Criticality Hazards Analysis

A View from the UK

Fred Winstanley
Safety & Risk Management
Sellafield Ltd
June 2010

© Nuclear Decommissioning Authority 2010
Aims of Presentation

• Overview of Sellafield Ltd ‘Hazards Analysis’ process
  – Compare and contrast with US techniques and processes

• Concentrating on:
  – Application of ALARP principle
  – Optioneering
  – Fault tolerance (Design Basis Accident Analysis)
  – Specifying safety requirements
Safety Criteria and Methodology

Legal requirements

Regulatory expectation → Company criteria

Risk must be ALARP

Methodology

Probabilistic Safety Analysis

Design Basis Accident Analysis

Safety Hierarchy
Is Criticality Risk ‘Acceptable’?

• Based on risk to worker/public

• ALARP is key

Increasing Risk

Unacceptable

Basic Safety Level

Risks may be tolerable if can show to be ALARP

Basic Safety Objective

Broadly Acceptable

(1E-4/y)

(1E-6/y)
ALARP – key aspects

- Safety Hierarchy
- Quality
- ‘Independence’
- Fault tolerance (DBAA)
- Quantity
- Overall risk
- Good practice
- Standards
- Design
- Optioneering
- Process
- Siting
- Good practice
- Standards
Sellafield Site
ALARP – key aspects

- Quality
- ‘Independence’
- Quantity
- Safety Hierarchy
- Overall risk
- Fault tolerance (DBAA)
- Good practice
- Design
- Optioneering
- Process
- Siting
- Standards

ALARP

- Safety Hierarchy
- Overall risk
- Good practice
- Standards
- Design
- Process
- Siting
- Fault tolerance (DBAA)
- ‘Independence’
- Quantity
- Quality

Sellafieldd Ltd

20 June 2010
Safety Assessment Process

Fault identification

Safety Assessments

Engineering requirements

‘Substantiation’

Operational requirements

Plant documentation (Clearance Certificates, Compliance & Maintenance Schedules, Outage arrangements)
An ongoing process

Fault ID

- Ongoing discussions
- Plant walkdown
- Parameter changes
- Standard faults/contingencies
- Expert opinion/experience
- Change design/process

Fault Analysis

- ‘Incredibility’
- ‘Deterministic’
- Safety requirements (protection/mitigation)

Teamwork!
HAZAP and HAZOP 0 - Optioneering

**HAZAP** – identify inherent hazards associated with the processes and the materials involved (pre HAZOP 0)

**HAZOP 0** - Identify principal hazards due to materials present / proposed process (standard HAZOP 1 keywords)

- Ensure Hazard Management strategy available for each fault.
  - can these hazards be eliminated?
  - if not, how can the hazard be managed - propose options
- Record and challenge any assumptions with the process
# HAZOP 1

- Used to consider outline designs / processes
- Check Hazard Management strategy.
- Support to optioneering and process selection.

<table>
<thead>
<tr>
<th>DEVIATION</th>
<th>CAUSE</th>
<th>CONSEQUENCE</th>
<th>SAFEGUARDS</th>
</tr>
</thead>
</table>
| Criticality | Moderator ingress to crate. | Criticality | 1. Do not move under wet weather conditions.  
2. Multiple barriers i.e. iso-freight and over-crate during transport. |
HAZOP 2

- Failure based approach (Bottom Up – fault led).
- Used to analyse detailed designs and operational processes.
- Identify specific initiating events

<table>
<thead>
<tr>
<th>DEVIATION</th>
<th>CAUSE</th>
<th>CONSEQUENCE</th>
<th>SAFEGUARDS</th>
</tr>
</thead>
</table>
| Movement Less/Part only | Cradle not present to receive can. | Potential to drop cans - potential for criticality if multiple cans are dropped over an extended period of time. Ctg: [OP] [CR] | 1. Cradle needs to be physically present to open gate.  
2. Control system confirms cradle is present prior to transferring can. |
HAZOP – General Points

• HAZOP studies are structured and systematic

• HAZOP is a widely accepted technique for hazard identification

• HAZOP is only as good as the HAZOP team/information available

• HAZOP is not guaranteed to identify all potential fault initiators

• HAZOP is not always the best fault identification technique
An ongoing process

- Fault ID
- Ongoing discussions
- Plant walkdown
- Parameter changes
- Standard faults/contingencies
- Expert opinion/experience
- Change design/process
- Safety requirements (protection/mitigation)
- ‘Incredibility’
- ‘Deterministic’
- Fault Analysis
- Teamwork!
‘Is Risk Acceptable?’ – No DBA Requirements

‘Initiators’

1. ‘Deterministic’
2. ‘Deterministic’
3. Not Credible/ ‘Incredible’

Normal conditions
Safe Envelope

ALARP?

Record assumptions

Critical
Defense in Depth/ Fault Tolerance

• Historically used Double Contingency Principle:
  – ‘… at least two unlikely, independent and concurrent changes … before a criticality accident is possible.’

• Now use Design Basis Accident Analysis (DBAA) Methodology:
  – A robust demonstration of the fault tolerance of the design i.e. the degree of defense-in-depth
    – Quantity
    – Quality (Hierarchy, robustness/ reliability)
    – Independence
**Minimum number of DBA Safety Measures**

<table>
<thead>
<tr>
<th>Dose (mSv)</th>
<th>&lt;1E-5/y</th>
<th>1E-5 – 1E-3/y</th>
<th>&gt;1E-3/y</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;20</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>20 - 1000</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>&gt;1000</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

1000mSv = 100Rem

A ‘safety measure’ must provide a complete line of defense
‘Is Risk Acceptable’ – With DBA Requirements

‘Initiators’

Normal conditions

Safe Envelope

Critical

4 ★

‘Credible’ – need DBA

5 ★

Quantity ☺

6 ★

Protective Safety Measures

Quality/Risk/ALARP?

Record assumptions

Sellafield Ltd
Measures of Success?

Adequate ‘fault tolerance’

Risk targets satisfied?

Shortfalls?

Safety Hierarchy/Good practice
## Specifying Safety Requirements

### Record all Assumptions and Requirements

<table>
<thead>
<tr>
<th>Structure, System or Component</th>
<th>Safety Function(s)</th>
<th>Safety Function Class</th>
<th>Design/Performance/ Additional Requirements</th>
</tr>
</thead>
</table>
| Storage Racking               | To ensure that packages within the store are retained within a criticality safe geometry for normal, credible fault and seismic conditions. | 1                     | 1. To maintain centre to centre separation distances of at least \( xx \) mm vertical and \( xx \) mm horizontal between packages in the storage racks.  
2. Seismically qualified to withstand DBE (0.25g).  
3. Storage rack no longer than \( xx \) mm  
4. Storage racks will not collect and retain water |
Include ALL requirements

Important for completeness, maintenance and checking independence

<table>
<thead>
<tr>
<th>Description</th>
<th>Detection</th>
<th>Decision</th>
<th>Termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention of further liquor arising in Vessel xxx</td>
<td>Level indicator in Vessel xxx and high level alarm in control room</td>
<td>If Vessel xxx high level alarm is activated, close Valve B</td>
<td>Manual valve B on feed line to Vessel xxx</td>
</tr>
</tbody>
</table>

Equipment  Operator  Equipment
Summary

• Lots of similar concepts … with different names

• Differences
  – Different Regulatory system
  – More emphasis on ALARP?

• Fault tolerance (DBA) vs Double Contingency
Question

• Which is ‘safer’?
  – Operator control
  – Automated control system