysis. Something has gone wrong…what next? (Actual or postulated)
LOPA (Layers of Protection Analysis)	What diverse means of achieving safe states dare there, in case one fails?
Functional Safety per AS IEC 61508/61511	Justification of electrical, electronic, programmable system performance. "The safety of functions."
Major Hazard Facilities	Legislation supported by guides from Safe Work Australia (Good model of systems safety)

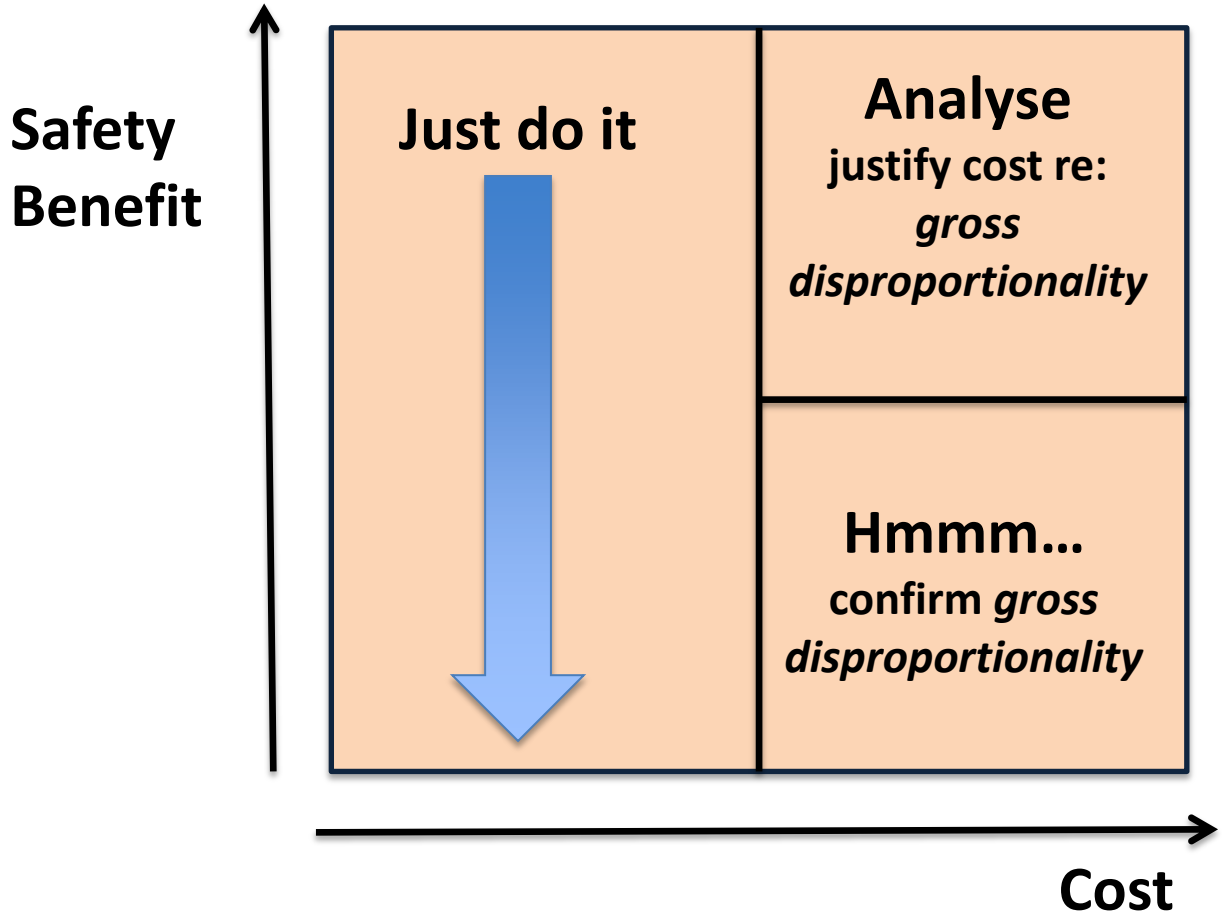
Comments on safety practices, tools & techniques

- When discussion these matters with other safety professionals, there are a lot of ways to achieve safe outcomes, and people have preferred processes.
- A lot depends on individual experiences. Sometimes, there are “no rights and wrongs”, sometimes there are!
- **My opinion:** be careful which messages you adopt for your context, and tailor advice and information to your needs

Why do we need a Safety in Design process?

- You don't, if your engineering process covers the requirements
- However, Identifying SiD as a process is 'in vogue' & easy to communicate
- Need to answer: "*Can we make it safer SFAIRP?*"
- *More later…*

SFAIRP & reasonable practicability: our understanding



Is this different from the ALARP principle?

Are these ALARP studies?

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Safety in Design

If it can happen, it will happen

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Context - ElectraNet

- ElectraNet is SA's high-voltage transmission network service provider (TNSP)
- 275kV and 132kV transmission network
- ElectraNet contracts-out a lot of design and construct (D&C) packages and maintenance
- For substations, transmission lines, telecommunication systems
- ElectraNet also does detail design

Context – timescale – 2 years in development

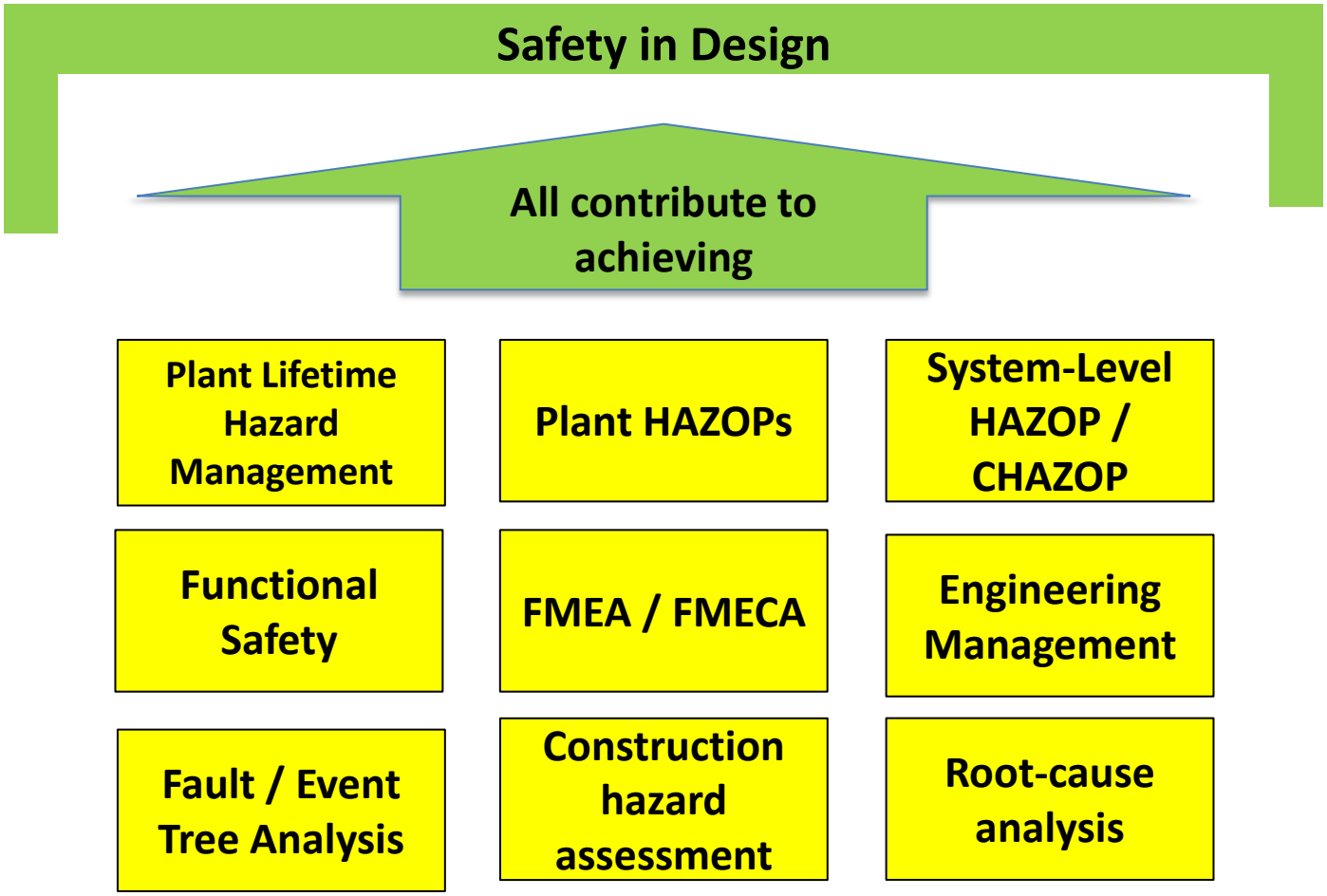
Hamish McCarter has 'championed' process development

- April 2011 Kick-off: Hamish presents to exec: "Current approach best described as 'informal and ad-hoc'"
- June 2012: Gap Analysis & strategy to 'fill the gaps'
- Nov 2012: Minimum requirements to meet WHS legislation available within ElectraNet
- Nov 2012: SiD Working Group inaugurated
  - 2 lifecycles: review process, then support SiD
- June 2013: Process and training developed
- 15 July 2013: AMC endorsed SiD for all new projects

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

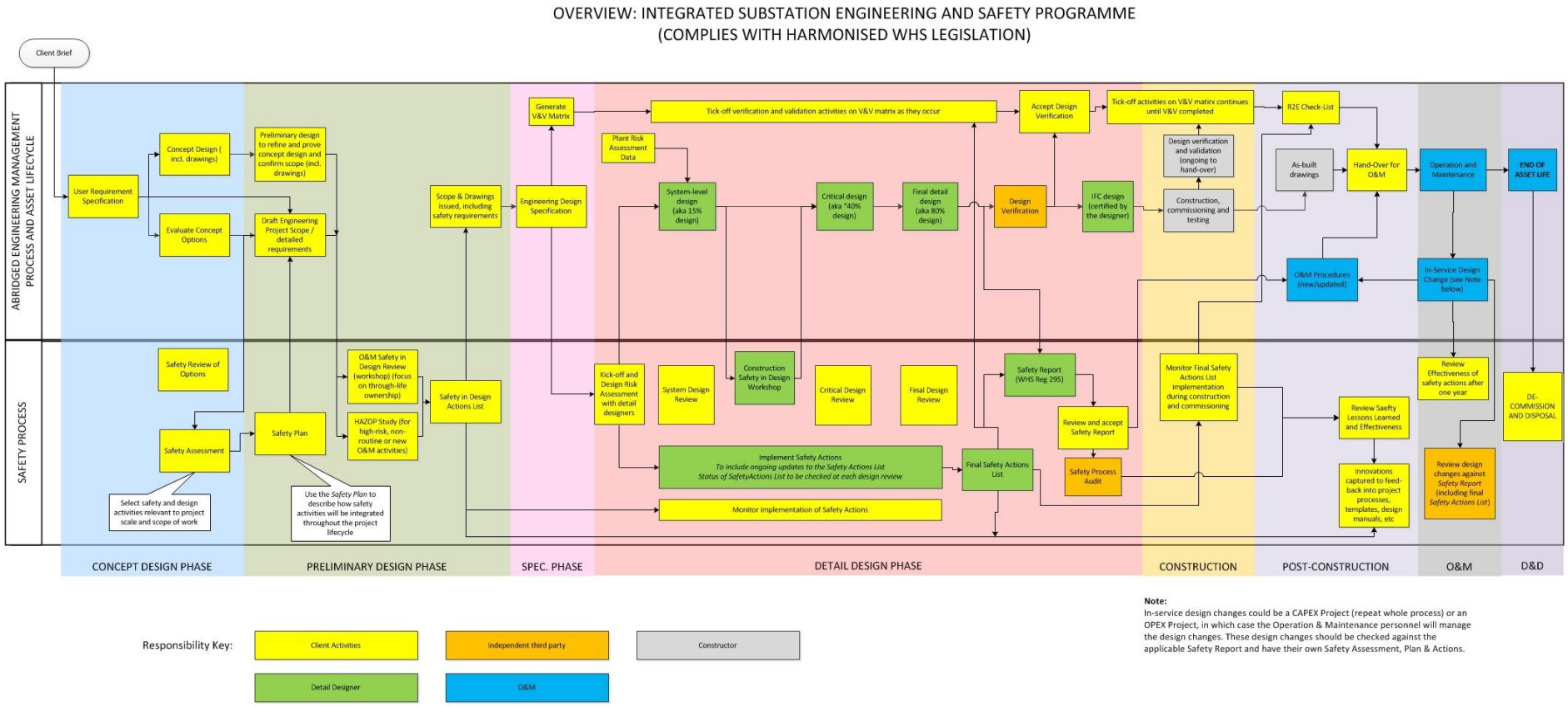
Context: ElectraNet SiD 'Umbrella' over design tools



ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Context: the process



ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Process design

A **structured and systematic process** to reveal hazards and how to eliminate them SFAIRP, or reduce the risks associated with them SFAIRP

Promotes **safety thinking from early in the design process**

Is **not a risk assessment** (as with CHAIR and HAZOP)

The procedure is based on:

- A systems-engineering approach to integrating safety and engineering
- WorkCover NSW's 'CHAIR' process (Construction Hazard Assessment Implication Review)
- HAZOP study workshops, as per AS IEC 61882

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Context – ElectraNet – lots of external stakeholders

The process is designed to comply with guidance / requirements from:

- Work Health and Safety (WHS) 2012 legislation
- The Electricity Act
- Safe Work Australia / SafeWork SA
  (Code of Practice for Safe Design of Structures)
- AS 5577: Electricity network safety management systems
- Energy Networks Australia
- Electrical Regulatory Authorities Council (ERAC)
- Cigré
- Standing Council on Energy and Resources (SCER) (formerly MCE)
- Australian Energy Market Commission (AEMC) (the NER)
- The Essential Services Commission of South Australia (ESCOSA) and the Electricity Transmission Code (ETC)

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Two key process steps

The **assessment form** tailors the SiD program to the scope, scale and complexity of the project.

- It's a very important step! Makes the process practical
- Also achieves buy-in from the start

SiD Review is the process 'cornerstone', to identify:

- What tasks will be carried out throughout O&M?
- What hazards will be presented to end users when carrying out these tasks?
- Are there things we can do during design to make the tasks safer?

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

SiD Reviews ('workshops')

Analyse tasks carried out during:

- Operation & Maintenance
- Outages
- Planned Upgrades
- Decommissioning
- Disposal
- **Construction**: separate workshop

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Foresight: Asset Lifecycle

Engineers need to demonstrate CONSIDERATION and FORESIGHT throughout:

CONCEPT
ASSESSMENT
DESIGN
MANUFACTURE
TRANSPORT
CONSTRUCT
COMMISSION

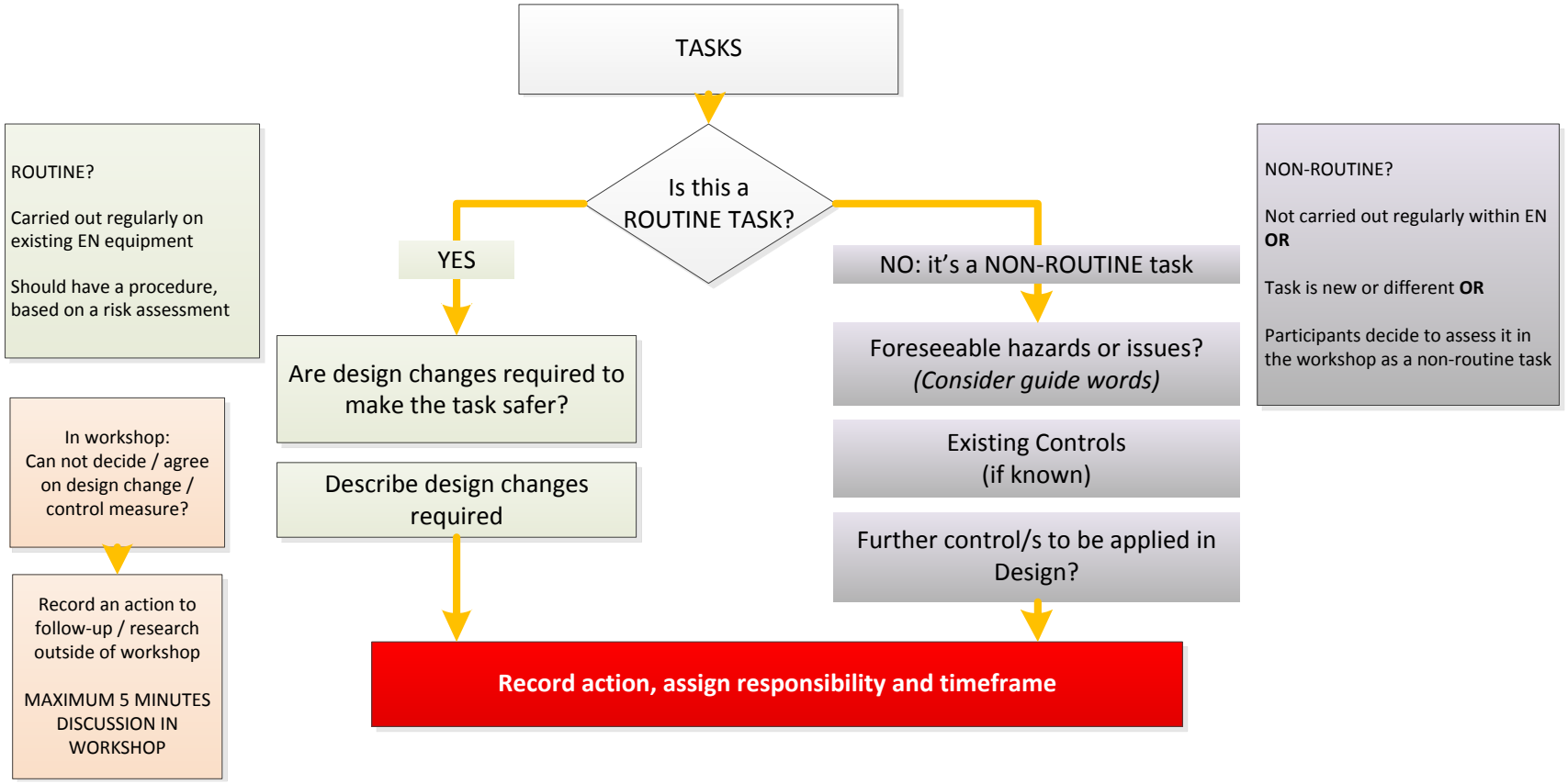
USE / OPERATE
MAINTAIN
REPAIR
REFURBISH
MODIFY
DECOMMISSION
DEMOLISH
DISMANTLE
DISPOSE

Bold items = ElectraNet activities

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

SiD Reviews ('workshops')



ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Communication is key!

- The ‘cornerstones’ to SiD are the two reviews and the actions identified
- To get the most benefit, consultation needs to commence prior (refer to previous slide)
- Investment in SiD will pay for itself as long as the actions are addressed
- Communicate at each stage: ‘pass the baton’: it’s part of the responsibility under the WHS Act

Case Study: Strategy and Planning

- SiD is nothing new
- ElectraNet already had some good safety processes, but they were not coordinated with respect to design
- People had different perceptions about what SiD is and means, and who is responsible for it
- Legally, it was assumed by some that SiD was the prerogative of detailed designers
- Achieving SiD is an engineering discipline, and needs the support of:
  - the WHS team (or OH&S / SQE etc team)
  - Risk Manager
  - Legal team
- AS/NZS ISO 31,000 alone does not achieve SiD
- **What people believe is occurring and what is actually occurring are sometimes different**
- Couldn't find OTS solution

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Case Study: Developing the new process

- The process was developed under ElectraNet's EMS
- ElectraNet also developed a Plant Risk Assessment procedure
- The new process is very good: certainly 'a best practice"
- ElectraNet use the SiD process as the umbrella for all safe design tools
- People need to be reminded to check what actually goes wrong (historically) to help them focus on the key issues in SiD
- As with HAZOPs, it is important NOT TO rank likelihood and severity during SiD reviews.

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Case Study: Developing the new process

- **The use of check-lists evokes a lot of debate**
- There are misunderstandings and differing opinions about ALARP and SFAIRP
- SiD requires a systematic process to ensure coverage
- Addressing SiD assists adopting in the field: new processes, tools, techniques and equipment types
- SiD needs to be integrated with the engineering management process, 'cradle to grave'
- Present Value (PV) models, used to assist decision making, are contradictory to SiD ideals

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Case Study: Deploying the new process

- People don't have the time for it! So how to engage them?
- SiD requires leadership and tenacity to implement safe features and engineered safeguards as opposed to creating a tick-list of why "everything is already OK'
- Needs a 'coalition of support' in the business
- **Selling the added value of spending up-front can be very difficult!** Yet it makes so much sense.
- It takes time to change a culture
- Need to take key contractors for the ride
- PMs and cost controllers need to buy-in, and **they need support from the executive**
- **The SiD Working Group was an excellent thing to have done**

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Case Study: Using the new SiD process

- Tailoring the process to ElectraNet was a good move
- **Human behaviours towards, and reactions to, SiD requirements is an issue throughout: the SiD process; designs; costs; implementation; working on-site.**
- "Demonstrating foresight" (WHS requirement) is like pulling teeth
- The process has to be detailed and thorough, yet practical
- Got to allow time and cost
- SiD COSTS MONEY – AND PEOPLE DO NOT LIKE THAT - Tailor SiD programme to scope, scale and complexity of the design
- Some engineers do not enjoy going through systematic procedures.
- Need to reign-in the sensationalists!
- What IS a standard?
- Clear engineering authority is important
- Communication is key
- Everyone is busy!

ESM ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Case Study: Training

- Training has been essential
- Internal and key contractors
- People need to discover and then learn about SFAIRP and ALARP and the implications of them
- Understanding what SFAIRP means to the organisation and to projects is important
- Hazard capture workshops need to be driven to succeed

Training courses

ElectraNet has two training courses tailored to its SiD process:

Module 1: Understanding Safety in Design
for participants and practitioners
"Why?"
4 hours classroom, 2 hours after class

Module 2: ElectraNet Safety in Design
for practitioners (typically engineers and designers)
"How?"
2 hours classroom, 3 hours after class

On-line training / induction module for all staff in development

First application of the process: new substation

- Approx. 140 SiD actions on a 2-3 year, $40M project.
- Only 100 were related to safety: 40 were design or information-related actions.
- Actions fell into 4 categories:
  - **"Just do it"** – cheap things that improve safety
  - "**Err…not sure**" – analysis required. This is especially true for the high-cost safety features that may save a minor injury in 20 years' time. It's hard to determine what is reasonably practicable, especially if PV models are used in the cost/benefit analyses.
  - "**Need to do more work**" – further meetings / analyses / data required to make determination whether something will improve safety.
  - "**Check the standard**" – Working in accordance with standards is a very good indication that you are safe SFAIRP. Usually, participants in SiD reviews don't know the standards sufficiently to decide at the meeting.

First application of the process: new substation

Out of the 146 actions, around 6 are double-ups. Assuming 140 actions:

- 78 relate to safety of people (mostly of personnel as opposed to the general public)
- 12 relate to equipment safety (hence security of supply)
- 3 relate to environmental safety
- 11 relate to all three
- 26 are design issues
- 10 are not design or safety issues

In percentages:
74% safety
19% design
7% other

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Hindsight

- **HAVE A GUIDE BOOK** with pictures in – give to all engineers – it brings it all to life. Include generic SiD requirements – helps with: *"So what am I actually trying to do?"*
- Hamish: *"We really needed to follow something like Kotter's 8 step change model, starting with establishing urgency (which the workplace harmonization laws under the WHS helped achieve)."*
- Me: we did this pretty well!

Almost closing comments

- **Do you need a SiD process?**
- Yes, if you are not capturing SiD requirements in your design requirement specifications
- I still believe SiD is better integrated into the User Requirements process (and that capturing SiD requirements at the user-requirement stage is a good way to save money in the long term)
- The longer you leave it, the more rework: rework is a ‘time and cost killer’.

Comments on tools, practices, techniques

- When you get talking about these matters with other safety professionals, there are a lot of ways to achieve safe outcomes, and people have preferred processes.
- A lot depends on individual experiences. Sometimes, there are “no rights and wrongs”, sometimes there are!
- The net result is that you have to be careful who you listen to.

Further information

- Safe Work Australia's *Code of Practice for the Safe Design of Structures*
- Safe Work Australia's guide to *reasonably practicable*
- AS IEC 61882 for HAZOP studies (HAZOPs are required for new, novel or high-risk human-to-asset interfaces, eg: new construction techniques)

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems