Perspectives on:
Safety in Design

Presentation at EA, Adelaide, 20/4/16

Mike Hurd
Engineering. Systems. Management. Pty Ltd, Adelaide.

ENGINEERING
SYSTEMS
MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Safety in Design – where has it come from?

Safety in Design is a contemporary term that has become common in the context of the harmonised WHS-legislated duties of designers, and draws attention to procedures and steps that would ideally be built-into engineering and project-delivery processes but sometimes are not.

In the absence of such processes, having a <u>specific SiD process</u> is a good way to draw attention to the requirements until it becomes embedded as an organisation's 'business as usual'.

Perspectives

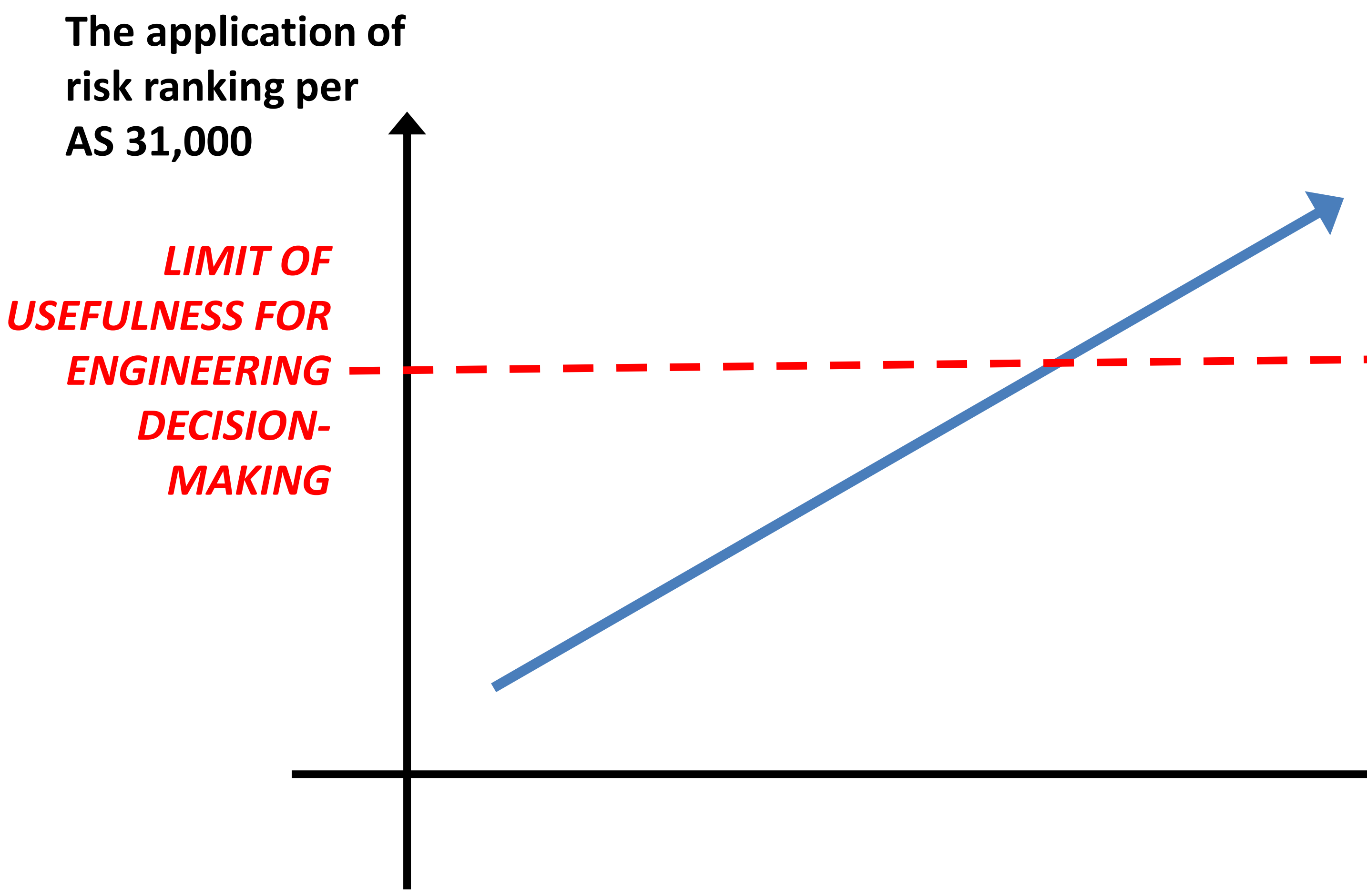
- **What is SiD?**
  - *Safe Design (SD)*
  - *Safety by Design (SBD)*
  - *Safety through Design (STD)*
  - *Engineered Safety*

- What **isn't** SiD?
  - *Intrinsic safety (that's different)*
  - *Risk Assessment*

- Where has risk assessment gone wrong?

- **What does success look like?**

Perspective: risk assessment gone too far



The issue is BEHAVIOURS, not the principle.

My Perspectives:
Safety in Design – 1 of 2

- **My view was that SiD represented a failure in the design process to address the user requirements, construction and maintenance safety requirements**
- **I didn't 'get' what SiD was doing**
- **My engineering 'upbringing' in defence** was that safety was addressed through requirements capture and systems engineering.
- **The shocks outside defence**:
  - *What URS? What spec? What interfaces? What integration? What systems engineering? What traceability? What configuration management?*
  - The 'traditional approach': Going straight from brief to design!
- **First experiences of SiD**
  - No targets set, as I would expect for functionally-safe designs
  - Variable attention to maintainability & through-life support in the design
  - Good formats, and good outcomes, but incomplete owing to **lack of time**!
- **Revelation**: SiD is a systematic, structured process for analysing the human-to-asset interfaces (and asset to environment). It is different from a HAZOP because HAZOP is intended to analyse deviations from design intent.

My Perspectives:
Safety in Design – 2 of 2

- **The surprising revelations of the harmonised WHS laws**
  - Previous OH(W)&S laws covered duties of designers, but less explicitly
  - The usage of SiD as a ‘thing to do’ and code of practice
  - Not a concern, if you have an engineering management system / process
- **Recognising the value of labelling “SiD**” as a ‘thing to do’, because it does not appear to be done well otherwise
- **Splitting–out** SiD in my generic Engineering Process Map
- **Developing** the ideas, testing and refining
- **Cultural barriers** to eliminating hazards / reducing risks SFAIRP:
  - Too much to do; too costly
  - What value does this add?
  - We don’t need it
- **Current status:**
  - SiD has a place, because the profile needs to be raised to address the **statistically significant safety problems**
  - I still believe it reflects ‘not doing things properly in the first place’
  - It would be nice to SiD ‘melt-away into’ doing things properly.
  - There is still confusing between SiD, PHA, HAZOP, FMEA, risk assessment, etc

What is SiD?

Throughout design, keep asking yourself and each other:

Can we make it safer?

<u>And if not, why not?</u> (under WHS legislation you needs to be able to demonstrate *reasoning* and *justification*)

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

Are things getting safer?

2002 NOHSCC Findings:
37%

2012 findings
36%

2015 SafeWork SA (anecdotal / not researched)
30%

… incidents, injuries or fatalities could have been averted at the **design stage.**

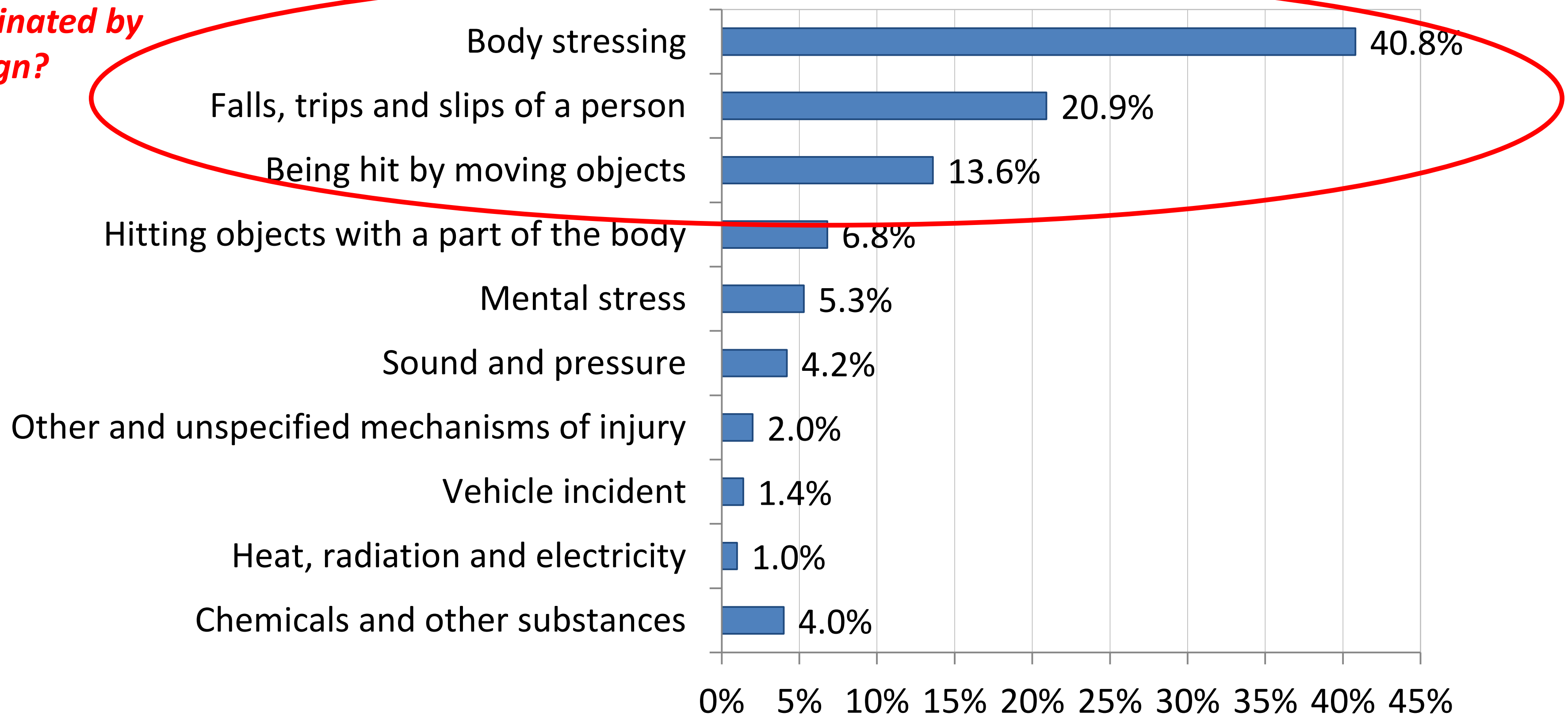
ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Australian Workplace Injuries

Serious Claims: Percentage by Mechanism of Injury/Disease, 2009-10

Surely, these can be eliminated by design?



ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

The design stage…

CONCEPT	ASSESS-MENT	DESIGN	MANU-FACTURE	CON-STRUCT	COMM-ISSION	IN-SERVICE	DECOM./ DISPOSE
Brief / URS / Concept design	Options Scope Specif’n	Detail design	IFC	As-built	Changes Mark-ups DCC	Mod’s, upgrades refurb A&A	Mod’s
Engineer	Engineer	Designer	Designer	Engineer/ Designer	Engineer	Engineer	Engineer

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

What is SiD?

Safe Design = Good Design

It's a simple equation

What is good design?

Good Design = Good Engineering

What constitutes good engineering?

Before doing any design work:

- Competent people
- Design Change Control procedure, through-life
- Verification and Validation process
- Engineering Authority Structure
- Engineering process

Per piece of engineering or design work (per project):

- Information transfer plan
- Human-to Asset interface matrix
- Requirement Specification (or URS)
- TALK to users
- Spec. for detail design

What is Engineered Safety?

Practice / tool / technique	Used for….
Safety in Design / PHA (Also ‘CHAIR’)	What will be the ‘human-to-asset’, environment-to-asset, and asset-to-asset interfaces, and can we make them safer?
Systems / Process 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	Systematic 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). Requires a **SAFETY CASE**

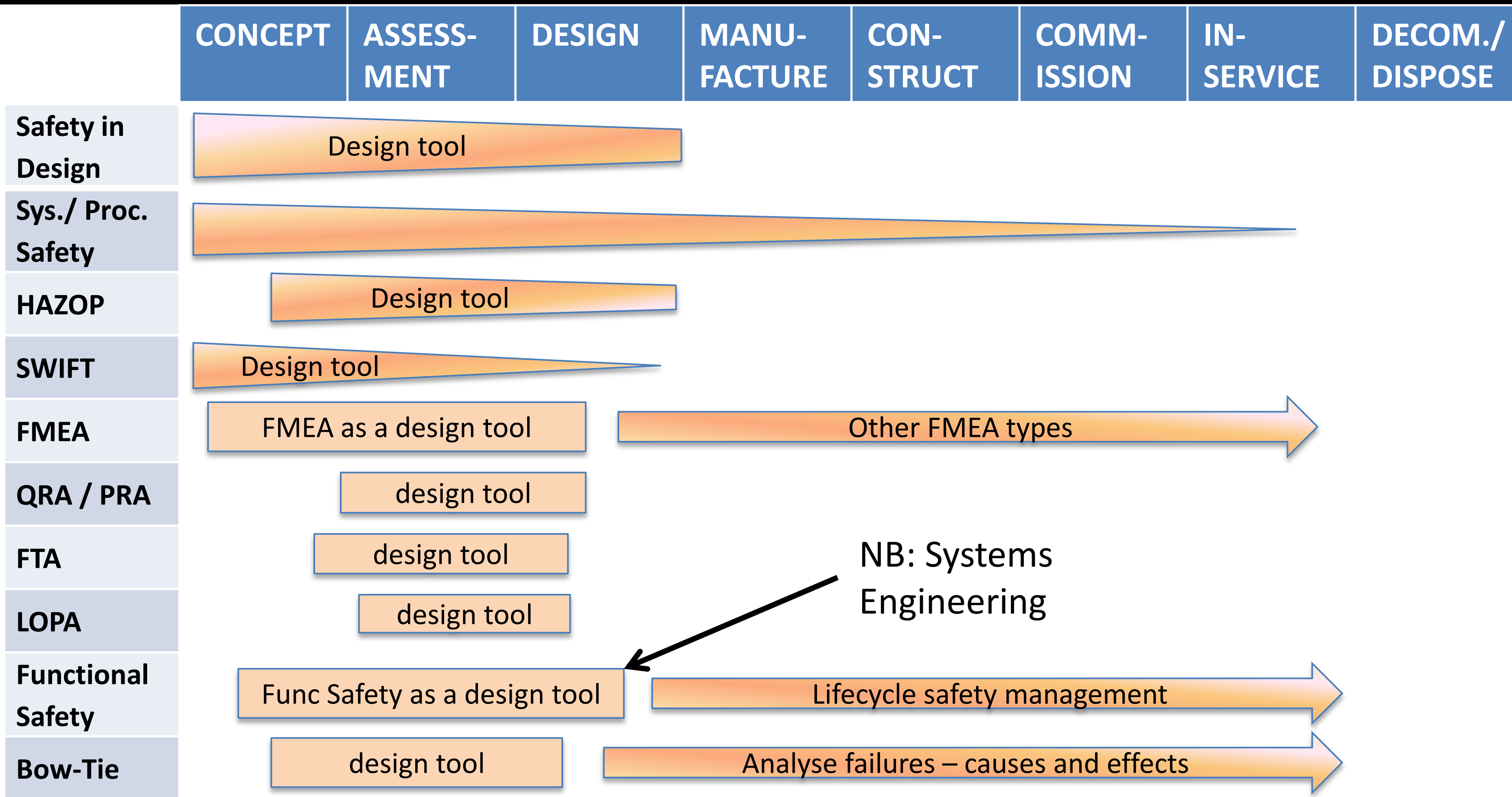
Context: SiD 'Umbrella' over design tools

Safety in Design

All contribute to achieving

Plant Lifetime Hazard Management	Plant HAZOPs	System-Level HAZOP / CHAZOP
Functional Safety	FMEA / FMECA	Engineering Management
Fault / Event Tree Analysis	Construction hazard assessment	Root-cause analysis

Engineered Safety: tools, practices and techniques, and their applicability throughout the engineering lifecycle, indicating effectiveness



ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Ten Steps of SiD

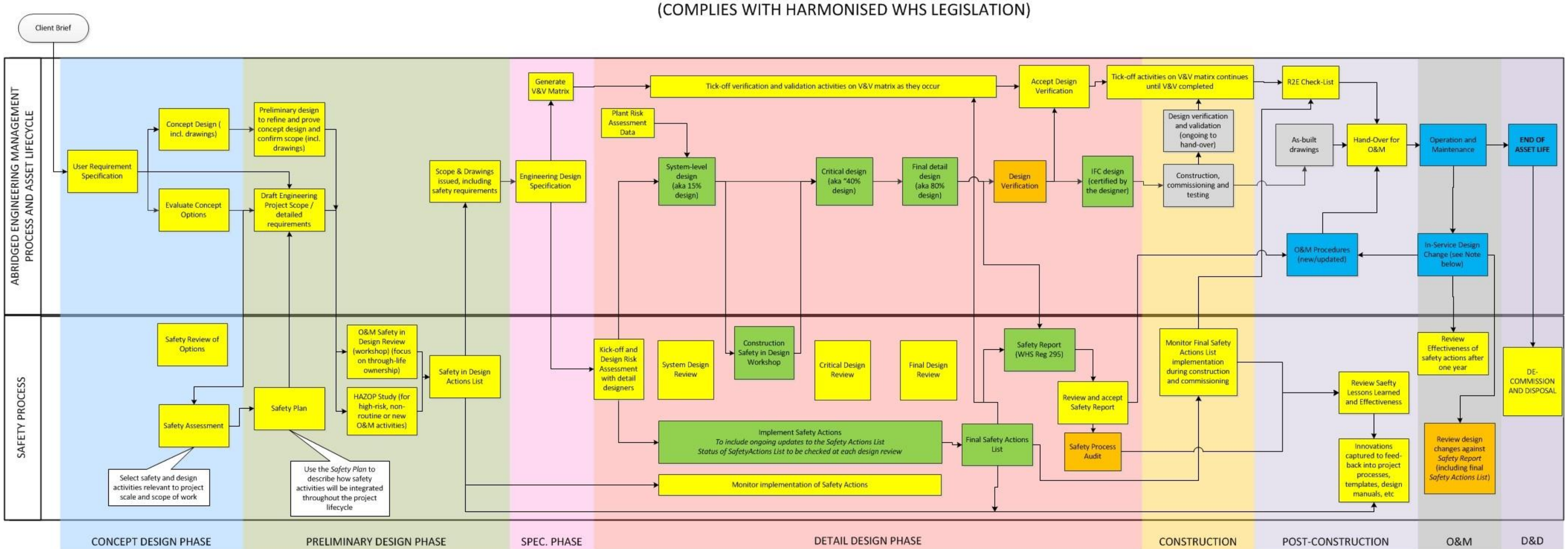
1. LESSONS LEARNT
2. DETERMINE SAFETY IN DESIGN REQUIREMENTS:
3. EARLY ENGAGEMENT OF O&M / HAZARD REGISTER:
4. CONDUCT OTHER SAFETY STUDIES
5. ALIGN UNDERSTANDING
6. EARLY ENGAGEMENT OF STAKEHOLDERS (CONSTRUCTION & COMMISSIONING)
7. LIVE HAZARD TRACKING
8. INFORMATION TRANSFER & **Safety Report** (SiD Report) (WHS Reg 295)
9. VERIFY AND VALIDATE SAFETY IN DESIGN ACTIONS
10. SAFETY IN DESIGN LESSONS LEARNT

Safety in Design – Ten Steps *(A minimum set of activities?)*

	WHAT?	DELIVERABLE	WHEN?
1	**Find lessons learned** *Put them in the requirements spec.* *Start a hazard register*	Lessons learned list / hazard register. Keep it live throughout the project.	At the start of design / after the brief / as part of writing the R Spec
2	**SiD Impact Assessment** *Determine SiD requirements*	Signed assessment form	When there is a concept to conduct a meaningful assessment
3	**SiD Management Plan** *Who does what, when?*	Signed plan, with project plan / design plan (or within one of them)	When you know the preferred engineering / design option
4	**SID Review of O&M** *Early engagement of O&M / HAZARD REGISTER*	Updated hazard register, With hazards, and means to address them, per hierarchy of controls. Confidence in the design	When you have a draft scope
5	**Other safety studies** *HAZOP, FMEA, bow-tie, etc*	Study reports	Per the plan: when they are appropriate in the design lifecycle
6	**Align understanding: SiD programme and roles and responsibilities** *1 hour meeting*	Meeting minutes, signed	At D&C contract kick-off meeting(s)
7	**SID Review of Construction and Commissioning** *Early engagement of C&C staff / update HAZARD REGISTER*	Updated hazard register, with hazards, and means to address them, per hierarchy of controls. Confidence in the design	As soon as there is sufficient information to review. Around 15-40% detail design (scheme design, general arrangements)
8	**Keep track of identified hazards**	Updated hazard register	Throughout the design lifecycle, and into O&M
9	**Safety Report (SiD Report)** *WHS Regulation 295 for Structures – and plant too, according to the guidance for plant*	SiD (Safety) Report	At the end of Detail Design, with the design report. *Format not specified, eg: can put on a drawing.*
10	**Capture lessons learned**	Lessons learned in single register in the organisation	Throughout

Process integration

OVERVIEW: INTEGRATED SUBSTATION ENGINEERING AND SAFETY PROGRAMME
(COMPLIES WITH HARMONISED WHS LEGISLATION)



Responsibility Key:

Client Activities	Independent third party	Constructor
Detail Designer	O&M	

Note:
In-service design changes could be a CAPEX Project (repeat whole process) or an OPEX Project, in which case the Operation & Maintenance personnel will manage the design changes. These design changes should be checked against the applicable Safety Report and have their own Safety Assessment, Plan & Actions.

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

The Requirement Specification

Requirement Categories

Lifetime
Availability
Reliability
Maintainability
Spares
Refurbishment
End of Life
Replacement
Decommissioning
Disposal

Function
Performance
Environmental compliance
Safety Engineering
OH&S
Delivery
Cost/financial
Project Management
Policy
Interface - External to system
Interface - Internal to System
Environment (impact on)
Through-Life Support
Physical characteristics
Resources (people, money, time, tools, materials)
Design Process
Security or privacy
QA. QC & certification

Foresight in the 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 = client activities?

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Human-to-Asset Interfaces

You can do this for environment-to-asset interfaces too

ASSET LIFECYCLE HUMANS	*CONSTRUCT*	*COMMISSION*	*HAND-OVER*	*OPERATE*	*MAINTAIN*	*D&D*
Trades / Skilled	✓	✓				✓
Visitors (‘*bloody engineers*’)	✓	✓		✓	✓	
Surveyors	✓				✓	
Maintenance staff					✓	✓
Cleaners			✓		✓	
Inspectors / auditors	✓	✓	✓	✓		✓

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

Foresight: Asset Lifecycle

Engineers need to demonstrate CONSIDERATION and FORESIGHT throughout:

CONCEPT
ASSESSMENT
DESIGN
MANUFACTURE
TRANSPORT
CONSTRUCT
COMMISSION

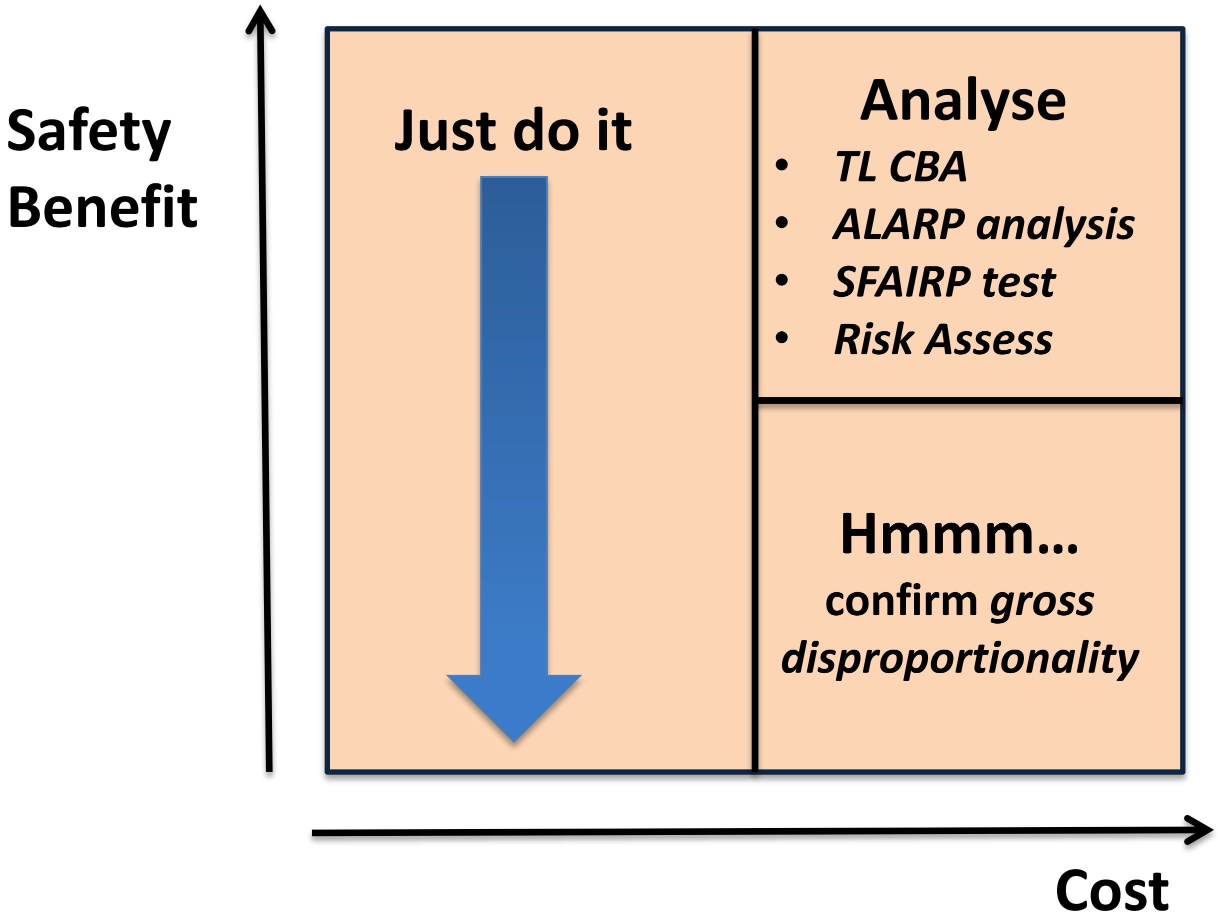
USE / OPERATE
MAINTAIN
REPAIR
REFURBISH
MODIFY
DECOMMISSION
DEMOLISH
DISMANTLE
DISPOSE

Bold items = client activities

ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Reasonable Practicability



ENGINEERING SYSTEMS MANAGEMENT

Engineering Management
Systems Engineering
Management Systems

Contributors to a safe state:

Safety Culture:

- *Recognition of differences between OHS, Engineered Safety (System safety, process safety)*
- *Recognition of the different tools, practices and techniques that give-rise to safe assets*

Leadership:

- *Top-down, messages and belief*
- *Governance structure in-place*
- *Chief Engineer, with authority to say "NO" and 'STOP'*
- *Clear Engineering Authority*
- *Proper gate reviews*
- *Stick to the Processes: agree how to apply (tailor) them up-front, then nil acceptance of cutting corners*

Engineered Safety

Engineering Process:

- *Requirements Spec*
- *User's consulted*
- *Stakeholder Consultation*
- *Standards baseline*
- *Spec for detail design*
- *Competence throughout*

Training:

- *Engineering Processes*
- *Safety tools and practices*
- *Governance*
- *WHS legislation: PCBU, Officer, Worker, duties of all, etc*
- *Roles and responsibilities*

Review:

What is SiD?	Clear, mandatory steps throughout the engineering and design lifecycles, to plan for and address safety requirements (focus on HAZARDS). The PROPER application of the tools, practices and techniques that give-rise to safer outcomes
What isn't SiD?	Risk ranking, single workshops, the application of AS 31,000
Where has risk assessment gone wrong?	Over-use of risk ranking in relation to assessing safety hazards. Leads to false sense of security and achievement

Review:

What does success look like? **The tangible**	**ULTIMATELY: FEWER SAFETY INCIDENTS, INJURIES AND FATALITIES** Having an engineering management process, including: • Single repository of lessons learned in the organisation, managed by an individual • Design Change Control process • Verification and Validation process • Requirement specifications, that include safety and human factors • Engineering Authority Structure • Two roles: senior engineering manager and chief engineer • A documented engineering process • Templates, with mandatory fields • An absence of ‘tick-box engineering’ • **Focus on HAZARDS, not RISKS** • **ONE HAZARD REGISTER for your project** (or, at least, all registers on ONE PLACE) • SiD Information Package: single point of information for the organisation’s SiD process, plus GUIDANCE • Clear SiD requirements in CONTRACTS – or risk getting poor outputs

Review:

The less-tangible	• Leadership: participatory, supportive and visible • Training • SiD principles: clear, well-communicated. Overt, not hidden. • Culture: the willingness to say ’no’, and supportive / professional when this occurs • Understanding the difference between hazards and risks • Understanding the difference between a constructability review and construction SiD review • Understanding the concept of ‘Design Intent’ • SiD Focus Group: consultative review group, accountable to leadership team • Clear Accountability: stakeholders know what is required of them • Audits

Summary of perspectives

1. SiD is part of the engineering and design lifecycles
2. ‘Built-in, not bolt-on’ (like quality)
3. It is not difficult
4. It starts at the beginning
5. Requires systematic approach
6. Talk about hazards, and the hierarchy of controls
7. Is not risk assessment, but contributes to overall risk reduction