LESSONS LEARNT FROM THE UK GENERIC DESIGN ASSESSMENT PROCESS

Dr R Moscrop†, Dr J R Jones*, Prof A Tehrani†, R Exley†

Office for Nuclear Regulation

*St James House, Cheltenham, GL50 3PR
†Redgrave Court, Bootle, Merseyside, L20 7HS
GENERIC DESIGN ASSESSMENT INTENT

Office for Nuclear Regulation (ONR) has developed a design acceptance process to enable:

– advice to vendors on licensing
– early interaction with reactor designers
– financial, project and regulatory risk reduction
The Tolerability of Risk Framework

- Reduce risk as far as reasonably practicable
- Consideration of both dose and potential societal harm
- Relevant Good Practice (RGP) is a starting point
ONR Target Levels for Off-site Exposure

- If intolerable, additional protection is mandated;
- If protection is provided, new plant should be designed for success, i.e. to meet the Basic Safety Objective (BSO)
Basic Elements of a Comprehensive Safety Justification

• Comprehensive fault and hazard protection schedule

• A graded approach to safety analysis:
  Deterministic analysis covering both design basis and design extension conditions;
  Integrated with probabilistic safety analysis

• Deterministic demonstration of redundancy and diversity

• Design and manufacture based on the safety function category and system safety class
Faults Often Omitted

- Common-mode failure of essential support systems
- Spurious computer software failure on multiple C&I platforms (including the primary protection system)
- Shutdown and part-power operations
- Spent fuel pool and fuel handling
- Heterogeneous boron dilution (on PWRs)
- Internal and external hazards
Defense in Depth and Design Extension

Analysis of risk-significant faults beyond the design basis is not new to the UK and comprises:

- DEC-A sequences for which prevention of severe fuel damage supports Level 1 PSA
- DEC-B sequences for which severe accident mitigation supports Level 2 PSA
DEC-A Analysis

Fault sequences with additional random failures up to a frequency of 1E-7/yr:

- Events during all defined operational states of the plant
- Events resulting from internal or external hazards
- Common cause failures
DEC-B Analysis

- Recognises additional plant risk from unanticipated events;
- Considers selected postulated faults with extensive protection failure leading to core damage;
- Confirms that the consequences of core damage will not lead to a large early release of activity.
Example of Requirements Derived from DEC Analysis

• Upgrading of diverse safety systems to meet Class 2 requirements;

• Hard-wired diverse protection system to provide functional diversity for failures in the computer based primary protection system;

• Provision of additional actuation signals.
Additional Accident Analysis

- Passive single failures including accumulator non-return (check) valves
- LOCA faults with the potential for containment bypass
- Consequential SGTR failures following steam-line faults
- Consequential LOCA faults following SRV lift
- The transition from the controlled state to the safe shutdown state
Closing Remarks

The intention of this system of regulation:

- is not to provide a prescriptive set of steps by which utilities can meet regulatory requirements
- is to set flexible guidelines which allow utilities to operate safely and to engage constructively with ONR
Final Thought

The aim should be to provide a robust demonstration of fault tolerance and that all reasonably practical measures have been taken to reduce the risk to a broadly acceptable level.

Final thought – a simple ALARP challenge

What more *could* you do?
And why *can’t* you do it?