Design basis accident
Design extension conditions
Design basis
Basis for WENRA DiD structure
Consequences of accidents: general expectations

Vienna Declaration
New NPPs are to be designed, sited, and constructed, consistent with the objective of preventing accidents ... and, should an accident occur, mitigating possible releases of radionuclides causing long-term off-site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.

Off-site consequences

Accident acceptable/tolerable consequences

Postulated Accidents « types » (DBA, BDBA, DEC...)

SSR-2/1
4.3 The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

SSR-2/1
5.31 The design shall be such that DECs that could lead to significant radioactive releases are practically eliminated. If not, for DECs that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.
Consequences of accidents : general expectations

SSR-2/1
4.3 The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are **practically eliminated** and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

SSR-2/1
5.31 The design shall be such that DECs that could lead to significant radioactive releases are **practically eliminated**. If not, for DECs that cannot be **practically eliminated**, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.

Postulated Accidents « types »
(DBA, BDBA, DEC...)
Consequences of accidents: technical criteria

Postulated Accidents « types » (DBA, BDBA, DEC...)

Off-site consequences

Acceptance / surrogate criteria

Accident acceptable/tolerable consequences
Adequacy of plant design and operation
Assessment of accidents and their consequences

Postulated Accidents « types »
(DBA, BDBA, DEC...)

Accident assessment rules/methods

Conservative

Realistic

Acceptance / surrogate criteria

Off-site consequences

Accident acceptable/tolerable consequences

Deterministic

Probabilistic

Conservative

Realistic
Accident scenarios: how to identify them

- External hazards
- Internal hazards
- Equipment failure(s)
- Human « failure(s) »

Initially, Engineer’s experience and imagination

Later on, Computer-aided “imagination” (PSA)
Assessment of postulated accidents

• Deterministic approach to identify accidents
  • It is postulated that the single initiating event (failure...) occurs (probability = 1)
  • Identified consequential failures are postulated to occur

• Conservative approach to assess consequences of accidents
  • Penalizing hypothesis
    • Single failure criteria
    • Availability of equipment
    • Performance of equipment
    • ....
  • Conservative calculations
  • Margins to cover uncertainties in knowledge and phenomena
Accidents postulated: list evolves in time

Conservative methodology

DBA

Commissioning of NPP

BDBA

Realistic

Deterministic approach

Experience feedback

PSA

1960 - 1990
Accidents postulated: list evolves in time

Deterministic conservative  |  Realistic
---|---
DBA  |  BDBA

Conservative methodology  |  Realistic
---|---
Deterministic + PSA

DBA  |  DEC

Commissioning of NPP

1960 - 1990

1990 - ...

Commissioning of NPP
Accidents postulated: list evolves in time

« old » plant

DBA

(initial) safety design
(demonstrated) envelope

Actual safety
(demonstrated) envelope

« new » plant

DBA + DEC

Design provisions to practically eliminate sequences leading to large or early releases

DEC

BDBA + other accidents

DEC

Accidents with core-melt + other accidents

DBA

BDBA
What SSC for which plant state?
What SSC to protect against/to resist to hazards?

<table>
<thead>
<tr>
<th></th>
<th>Normal operation</th>
<th>AOO</th>
<th>DBA</th>
<th>BDBA DEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment A</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment B</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Structure C</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Equipment D</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>System E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Normal operation
- AOO
- DBA
- BDBA DEC

- Internal hazards
- External hazards

- Equipment A ✓
- Equipment B ✓ ✓
- Structure C ✓ ✓ ✓ ✓ ✓
- Equipment D ✓
- System E ✓ ✓
Design basis/envelope of a SSC

Structure C design shall account for expected or calculated loads and performance resulting from all ✓ plant states and hazards.

Equipment D design shall account for expected or calculated loads and performance resulting from all ✓ plant states and hazards.

System E design shall account for expected or calculated loads and performance resulting from all ✓ plant states and hazards.
## WENRA DiD structure

<table>
<thead>
<tr>
<th>Levels of defence in depth</th>
<th>Objective</th>
<th>Essential means</th>
<th>Radiological consequences</th>
<th>Associated plant condition categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.a</td>
<td>Control of accident to limit radiological releases and prevent escalation to core melt conditions</td>
<td>Reactor protection system, safety systems, accident procedures</td>
<td>No off-site radiological impact or only minor radiological impact</td>
</tr>
<tr>
<td></td>
<td>3.b</td>
<td></td>
<td>Additional safety features, accident procedures</td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td></td>
<td></td>
<td></td>
<td>DEC without core-melt</td>
</tr>
<tr>
<td>Level 4</td>
<td></td>
<td>Control of accidents with core melt to limit off-site releases</td>
<td>Complementary safety features, Management of accidents with core melt (severe accidents)</td>
<td>Off-site radiological impact may imply limited protective measures in area and time</td>
</tr>
</tbody>
</table>

---

(1) Even though no new safety level of defence is suggested, a clear distinction between means and conditions for sub-levels 3.a and 3.b is lined out. The postulated multiple failure events are considered as a part of the Design Extension Conditions in IAEA SSR-2/1.

(2) Associated plant conditions being now considered at DiD level 3 are broader than those for existing reactors as they now include some of the accidents that were previously considered as “beyond design” (level 3.b). For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if appropriately justified. However the maximum tolerable radiological consequences for multiple failure events (level 3.b) and for postulated single failure events (level 3.a) are bounded by Objective...
WENRA DiD structure: rationale for 3a/3b

- Several scenarios that are considered beyond design basis for most existing reactors are now included from the beginning in the design for new reactors (postulated multiple failure events and core melt accidents).

- In the DiD approach, the objectives of the different levels of defence are mainly defined as successive steps in the protection against the escalation of accident situations.

- The phenomena involved in accidents with core/fuel melt (severe accidents) differ radically from those which do not involve a core melt. Therefore core melt accidents should be treated on a specific level of Defence-in-Depth.

- The question has been discussed by RHWG whether for multiple failure events, a new level of defence should be defined, because safety systems which are needed to control postulated single initiating events are postulated to fail and thus another level of defence should take over. However, the single initiating events and multiple failure events are two complementary approaches that share the same objective: controlling accidents to prevent their escalation to core melt conditions.
  - Hence, at this stage of the discussion, it has been proposed to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3.a and 3.b).

- In addition, for new reactors, design features that aim at preventing a core melt condition and that are credited in the safety demonstration should not belong to the same level of defence as the design features that aim at controlling a core melt accident that was not prevented. However, should a core melt accident occur, all plant equipment still available may be used.
Draft IAEA tecdoc on SSR-2/1
Suggested topics to discuss by NUSSC volunteers

• « Easy » topics
  • Design basis accident
  • Design basis
  • Use of non-permanent equipment
  • List of DECs (without fuel damage)

• « Highly Challenging » topics
  • Defence in depth

• « Not so challenging » topics
  • Concept of practical elimination