Safety Analysis: Event Classification

Lecturer
Lesson IV 1_2

Workshop Information
IAEA Workshop

City, Country
XX - XX Month, Year
Deterministic Safety Analysis

- Nuclear industry has adopted the “defence-in-depth” approach, in order to maintain the effectiveness of physical barriers between radiation sources and radioactive materials and workers, members of public and environment, in operational states and, for some barriers, in accident conditions.

- There are several “lines of defence”.
Deterministic Safety Analysis

– DESIGN BASIS: the range of conditions and events taken explicitly into account in the design of a plant, so that the plant can withstand them w/o exceeding authorised limits, by the planned operation or safety systems.

– DETERMINISTIC SAFETY ASSESSMENT: aims to determine the effectiveness of “lines of defence”.

– DSA establish and confirm the DB for items important to safety, ensuring that the plant design meets safety and radiological criteria (integrity of barriers).
Deterministic Safety Analysis

The basis of DSA is establishing a set of so called “design basis events” (DBEs) and analysing their consequences by means of calculational methodologies (that include computer codes).

A DBE is described by:

- Specified failure (or set of failures)
- Conservative initial conditions
- All the control and safety systems operated as designed
## Deterministic Safety Analysis

<table>
<thead>
<tr>
<th>plant states</th>
<th>operational states</th>
<th>accident conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>anticipated</td>
<td>design basis accidents</td>
</tr>
<tr>
<td>operation</td>
<td>operational</td>
<td>beyond design basis accidents</td>
</tr>
<tr>
<td></td>
<td>occurrences</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td>design basis</td>
<td>b</td>
</tr>
<tr>
<td></td>
<td>accidents</td>
<td>severe accidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accident management</td>
</tr>
</tbody>
</table>

- **a** = *Accident conditions* which are not explicitly considered *design basis accidents* but are encompassed by them.
- **b** = *Beyond design basis accidents* without significant core degradation.
Deterministic Safety Analysis

- The DBEs are classified in CATEGORIES, roughly depending on their expected occurrence frequency and potential consequences.

- In such categories are included Anticipated Operational Occurrences (AOOs), and Design Basis Accidents (DBAs).

- For each category, the DSA checks that the design meets the ACCEPTANCE CRITERIA, that normally reflect the criteria used by designers or operators and are consistent with the requirements of the regulatory body.
**Deterministic Safety Analysis**

- **ACCEPTANCE CRITERIA**: ensure that an adequate level of defence in depth is maintained by preventing damage to barriers and unacceptable radiological releases.

- Two levels:
  - Global/high level criteria related to doses to the public or prevention of consequential pressure boundary failure. Often defined in law or by the regulatory body.
  - Detailed criteria defined by designer or analyst. Sufficient, but not necessary to meet the global ones.
DSA: Acceptance Criteria

- More stringent criteria often applied for events with a higher frequency of occurrence.
- Detailed acceptance criteria could include:
  - An event should not generate a subsequent more serious plant condition w/o the occurrence of a further independent failure.
  - No consequential loss of function of the safety systems needed to mitigate the consequences of an accident.
  - Systems for accident mitigation: designed to withstand loads, stresses and environmental conditions for the accidents.
  - Pressure in primary and secondary systems should not exceed design limits.
DSA: Acceptance Criteria

- Allowed number of fuel cladding failures: established for each type of PIE to meet the global radiological criteria.
- LOCA criteria.
- Containment criteria.
Deterministic Safety Analysis

- Postulated Initiating Events (PIEs) : starting point for the DSA. They are identified events that to AOOs or accident conditions, including equipment failure, human errors and external events (natural or human-induced).

- The set of PIEs includes events of very low frequency or consequences, at least at the beginning of the process. Some of them can be eliminated subsequently.

- PIEs classified in terms of frequency of occurrence.
Deterministic Safety Analysis

- AOOs: operational processes deviating from normal operation that have the potential to challenge the safety of the reactor. According to design provisions, AOOs do not cause any significant damage to items important to safety, nor lead to accident conditions.

- AOOs are expected to occur at least once during the operating lifetime of the plant (frequency of occurrence higher than 0.01 per reactor and year).
Deterministic Safety Analysis

- DBAs: accident conditions against which a nuclear plant is designed, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

- DBAs are not expected to occur during the lifetime of the plant (frequency $10^{-2}$ to $10^{-5}$ per reactor and year, but some like LBLOCA are even less frequent).

- PIEs identified as initiators of AOOs are also potential initiators of DBAs.

- PIEs leading to DBAs have the same categories than for AOOs.
Deterministic Safety Analysis

– Once identified, PIEs are grouped, and for each group a bounding case is chosen for analysis (in general, one for each safety parameter), looking for the most severe challenges to the main safety functions.

– DBAs are basis for the design of the reactivity control systems, RCS, ESF, electric power systems and various auxiliary systems important to safety.

– Modifications of plants: the assessment is focused on affected DB events. The methodology may need some change: new acceptance criteria, new tools, etc.
Deterministic Safety Analysis

- DSA states if a reactor design is adequate and licensable.

- DSA is a tool in developing plan protection and control systems setpoints and control parameters, and the Technical Specifications of the plant.

- Why “deterministic”? Traditionally:
  - No probabilities in the calculation (in principle)
  - Results are single numerical values with probability 1

- But this is not true for “best-estimate” analyses !!!
Deterministic Safety Analysis

– **DSA versus PSA (Probabilistic Safety Analysis):**
  - Both approaches are necessary, because they are complementary.
  - When the insights from both approaches are not consistent, further specific studies are needed.

– **DSA can be:**
  - Conservative (worst-case, pessimistic), traditional approach.
  - Best-estimate or realistic, newer approach, it includes an uncertainty quantification of the results.
Deterministic Safety Analysis

- DSA carried out by:
  - Designer: as part of the design and construction process
  - Operating organization, to confirm the design

- DSA must be parallel to the design process, with iteration between them. The final SA must reflect the final plant design.

- DSA is used for evaluating design changes, supporting decision-making processes, revealing new issues, etc.

- Also:
  - Periodic SA of an operating plant
  - Safety justification of a design modification
Deterministic Safety Analysis

- DSA demonstrates the effectiveness of the equipment incorporated to prevent escalation of AOOs and DBAs to severe accidents and to mitigate their effects.

- DSA demonstrates that the safety systems can:
  
  • Shutdown the reactor and maintain it in safe shutdown condition during and after DBA.
  
  • Remove residual heat from the core after reactor shutdown from all operational states and DBA conditions.
  
  • Ensure that radioactive releases during DBA are below acceptable limits.
Deterministic Safety Analysis

– DSA for normal operation of the plant:

• Ensures that normal operation is safe, with radiological doses and releases of radioactive materials within acceptable limits (also checking if they are ALARA), and with plant parameters not exceeding operating limits.

• Should establish the conditions and limitations for safe operation, including:
  
  ▶ Safety limits for reactor protection and control and other engineered safety systems.
  
  ▶ Operational limits and reference settings for the control system.
  
  ▶ Procedural constraints for operational control of processes.
  
  ▶ Identification of allowable operating configurations.