Office for Nuclear Regulation

Defence in Depth – A UK Perspective

Senior Regulators Meeting
IAEA General Conference 2014

Dr Andy Hall
Chief Nuclear Inspector

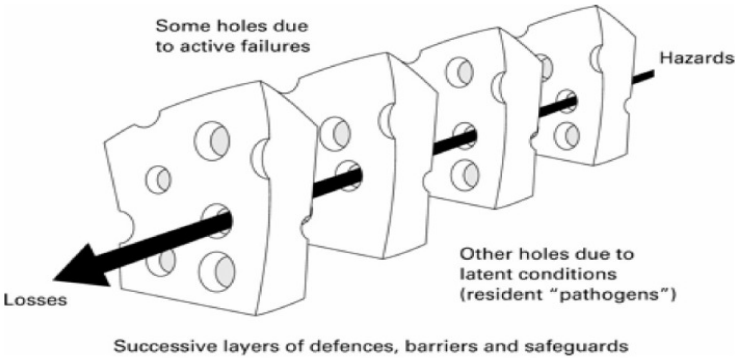


Contents

- Why do we need Defence in Depth?
- Overview of UK Requirements
- Application of Deterministic Safety Principles and their Limitations
- Achieving a Balanced Design
- Severe Accident Analysis
- Contribution of Human and Organisational Factors to Defence in Depth

Why do we need Defence in Depth?

- Defence in depth developed from military concept, providing multiple barriers to attack.
- Concept of providing multiple physical barriers (and protection to prevent breach of these barriers) is an established part of UK nuclear safety goal setting regime.
- Compensates for uncertainty caused by equipment failure and human error.



No barrier is infallible – no mater how apparent its robustness

UK Requirements for Defence in Depth

Nuclear Safety

- ONR's Safety Assessment Principles (SAPs) define ONR's expectations for Defence in Depth:

  Facilities should be designed and operated so that defence in depth against potentially significant faults is achieved by provision of multiple independent barriers to fault progression.

- Achieved by:
  - Preventing deviations from normal operation
  - Providing safety margins to allow detection and action to prevent fault escalation
  - Provision of safety measures to terminate faults before they progress to accidents
  - Provision of additional measures to prevent severe accidents
  - Mitigation of radiological consequences.

  (Based on IAEA Safety Standard: SSR-2/1)

UK Requirements for Defence In Depth

- UK expects licensees to take a proportionate approach to demonstrating defence in depth, as part of a nuclear safety case.
- Starting point: a thorough and systematic hazard and fault identification.
- Demonstration that the design confirms to good engineering practice and sound safety principles.
- Analysis of faults using complimentary techniques of:
  - Design Basis Analysis (DBA)
  - Probabilistic Safety Analysis (PSA)
  - Severe Accident Analysis (SAA) – if necessary.

Application of Deterministic Safety Principles

- Effective application of DBA will ensure that the design has robust protection, even when making conservative assumptions for normal operations and allowances for single failures.
- Design for reliability – key principles:
  - Redundancy, to avoid the effects of random failure
  - Diversity and Segregation, to avoid the effects of common cause failure
  - Single failure criterion.

Limitations of Deterministic Approach

- DBA makes conservative and sometime unrealistic assumptions.
- DBA does not consider the full range of faults.
- The simplifications and conservatisms in DBA can mask strengths and weaknesses in the design of complex systems.
- Judging the overall risk presented by the facility may not be possible with DBA.
- DBA is important for categorisation and classification, defining design standards etc. but it does not always give reliability requirements for SSCs.

Achieving a balanced design

- Deterministic Analysis alone may not be sufficient to demonstrate the safety of a facility.
- For major hazard facilities, DBA is complimented by Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA).
- Together they ensure adequate levels of defence in depth are achieved in totality:
  - DBA: to ensure the design is robust, fault tolerant and has effective safety measures
  - PSA: to ensure overall risks are acceptable and balanced; and to understand strengths, weaknesses and inter-dependencies in the overall design; to evaluate potential for multiple failures.
  - SAA: to determine further reasonably practicable measures to improve defence in depth.

Application of PSA to Inform Defence in Depth

- PSA should be used to inform the design process.
- Application of PSA permits analysis of:
  - complex interactions and interdependencies between systems
  - multiple failures
  - reliability of barriers to a release
  - claims on human action and their reliability.
- Best-estimate methods and data should be used.

Severe Accident Analysis

- For facilities with a significant nuclear hazard, ONR expects SAA.
- Approach results in the following being considered:
  - high consequence scenarios of low frequency (beyond DBA),
  - design basis scenarios where DBA measures have failed,
  - Scenarios not traditionally covered in UK safety case being considered, e.g. malevolent acts.
- Best-estimate methods and data should be used.

Contribution of Human and Organisational Factors to Defence in Depth

- Human action makes an important contribution to maintaining safety of nuclear installations.
- The contribution that human and organisation factors makes to defence in depth should be considered at all levels of Defence in Depth.
- Defence in Depth concepts such as redundancy, diversity, and segregation should be considered in task analysis.

Contribution of Human and Organisational Factors to Defence in Depth

- UK requires licensees to adopt a systematic approach to identify safety claims on human action and demonstrate:
  - Feasibility and achievability of claims
  - Margins provide appropriate response times to ensure reliable detection and recovery.
  - Necessary error detection and recovery systems are in-place
  - Independence from other levels of protection/ human actions
  - Consideration to Human errors that may contribute to hardware failures (e.g. maintenance errors).

Conclusions

- Defence in Depth is an important tenet of the UK's goal setting safety regime.
- Rigorous application of deterministic principles will result in a design with multiple barriers.
- Severe Accident Analysis should be used (if appropriate) to determine further reasonably practical measures to improve defence in depth.
- Probabilistic Safety Analysis should be used to inform decisions, to achieve a balanced design.
- The same planning, analysis and substantiation is required for claims on human action as for engineered protection.