ON SOME CHALLENGES IN DEFINING AND USING DEFENSE IN DEPTH AND SAFETY MARGIN CONCEPTS, AS HIGHLIGHTED BY THE SAFETY IMPROVEMENT PROCESS

Dr. ing. Dan SERBANESCU
Romanian Academy, Division of Logic, Models in Science of the Romanian Committee for History and Philosophy of Science
Bucharest, Romania
Email: dan.serbanescu1953@yahoo.com

International Atomic Energy Agency - IAEA
International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants CN-251
Vienna, Austria
6 - 9 June 2017
GOAL

• To present results on the evaluation performed by the author for the duration of two decades in Nuclear Power Plants (NPP) safety projects in a special set of cases.

• The focus is on the lessons learnt from the perspective of the safety decisions for NPP for almost four decades.

• The presented issues reflect insights resulted from the author’s participation in safety analyses and reviews for the same national nuclear project for the last four decades and a prediction on the expected dominating issues in those cases for the next ten years.

• The presented issues represent a specific experience and represent author’s view.

• Presentation in the paper is in a “story telling”. However for a detailed systematic evaluation using decision criteria and mathematical tools see:

SERBANESCU D., A specific experience on some challenges in defining and using defense in depth and safety margin concepts, as highlighted by the safety improvement process, *elaborate information for the paper submitted to IAEA for conference Topical Issues on Nuclear Safety* DOI:10.13141/RE.2.1.4859.2488
[https://www.researchgate.net/publication/316542989_A_specific_experience_on_some_challenges_in_defining_and_using_defense_in_depth_and_safety_margin_concepts_as_highlighted_by_the_safety_improvement_process](https://www.researchgate.net/publication/316542989_A_specific_experience_on_some_challenges_in_defining_and_using_defense_in_depth_and_safety_margin_concepts_as_highlighted_by_the_safety_improvement_process)
Review cases

Case A  Licensing process of Cernavoda NPP unit 1 and decisions on restart Cernavoda unit 2 construction, aside with the decision on conservation of units 3-5. This involved the period of completion of construction of unit 1, commissioning of unit 1 by an international consortium and first initial year of operation of unit 1. In unit 2 continuations of works for construction but at a slower pace. The period was 1993-1997.

Case B  Licensing of Cernavoda passing into a mature stage of operation and restarting of construction of unit 2. This period was 1997-2000.

Case C  Mature operation of unit 1 and first initial operation of unit 2. This period is from 2000-2010.

Case D  Preparation for refurbishment for unit 1 and evaluations on new generation IV type of research reactors to be built, preparations to restart activities for completion of units 3 and 4. Period is 2012-2017.

Case E  Foreseen period of refurbishment of unit 1, start of preparation of refurbishment for unit 2, possible commissioning of units 3 and 4, possible construction of new generation IV research reactor. Period is from 2017 on, with a projection on the next ten years.
ON SOME CHALLENGES IN DEFINING AND USING DEFENSE IN DEPTH AND SAFETY MARGIN CONCEPTS, AS HIGHLIGHTED BY THE SAFETY IMPROVEMENT PROCESS - Dr.ing. Dan SERBANESCU - Romanian Academy, Division of Logic, Models in Science
ON SOME CHALLENGES IN DEFINING AND USING DEFENSE IN DEPTH AND SAFETY MARGIN CONCEPTS, AS HIGHLIGHTED BY THE SAFETY IMPROVEMENT PROCESS - Dr.ing. Dan SERBANESCU  Romanian Academy, Division of Logic, Models in Science
Nuclear fission reactors – human made and nature made

CHICAGO PILE 1942-1943

OKLO GABON CCA 2 BLN YEARS AGO
Strategies for a period starting from safety reviews

S1 (Period 1 - Cases A, B and C) - During this phase the safety concepts are consolidated and recognized internationally in standard like format, defined as the first period. Vendors are adapting the initial safety philosophy to the changes required to fit the national regulations (of USNRC type) and a national licensing process organized like a regulatory project was defined. New set of regulations are under preparation, enveloping the experience gained. Interface and full implementation of safety approaches from IAEA, EU and Canada were used as guiding expertise. The first reports under Convention on Nuclear Safety are submitted and Romania is in preparation for aligning safety approaches to EU set of requirements.

S2 (Period 2 Case D) - In this phase the safety concepts, national regulatory approaches were consolidated. Special issues were under research for advanced new generations of NPP and / or restart of units 3-4, as well as lifetime extension issues. Consolidation considered a certain optimism (specific to the “nuclear renaissance” period actually) and did not anticipate intense actions to review approaches to be adopted after Fukushima accident. During this period Romania became member of the EU and mature regulatory environment

S3 (Period 3 - Case E) - This is dominated by post Fukushima actions and events on safety. There is ongoing work (at international level reflected also at national level) on issues like independence of all the safety layers of the Defense in Depth (DiD) and the issues related to the extension of the Design basis Accidents (DBA) in the format of Design Extended Conditions (DEC), that tackles the issues of Safety Margins.
Specific features of the inputs for decision for the evaluated cases (1)

For the period 1

The set of safety documents developed by the owner of the CANDU concepts at the level of the 1980’s and later on with the updates from the Vendor and experience of other CANDU owners. Core Damage Frequency (CDF) and other risk metrics insights as per the PSA level 1 developed in Romania for Cernavoda NPP in the early 1990’s and reviewed to a more mature state up to 2000. The probabilistic safety envelope of the CANDU concept defined originally by the Canadian designer in a set of Reliability Analyses (RA) and Safety Design Matrices (SDM). Results from the commissioning process of Unit1 and the intensive interface with IAEA and Canadian regulator.
Regulatory experience gained after the licensing process of unit 1 and systematic review of the regulatory pyramid in order to document the new status.
Specific features of the inputs for decision for the evaluated cases (2)
For the period 2

The review of compliance with DiD and SM and of the postulated events (including possible extension of DBA list) were considered based on the experience from unit 1 and coordinated with international and CANDU owners evaluations. Design changes as implemented to consolidate the SM and the DiD layers in accordance with experience from CANDU community. A plant specific PSA level 1 for internal and external events completed and its use for operation and as risk monitor started. PSA level 1 becoming part of the required licensing safety documentation and used for current operation of units. PSA level 2 and severe accidents evaluations (Severe Accidents Management Guidelines – SAMG).

Full scale Long Term Operation (LTO) and ageing programs.

Develop and implement Periodical Safety Review (PSR)
Implementation of risk management throughout all the plant processes – hardware and software and use of the elements of Risk Informed Decision Making (RIDM) for decisions on SM and DiD.
Specific features of the inputs for decision for the evaluated cases (3)

For the period 2

Alignment to new EU safety directives and preparation for the first reports under it
Participation in international actions on review the DBA and adopt DEC concepts, with direct impact on national approach on DiD and SM for plants in operation and their long term perspective and for the restart of construction of units 3 and 4.
Completed PSA level 2 and severe accidents evaluations review
Work on specific CANDU issues of refurbishment of an operating unit in order to extend the operating lifetime.
Work on restarting a project of NPP after it is was stopped and conservation assured for a long period of time.
Specific features of the inputs for decision for the evaluated cases (4)

For the period 3

Implementation full scale of LTO and specifics of refurbishment for unit 1. Continuation of alignment to new EU safety directives and preparation for the reports under it as per WENRA agreed guidelines
Final decisions and implementation on DEC for old and new units.
Decisions on specifics of licensing for research reactors of generation IV.
Preparations for shutdown and decommissioning of unit 1 and refurbishment for unit 2.
Main results

The main insights based on expert evaluations are in accordance with the detailed list and description of the MCDA tools used as an alternative to expert judgment as presented in [1]. Those insights illustrate some major aspects on SM and DiD, as well as on safety in general, and they are listed as perceived by the author:

On safety and safety programs in general:

• There is a high impact on the implementation work for regulating and self-regulating on safety if the nuclear program for a country has a first start, with a vendor from a country owning the concept. To make things more complicated the safety concepts of the owner itself and the community of that NPP type evolves from the moment the plant starts to be built to the moment it has to be regulated as an operating plant.
• It is of high priority to build and make operable a regulatory safety environment in an importing NPP country, as there is no substitute for the need to build the own national capabilities and human expertise.
• The importing country has a very difficult task to build and preserve the knowledge accumulated and the staff trained at the end of the initial process.
• NPP is an evolving technology, with all the implications of this classification and the evaluations of its major accidents (for details see [4]).
- On specific safety issues, including DiD and SM (1)

• If the importing country of a NPP has initial regulatory framework having differences on safety issues (including the manner DiD and SM are considered) than there is a tremendous case by case work, that needs also international support in order to implement the best SM and DiD concepts for the new built.

• For the cases under periods 1 to 2 the paper underlines the fact that the conceptual framework considering SM and DiD came asymptotically to an equilibrium from the regulatory point of view, reflecting the maturity reached on safety issues at the national level.

• However this asymptotic level indicates in author’s opinion on a possible resurgence of the more “traditional” deterministic evaluations in the future. This means that the trend of an increased role of intrinsic safety features, of using passive components improving human and organizational factors contribution to the safety evaluation is going to be maintained.

• The final safety decisions taken for all the cases were considered and are confirmed as solid conservative ones, while not putting a burden on the licensing process. However the decision process was based on systematic evaluation of inputs, use of MCDA tools and international peer review and support.
Results of comparison of benchmarking type for the safety evaluations for Cernavoda NPP unit 1[6]

Example of results from PSA level 1 versions of 1995-2000 used to review SM and DiD issues [6]
### DETAILED CRITERIA FOR THE EVALUATION OF RESULTS

<table>
<thead>
<tr>
<th>CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR1</td>
<td>CRU</td>
</tr>
<tr>
<td>CR2</td>
<td>CRC</td>
</tr>
<tr>
<td>CR3</td>
<td>LEC</td>
</tr>
<tr>
<td>CR4</td>
<td>SM</td>
</tr>
<tr>
<td>CR5</td>
<td>DIDA</td>
</tr>
<tr>
<td>CR6</td>
<td>DIDI</td>
</tr>
<tr>
<td>CR7</td>
<td>CEE</td>
</tr>
<tr>
<td>CR8</td>
<td>DPC</td>
</tr>
<tr>
<td>CR9</td>
<td>CHC</td>
</tr>
<tr>
<td>CR10</td>
<td>CGEN</td>
</tr>
<tr>
<td>CR11</td>
<td>CSIT</td>
</tr>
<tr>
<td>CR12</td>
<td>CEP</td>
</tr>
</tbody>
</table>

**Criteria to evaluate results**

- **BAS-U1**: General requirements for safety analysis and evaluation.
- **EQUIV RO**: Equivalence rules.
- **PRA.1**: Probabilistic Risk Assessment.
- **PERIOD I 90-00**: First period of operation.
- **U2**: Unit 2.
- **GII+**: Generation II+.
- **AGE**: Age.
- **PERIOD II 00-11**: Second period of operation.
- **L2**: Unit 2.
- **RESTART**: Restart conditions.
- **REFURB**: Refurbishment.
- **PERIOD III 11-17**: Third period of operation.
- **PERIOD IV NEXT 10 YEARS**

<table>
<thead>
<tr>
<th>Code</th>
<th>Period I</th>
<th>Period II</th>
<th>Period III</th>
<th>Period IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRU</td>
<td>L M M M</td>
<td>L L L M</td>
<td>L M L L L</td>
<td>L M</td>
</tr>
<tr>
<td>CRC</td>
<td>H M L M</td>
<td>H M L M</td>
<td>M L L L L</td>
<td>L M</td>
</tr>
<tr>
<td>LEC</td>
<td>M H M M</td>
<td>M H L M</td>
<td>M M M M M</td>
<td>M H</td>
</tr>
<tr>
<td>SM</td>
<td>M M L M</td>
<td>M H H H</td>
<td>M H H H H</td>
<td>H H</td>
</tr>
<tr>
<td>DIDA</td>
<td>M M L M</td>
<td>M H M M</td>
<td>M H M M H</td>
<td>H H</td>
</tr>
<tr>
<td>DIDI</td>
<td>L L M L</td>
<td>L M L M</td>
<td>M M M M M</td>
<td>M M</td>
</tr>
<tr>
<td>CEE</td>
<td>L L L L</td>
<td>L L L L</td>
<td>L L L L L</td>
<td>L M</td>
</tr>
<tr>
<td>DPC</td>
<td>M M L M</td>
<td>M H L M</td>
<td>M L M M M</td>
<td>M M</td>
</tr>
<tr>
<td>CHC</td>
<td>L L L L</td>
<td>L L L L</td>
<td>M M M M M</td>
<td>M M</td>
</tr>
<tr>
<td>CGEN</td>
<td>L M M M</td>
<td>M H M M</td>
<td>M H H H H</td>
<td>H H</td>
</tr>
<tr>
<td>CSIT</td>
<td>L M L L</td>
<td>L M L L</td>
<td>M L L L L</td>
<td>M M</td>
</tr>
<tr>
<td>CEP</td>
<td>L M L L</td>
<td>L M L L</td>
<td>M M M M M</td>
<td>M H</td>
</tr>
<tr>
<td>CR TOT</td>
<td>L M L M</td>
<td>L M L M</td>
<td>M M M M M</td>
<td>M M</td>
</tr>
</tbody>
</table>
# SUMMARY OF THE IMPACT ON SM AND DiD FOR THE CONSIDERED CASES

<table>
<thead>
<tr>
<th>STRATEGIES-CASES-METHODS</th>
<th>RESULTS - MAIN FEATURES</th>
<th>IMPACT ON SM &amp; DiD TYPE OF IMPACT ON SM &amp; DiD</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRATEGY</td>
<td>CASE</td>
<td>METHOD</td>
</tr>
<tr>
<td>S1</td>
<td>BAS-U1</td>
<td>M2</td>
</tr>
<tr>
<td></td>
<td>EQUIV RO</td>
<td>M2</td>
</tr>
<tr>
<td></td>
<td>PRA 1</td>
<td>M1</td>
</tr>
<tr>
<td>S2</td>
<td>U2</td>
<td>M2MOD</td>
</tr>
<tr>
<td></td>
<td>PBMR</td>
<td>M3 P</td>
</tr>
<tr>
<td></td>
<td>AGE</td>
<td>M4 A</td>
</tr>
<tr>
<td>S3</td>
<td>L2 U1 2</td>
<td>M5 ST</td>
</tr>
<tr>
<td></td>
<td>REST</td>
<td>M5WE</td>
</tr>
<tr>
<td></td>
<td>REFURB</td>
<td>M5 WE</td>
</tr>
</tbody>
</table>
Impact on SM and DiD for the evaluated cases in the periods 1 to 3 and forecast for period 4
Impact on complementary criteria for the evaluation of SM and DiD in the considered cases in the periods 1 to 3 and forecast for period 4
On specific safety issues, including DiD and SM (2)

- On the other side it is also noted that the change control in the era or post Fukushima changes becomes of highest priority for maintaining the initial designed set of SM and DiD layers. It might be that by avoiding cliff edge effects (CEE) for instance, future changes of post Fukushima type may endanger basic safety feature already existent in the initial basic design,
- In our opinion this is the best way how changes have to be made extremely carefully
ON SOME CHALLENGES IN DEFINING AND USING DEFENSE IN DEPTH AND SAFETY MARGIN CONCEPTS, AS HIGHLIGHTED BY THE SAFETY IMPROVEMENT PROCESS - Dr.ing. Dan SERBANESCU, Romanian Academy, Division of Logic, Models in Science

Summary of evolution of impact on SM and DiD of various safety actions taken for the cases in Table 1
CONCLUSIONS

• The paper presents the evaluation performed in a specific case of NPP cases within a significant period for the lifecycle.

• There are many insights from the practical experience of performing safety evaluation with the objective to check the level of compliance with safety requirements, protection in layers (DiD) and the level of available SM and hence to judge on the conservatism of the decisions taken. The cases are related to real situations and therefore experience could be of use for further similar cases.

• The paper presents also some insights on the potential issues of concern in the safety evaluations, of which SM and DiD evolutions were considered dominant. However, it is mentioned that it should not be forgotten the fact that NPP is a technology and that SM and DiD approaches (for example if we take the interpretation proposed in [4]) are changing systematically and a continuous update is needed for the safety regulatory environment.
• Serbanescu D., A New Approach In Nuclear Risk Theory, in the IAEA document Use OF PSA in the regulatory process, Vienna, Austria, 26-29 April 1993
• Serbanescu D., CNCAN basic requirements for the PSA level 1, Specialist meeting on Use of the PSA in the regulatory process, IAEA Vienna 26-29 April 1993
• Serbanescu D., Systematic biases in event review and their impact on learning process