Application of the concept of defense in depth to EPR design

Etienne COURTIN
Vienna – June 2017
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- DID3a: Design Basis Conditions (DBC)
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
Application of DID concept to EPR design - Summary

- **DID1**: normal operation
- **DID2**: upset conditions
- **DID3a**: Design Basis Conditions (DBC)
- **DID3b**: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- **DID4**: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
DID1: normal operation

- Purpose: prevention of upset and accident conditions
- Mean: high reliability of normal operation SSCs
- Reliability achieved through
  - High quality
  - Compliance with normal operation procedures
  - Maintenance
  - Inspection
Defense in depth: SB LOCA

Radiological Consequences

DID1
High quality of pipes belonging to RCS
Monitoring of RCS mechanical loads and chemical conditions
Inspection of welds and sensitive areas

Normal operation and AOO

Normal operation limit

High frequency

Low frequency
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- DID3a: Design Basis Conditions (DBC)
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
DID2: upset conditions

- Single initiating event postulated

- Purpose:
  - No escalation to accident conditions
  - No damage to reactor barriers
  - Bring back the plant to normal operating conditions

- Means: Control and limitation systems

- Radiological consequences are kept within normal operation limits
Defense in depth: SB LOCA

**Radiological Consequences**

**DID2: SB LOCA w/ CVCS available**
- Letdown closure + Automatic start of 2nd CVCS pump
- Manual plant shutdown

**DID1**
- High quality of pipes belonging to RCS
- Monitoring of RCS mechanical loads and chemical conditions
- Inspection of welds and sensitive areas

**Normal operation and AOO**

- High frequency
- Low frequency

**Normal operation limit**
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- **DID3a: Design Basis Conditions (DBC)**
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
DID3a: Design Basis Conditions (DBC)

- All relevant single initiating events are considered to build the list of DBC (PIE)
- Bounding DBC scenarios are built to cover the potential consequences of groups of PIEs:
  - Affecting in the same way the plant main parameters
  - Having the same range of frequency
- All plant modes are considered, in particular in shutdown mode (RCS open, refuelling,…)
- Accidents in fuel pool are postulated
- Main analysis rules:
  - Credit safety systems
  - Normal operation systems not credited
  - Conservative assumptions and methodologies
  - Single failure criteria and preventive maintenance, if applicable
- No significant radiological consequences outside the plant
Defense in depth: SB LOCA

Radiological Consequences

DID2: SB LOCA w/ CVCS available
- Letdown closure + Automatic start of 2nd CVCS pump (PRZ level control)
- Manual plant shutdown

DID1
- High quality of pipes belonging to RCS
- Monitoring of RCS mechanical loads and chemical conditions
- Inspection of welds and sensitive areas

DID3a: SB LOCA w/o CVCS
- Reactor trip
- Safety injection (MHSI + LHSI)
- SG and normal cooling chain

Normal operation limit

No consequences on population

Normal operation and AOO

Consistent with CDF target

High frequency

Low frequency

DBA

IAEA – Novel Design – Defense in depth
05/10/2016- p.12

The information in this document is AREVA property and is intended solely for the addressees. Reproduction and distribution are prohibited. Thank you.
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- DID3a: Design Basis Conditions (DBC)
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
DID3b: Design Extension without core melt (DEC-A)

- DEC-A purpose is to demonstrate core melt prevention
  - Deterministic demonstration
  - Based on probabilistic considerations
- Complex sequences with multiple failures should be considered in the design
- Common cause failures are postulated on safety systems
- Two main types of DEC-A:
  - Frequent DBC combined with CCF on a safety system
    - Example: ATWS = DBC2 combined with CCF on reactor shutdown
  - CCF on a support system during normal operation
    - Example: Total loss of heat sink
Overall DEC-A approach

![Graph showing the overall DEC-A approach. The x-axis represents high and low frequency, while the y-axis represents initiating event frequency. The graph is divided into sections for Main line reliability (safety systems) and Diverse line reliability (DEC features). The overall CDF target is indicated by an arrow.]
How to build the list of DEC-A?

- Build a list of plausible complex sequences
  - List all safety systems credited in DBC
  - For each safety system:
    - Postulated a CCF on the safety system
    - Identify the PIEs where this system is credited
    - Keep the plausible combinations
    - Group the various sequences in a representative sequence that covers the others
  - Identify a diversified system that can be used as a back-up to ensure the same function:
    - Either an existing safety system not affected by the CCF
    - Or a dedicated feature for DEC
    - Normal operation systems are not credited

- Identify the representative sequences that need a safety demonstration: list of DEC-A
## DEC-A Some examples

<table>
<thead>
<tr>
<th>DEC-A sequence</th>
<th>Diversified strategy</th>
<th>Dedicated DEC-A feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOO + Failure of reactor trip (ATWS)</td>
<td>Boron injection by EBS</td>
<td>Automatic start of EBS</td>
</tr>
<tr>
<td>AOO + Failure of Protection System (PS)</td>
<td>Diversified protection signals</td>
<td>Diversified automation system</td>
</tr>
<tr>
<td>AOO + Failure of SG</td>
<td>Feed &amp; Bleed</td>
<td>Opening of pressurizer discharge system</td>
</tr>
<tr>
<td>LOOP + failure of EDGs</td>
<td>Ultimate DG</td>
<td>Manual start of Ultimate DG</td>
</tr>
<tr>
<td>SB LOCA + CCF on MHSI</td>
<td>Injection into RCS by LHSI</td>
<td>Fast cooling</td>
</tr>
<tr>
<td>Total loss of heat sink – Hot shutdown</td>
<td>Heat removal by Steam Generators</td>
<td>Refill EFW tanks</td>
</tr>
<tr>
<td>Total loss of heat sink – Cold shutdown</td>
<td>RCS Boiling and containment cooling</td>
<td>Heat removal by CHRS (diversified cooling chain)</td>
</tr>
</tbody>
</table>
DEC-A analysis are less conservative than DBC

However DEC-A analysis are still conservative in order to provide high confidence in the results

Usually:
- Use of DBC models
- Penalization of the most significant plant parameters
- No SFC nor maintenance

DBC4 safety criteria

PSA support studies are NOT accepted as DEC-A analysis:
- Realistic assumptions and modelling
- => insufficient confidence in the safety margins
**Defense in depth**

**Radiological Consequences**

- **DID1**: High quality of pipes belonging to RCS
  - Monitoring of RCS mechanical loads and chemical conditions
  - Inspection of welds and sensitive areas

- **DID2**: SB LOCA w/ CVCS available
  - Letdown closure + Automatic start of 2\textsuperscript{nd} CVCS pump (PRZ level control)
  - Manual plant shutdown

- **DID3a**: SB LOCA w/o CVCS
  - Reactor trip
  - Safety injection (MHSI+LHSI)
  - SG and normal cooling chain

- **DID3b**: SB LOCA w/o MHSI
  - Reactor trip
  - Diversed injection (Fast cooling + LHSI)
  - SG and normal cooling chain

**Normal operation and AOO**

- Consistent with CDF target

**High frequency**

**Low frequency**
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- DID3a: Design Basis Conditions (DBC)
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
DID4: Core melt sequences (DEC-B)

- Regardless of the efficiency of core melt prevention implemented
- Credible core melt sequences are postulated to design the DEC-B features
- The reference sequences representative of the main physical challenge to the containment integrity:
  - SB LOCA
  - LB LOCA
  - Loss of AC power
  - Total loss of feedwater
- Additional extreme sequences are analyzed in order to assess the DEC-B features robustness and the available grace time
- Realistic analysis
- Modelization of phenomena is based on experiments: uncertainties to be considered according to the knowledge sometimes limited
**Aim of DEC-B analysis is to prove that radiological consequences only require protective measures limited in area and time => Main concern is the efficiency of containment**

<table>
<thead>
<tr>
<th>Containment failure mode</th>
<th>DEC-B features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Containment Heating (DCH)</td>
<td>Fast depressurization by Pressurizer Discharge System (PDS)</td>
</tr>
<tr>
<td>Hydrogen explosion</td>
<td>H2 recombiners</td>
</tr>
<tr>
<td>Steam explosion</td>
<td>Dry vessel pit Corium spreading before flooding</td>
</tr>
<tr>
<td>Basemat failure</td>
<td>Spreading area Flooding of spreading area</td>
</tr>
<tr>
<td>High pressure</td>
<td>Containment spray Containment heat removal with dedicated and diversified cooling chain Dedicated ultimate diesel generator</td>
</tr>
</tbody>
</table>
Radiological Consequences

Consequences
- Limited in area and time
- No consequences on population

Normal operation limit

High frequency

Low frequency

DID1: High quality of pipes belonging to RCS
- Monitoring of RCS mechanical loads and chemical conditions
- Inspection of welds and sensitive areas

DID2: SB LOCA w/ CVCS available
- Letdown closure + Automatic start of 2nd CVCS pump (PRZ level control)
- Manual plant shutdown

DID3a: SB LOCA w/o CVCS
- Reactor trip
- Safety injection (MHSI+LHSI)
- SG and normal cooling chain

DID3b: SB LOCA w/o MHSI
- Reactor trip
- Diversed injection (Fast cooling + LHSI)
- SG and normal cooling chain

DID4: SB LOCA w/o SI
- Spreading area
- Diversified cooling chain
- Containment

Consistent with CDF target
Consistent with LERF target

DBA
DEC-A
DEC-B

IAEA – Novel Design – Defense in depth
05/10/2016- p.23

The information in this document is AREVA property and is intended solely for the addressees. Reproduction and distribution are prohibited. Thank you

RESTRICTED AREVA
Application of DID concept to EPR design - Summary

- DID1: normal operation
- DID2: upset conditions
- DID3a: Design Basis Conditions (DBC)
- DID3b: Design Extension Conditions without core melt (DEC-A)
  - Purpose of DEC-A
  - Build the list of DEC-A
  - Analysis rules
- DID4: Design Extension Conditions with core melt (DEC-B)
- Practical elimination
Situations Practically Eliminated (SPE)

- Inacceptable consequences according to SSR-2/1:
  - Large releases (long term contamination)
  - Early releases (no time to protect people)
  - High radiation doses (no more access possible to the site)

- All situations potentially leading to these consequences should be proved "with a high level of confidence to be extremely unlikely to arise"

- Among them, there are specific situations of severe accident where large and early releases cannot be reasonably prevented:
  - Sudden and irreversible failure of containment (explosion)
  - Plant mode or plant location with limited containment ability (spent fuel pool, maintenance with reactor building initially open)

- According to French practice, EPR demonstration of practical elimination focuses on those severe accident situations that may lead to large and early releases
Practical Elimination
List of situations

- Deterministic identification of plausible situations to be practically eliminated
- \( \Rightarrow \) limited list of Situations Practically Eliminated (SPE)
- Identification of plausible sequences leading to those situations
- Design of a set of lines of defense to achieve of very low frequency of each sequence:
  - Independence between lines
  - Overall reliability of the set of lines (classification, maintenance)
  - Robustness of the set of lines in case of hazard (including extreme external hazard)
## Practical Elimination

### List of situations

<table>
<thead>
<tr>
<th>Type of situation</th>
<th>Example of situation</th>
<th>Plausible sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe accident situations leading to specific energetic phenomena occurring after fuel melting</td>
<td>Severe accident leading to hydrogen explosion</td>
<td>Any severe accident sequence</td>
</tr>
<tr>
<td></td>
<td>Severe accident leading to high pressure RPV failure and Direct Containment Heating (DCH)</td>
<td>Any high pressure severe accident sequence</td>
</tr>
<tr>
<td>Severe accident situations resulting from energetic phenomena before core melt</td>
<td>Severe accident resulting from core prompt criticality after massive reactivity insertion</td>
<td>Heterogeneous dilution</td>
</tr>
<tr>
<td>Severe accident occurring in a plant mode or plant location with limited containment ability</td>
<td>Fuel melt in the spent fuel pool (during handling or storage)</td>
<td>Total loss of fuel pool cooling</td>
</tr>
<tr>
<td></td>
<td>Severe accident during cold shutdown with reactor building open for maintenance</td>
<td>Total loss of heat sink with equipment hatch open</td>
</tr>
</tbody>
</table>