Comments and questions to Draft safety guide DS 508 “Application of the Safety Approach to the Design of Nuclear Power Plants” (revision received via e-mail 10/01/2020)

1. The name of the Draft safety guide DS 508 changed from what is indicated in DPP, instead of “Assessment of the Application ...” only “Application ...” is indicated. Also in DPP it’s explicitly stated that: “The objective of this safety guide is to provide recommendations on the assessment of the implementation of selected requirements in SSR 2/1, Rev.1, and GSR Part 4, Rev. 1, relating to defence in depth and practical elimination of event sequences leading to early radioactive releases or large radioactive releases”.

Concrete paras (requirements) SSR-2/1, GSR-4 are listed in Section 5 of the DPP. In the sections “background”, “objective”, “scope” of the DS 508 new revision these explanations are not included. Instead, there is ambiguous information about the scope and objectives of the developed guide, for example:

- in para 1.4 DS 508 with reference to GSR Part 4 is stated “specific and detailed guidance is needed to address specific aspects of relevance for a comprehensive and sound safety assessment”. But in fact, the safety guide DS 508 focuses on the implementation of only the requirements of SSR-2/1, and not their assessment. In paragraphs 2.15 ÷ 2.19 DS 508 the general assessment recommendations are actually repeated, but there are no special recommendations explaining the provisions of GSR Part 4 in relation to the issues under consideration;

- in para 1.10 DS 508: «The scope of this safety guide is focused on the implementation and assessment of the additional measures mentioned in 1.3 as they relate to defence in depth and safety functions, and to the practical elimination of event sequences that would lead to early radioactive releases or large radioactive releases ...»), but in para 1.3 is stated «measures for strengthening the implementation of defence in depth by: a. Considering design extension conditions», also in para 1.11 is stated «The guide is not intended to provide specific recommendations for the design of safety features for design extension conditions or for any other plant states. These are provided in the safety guides for the design of various types of plant systems» (at the same time, it is not indicated what kind of guides is referenced - there is no specific link to such a document);

- in para 1.13 DS 508 «Section 2 introduces the overall safety approach in the design for preventing harmful consequences to workers and the public»;

- in para 2.6 DS 508 “This safety guide in primarily focus on safety measures in the nuclear power plant design”.

1
It is proposed in Section 1 of the DS 508 to more clearly define the goals and objectives of this safety guide, as well as indicate the specific requirements of SSR-2/1 and GSR part 4, which are discussed in this safety guide.

2. DS 508 contains a large amount of text, which is a quotation of other IAEA documents without any additional explanation, primarily SSR-2/1, SF-1. For example:
   - paras 2.2, 2.4 quote twice fundamental security principle 8 SF-1;
   - all para 2.7 is a quote of the requirement of para 4.9 SSR-2/1 without any comment. The same in paras. 2.13, 3.52, 3.53;
   - para 2.9 (quote requirements SSR-2/1 to DiD);
   - para 3.58 (provided with reference to para 5.29 SSR-2/1 which actually the same as the text specified in para 3.58 DS 508);
   - also see. paras 2.36, 3.30, and others.

   It is proposed, where possible, to reduce the quotation of the text, in some cases replacing it with a general description of the topic with reference to a specific paragraph of the IAEA standard and comments about this IAEA requirements.

3. DS 508 does not contain information (provisions) about assessment (process of assessment) of list of scenarios that considered as “practically eliminated”

   Please clarify:
   - In what form this analysis and its substantiation should be documented (should such a list be presented in the sections of the SAR devoted to accident analysis)?
   - How should “practical elimination” of a number of events (that, according to Appendix A, should be included in the list of “practically eliminated”, for example, a hydrogen explosion) be evaluated if there is a possibility of failure of the means for DEC-B management in severe accidents and there are no results of direct experiments, confirming their unambiguous work in any conditions?
   - Should we take into account possibility of realization of “practically eliminated” scenarios with the aim of taking measures to eliminate their consequences at level 5 of DiD?
4. In para 1.13 DS 508 is stated «Section 3 addresses the need to establish safety provisions for minimizing radiological consequences in case of very unlikely plant conditions exceeding the plant design envelope in the framework of the implementation of defence in depth».

But section 3 is called “Implementation and assessment of the concept of defence in depth”.

5. In para 2.12 DS 508 “The occurrence of unexpected and very unlikely extreme scenarios should be considered and their consequences assessed, regardless of all the design provisions implemented to prevent postulated accidents from escalating to more severe consequences, and to make the likelihood of an accident with serious radiological consequences extremely low, This is also a lesson learned from the Fukushima Daiichi accident”.

Please clarify what scenarios (“unexpected and very unlikely extreme”) are involved - scenarios considered at level 5 of the DiD? How should they be assessed and what measures should be taken?

6. In para 3.18 DS 508 “Design basis accidents conditions … The operation of safety systems should be automatic not requiring the need of human intervention and their reliability should be very high. …”.

But according to para 7.37, 7.38 SSG-2 operator intervention is permitted in some cases “if it can be shown that the event sequence and the plant specific boundary conditions allow for carrying out the assumed actions”.

7. In para 3.28 DS 508 “Containment leakage in a severe accident should remain below the design leakage rate limit for sufficient time to allow implementation of emergency measures. Beyond this time, containment leakage that would lead to exceeding the small and large release safety goals should be precluded. This may be achieved by provision of adequate filtered containment venting along with other features”.

But the issue of ventilation of the containment in the accident condition (especially severe ones) is a difficult task, failure and incorrect operation of the ventilation system can lead to a large release (bypass of the containment) so it is proposed to add the need to analyze the operability of filter materials (or other filtration devices) in a severe accident to the list of necessary analyzes specified in para 3.29.

It is also worth noting that the failure of the containment filtration system in a severe accident conditions (in the absence of sufficient control over the filter elements) can lead to a large emergency release in a fairly short time and, thus, this case can be considered as one of the cases that, under certain circumstances, can lead to a "cliff edge effect”

What kind of “conditions having harmful effects for the people and the environment” are discussed in this para? Any or all related to nuclear and radiation safety?
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Why is independence important for such systems if it’s said that their failure already creates undesirable conditions?</strong></td>
<td></td>
</tr>
<tr>
<td><strong>9.</strong></td>
<td>According to 4.28 DS 508 “Design provision and operational provision for “practical elimination” of some severe accident conditions may be vulnerable to potential human errors prior to the accident. In such a case, the SSCs used to deliver the action are subject to relevant operational provisions to limit the occurrence of human errors (e.g. periodic testing, in-service inspections, commissioning tests following maintenance activities…).” Please clarify: How do these measures reduce the mentioned “human errors”, as they are implemented in any case during operation of NPP, but at the same time, as a rule, they do not take into account the conditions of a “severe accident” (it should be noted that these requirements are already given in paragraph 4.26 DS 508).</td>
</tr>
<tr>
<td><strong>10.</strong></td>
<td>In para 4.42 DS 508 is stated: “Considering the above, demonstration of physical impossibility cannot rely on measures requiring active components or human interactions”. Please clarify whether passive safety systems can be considered in this case. Can we use passive systems (including those using active components) to demonstrate “practical elimination”, in what extent?</td>
</tr>
<tr>
<td><strong>11.</strong></td>
<td>Is it possible to consider situations with the modification of NPP elements as requiring a mandatory revision of the concept of scenarios previously recognized as “practically eliminated”? Should we revise “practically eliminated” scenarios each time when a periodic safety assessment provided? What approaches should we use to document and evaluate current list of events, initially (in the design) recognized as “practically eliminated”, during the operation of NPP’s unit?</td>
</tr>
<tr>
<td><strong>12.</strong></td>
<td>It’s proposed to add recommendations into Section 4 similar to those contained in the «RHWG report for the attention of WENRA Report Practical Elimination Applied to New NPP Designs - Key Elements and Expectations. 17 September 2019» with regard to: - role of administrative measures; - provisions important for achieving practical elimination have to remain in place and valid throughout the plant lifetime. It is proposed to move the provisions of paras 4.26, 4.31 DS 508 to these sections</td>
</tr>
<tr>
<td><strong>13.</strong></td>
<td>Please clarify whether when formulating cases that should be practically eliminated in relation to the SPF (indicated in paras A.7 ÷ A.9 of Appendix A DS 508), is it necessary to take into account situations arising from fuel overload and repair of the SPF compartments, including the case of the reactor core being completely unloaded into the SPF?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| **14.** | Please clarify IAEA's approach to accidents that are considered "practically eliminated" because they are accepted as "to be extremely unlikely to arise"? Is these accidents should be taken into account in emergency planning at the level 5 of DiD, and do these scenarios of accident need to study to determine the impact of these accidents?

*Note. According to Russian General safety provision for safety of NPP (NP-001-15) the approach to development of technical and organizational measures, aimed at preventing accidents and constraining their consequences:*

- If a large accident release probability is more than $10^{-7}$ per year: the NPP design shall provide for additional technical features (including special technical means for BDBA management) to manage accidents with the purpose of decreasing the probability of accidents and mitigating their consequences
- For the BDBAs that are not exempted due to inherent safety features of the reactor and principles of its arrangement regardless their probability, organizational measures shall be developed to manage such accidents including measures for decreasing radiation exposure for the personnel, public, and environment by implementing plans of actions for protection of personnel and public in case of an accident.

| **15.** | WENRA document “Guidance Document Issue F: Design Extension of Existing Reactors 29 September, 2014”) states:

- «When analysing a sequence in the framework of DEC analysis, an end state should be defined and justified for this analysis. For DEC A, the “defined end state” could be a “safe state” as defined in IAEA SSR-2/1»;
- «in case of DEC B, it is unlikely to reach such a safe state. Therefore, the DEC B analysis should cover a reasonable period of time, until some other defined end state is reached. This could be a “controlled state after severe accident”. This is a state after a severe accident where decay heat removal is ensured, the damaged or molten fuel is stabilized, re-criticality is prevented and long term confinement is ensured to the extent that there is limited release of radioactive nuclides»

In section 3 of DS 508, it is proposed to make similar provisions accompanied by a block diagram (as in figure 1 of the above-mentioned WENRA document)

To section «MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF VERY UNLIKELY CONDITIONS EXCEEDING THE PLANT DESIGN ENVELOPE»

| **16.** | Section 9 “DESIGN FOR EXTERNAL HAZARDS” TECDOC-1791 ends with text: “The implications of the requirement above have not yet been formally addressed in any safety standard of the IAEA, but it is clear that there are some important issues to be addressed and resolved. In particular, it is necessary to compile the list of
the equipment ultimately necessary to prevent an early radioactive release or a large radioactive release and then to provide guidance on the external events to include in the design basis of these equipment and on the rules for their design and qualification, and for the assessment of the margins”.

Also, in para 7.2.2 TECDOC-1791 is stated: «For some external hazards it may not be not practical or even possible to demonstrate that the occurrence of a hazard of such severity that could cause extensive plant damage leading to a large or early radioactive release, and therefore needing to be practically eliminated, is below a threshold of frequency such as 10-6/year».

But in DS 508, these issues regarding external events are not considered in sufficient quantities, with the exception of certain provisions contained in paras 2.20 ÷ 2.35 DS 508, to which there are also questions and suggestions (see below)

### 17.
In para 2.20 ÷ 2.35 DS 508 are considered «very unlikely extreme scenarios exceeding the design envelope of the nuclear power plant».
Please clarify: How could these scenarios be taken into account in the DiD levels (at what level are they considered)?

### 18.
Please clarify requirements used to evaluate “fixed or non-permanent equipment stored on-site or off-site», mentioned in para 2.22 DS 508?
Also in para 2.26 DS 508 is stated: «To make more reliable the coping strategies an adequate balance between fixed equipment and non-permanent equipment should be implemented».
Does the mentioned equipment belong to elements intended for DEC? (in the text does not mention at which DiD level the equipment is used, as a rule non-permanent equipment is only used at DEC or at level 5 DiD).

### 19.
In para 2.27 DS 508 it is proposed to add that in conditions of extreme external events (primarily leading to SBO), one of the preferred strategy (depend on the character of event) is to use passive systems together with non-permanent equipment, which can be used to prolong the operation of passive systems.

### 20.
In para 2.29 DS 508, after: “The ability to deliver and operate non-permanent equipment on time should also be demonstrated under bad meteorological conditions at the site”, it is proposed to add "especially in conditions of sub-zero air temperature".
Also in para 2.29 DS 508 it is proposed to specify: "the possibility of quick repairs and the availability of spare parts for non-permanent equipment should be taken into account."
21. Please clarify п. 2.31 DS 508 «To increase credibility of the coping strategies an estimate of the time available for the implementation of the operator actions before cliff edge should be made».
Shouldn't we try to avoid situations with the emergence of the “cliff edge effect”? How should specified time be calculated in relation to "CONDITIONS EXCEEDING THE PLANT DESIGN ENVELOPE", especially in the case of external hazards (also it’s look like this paragraph duplicate the provisions of paragraph 2.24 DS 508).

### Additional comments

<table>
<thead>
<tr>
<th>22.</th>
<th><strong>Add at the paragraph 3.14 DS 508 after words «the engineered safety features (safety systems) is foreseen»</strong>&lt;br&gt;<strong>An important aspect of preventing an escalation to accident conditions for failures or deviations from normal operation is careful selection and justification of the safety limits.</strong>&lt;br&gt;<strong>According to IAEA safety glossary, Safety limits are «Limits on operational parameters within which an authorized facility has been shown to be safe».</strong>&lt;br&gt;<strong>Nuclear facility is safe if its radiation impact on personnel, public, and environment does not lead to exposure higher than the doses established for personnel and public radiation exposure in standards for emissions and releases in case of normal operation and operational occurrences, including DBAs.</strong>&lt;br&gt;<strong>It means that the analysis of DBAs (including DEC) should not be limited by initial states corresponding to normal operating conditions, but should include initial states characterized by operational parameters from the area limited by the safety limits. Most unfavorable, but possible combination of these parameters should be taken into account. For example, it should be shown that when the reactor is operating at a thermal power level corresponding to the safety limits, for all DBA’s (including DEC) radiation impact will be below the limits set for these accidents and will remain at a reasonably achievable low level. Herewith, most unfavorable, but possible combination of other operational parameters (such as axial offset, flow/power ratio, input temperature of the coolant, etc.) should be considered.</strong>&lt;br&gt;<strong>It is important to emphasize that the safety limits should not be confused with the acceptance criteria used in the analysis of accident processes. For example, the fuel melting point which often used as an acceptance criterion in safety analyses of water-cooled reactors can’t be used as safety limit. If in the initial state the fuel temperature were close to the melting point, the installation would not be considered safe, taking into account the DBAs (including DEC) that could occur in this initial state. On the other hand individual safety limits can serve as acceptance criteria which provides greater conservatism in the safety analysis.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As practice shows the safety justification, including analysis of DBAs is carried out as a rule for initial states corresponding to normal operating conditions. The values of operational parameters in this case vary within the normal operational limits while according to the IAEA Glossary the safety of the facility should be demonstrated for a wider range of initial states operational parameters of which are limited by the safety limits. The proposed amendment focuses on this issue. Such approach will provide more realistic assessment of safety margins, more reliable</td>
</tr>
</tbody>
</table>
Commentary on section 4 DS 508

The separation of accidents proposed in DS508 into DBAs (including DEC) and “practically eliminated” instead of DBAs and BDBAs seems unjustified.

According to Table 1 DS508 DBAs (including DEC) cover scenarios where absence of early or large radioactive releases can be proven by deterministic methods.

In accordance with this definition BDBAs should be classified as accidents for which there is a possibility of such releases.

According to recommendation 2.11 SSR-2 (Rev.1) these conditions should be considered with a high level of confidence to be extremely unlikely to arise. How “extremely unlikely” is set in each country separately by the national regulator. For example, according to Russian regulatory requirement (NP-001-15): “Integrated probability (for each NPP unit) of large emergency release shall not exceed of $10^{-7}$ per year”.

The procedure for selecting individual scenarios to prove “practical elimination” and their categorization proposed in paras 4.16-4.20 DS 508, is practically no different from the traditional approach to defining scenarios of severe BDBAs.

The demonstration of a "practical elimination" is also not in principle different from the traditional analysis of severe BDBAs. In BDBAs analysis the probability and scale of an early or large release can only be determined and conclusion can be made on the conformity of recommendation 2.11 SSR-2/1 (Rev. 1).

If the considered scenario of BDBA does not lead to an early or large release, it can be classified as DEC.

Thus, in order to achieve the goal set forth in para 2.11 of SSR-2/1 (Rev. 1), it is not necessary to introduce a new term of "practical elimination" accidents or scenarios. For this, the already existing and universally accepted concept of BDBA or severe BDBA is quite sufficient.

In this regard, it is proposed section 4 "Practical elimination ..." replace with section 4. "Severe BDBAs ....".

According to the Ockham’s razor "Entities should not be multiplied without necessity" In our opinion, there is no real necessity for the concept of “practical elimination” in such a wide scope as it was done in the DS508.

The repeated mention of "practical elimination" and lengthy explanations of this concept create distrust of him, as an advertising slogan, and not a technical term.

In our opinion, the explanation given in Note 2.11 of SSR-2/1 (Rev.1) regarding the “practical elimination” is sufficient to unambiguously understand this paragraph.
| 24. | **Annex 1 DS 508. Add at the end of paragraph A.1**  
An accident with the break of a reactor vessel should not be excluded from consideration only on the basis of the low probability of the initiating event. In view of the extremely large and rapid radioactive release following a break of vessel and possible destruction of the containment, the safety demonstration should be based on risks-informed approaches to the environment and the population. | An accident with the break of a reactor vessel can have extraordinary consequences and therefore requires an individual approach. |
| 25. | **Annex 1 DS 508. Add at the end of paragraph A.8**  
An accident with the sudden insertion of cold or un-borated water plug into a reactor core should not be excluded from consideration only on the basis of the low probability of the initial event. In view of the extremely large and rapid radioactive release resulting from the acceleration of a fast neutron reactor and the possible destruction of the containment, the safety demonstration should be based on risks-informed approaches to the environment and the population. | An accident with a with the sudden insertion of cold or un-borated water plug into a reactor core can have extraordinary consequences and therefore requires an individual approach. |