Perspectives on: Safety in Design

Presentation at EA, Adelaide, 20/4/16

Mike Hurd

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 specific SiD process is a good way to draw attention to the requirements until it becomes embedded as an organisation’s ‘business as usual’.
• 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 application of risk ranking per AS 31,000

LIMIT OF USEFULNESS FOR ENGINEERING DECISION-MAKING

The issue is BEHAVIOURS, not the principle.
• 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:
  • 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.
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?*

And if not, why not? (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.
Surely, these can be eliminated by design?
The design stage...

<table>
<thead>
<tr>
<th>CONCEPT</th>
<th>ASSESSMENT</th>
<th>DESIGN</th>
<th>MANUFACTURE</th>
<th>CONSTRUCT</th>
<th>COMMISSION</th>
<th>IN-SERVICE</th>
<th>DECOM./DISPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief / URS / Concept design</td>
<td>Options Scope Specif’n</td>
<td>Detail design</td>
<td>IFC</td>
<td>As-built</td>
<td>Changes Mark-ups DCC</td>
<td>Mod’s, upgrades refurb A&amp;A</td>
<td>Mod’s</td>
</tr>
<tr>
<td>Engineer</td>
<td>Engineer</td>
<td>Designer</td>
<td>Engineer/Designer</td>
<td>Engineer/Designer</td>
<td>Engineer</td>
<td>Engineer</td>
<td>Engineer</td>
</tr>
</tbody>
</table>

Copyright © Engineering. Systems. Management. Pty Ltd
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?

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

Copyright © Engineering. Systems. Management. Pty Ltd
Context: SiD ‘Umbrella’ over design tools

Safety in Design

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

All contribute to achieving

Copyright © Engineering. Systems. Management. Pty Ltd
Engineered Safety: tools, practices and techniques, and their applicability throughout the engineering lifecycle, indicating effectiveness

<table>
<thead>
<tr>
<th>CONCEPT</th>
<th>ASSESS-MENT</th>
<th>DESIGN</th>
<th>MANU-FACTURE</th>
<th>CON-STRUCT</th>
<th>COMMISSION</th>
<th>IN-SERVICE</th>
<th>DECOM./DISPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety in Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sys./ Proc. Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAZOP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIFT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMEA</td>
<td>FMEA as a design tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QRA / PRA</td>
<td>design tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTA</td>
<td>design tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOPA</td>
<td>design tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bow-Tie</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Design tool

Other FMEA types

NB: Systems Engineering

Lifecycle safety management

Analyse failures – causes and effects

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?)*

<table>
<thead>
<tr>
<th>WHAT?</th>
<th>DELIVERABLE</th>
<th>WHEN?</th>
</tr>
</thead>
</table>
| 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)

Concept Design (incl. drawings)

User Requirement Specification

Engineering Management

SOP Engineering Request Report (with stamp)

Detailed Allowables

Scope & Drawings issued including safety requirements

SAFETY PROCESS

Safaris Review ofOpinions

Saferies Plan

Safety Plan (High risk, non-compliance at new QLM activities)

Risk Register Design Review (workshop) (Hazardous plant throughout the ownership)

Safety or Design Actions List

Safety or Design Actions List

SAFETY DESIGN EFFICIENCY

IMPLEMENTATION OF SAFETY ACTIONS

To include ongoing updates to the Safety Actions List (Status of Safety Actions List to be checked at each design review

Monitor implementation of Site Actions

Systematic Design

Critical Design

Final Design Approved

Design Verifications

Consecutive, commissioning and testing

Development, Change Use New

Lifecycle

CONSTRUCTION

POST-CONSTRUCTION

O&M

D&D

Responsibility Key:

Client Activities

Detailed Design

Independent Third Party

Contractor

Notes:

In-service design changes could be a CMPS Project (except whole process) or an O&M 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, Plans & Actions.
The Requirement Specification

Requirement Categories

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

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

Copyright © Engineering. Systems. Management. Pty Ltd
Foresight in the Asset Lifecycle

Engineers need to demonstrate CONSIDERATION and FORESIGHT throughout:

<table>
<thead>
<tr>
<th>Conceptual Phase</th>
<th>Operational Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Use / Operate</td>
</tr>
<tr>
<td>Assessment</td>
<td>Maintain</td>
</tr>
<tr>
<td>Design</td>
<td>Repair</td>
</tr>
<tr>
<td>Manufacture</td>
<td>Refurbish</td>
</tr>
<tr>
<td>Transport</td>
<td>Modify</td>
</tr>
<tr>
<td>Construct</td>
<td>Decommission</td>
</tr>
<tr>
<td>Commission</td>
<td>Demolish</td>
</tr>
</tbody>
</table>

*Bold items = client activities?*
Human-to-Asset Interfaces

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

<table>
<thead>
<tr>
<th>ASSET LIFECYCLE</th>
<th>CONSTRUCT</th>
<th>COMMISSION</th>
<th>HAND-OVER</th>
<th>OPERATE</th>
<th>MAINTAIN</th>
<th>D&amp;D</th>
</tr>
</thead>
<tbody>
<tr>
<td>HUMANS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trades / Skilled</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Visitors ('bloody engineers')</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Surveyors</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Maintenance staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cleaners</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Inspectors / auditors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Copyright © Engineering. Systems. Management. Pty Ltd
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?
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*
Reasonable Practicability

Safety
Benefit

Just do it

Analyse
- TL CBA
- ALARP analysis
- SFAIRP test
- Risk Assess

Hmmm...
confirm *gross disproportionality*

Cost
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

**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:**

<table>
<thead>
<tr>
<th>What is SiD?</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>What isn’t SiD?</td>
<td>Risk ranking, single workshops, the application of AS 31,000</td>
</tr>
<tr>
<td>Where has risk assessment gone wrong?</td>
<td>Over-use of risk ranking in relation to assessing safety hazards. Leads to false sense of security and achievement</td>
</tr>
<tr>
<td>What does success look like?</td>
<td>ULTIMATELY: FEWER SAFETY INCIDENTS, INJURIES AND FATALITIES</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Having an engineering management process, including:</td>
</tr>
<tr>
<td></td>
<td>• Single repository of lessons learned in the organisation, managed by an individual</td>
</tr>
<tr>
<td></td>
<td>• Design Change Control process</td>
</tr>
<tr>
<td></td>
<td>• Verification and Validation process</td>
</tr>
<tr>
<td></td>
<td>• Requirement specifications, that include safety and human factors</td>
</tr>
<tr>
<td></td>
<td>• Engineering Authority Structure</td>
</tr>
<tr>
<td></td>
<td>• Two roles: senior engineering manager and chief engineer</td>
</tr>
<tr>
<td></td>
<td>• A documented engineering process</td>
</tr>
<tr>
<td></td>
<td>• Templates, with mandatory fields</td>
</tr>
<tr>
<td></td>
<td>• An absence of ‘tick-box engineering’</td>
</tr>
<tr>
<td></td>
<td>• <strong>Focus on HAZARDS, not RISKS</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>ONE HAZARD REGISTER for your project</strong> (or, at least, all registers on ONE PLACE)</td>
</tr>
<tr>
<td></td>
<td>• SiD Information Package: single point of information for the organisation’s SiD process, plus GUIDANCE</td>
</tr>
<tr>
<td></td>
<td>• Clear SiD requirements in <strong>CONTRACTS</strong> – or risk getting poor outputs</td>
</tr>
</tbody>
</table>
**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