Criticality Hazards Analysis

A View from the UK

Fred Winstanley
Safety & Risk Management
Sellafield Ltd
June 2010

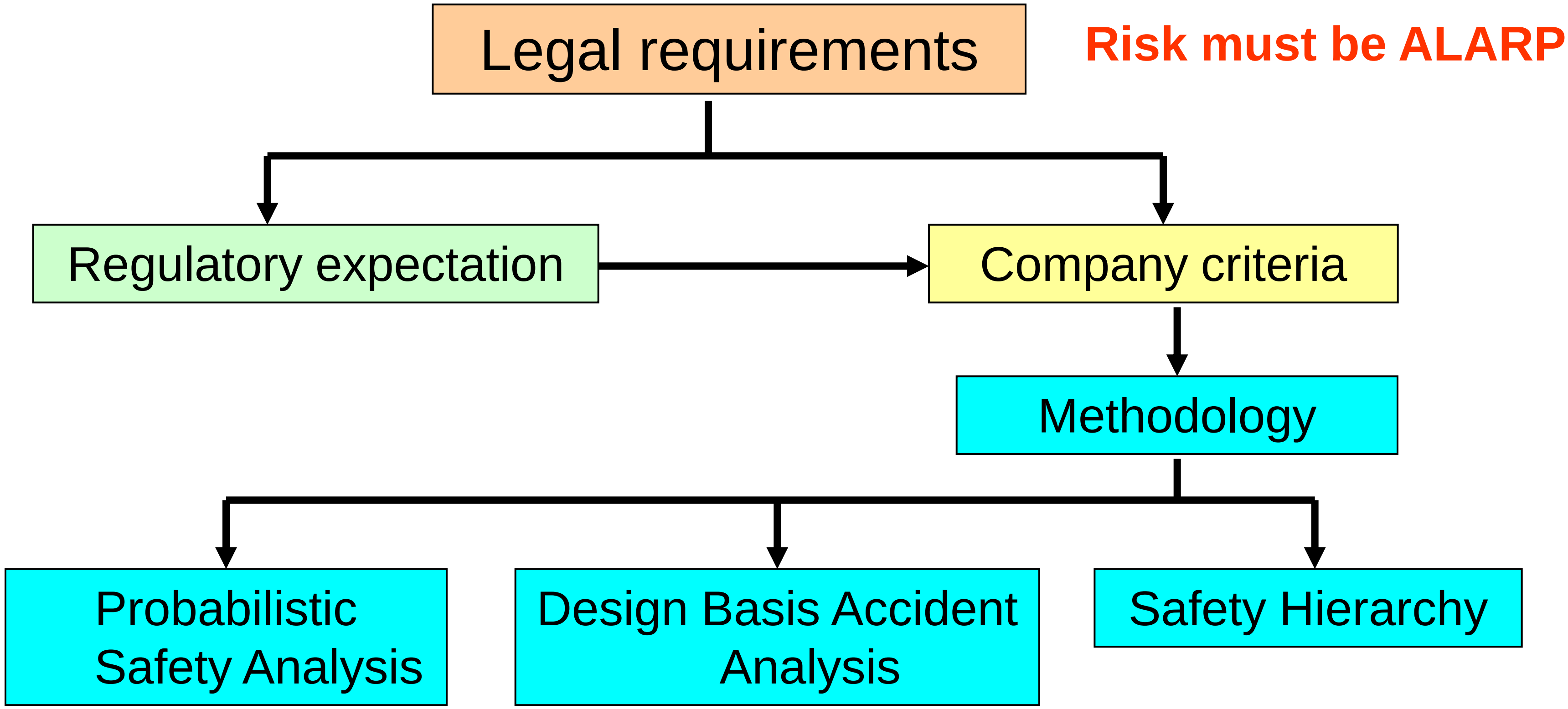
Sellafield Ltd

Aims of Presentation

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

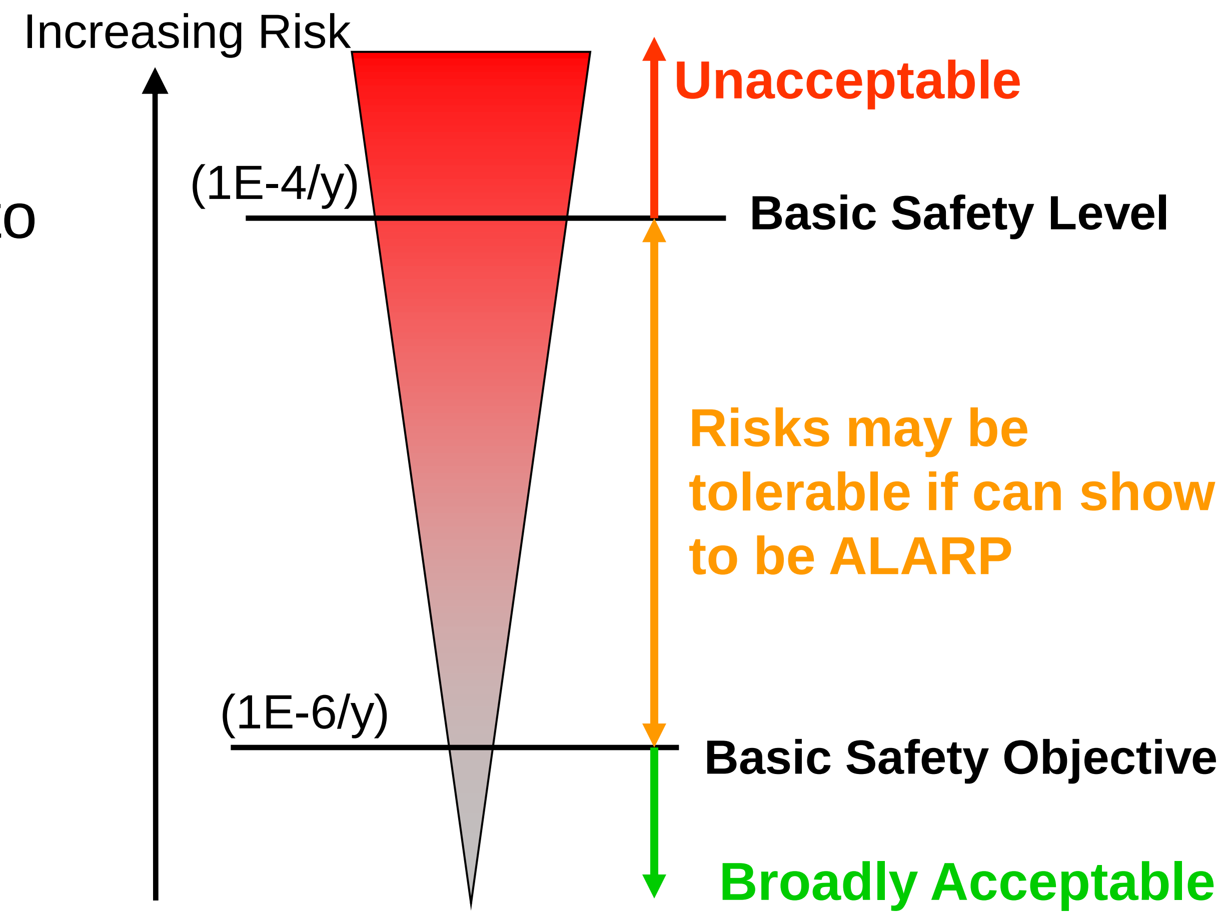
- Concentrating on:
  - Application of ALARP principle
  - Optioneering
  - Fault tolerance (Design Basis Accident Analysis)
  - Specifying safety requirements

Safety Criteria and Methodology

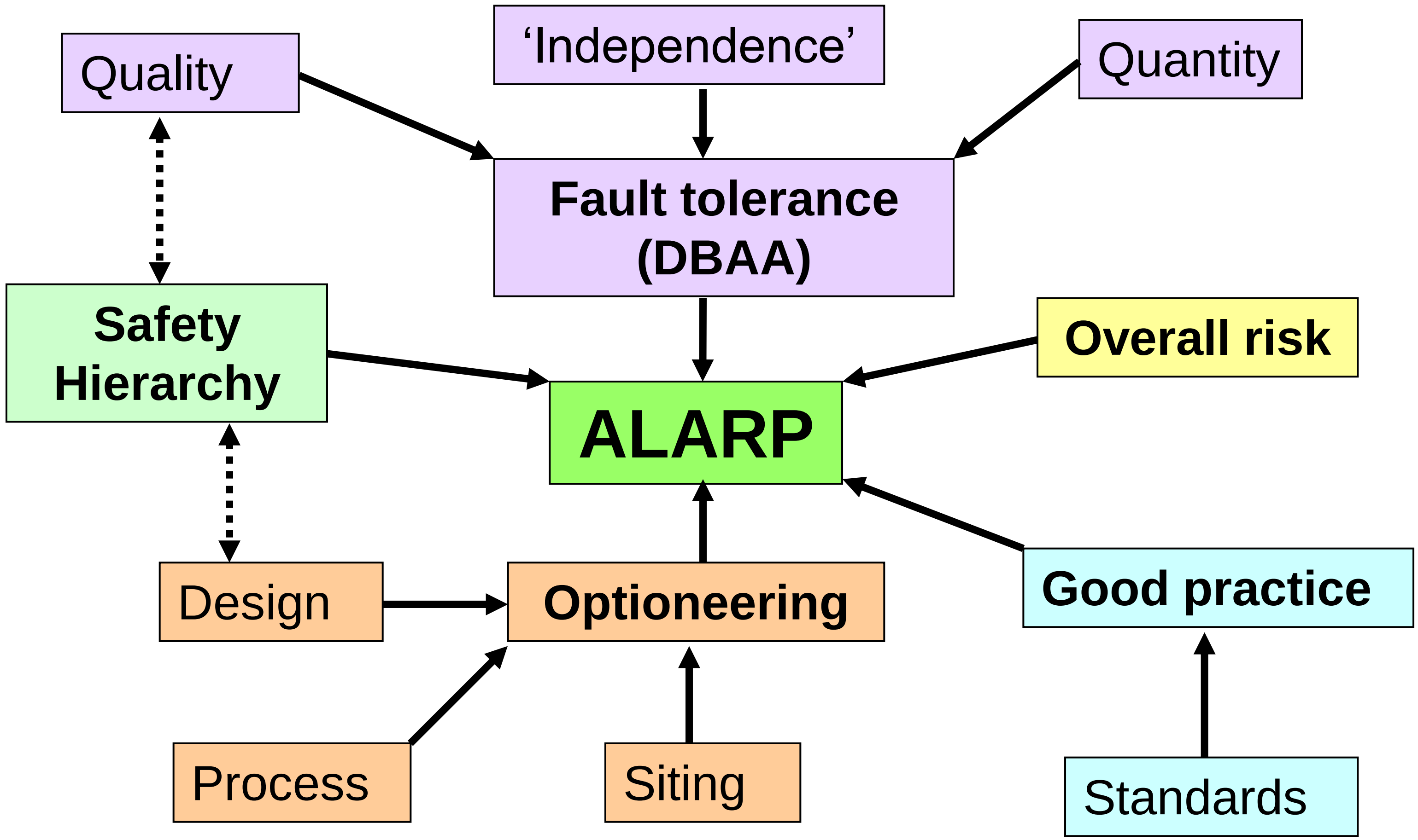


Is Criticality Risk 'Acceptable'?

- Based on risk to worker/ public
- ALARP is key



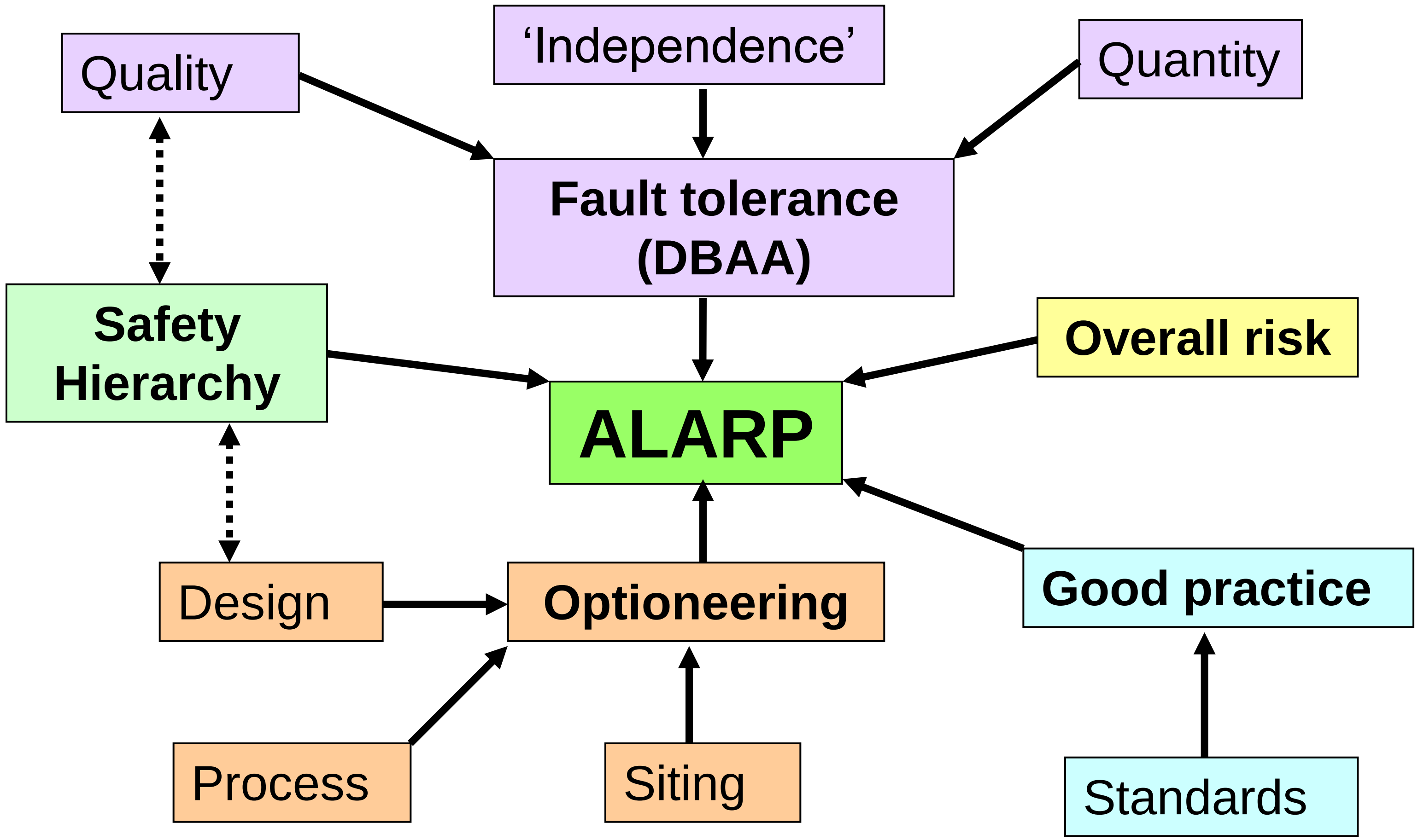
ALARP – key aspects



Sellafield Site

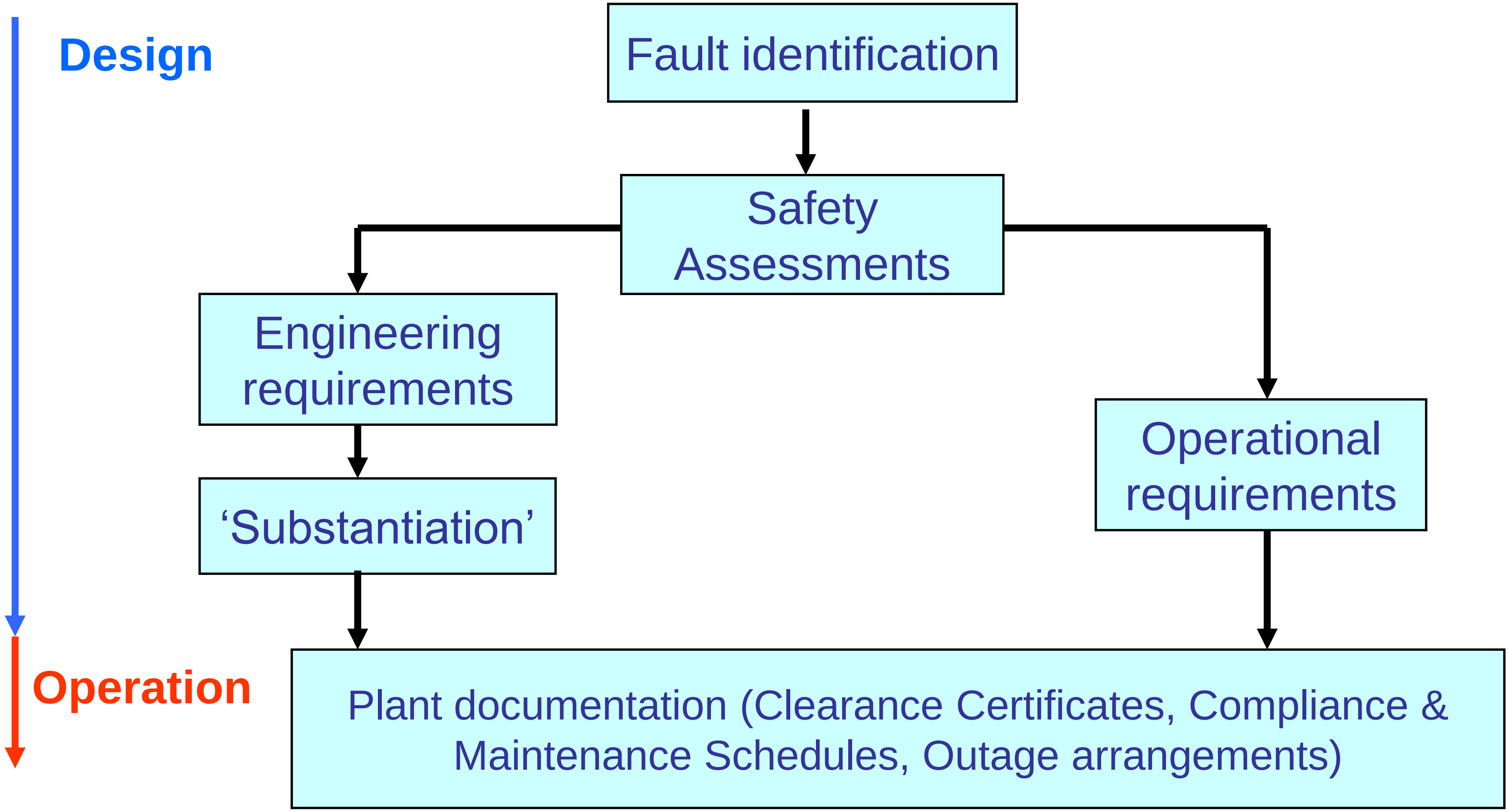
Sellafield Ltd

ALARP – key aspects

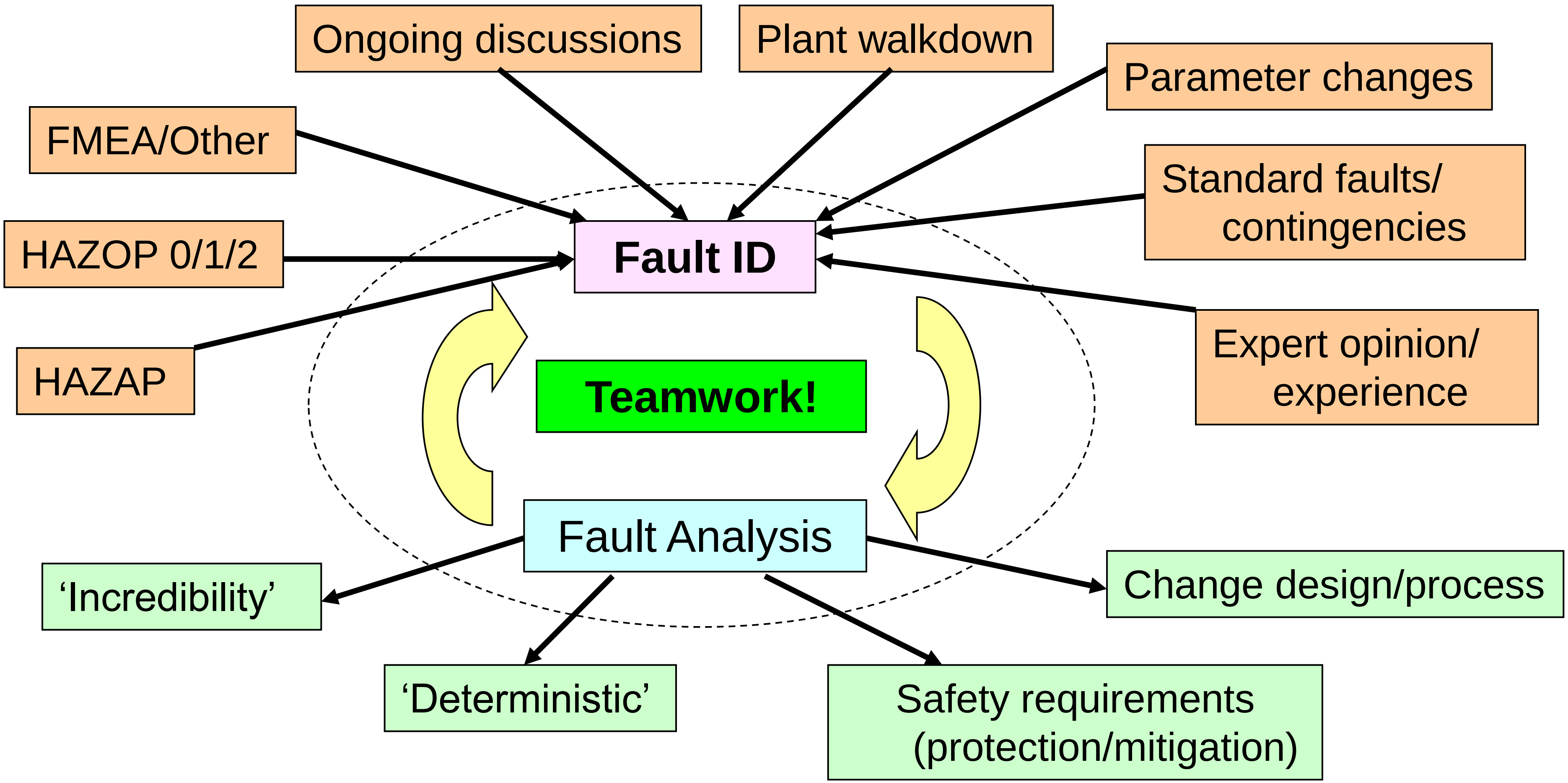


Sellafield Ltd

Safety Assessment Process



An ongoing process



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.

DEVIATION	CAUSE	CONSEQUENCE	SAFEGUARDS
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

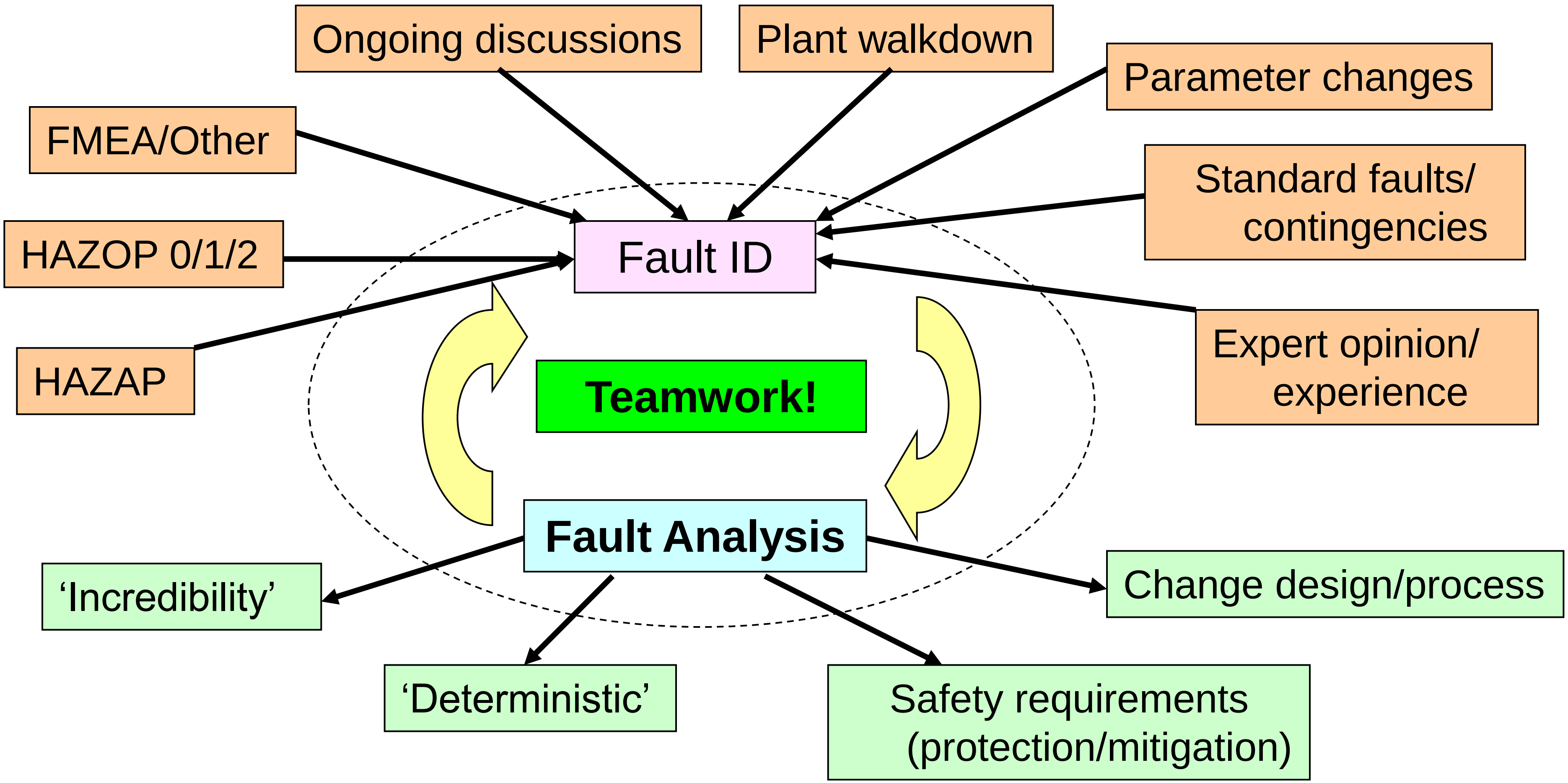
DEVIATION	CAUSE	CONSEQUENCE	SAFEGUARDS
Movement Less/Part only	Cradle not present to receive can.	Potential to drop cans - potential for criticality if multiple cans are dropped over an extended period of time. Ctgy: [OP] [CR]	1. Cradle needs to be physically present to open gate. 2. Control system confirms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

HAZOP – General Points

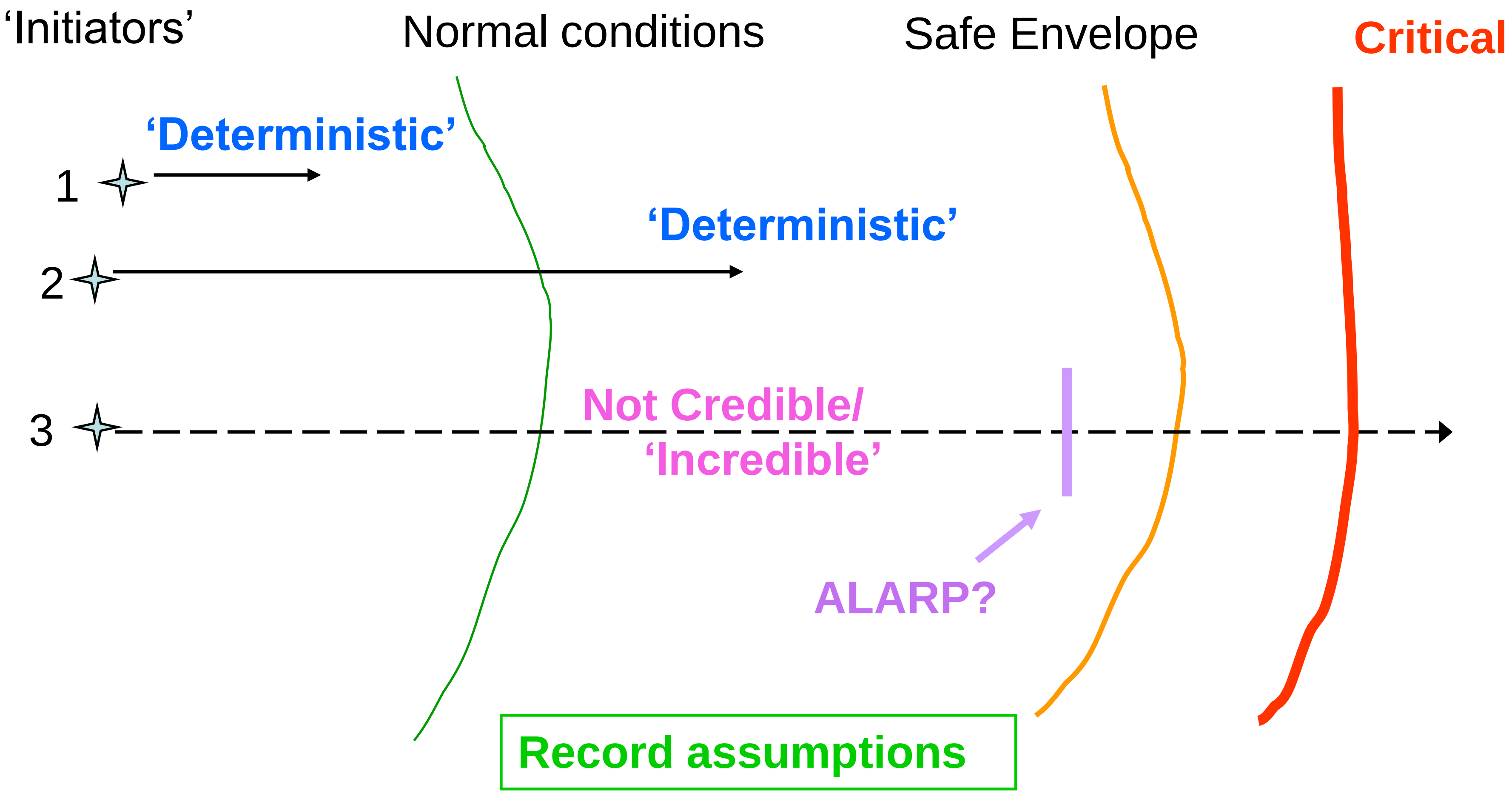
- HAZOP studies are structured and systematic
- HAZOP is a widely accepted technique for hazard identification

- **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



‘Is Risk Acceptable?’ – No DBA Requirements



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

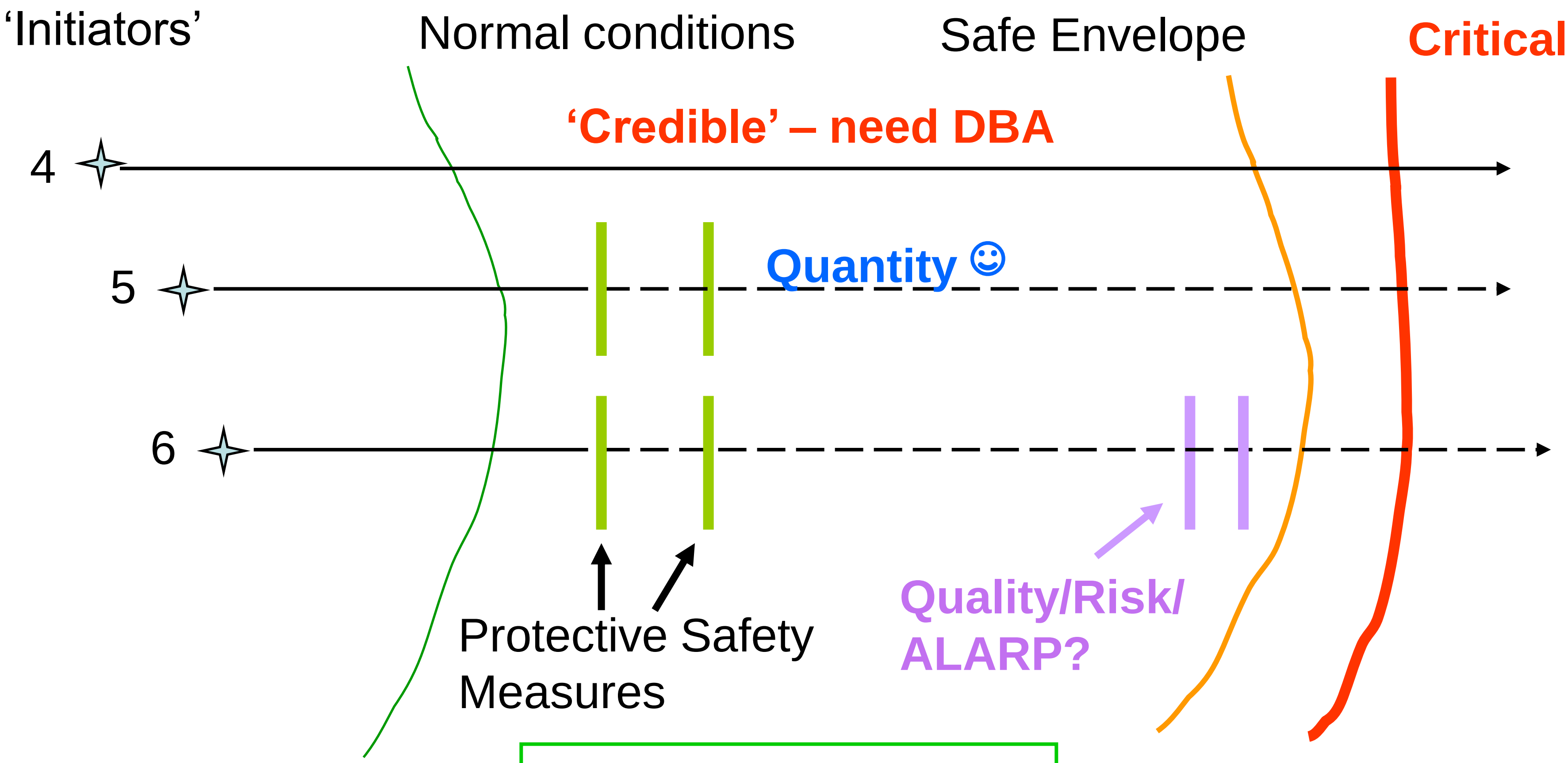
	Frequency of criticality with no 'protection'		
Dose (mSv)	<1E-5/y	1E-5 – 1E-3/y	>1E-3/y
<20	0	0	2
20 - 1000	0	1	2
>1000	0	2	2

1000mSv = 100Rem

A '**safety measure'** must provide a complete line of defense

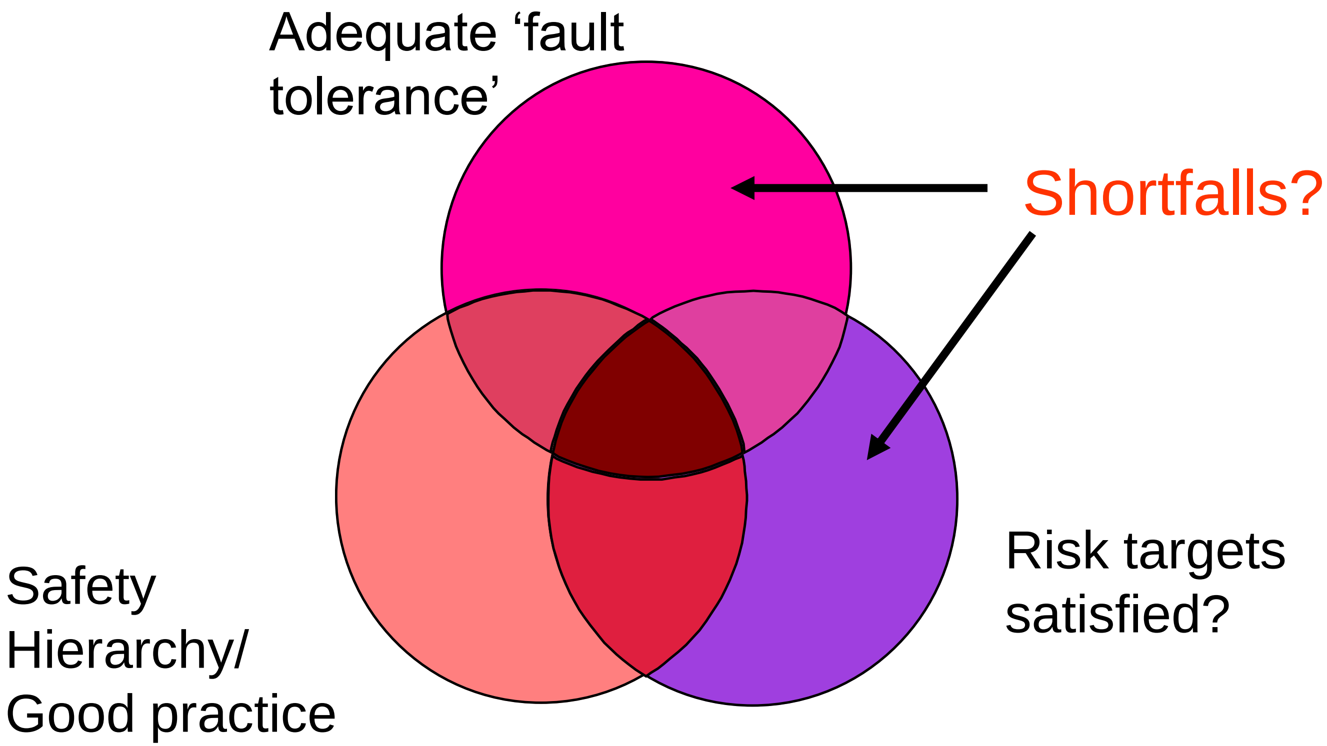
Sellafield Ltd

'Is Risk Acceptable' – With DBA Requirements



Record assumptions

Measures of Success?



Specifying Safety Requirements

Record all Assumptions and Requirements

Structure, System or Component	Safety Function(s)	Safety Function Class	Design/Performance/ Additional Requirements
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

Sellafield Ltd

Include ALL requirements

Important for completeness, maintenance and checking independence

Description	Detection	Decision	Termination
Prevention of further liquor arising in Vessel *xxx*	Level indicator in Vessel *xxx* and high level alarm in control room	If Vessel *xxx* high level alarm is activated, close Valve B	Manual valve B on feed line to Vessel *xxx*

Equipment **Operator** **Equipment**

Summary

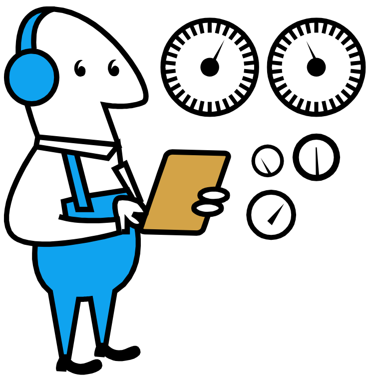
- Lots of similar concepts … with different names

- Differences
  - Different Regulatory system
  - More emphasis on ALARP?

- Fault tolerance (DBA) vs Double Contingency

Question

- Which is 'safer'?
  - Operator control



or

  - Automated control system