| COMMENTS BY REVIEWER<br>Reviewer: Page…. of….<br>Country/Organization: Russian Federation/SEC NRS Date: November 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | 3.39<br><br><br><br><br><br><br><br><br><br>4.38 | Effectiveness of safety provisions for each level of defence in depth is assessed through ~~engineering assessment and~~ deterministic analysis involving the use of validated and verified codes and models to demonstrate that acceptance criteria are met with sufficient margins.<br><br>Analysis of severe accidents should be performed using a realistic approach (Option 4 in Table 1, Section 2 of SSG-2 Rev.1[4]) to the extent practicable. Because, explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.<br><br>(*We propose to add in Para 4.38 information about the criteria when the performing of the uncertainty* | There is no definition of the term «the engineering assessment» in DS 508.<br><br>According to Requirement 18 of GSR Part 4 rev.1, uncertainty analysis shall be performed and taken into account in the results of the safety analysis. In other hand, according to Para 4.38 of DS508 and Para 7.54 of SSG-2 (Rev.1), in some cases uncertainty analysis should not be performed for severe accidents analysis results. But neither SSG-2 (Rev.1) nor DS 508 do not provide any details on the criteria when the performing of | Y | 3.39<br>Changed to assessment of engineering aspects<br><br>Do you think that DSA, with the scope included in SSG-2 or chapter 15 of the SAR is sufficient for a safety demonstration ?<br><br>Deterministic Safety analysis in the Safety Glossary is defined as:<br><br>Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result.<br><br>Don't we need a better definition?<br><br>Do you thing DSA, considering a better definition is sufficient?<br><br>How do you call what you find in chapters 4,5,6, etc?<br>Are all these chapters irrelevant ?<br><br>I can find several definitions for engineering assessment in Google<br><br><br>4.38 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | *analysis is necessary for severe accidents analysis results.)* | the uncertainty analysis is necessary for severe accidents analysis results. | | Requirement 18 of GSR Part 4 rev.1 is about computer codes<br><br>***Requirement 18: Use of computer codes***<br>***Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation***<br><br>*The uncertainties, approximations made in the models, and shortcomings in the models and the underlying basis of data, and how these are to be taken into account in the safety analysis, shall all be identified and specified in the validation process. In addition, it shall be ensured that users of the code have sufficient experience in the application of the code to the type of facility or activity to be analysed.*<br><br>It says something different from what you say in the comment<br><br>SSG-2 says<br><br>*For design extension conditions without significant fuel degradation, in principle the combined approach or the best estimate approach with quantification of uncertainties (best estimate plus uncertainty), as applicable for design basis accidents, may be used. However, in line with the general rules for analysis of design extension conditions, best estimate analysis without a quantification of uncertainties may also be used, subject to consideration of the caveats and conditions indicated in paras 7.55 and 7.67.*<br><br>DS508 says Because explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.<br><br>This is totally consistent with SSG-2 , par 6.67<br><br>Analysis of severe accidents should be performed using a realistic approach (Option 4 in Table 1, Section 2) to the extent practicable. Since explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses<br><br>Where is the problem?<br><br>Is DS508 supposed to go beyond SSG-2 in elaborating about uncertainty analysis in severe accidents? |

**DS508 Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants, 18th September 2020 STEP 7**

| COMMENTS BY REVIEWER<br>Reviewer: M-L Järvinen Page.... of....<br>Country/Organization: Finland/STUK Date: 29th October 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | 3.4 | An association of the levels of defence in depth with plant states considered in the design is frequently undertaken for design safety and operational safety. The introduction of DEC in the plant design basis has resulted in two different interpretations by States regarding the correspondence between plant states considered in the design and levels of defence in depth. These two approaches are represented in Table 1. Approach 1 (i.e. the association of DEC without core melt to level 3) has the advantage that each level has clear objectives regarding the progression of the accident and the protection of the barriers, i.e. level 3 to prevent damage to the reactor core and level 4 to mitigate severe accidents for preventing off site contamination. Radiological acceptable limits for DEC without core melt are the same or similar as for DBA. Also, the physical phenomena in case of DBA and DEC without significant fuel degradation core are similar, although there are differences in the analysis. In contrast, severe accidents are characterized by completely different | Please replace facilitates by emphasizes.<br><br>Best estimate methods are used in both approaches for assessment of DECs. | Yes | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | physical phenomena. However, approach 2 (i.e. the grouping of DEC without core melt and with core melt in level 4) ~~facilitates~~ emphasizes the differentiation between the set of rules for design and for safety assessment to be applied for DEC and the rules to be applied to DBA. | | | | | |
| 2. | 3.20 | The use of available safety systems, when possible, in DEC without significant fuel degradation has the important advantage that safety systems are designed with very stringent reliability criteria. In such cases, the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result (in particular regarding the prevention of cliff edge effects) that cannot be simply achieved by best estimate calculations. If the rules were the same, there would not be a need for differentiation between DBA and DEC. | Please align with SSG-2. It cannot be achieved by best estimate calculations is not clear.<br><br>SSG-2 (rev.1) states that:<br>7.55.When best estimate analysis is performed, the margins to avoid cliff edge effects should be demonstrated to be adequate. This may be done, for example, by means of sensitivity analysis demonstrating, to the extent practicable that when more conservative assumptions are made about dominant parameters, there are still margins to the loss of integrity of physical barrier | yes | In such cases, the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the results. Thus, when best estimate analysis is performed, the margins to avoid cliff edge effects should be demonstrated to be adequate. If the rules were the same, there would not be a need for differentiation between DBA and DEC. | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Lisäksi aikaisemmin on todettu (7.49), että yksittäisvikaa ei tarvitse ottaa huomioon. | | | | |
| 3. | 3.21 | As indicated in para. 3.17, DEC without significant fuel degradation have the potential to exceed the capabilities of safety systems designed for the mitigation of DBAs. However, the analysis of DBAs is required to be carried out conservatively to demonstrate compliance with established acceptance criteria. Therefore, for the conditions described in para. 3.12 (a) it may be possible to show that some safety systems would be capable of (and be qualified for) mitigating the event under consideration, based on best estimate analyses and less conservative assumptions. | Please check the reference, para. 3.12 (a) does not exist. Perhaps it should be 3.17 (a)? | Yes | | | |
| 4. | 3.23 | Design extension conditions should also be considered for some DBAs for which the use of ~~additional, if possible~~ diverse measures to cope with common-cause failures of safety systems is recommended. | Clarity, please delete ~~additional, if possible~~ | | | x | Wording is a bit different in the original text:<br><br>DBAs to acceptable levels by, if possible, the use of additional, diverse measures to cope….<br><br>The sentence is not unclear and there are cases in which (full) diversity is not |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | feasible. This has been a comment in the revision of SGs for design. For instance, it may be desirable to have diverse valves to depressurize the RPV, but some designers indicated that options are very limited. |
| 5. | 5.3, 5.11, 5.12, 5.16 | The situations where non-permanent equipment can be credited and where it cannot be credited should be clarified. | Please clarify and align with SSR-2/1.<br><br>In para. 5.3 it is said that non-permanent equipment should not be credited in demonstrating the adequacy of plant design with reference to SSG-2 (Rev. 1). According to para 5.11, 5.12 and 5.16 it is possible to credit non-permanent equipment in some cases.<br><br>Para 5.16 states that "…successful mitigation of an accident…" is very general and does not specify the type of | Paragraphs of SSR 2/1 are indicated in which the connections for non-permanent equipment are addressed.<br><br>This section of the SG is about "minimization of the radiological consequences of very unlikely conditions exceeding the plant design basis". Hence as indicated in 5.3 and inconsistency with SSG-2, non-permanent equipment can't be credited for demonstrating the adequacy of plant design.<br><br>Non-permanent equipment is not even required to be stored on the site. It is credited as part of accident management in conditions exceeding the plant design basis when its use is feasible (e.g. sufficient time), it is tested and maintained, people is trained, etc.<br><br>5.16 changed to | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | accidents where non-permanent equipment should be credited. | "Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for accident management to prevent unacceptable radiological consequences".<br><br>Hopefully it is now more clear | | | |
| 6. | 4.2 | With regard to design, 'practical elimination' is ~~normally be~~ considered to refer only to those events or sequences of events leading to or involving significant fuel degradation, i.e. a 'severe accident', for which the confinement of radioactive materials cannot be reasonably achieved. Those accident sequences have to be considered in the design for 'practical elimination', either by physical impossibility or by being extremely unlikely to occur with a high level of confidence. | It would be preferable to formulate the text clearly as a recommendation of IAEA rather than a general statement.<br><br>The interpretation of IAEA requirements as regards the application of practical elimination of early release to design basis accidents would need clear guidance from IAEA. If practical elimination were to be applied to DBEs and DECs without significant fuel damage in addition to the usual dose limits, some guidance on the methodology should be | Yes | Correction made<br><br>I don't understand the explanations in this comment | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | given. For example, should the probability of failures in addition to the normally postulated single failure be considered. | | | | |
| 7. | General e.g. 2.6 | The expression "and do not necessitate any off-site protective actions" would require some references or other indications of what IAEA considers appropriate limits for off-site actions. | In some member states the indicative operational limits, e.g., for sheltering indoors are very low and might be very strict as design limits for some DBAs, e.g. primary-secondary leaks. | | | | I understand the point, but this tries to address in DS508 a problem that perhaps had to be considered in SSR 2/1 or in other guide.<br>This was the consensus to formulate expectations about acceptable consequences for DBAs<br><br>If a country sets very low limits for activating protective measures, then either the performance of systems to control some DBAs. e.g. SGTR, is improved or it is admitted that they are sufficiently unlikely |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8. | 3.19 | (a) Less stringent design requirements than for DBA can be applied, for example compliance with the single failure criterion is not required, equipment can have a lower safety class and less rigorous reliability measures are allowed | A word missing? | Yes corrected | | | |
| 9. | 3.17 (a) | An initiating event ~~less frequent than those considered for DBAs and~~ that exceeds capabilities of safety systems for mitigation of DBAs; | SSG-2 (rev.1) para 3.40 does not mention frequency of the events. Please correct to be inline with SSG-2 (rev.1). | | SSG-2 doesn't say it, but if some initiating event exceeds the capability of safety systems, it needs to be less frequent than a DBA, because otherwise the design approach is inconsistent.<br><br>Safety systems are designed for DBAs. A more frequent event should not exceed the capabilities of the relevant safety systems. | | |
| 10. | 2.10 | Harmful radiological consequences to the public can only arise from the occurrence of accidents. Therefore, the following chapters are devoted to the implementation and assessment of **design extension conditions within the concept** of defence in depth and the complementary need for demonstration of practical elimination of accident sequences that can lead to early radioactive releases or large radioactive releases. | Add text in bold to be consistent with title of chapter 3. | Yes added | | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| COMMENTS BY REVIEWER<br>Country/Organization: FRANCE Date:<br>pages | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | general | Using "mitigate/mitigating/mitigation" only for severe accidents and "control" for other accidents would help and would avoid misunderstanding | | y | I don't have a big problem with that, but I have to note that in other standards, e.g. SG-53 and in the safety glossary, mitigation is used for accidents in general and occasionally for other purposes<br><br>In TECDOC 1791 we tried to clarify the terms "prevention" and "mitigation" | | |
| 2. | General | Please ensure consistency with SSG-2/3/4 and clearly identify which articles of the current draft are complementary regarding these guidances | SSG-2/3/4 are the documents that provide guidance for NPP deterministic safety assessment and PSA. They are mentioned in some articles but article 1.10 does not clearly states that they have been considered to ensure consistency. | | | | SSG 3 and SSG 4 for PSA don't deal with DEC and PE explicitly.<br><br>As for DSA, what you are suggesting for SSG-2 is a tedious work.<br><br>For which purpose? |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3. | 1.3 – p1 | GSR Part 4: Safety Assessment of Facilities and Activities, also revised after the Fukushima Dai-ichi accident [2], provides requirements for safety assessment covering the whole lifecycle of all types of nuclear facilities and activities. ~~Requirements for safety assessment of the design in this publication are not sufficiently detailed for nuclear power plants. However, specific requirements for safety assessment and safety analysis of nuclear power plants are established in SSR-2/1 (Rev. 1) [1], and these need to be considered to address specific aspects of relevance for nuclear power plant design.~~ Although requirements for safety assessment of the design in GSR Part 4 give some consideration to design requirements in SSR 2/1 (rev.1), they are not sufficiently detailed, and therefore specific and detailed guidance is needed to address specific aspects of relevance for a comprehensive and sound safety assessment of the nuclear power plant design. | Sentence is not clear enough and not easy to understand + ref [1] is not related to assessment/analysis. Thus proposal to come back to the consensus achieved during NUSSC members meeting in Feb 20 | y | All text in chapter 1 was revised paragraph by paragraph at the WG of NUSSC.<br>I have only included the comments of the technical editor.<br><br>SSR 2/1 has two requirements for safety assessment and for safety analysis (specific for NPPS)<br>This is what we say<br><br>GRS part 4 doesn't give consideration to requirements in SSR 2/1, which was published later. It only says for safety analysis:<br>*Both deterministic and probabilistic approaches shall be included in the safety analysis*.<br><br>The guidance is needed on req. 42 of SSR 2/1<br><br>It is not worth discussing it. If you insist I will implement it | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4. | 1.4 – p1 | The objective of this Safety Guide is to provide recommendations on the implementation of the selected requirements in SSR-2/1 (Rev. 1) [1] that are related to defence in depth and practical elimination of event sequences leading to early radioactive releases or large radioactive releases. The recommendations in relation to defence in depth in this Safety Guide are focused on design aspects, in particular on those aspects associated with DEC. This Safety Guide is also aimed at addressing at a high level the safety assessment related to these design aspects. | Proposal aims at ensuring consistency with the consensus achieved during NUSSC members meeting in Feb 20 | y | Included. It was removed by the editor.<br><br>It is clear from the sentence | | |
| 5. | 1.5 – p2 | This Safety Guide is intended for use by organizations involved in the verification, review and assessment of safety of nuclear power plants. It is also intended to be of use to organizations involved in the design, manufacture, construction, modification, and operation, ~~and in the provision of technical support for nuclear power plants, as well as by regulatory bodies~~ | Proposal aims at ensuring consistency with the consensus achieved during NUSSC members meeting in Feb 20 | | | | It was included following comments by other countries<br><br>I don't see a reason why it cannot be useful for RBs<br><br>I understand that if you provide comments to this guide, it must be of some use for the RB or its TSO |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6. | 2 (title) - p3 | ~~DESIGN APPROACH TO AVOID ACCIDENTS WITH HARMFUL CONSEQUENCES~~ Relevant requirements in SSR 2/1 [1] and GSR Part 4 [2], on which guidance is provided | The title shall be modified to ensure consistency with existing literature (e.g. the word "avoid" is never used with "harmful" and vice-versa) and consistency with article 1.13 (thus with the consensus achieved during NUSSC members meeting in Feb 20) | | | | I don't think that other members of NUSSC disagree with this title and don't understand the problem with this combination, but I am open to other expression like prevent instead of avoid<br><br>The proposal is not a good title por a section<br><br>This is only consistent with the following comments of eliminating everything that are not quotations from the requirements |
| 7. | 2.1 – p3 | ~~Principle 8 on prevention and mitigation of accidents in SF-1 [3] states that "All practical efforts must be made to prevent and mitigate nuclear or radiation accidents" and furthermore that "The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'".~~ | Reference to SF-1 provides no added value in this guidance, is misleading and is not consistent with the consensus achieved during NUSSC members meeting in Feb 20 nor article 1.13 | | | | If NUSSC agrees it will be deleted |
| 8. | 2.2 – p3 | ~~The implementation of defence in depth, as described in SF-1 [3], comprises safety measures of various types. This Safety Guide is primarily focused on design measures for nuclear power plants as described in [1] and more specifically on design measures for the mitigation of accidents, including those implemented to facilitate accident management.~~ | Reference to SF-1 provides no added value in this guidance, is misleading and is not consistent with the consensus achieved during NUSSC members meeting in Feb 20 nor article 1.13 | | | | If NUSSC agrees it will be deleted |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9. | 2.6 – p4 | ~~The requirements in paras 2.3–2.5 establish the safety approach for the design and specifically establish the need for radiological consequences of accident conditions to be not only below acceptable limits but to be as low as reasonably achievable (ALARA). In addition, it needs to be demonstrated in the design that plant states that could lead to high radiation doses or to a large radioactive release have been 'practically eliminated'. Further~~ Some other requirements ~~in relation to acceptable limits for categories of plant states and more specifically for accident conditions are also specified~~ of SSR-2/1 (Rev. 1) [1] are also in relation with potential consequences of accident conditions, namely: | The previous requirements shall not be rephrased with modifications. Moreover, it is disputable if it is an objective or an approach or something else<br><br>The requirements below do not mention "acceptable" limits | | | | If NUSSC agrees it will be deleted |
| 10. | 2.7 – p4 | This Safety Guide is focused on the protection of the public and the environment in accident conditions, which should be assessed notably regarding the ~~by verifying~~ compliance with a number of requirements in SSR-2/1 (Rev. 1) [1]… | According to safety glossary, assessment is more than just a "verification" | Y | Implemented | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11. | 2.8 – p5 | ~~In accordance with Requirement 5 of SSR-2/2 (Rev. 1) [1], radioactive releases in accident conditions are required to be below acceptable limits and be as low as reasonably achievable.~~<br>~~In addition, the purpose of the fourth level of defence in depth is that off-site contamination is avoided or minimized. To this aim, a limit for the release of radioactive materials or on acceptable limit on effective dose should be specified for each category of accident conditions, and compliance with these limits should be verified. For accidents without significant fuel degradation, the releases are required to be minimized such that off-site protective measures (e.g. sheltering, evacuation) are not necessary. For accident with core melting, the releases are required to be such that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'. The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release. In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis.~~ | Req 5 has already been quoted in 2.3, there is no need to rephrase it.<br><br>Not consistent with 1.13 that mentions only requirements from SSR-2/1 and GSR part 4. This part of the article could be interpreted as new additional requirement. If it is rephrasing of existing requirement, it could be tricky thus not relevant for a guidance | | | | What for do we need this SG?<br><br>To copy and paste SSR 2/1 , to refer to SSG-2?<br><br>No addition clarification on terms that are not well understood and no additional recommendations.<br><br>Is it here some recommendation detrimental for safety?<br><br>If NUSSC agrees it will be deleted |
| 12. | 2.9 – p5 | ~~For normal operation or anticipated operational occurrences, there is limited uncertainty on plant state frequency and radiological impact, which can be monitored and is supported by many years of operating experience of previous plant designs. For less frequent plant states, i.e. accidents, there are larger uncertainties associated with the demonstration of plant state frequency and radiological consequences..~~ | Not consistent with 1.13 that mentions only requirements from SSR-2/1 and GSR part 4. This article could be interpreted as new additional requirement. If it is rephrasing of existing requirement, it could be tricky thus not relevant for a guidance | | | | Idem comment 11 |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13. | 2.10 – p5 | ~~Harmful radiological consequences to the public can only arise from the occurrence of accidents. Therefore, t~~The following chapters are devoted to the implementation and assessment of defence in depth and the complementary need for demonstration of practical elimination of accident sequences that can lead to early or large radioactive releases. | Not consistent with 1.13 that mentions only requirements from SSR-2/1 and GSR part 4. This part of the article could be interpreted as new additional requirement. If it is rephrasing of existing requirement, it could be tricky thus not relevant for a guidance | | | | Do you believe that harmful consequences for the public could be possible without occurring an accident? |
| 14. | 2.11 – p5/6 | ~~Recommendations on radiation protection in design of nuclear power plants are provided1 in IAEA Safety Standards Series No. NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants [12], and recommendations for protection of the public are provided in IAEA Safety Standards Series No. GSG-8, Radiation Protection of the Public and the Environment [13].~~ | Not consistent with 1.13 that mentions only requirements from SSR-2/1 and GSR part 4 (we should take care not to mention each and every guidance related to NPP or applicable to NPP) | | | | If NUSSC agrees it will be deleted |
| 15. | 3.1 – p6 | This section addresses the overall application of requirement 7 in [1] for defence in depth in the design of nuclear power plants with specific emphasis in design provisions for accident conditions and the overall l assessment of its implementation with specific focus in the reactor core as main source of radioactivity. ~~For other sources of radiation or potential releases of radioactive materials, the implementation of a defence in depth strategy will depend on the amount and isotopic composition of radionuclides, on the effectiveness and leak tightness of the individual confinement barriers as well as the potential challenges for the integrity of the barriers and the consequences of their failures.~~ | This sentence is more or less re-phrasing of part of SSR-2/1-art.2.14 and not consistent with it: in this article, it is said that the number of barriers will depend, not the implementation of DiD | | | | Do you honestly believe that for other source the only thing that changes is the number of barriers?<br><br>What is the expected added value of this guide with this type of comment ? |
| 16. | 3.2 – p6 | The concept of defence in depth for nuclear power plants is described in SSR 2/1 Rev. 1, par. ~~2.13~~ 2.12 to 2.14 [1].<br><br>~~An overall strategy of defense in depth, when properly implemented in the design, achieves the objective that no single human or equipment failure will lead to harm to the public, and to no or little harm in the event of combinations of failures~~ | These SSR-2/1 articles should have also been mentioned in chapter 2. The statement is not limited to 2.13.<br>It is a non complete re-phrasing (thus introduces potential misleading) of SF-1 – 3.31 and objective of DiD is out of scope of this guidance according to art 1.4 | | | | We deal with DiD but the objective of DiD is out if the scope of this guide !!! |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 17. | 3.3 | For the implementation of safety provisions at each level of DiD according to these articles, there are notably three aspects of importance as follows:<br>a. ~~The~~ performance of the safety provisions implemented to meet the objective of each level ~~acceptance criteria for,~~ notably regarding the integrity of the barrier(s) that should be protected;<br>b ~~the reliability of~~ safety provisions to ensure that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level~~, with a sufficient level of confidence~~<br>c adequate independence from the safety provisions implemented at the previous and the successive levels of defence in depth | We should be careful regarding the exhaustiveness of these articles.<br><br>2.13 of SSR-2/1 does not mention only barriers as objectives<br><br>b is not clear. Proposition tries to make it clearer. If not, c is sufficient and b should be deleted | y | Changes made in relation to a)<br><br>b) The reliability of safety measures to demonstrate with a sufficient level of confidence that a certain plant condition….<br><br>The aspect of reliability is essential | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 18. | 3.4 p 67 | An association of the levels of defence in depth with plant states considered in the design is frequently undertaken and could be presented differently ~~for design safety and operational safety. The introduction of DEC in the plant design basis has resulted in two different interpretations~~ by Member States regarding the correspondence between plant states considered in the design and levels of defence in depth.<br>These two approaches are globally represented in Table 1 to help understanding and this table should not be interpreted as recommendation. Approach 1 (i.e. the association of DEC without significant fuel degradation ~~core melt~~ to level 3) enhances the link between levels and objectives ~~has the advantage that each level has clear objectives regarding the progression of the accident and the protection of the barriers, i.e. level 3 to prevent damage to the reactor core and level 4 to mitigate severe accidents for preventing off site contamination~~. (no fuel melt, radiological acceptable limits for DEC without significant fuel degradation ~~core melt~~ are the same or similar as for DBA). Also, the physical phenomena in case of DBA and DEC without significant fuel degradation ~~core~~ are similar., ~~although there are differences in the analysis.~~ In contrast, severe accidents are characterized by completely different physical phenomena. ~~However,~~ Approach 2 (i.e. the grouping of DEC without significant fuel degradation ~~core melt~~ and with core melt in level 4) ~~facilitates~~ enhances the differentiation between the set of rules for design and for safety assessment to be applied for DEC and the rules to be applied to DBA. | To avoid enhancing opposition between approaches<br><br>To be consistent with the glossary/plant states<br>To avoid enhancing opposition between approaches | Y | I can leave with the changes.<br>It is clear that it is not a recommendation. For the part in yellow, I don't think it is a good expression | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 19. | 3.5-p7/8 | ~~Normal operation comprises a series of plant operation modes defined in the documentation governing the operation of the plant (such as plant Technical Specifications in some countries) that range from power operation to reactor refuelling, in which no failures have taken place, and no equipment is unavailable that would prevent the intended accomplishment of the goals of the operational mode. Plant states other than normal operation are reached either directly by the occurrence of postulated initiating events for the applicable modes of operation or through failures in mitigating the consequences of such events in the first place. Their impact on the plant is the main basis for establishing the safety provisions that are necessary at each plant state. For these reasons, it has been more convenient in this safety guide to address the design safety provisions necessary for each plant state, rather than for each level of defence. In this way also, the significance and importance of design extension conditions for the safety approach is emphasized~~ | This article provides no guidance and is not consistent with article 1.13 and title 3 which is related to DEC. | | | | The coverage of operational states was agreed at the WG of NUSSC |
| 20. | 3.6 | ~~para 4.13 of SSR-2/1 (Rev.1) states: "The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.". Therefore, design provisions for operational states should have adequate capabilities to keep integrity of the first barrier for confinement of radioactive materials (i.e. the fuel cladding) and to prevent a significant release of primary coolant and an evolution to design basis accident conditions, for which the actuation of the engineered safety features (safety systems) is foreseen~~ | The first part of the article is a quotation, then there's an explanation with:<br>- no link with the quotation, which does not mention releases<br>- rephrasing with wording which does not seem to be adequate (the word "avoid" cannot replace "prevent").<br>Further, this article does not provide any guidance. | | | | What is expected from this safety guide? |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 21. | 3.7 - p8 | The provisions for normal operation and AOO should have a reliability commensurate with ~~consistent with the~~ highest frequency of postulated initiating events for design basis accidents, which is (usually expected to be lower than 10-2 per reactor-year), ~~the reliability of safety provisions for anticipated operational occurences should be such that the frequency of transition into an accident condition is significantly lower than this value~~. | Consider deletion as it does not provide clear operational guidance.<br>Otherwise, reword as proposed:<br>Estimated frequency of accidents does not rely only on AOO provisions reliability<br>Thus a more general recommendation is more adequate | y | I can agree on a better wording, but the result of failing to control an AOO (no matter if the SAR only takes credit for safety systems) is normally a DBA. The reliability of safety provisions for DBA matters because accidents should be prevented and as a matter of fact the reliability of safety measures for AOO ar reliably enough to make the frequency of DBAs much lower than 10-2 /y . | | |
| 22. | 3.8-3.9-3.10 – p 8 | …<br>Consequently and according to art 2.13 of SSR-2/1 Rev. 1, specific design provisions (safety systems) should be implemented to limit ~~mitigate~~ the ~~radiological~~ consequences of DBAs through the prevention of significant fuel damage and damage to the containment boundary in order to limit the radiological consequences to the public and the environment to the extent that no,or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions. ~~no special measures are required for the protection of the public.~~ | Prevention of fuel degradation is missing if 2.13 not quoted<br>To help guidance, it is better not to use “mitigate” for DBA<br><br>Rephrasing 5.25 is misleading and not useful | y | | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 23. | 3.11 – p9 | Design basis accidents are postulated events that are not expected to occur during the lifetime of the plant. The most frequent events categorized as DBAs should have an expected frequency below 10-2 per reactor-year. The operation of safety systems designed to control DBAs should rely on automatic actuation and should not involve human intervention for a sufficiently long period of time ~~and their reliability should be very high~~. Safety systems should be designed to ensure their reliable operation under postulated external hazards and prevailing environmental conditions. ~~The reliability of safety systems should be such that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the safety goals of the plant (for new nuclear power plants typically below 10-5 per reactor-year). If this is not the case, DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate to achieve such goals.~~ | This does not provide guidance: very high reliability is expected for many SSCs important to safety<br><br>This is not understandable and reliability of safety systems is not only based on probabilistic calculation. | | | | Is it wrong?<br><br>We cannot set numbers here<br><br>Someone disagree that apart from SSC class 1, like the RCPB, the safety systems are not designed using the highest requirements for reliability?<br><br>Reliability is a probabilistic concept. Reliability is not achieved by analysis,<br><br>If this is not understandable, say why<br><br>The use of DEC is closely related to frequencies (Req.13) |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 24. | 3.12 – p9 | If the design of the containment is such that in the case of the most limiting DBAs the intervention of cooling or pressure reduction systems (e.g. containment spray) is necessary to ensure the integrity of the containment boundary, such systems should be designed, constructed and maintained to ensure a ~~very high~~ reliability commensurate with the consideration that, ~~since~~ their failure would not only lead to a severe accident but also jeopardize the subsequent measures for its mitigation. ~~For the same reason,~~ containment isolation provisions in case of DBAs should also be designed to have very high sufficient reliability for ensuring that acceptable limits for radiological consequences are not exceeded and sufficient coolant inventory can be maintained if applicable. in Section 4.. ~~Severe accidents with an open containment constitute one of the plant conditions to be practically eliminated that are addressed in section 4.~~ | We might live with the first sentence but there is no really guidance<br>High reliability: see above<br><br>The second sentence should be clarified and the link between containment isolation and inventory is not clear<br><br>The last sentence has not link with DBA | | | | See answer to comment before<br><br>Specially in this case reliability needs to be very high for the reasons explained<br><br>Last sentence is only pointing to section 4.<br><br>It can be deleted<br><br>If the containment is not isolated, eventually the cooling inventory will be lost. It can be removed |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 25. | 3.16 and 3.17 – p10 | Consider replacement of this articles by : "SSG-2 articles 3.39 and 3.40 provide guidance regarding development of "deterministically derived list of design extension conditions without significant fuel degradation … " + exact quotation of these articles | Consistency with SSG-2 shall be ensured and 3.16/17 deal with exactly the same topic as these articles of SSG-2. | | | | If you don't want any explanation in relation to DEC or on plant states, no recommendations on reliability and quoting SSG-2, please explain me the purpose of this guide<br><br>SSG-2 for the purpose of DSA addresses the identification of both types of DEC and the cases for P.E. |
| 26. | 3.18 and 3.20 – p10 | These articles should be replaced by quotation of SSG-2 articles 7.47 and 7.48 | SSG-2 articles provide more complete guidance and deal with exactly the same topic. Replacement will ensure consistency | | | | See answer to 25 |
| 27. | 3.21 – p10/11 | Consider deletion | This article provide no guidance as its topics are already included in other articles | | | | See answer to 25 |
| 28. | 3.22 – p11 | ~~Design extension conditions should be considered for failures of safety systems designed both to cope with anticipated operational occurrences and DBAs. These~~ According to SSG-2 article 41, the list of DEC without significant fuel degradation includes in many designs the anticipated transients without scram and station blackout.<br>3 | To ensure consistency with SSG-2, it is better to mention it when dealing with the same topic | | | | See answer to 25 |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 29. | 3.23 – p11 | Design extension conditions should also be considered to identify provision to be implemented to reduce the frequency of severe accidents caused by failures in the mitigation of some DBAs to acceptable levels by, if possible, the use of additional, diverse measures to cope with common cause failures of safety systems. | DEC consideration will not reduce frequency by itself | y | | | |
| 30. | 3.24 – p11 | Design extension conditions without significant fuel degradation ~~constitute~~ contribute to a reinforcement of the design for some complex and unlikely failure sequences.<br><br>As some safety systems are designed to cope with various DBAs (e.g. the emergency core cooling is designed for several sizes and locations of loss of cooling accidents or main steam line breaks), safety features for DEC can help to reinforce the capability of the plant for specific sequences improving and balancing the risk profile: applying less stringent design or safety assessment criteria than for DBA conditions could help to identify reasonably practicable provisions to improve safety.<br><br>~~The reliability of safety systems should be high enough for DEC without significant fuel degradation to only be postulated exceptionally and to occur with a frequency lower than the most limiting DBAs~~ | DEC does not constitute a reinforcement by itself (provision implementation constitute a reinforcement)<br><br>The proposed modification clarifies what is understood through this sentence. If not accepted, please clarify the sentence<br><br>If not deleted, please clarify the sentence | y | An attempt would be made to clarify this sentence. I don't know what is not clear | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 31. | 3..25 – p11 | In accordance with paragraph 5.30 of SSR-2/1 rev1, a set of representative conditions of an accident with core melting should be ~~used~~ postulated to provide inputs for the design of the containment and of the safety features ~~ensuring its integrity~~. This set of accidents should be considered in the design of the corresponding safety features for DEC and should be a set of bounding cases that envelop other severe accidents with more limited degradation of the core~~, or lower loads on the SSCs that fulfil the confinement function~~ | Integrity may be a relevant word but have a very precise meaning which is not mentioned in 5.30<br><br>The end of the sentence is globally not clear. The last part is not correct: severe accidents are not considered to envelop accident with lower loads on the SSCs that fulill the confinement function for the 1st barrier | y | ensuring its integrity changed to ensuring its functionality<br><br>I have removed the last sentence. but I disagree<br>It is clear that it refers to the containment<br><br>SSG-53 addresses the loads on the containment for design, including those related to DEC | | |
| 32. | 3.29 – p12 | Consider replacement of article by reference to SSR-2/1 and SSG 53 | This article is not clear: during scope (topic of the guidance), the evaluation of release are obviously consistent with design leakage rate.<br>This article may also be a non useful rewording of objectives mentioned in SSR-2/1<br>Leaktighness of containment is delt with in SSG-53 4.98 to 4.103: art 3.29 seems to be a downgrading of these articles, notably 4.100 that requires At the design stage, a target leak rate should be set that is **well below the safety limit leak** rate (i.e. **well below the leak rate assumed in the assessment of possible radioactive releases arising from accident conditions**). | y | **This part is important and it will be discussed**<br><br>I agree on what you say in accordance with 4.100<br><br>It appears that other countries understand that the limit is just below the criterion for practical elimination | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 33. | 3.30 – p12 | A safety assessment of the design should be performed with consideration of the progression of severe accident phenomena ~~and their consequences, and addressing applicable topical issues such as the following:~~<br>~~— Corium stratification and criticality;~~<br>~~— Thermal-chemical interaction between corium, steel components and vessel;~~<br>~~— Heat transfer from corium to vessel or end-shield;~~<br>~~— Combustion of hydrogen and other gases;~~<br>~~— Steam explosion due to molten fuel-coolant interaction;~~<br>~~— Corium-concrete interaction;~~<br>~~— Containment overpressurization~~<br>~~— Containment overtemperature.~~<br>More detailed information is provided in SSG-2 (Rev. 1) [8], notably regarding the examples of potential phenomena for LWR | The best way to ensure consistency with SSG2- is just to refer to this guidance.<br>It is of high importance to highlight that the list is for LWR and is not always applicable, depending on the strategy | | SSG-2 has a list of severe accident phenomena in relation to analysis assumptions and treatment of uncertainties<br><br>I can delete but, what is wrong?<br><br>Is the deterministic safety analysis the only part of safety assessment?<br>Are you going to require in SSG-4 the alignment with SSG-2? | | |
| 34. | 3.31 – p12 | The concept of defence in depth, as implemented in the design of a nuclear power plant, is required to be assessed ~~to ensure that each level is adequately designed to meet its goals in terms of prevention, detection, limitation and mitigation.~~ according to ~~-~~Requirement 13 of GSR Part 4 (Rev. 1) [2], that states … | "is required" is not for a guidance document except if it quotes a requirement. Morever, "meet its goals" is sufficient without the unclear list of "…tion" | | | | Is required can be used instead of "shall" in a safety guide when referring to a requirement as it is the case req.13 in GSR part 4<br><br>SG can elaborate on the requirements. There is no value in just copying and pasting requirements |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 35. | 3.36 – p13-14 | For each identified source of radiation, the physical barriers (including the boundaries) should be identified and an evaluation of their robustness should be provided. The ~~following~~ aspects mentioned in SSG-2 should be taken into account in the evaluation.<br>(a) to (g) shall be deleted | Added value is not clear as they do not seem to provide guidance and seem to use different wording as requirements. | | | | I don’t see any of this in SSG-2 (just DSA)<br><br>Why there is no value? Are the recommendations wrong? |
| 36. | 3.37 – p14 | An analysis of the various mechanisms that could challenge or degrade ~~the integrity of the barriers or~~ the performance of the safety functions should be carried out in order to assess the adequacy of the safety provisions that are implemented to prevent the occurrence or stop the progression of such mechanisms. To the extent that different degradation mechanisms could necessitate different safety provisions, the adequacy and effectiveness of ~~the~~ every safety provisions should be assessed ~~separately for each degradation mechanism~~ | Barriers contribute to confinement safety function thus is included in “safety functions”<br><br>They shall not be assessed separately as there could be mutual impacts or interactions | y | Separately deleted, not the rest of the sentence | | |
| 37. | 3.39 – p14 | Consider deletion | No added value compared to SSG-2 (thus to 3.38) | | | | We cannot say that DSA should be performed? |
| 38. | 3.42 – p15 | SSR-2/1 Rev.1 requires that “the design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability” (req 24). It should be verified that this requirement ~~diversity~~ has been adequately implemented in the design of systems fulfilling the same ~~fundamental~~ safety function in different ~~plant states~~ levels of defence in depth ~~if a simultaneous failure of those systems would result in unacceptable damage to the fuel or radiological consequences~~. | This guidance should not establish new requirement: independency is expected between levels of DiD not plant states (SSR-2/1). The precision in 3.5 of this guidance does not allow to establish new requirement.<br>Moreover, diversity is not systematically expected.<br>This article does not provide any guidance but it is possible to establish a link with SSR-2/1 req 24 | | | | Here the purpose is to quote the requirement and not to provide guidance<br><br>The guidance is what you delete, namely when diversity would be relevant<br><br>Diversity is not systematically expected. The guide is recommending when it is relevant |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 39. | 3.43 – p15 | Consider deletion | - Assessment is not only frequency assessment<br>- Frequency should not be used without "estimated" in such a context<br>- DBA is not only to failure of AOO control | | | | If for deterministic analysis we only have to quote SSG-2 and the probabilistic considerations cannot be expressed, it doesn't make sense to develop this guide |
| 40. | 3.44- p15 | The ~~combined~~ reliability of the safety systems designed to ~~mitigate~~ limit the consequences of a DBA should be sufficient so that ~~to demonstrate with high confidence~~, that their probability of failure, including under the conditions expected for each accident sequence postulated, is ~~very~~ sufficiently low. ~~A failure probability below than 10-3 in order of magnitude would be consistent with the strict requirements for reliability imposed to safety systems and supported by operational experience and testing.~~ | Please explain "combined reliability"<br>Reliability of a system is not only reliability under certain conditions<br>This article is tricky and could limit reliability analysis to prob calculation<br>The concepts of "very" or "high confidence" are not understandable in this context<br>The figure is not justified. At a maximum, it could be presented as a practice in some MS | | | | Safety Glossary<br><br>**reliability**<br><br>The probability that a *system* or *component* or an item will meet its minimum performance *requirements* when called upon to do so, for a specified period of time and under stated *operating conditions*.<br><br>If numeric figures cannot be indicated, even in soft way values that are a minimum and qualitative expressions are not allowed, then what can be done?<br><br>Why such expressions are acceptable in other safety guides? |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 41. | 3.45 – p15 | ~~Any vulnerabilities that could result in the complete failure of a safety system should be identified and considered in combination with postulated initiating events to assess if they could escalate to a core melt accident. Usually, for each combination analysed, if the consequences exceed those acceptable for DBAs, separate, independent and diverse safety features (e.g. an alternate AC power supply in case of the total loss of the emergency power supply, or a separate and diverse decay heat removal chain), which are unlikely to fail due to the same common cause, need to be implemented to strengthen the defence in depth and to prevent core melt~~. | Overdemanding recommendation : it is expected to postulate systematically the failure of all safety systems during DBA<br>Need rewording | | | | " a safety system" not "All safety systems" |
| 42. | 3.46 – p15 | Safety features for DEC without significant fuel degradation should be ~~demonstrated to be~~ sufficiently reliable, including when considering ~~for~~ the accident sequences for which they are intended, in order to contribute to ensuring a core damage frequency below the established probabilistic targets. | Reliability of a system is not only reliability under certain conditions<br>Isn-t this article a tautology? | y | Demonstrated was the result of other comment in the previous version<br><br>The conditions for which they are intended could be removed because it can be considered something logical | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 43. | 3.47 – p15 | The capacity and reliability of safety features specifically designed to mitigate the consequences of DEC with core melting should be adequate to ensure that the containment integrity will not be jeopardized during any postulated core melt sequence~~. However, since the analysis of core melt and its impact on containment integrity is surrounded by considerable uncertainties, only a limited reliability can be attributed to those components necessary to ensure the containment integrity after a core melt accident~~ | This sentence fully downgrade the importance of severe accident consideration | | | | It is not downgrading severe accident consideration.<br><br>It is saying that the assessment cannot rely on a very low estimated probability of mitigating successfully a core melt accident. |
| 44. | 3.48 – p15 | The assessment should include an evaluation of the adequacy and effectiveness of the different accident management strategies defined to cope with extreme scenarios. ~~This evaluation should demonstrate that the likelihood of an accident having unacceptable consequences for people and the environment, and which relies on both fixed and nonpermanent equipment to mitigate the consequences of such an accident, is extremely low.~~ | This sentence is not acceptable and contradictory with existing requirement of SSR-2/1 depending on the meaning of "unacceptable". If the target is practically eliminated scenarios, they can not be mitigated and use of non permanent equipment is generally not adequate ("early" is not consistent with "non permanent" by essence) and "extremely low" is not sufficient | | | | We are not talking here about practical elimination<br><br>Extreme scenarios replaced by severe accident scenarios<br><br>The residual risk from failing to mitigate severe accidents should be very low (different from practical elimination) |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 45. | 3.52 – p16 | For example, a failure, whether equipment failure or human error, at one level of defence ~~or even combinations of failures at two levels of defence~~, should not propagate to jeopardise defence in depth at the subsequent levels. | This combination does not correspond to any requirement. To maintain this part of the recommendation, it should be explained which combination should be considered | y | Removed<br><br>One example was provided before in relation to DBA with failure to isolate the containment<br><br>Other is ATWS, where failure to trip the reactor in AOO, fails the control of reactivity in DBA | | |
| 46. | 3.54 – p17 | ~~In order to ensure a very low frequency of occurrence of sequences resulting in severe accidents or unacceptable releases,~~ it is necessary to demonstrate that the effectiveness of the levels of defence is not reduced by factors that compromise the independence of the levels of defence in depth. These factors are mentioned in following paragraphs~~.as follows~~:<br>3.5x ~~(a)~~ The relevance of sharing of systems or parts of systems for executing functions for different plant states, for example for normal operation and for design basis accidents should be justified.<br>3.5x ~~(b)~~consistently with req 24 of SSR-2/1 Rev.1, the design should take due account of the potential common cause failures that can impact different levels of defence in depth. Typical root causes of such failures are undetected human errors in design or manufacturing, human errors in the operation or maintenance, inadequate qualification or protection against internal or external hazards. | It has been already reminded that independency is expected. It is a principle, notwithstanding the reasons that could be mentioned | y | I would remove the 1st sentence<br><br>The items are factors that affect independence. Recommendations are in the following paragraphs<br><br>What it would me to justify the relevance of sharing ? | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 47. | 3.56 – p17 | As far as practicable, The sharing of systems or parts of them for executing functions for different categories of plant states should not be sought, unless it could be justified that it is benefitial for safety ~~avoided. However, since this might not be always practical or possible~~, if any sharing, it should be ensured that within the sequence of events that may follow a postulated initiating event, a system credited to respond in a given plant condition should not have been needed for a preceding condition. Thus, ~~complementary~~ safety features designed to mitigate the consequences of DEC without significant fuel degradation should be independent from SSCs postulated as already failed in the sequence. ~~This is especially important when safety systems are credited for the mitigation of DEC.~~ | Avoided has a specific meaning in Euratom Nuclear Safety Directive or Vienna declaration<br>Sharing could be beneficial for safety (for example reliability of system that are permanently in operation could be better)<br><br>For WENRA country, complementary safety features are for DEC with core melt | y | Partially<br><br>I don't get the point of the specific meaning of avoid. Prevent is perhaps better. Avopid is used in SSR 2/1 in relation to independence<br><br>Requirement 64: Separation of protection systems and control systems Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.<br><br>and yin many safety guides, including SSGF-2 probably better<br><br>One thing is the sharing to be acceptable and other to be beneficial for safety | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | I don't understand the reason to delete the last sentence. It is specifically important. | | |
| 48. | 3.57 – p 17 | ~~The SSCs needed for each postulated initiating event should be identified, and it should be shown by means of engineering analyses that the SSCs needed for implementing any one defence in depth level are sufficiently independent from the other levels. The adequacy of the achieved independence should also be assessed by probabilistic analyses.~~ | This article only repeats importance of independency and one way that contribute to verify the sufficiency of this independency | | | | This is the way to verify functional independency |
| 49. | 3.58 – p17 | The SSCs identified as necessary independent ~~systems and components used for different plant states~~ should be separated, ~~within~~ if located in the same safety division, from one another by distance or protective structures if there is a possibility for consequential failures arising from ~~a failure of a system or component for another plant state~~. a SSC | "Structures" are excluded without any reason.<br>This article is applicable as soon as independency is required, it is not necessary to detail | | | | Separation of structures can be difficult<br>The structure in itself can be the separation<br><br>The paragraph becomes less clear |
| 50. | 3.59 – p18 | ~~The systems needed for different plant states in accordance with the defence in depth concept should be functionally isolated from one another in such a way that a malfunction or failure in any plant state does not propagate to another. However,~~ practical limitations of design allow exemptions to independency, each of which should be justified. Thus, it is a common practice to use some safety systems for some anticipated operational occurrences. … | No new guidance<br>This article could be deleted | | | | This not about sharing but functional isolation<br><br>Not addressed before |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 51. | 3.61 – p18 | For instrumentation and control systems, it should be demonstrated that ~~defence in depth within the overall instrumentation and control architecture is achieved by means of~~ adequate independency should be achieved (see notably requirement 64 of SSR-2/1 rev.1) ~~lines of defence, so that the failure of one line of defence is compensated for by the following one. This can be achieved by implementing independence between different levels of defence in depth and independence between redundant functions and by design for reliably. Means of supporting design for reliability and reducing the likelihood of common cause failures in I&C systems are physical separation, electrical isolation, functional independence and independence from the effects of communications errors, and diversity.~~ and Further recommendations are provided in SSG-39 [7]. | This topic is very tricky and a reference to existing requirement and guidance is enough | | | | There is no agreement<br><br>I am receiving comments for more details and others for reducing<br><br>This change makes the paragraph useless and there would be no need to single out I&C systems |
| 52. | 4.3 – p 20 | The concept of… any core melt sequence, in accordance with the defence in depth concept. ~~However, these provisions may have limited capabilities that could not reasonably cope with some specific severe accident conditions; those are the conditions that should be explicitly identified and practically eliminated.~~ | These part is whether not useful or interpretable as contradictory with the rest of the paragraph | y | removed | | |
| 53. | 4.5- p 20 | ~~When a severe accident condition occurs, it is necessary to ensure that the massive amount of radioactive materials released from the nuclear fuel will be confined. Hence, when there is a condition of limited confinement, such as it happens in the fuel storage building or when the containment is open or there is a containment by-pass, the only way to prevent unacceptable releases is to avoid the occurrence of a severe accident. In such conditions, the unacceptability of the consequential radioactive releases is obvious, making it worthless to attempt to demonstrate that acceptance criteria can be met. Demonstrating that such severe accidents would be extremely unlikely is the only practical possibility.~~ | This view of some event sequences is oversimplified – except for fuel storage building maybe | | | | I don't see anything wrong<br>I don't see that a severe accident without containment integrity is not a case that |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 54. | 4..6 – p20 | ~~SSR-2/1 (Rev. 1) [1] does not provide quantitative acceptance criteria for the radiological consequences of accident conditions, or for the magnitude of what is to be considered an early radioactive release (which is site specific as it considers the time restrictions to implement protective measures), or a large radioactive release. Therefore, acceptable limits for radiation protection, as well as probabilistic criteria or target values for the purpose of demonstrating the low frequency of a core damage accident or accident sequences leading to radioactive releases, should be established, consistent with the regulatory requirements.~~ | Not consistent with some member states practices:<br>- large releases definition do not need to be quantified. The corresponding situation "qualitatively" lead to unacceptable releases;<br>- no probabilsitc criterion is needed as PE relies primarily on deterministic justification | | | | Nobody says that large releases have to be quantified, but the must be a criterion to identify the sequences that can lead to them<br><br>If the case is not impossible, the probability would matter when probabilistic evaluation can be performed?<br><br>What does it mean deterministic? Anything that it is not probabilistic?<br><br>The criteria indicated is for the mitigation of DEC w.c.d<br><br>How is it possible to design without them? |
| 55. | 4.7 – p20 | ~~When~~ if defining ~~these~~ radiological criteria or targets for early and large releases, it is necessary to establish a significant difference in magnitude … | See 4.6 | | | | See answer to 4.6 |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 56. | 4.9 – p20/21 | Practical elimination' is used to re-inforce DiD ~~confirm that all reasonably practicable design~~ through implementation of adequate provisions, and takes also due account of provisions that have been implemented, across all levels of defence in depth to ensure that plant conditions for which a large radioactive release or an early radioactive release could not be prevented, are physically impossible or highly unlikely with a high degree of confidence. ~~Sufficiently robust arguments and evidence are needed to demonstrate the reliability of the lines of defence that are in place. Where further features could be implemented, either for prevention of accidents or for mitigation of the consequences, they should be considered, as far as reasonably practicable~~ | Use of PE goes beyond the only "confirmation": definition of provisions is expected consistently with SSR-2/1<br><br>Demonstration is not in this paragraph | y | I can change confirm by demonstrate and reasonably praticable by adequate<br><br>I have already a long debate with the UK about the wording of role of PE in relation to DiD<br><br>Why I should delete the sentences at the end ? | | |
| 57. | 4.17 – p 23 | ~~It may be useful also to classify accident scenarios taking into account the progression from an initiating event to the consequences that need to be avoided. Three type of scenario can considered:~~<br>~~Type I: scenarios with an initiating event that leads directly to severe fuel damage and early failure of the confinement function.~~<br>~~Type II: severe accident scenarios with phenomena that induce early failure of the confinement function.~~<br>~~Type III: severe accident scenarios that result in late failure of the confinement function.~~ | This typology could be usefull in another context but is confusing here | | | | Proposal by ENISS<br><br>Is it wrong?<br>Why is it confusing? |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58. | 4.22 – p23 - 24 | The design of provisions for practical elimination should be done on a case-by-case basis and, where relevant, associated to the appropriate level of defence in depth ~~or plant state~~ at which the sequence of events would be interrupted to prevent unacceptable consequences. It should be verified that the ~~corresponding~~ appropriate engineering design rules and technical requirements have been followed to ensure that they would confidently achieve their safety function, under the prevailing conditions, e.g. the harsh environmental conditions associated to a severe accident. In assigning requirements, where relevant, appropriate testing, operational procedures, and in-operation monitoring as well as in-service testing and inspection should be considered. In assigning,~~The~~ requirements where relevant should also be considered ~~applied at~~ all steps from design to operation, including manufacture, construction or implementation on site, commissioning and periodic testing | Associate a provision to a plant state is not understandable<br><br>Not clear : practical elimination does not only rely on application of rules related to a level of DiD. These rules should be applied anyway<br><br>Not clear: it seems as if the guidance recommends to apply requirements | y | Provisions can be associated to DBA or to DEC, to a level of DiD it is more tricky<br><br>The sequence of events follows plant states not levels of DiD<br><br>~~corresponding~~ changed to appropriate<br><br>It has been explained that P.E is not achieved by adding some specific feature like the H2 recombiners and it relies on features at previous levels of DiD that make severe accident unlikely. The design rules are not the same at each level of DiD<br><br>The last sentence is correct. With changes it is not understandable | | |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 59. | 4.35 – p 26 | In practice, the physical impossibility approach is limited to very specific cases…. it would be heavily challenged.~~ An example could be the effect of heterogeneous boron dilution for which the main protection is provided by ensuring a negative reactivity coefficient for all possible combinations of the reactor power and coolant pressure and temperature. In this case, physical impossibility applies only to a prompt reactivity insertion accident.~~ | The example does not seem relevant or the most appropriate | | | | Why is it not relevant?<br><br>Which case would you propose as a candidate for the option of impossibility? |
| 60. | 4.36 – p26 | ~~The expression 'extremely unlikely' is by definition a probabilistic notion.~~. Although… | This too straightforward affirmation is disputable and provide non guidance | | | | Extremely unlikely is probabilistic if this is a scientific term |
| 61. | 5 – title – p27 | ~~MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF VERY UNLIKELY CONDITIONS EXCEEDING THE PLANT DESIGN BASIS~~ Implementation of design provisions for enabling the use of non-permanent equipment for power supply and cooling | The title is not consistent with 1.13 and could challenge the consensus achieved during NUSSC members meeting in Feb 20 | | | | Obviously the purpose is not to change the title, but by doing so removing a number of relevant paragraphs on external hazards, the reason why the requirements for enabling the connection of non permanent equipment has been introduced |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 62. | 5.1 | ~~The design basis of items important to safety at nuclear power plants is established taking into account the most limiting conditions under which they need to operate or maintain their integrity. However, it is possible, although very unlikely for a well designed nuclear power plant, that some conditions arise that exceed the margins of the design of some SSCs, thus impairing the fulfilment of safety functions. This is particularly important for the case of natural hazards, for which the occurrence of hazards of a magnitude that exceeds the safety margin of the most vulnerable SSC important to safety is generally a matter of probability. There have been cases in which some external natural hazards, such as extreme earthquakes, floods and tsunamis have exceeded the levels considered for the design as a result from the site evaluation. Paragraphs 5.21 and 5.21.A of SSR-2/1 (Rev. 1) [1] require sufficient margins against external hazards for such cases in the design7~~ | This article is out of scope of chapter 5 considering article 1.14. Moreover, its wording is not consistent with SSR-2/1 | | | | See previous comment |
| 63. | 5.8 – p29 | Consider deletion | Out of scope | | | | idem |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 64. | 5.11 – p29 | The use of non-permanent equipment should ~~be credited provided~~ be such that the time period needed for their installation and putting in service is less than the defined coping time with a specified margin for time sensitive operator actions. … | Consistency with art 5.3 that states that it should not be credited | | | | Non-permanent equipment should not be credited in demonstrating the adequacy of the nuclear power plant design<br><br>In the situations analysed, the design basis has been exceeded<br><br>If they can never be credited, they are useless |
| 65. | 5.12 – p29 | ~~If~~ Where relevant non-permanent equipment ~~is credited~~, ~~its~~ installation and use should be documented, and … | Consistency with art 5.3 that states that it should not be credited | | | | See comment 64 |
| 66. | 5.16 – p30 | ~~Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for demonstration of the successful mitigation of an accident to prevent unacceptable radiological consequences~~ | Consistency with art 5.3 that states that it should not be credited | | | | See comment 64 |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 67. | Annex I | Annex I to be removed<br><br>If not deleted, at a very minimum:<br>• Title should be replaced by "preliminary considerations in relation with practical elimination concept<br>• each part of annex I should be complemented with consideration of existing guidances regarding the topic they deal with (storage pool, main primary components, criticality…). | Regarding the concerns identified in the main text of the draft, it is better not to have detailed annexes that would potentially reinforce the challenge of requirements consistency (even if annex is not part of the document).<br>Principle of annex was agreed during NUSSC member meeting in February 20 but it was not expected to be as such.<br><br>In particular, deletion of Annex 1 is highly recommended:<br>- It seems to be a copy-paste of an annex of TECDOC 1791 which is not a consensual document. Even if annex is not part of a standard document, having the same annex is two different document would be a misleading message<br>- It does not consider existing guidances regarding the topic they deal with (storage pool, main primary components, criticality…). | | | | The annex was already available<br><br>It is taken from Tecdoc 1791, by the way the source of parts of SSG-2 in relation to DEC and P.E.<br><br>The Agency has the copyright of it. It is clear that the is not a consensus document (we had to obtain the permission of NUSSC to publish it however) . It can be used as a starting point. No need to reinvent the wheel to collect even more comments |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 68. | Annex II | Consider deletion | Regarding the concerns identified in the main text of the draft, it is better not to have detailed annexes that would potentially reinforce the challenge of requirements consistency (even if annex is not part of the document and even if principle of annex was agreed during NUSSC member meeting in February 20).<br>If not deleted, annex II should be modified as followed at a very minimum | | | | I was requested explicitly during the February meeting to develop this Annex, it is the Agency initiative<br><br>It has 8 paragraphs. What is the very minimum for you? |
| 69. | | Following comments are alternate proposal regarding deletion of annex II | | | | | |
| 70. | Annex II - title | APPLICATION OF THE GUIDANCE TO NUCLEAR POWER PLANTS DESIGNED ACCORDING TO EARLIER STANDARDS COMPARED TO SSR-2/1 (Rev. 1) | Tentative to have a title consistent with the text of the annex (II-1) | | | | SSG-53:<br>**PLANTS DESIGNED TO EARLIER STANDARDS**<br><br>Why should the titles be more complicated in this safety guide? |
| 71. | II.1 | II-1. Paragraph 1.3 … ~~This implies that the capability of existing plants to accommodate accident conditions not considered in their current design basis and the practical elimination of plant conditions that can lead to early radioactive releases or to large radioactive releases need to be assessed with the objective of further improving the level of safety.~~. | Quotation of SSR-2/1 is sufficient. Rephrasing it is tricky:<br>- what does "capability to accommodate" means regarding safety?<br>- "improving the level of safety" is nt clear and is not achieved just by assessment. | | | | It is clear that safety reassessment is the 1st step and that in itself safety assessment doesn't improve safety<br><br>It is included to understand about what aspects is this assessment |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 72. | II-4 | II-4 In relation to practical elimination, a number of measures may have been taken ~~for the practical elimination of some conditions leading to early or large radioactive releases. This includes~~ for instance for the prevention of the break of the reactor pressure vessel, fast reactivity insertion accidents or the severe fuel degradation in the irradiated fuel storage. However, a demonstration that the existing safety … | These measures couldn't have been taken for a concept that did not exist | y | Deleted | | |
| 73. | II-7 – p41 | ~~Safety systems of existing plants were designed for design basis accidents, without account being taken of the possibility of more severe accidents. However, the conservative deterministic approaches originally followed in the design might have resulted in the capability to withstand some situations more severe than those originally included in the design basis for existing plants. As indicated in para. 3.20, for design extension conditions without significant fuel degradation, it can be acceptable for postulated initiating events less frequent than those considered for DBAs to demonstrate that some safety systems would be capable of and qualified for mitigating the consequences of such events if best estimate analyses and less conservative assumptions are used. This is a possibility for existing nuclear power plants to demonstrate the capability for mitigation as a design extension condition of events not originally postulated in the design, such as the multiple rupture of steam generator tubes.~~ | This article does not comply with the title of the annex. It is a statement that existing plants with existing design may withstand some accidents not considered in its design if these accidents are studied with different rules | | | | What is the problem?<br><br>In a new plant this could be DEC, but not in an existing one ? |

**TITLE: DS 508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 74. | II-8 – p41 | The consideration of external events of a magnitude exceeding those considered for design, derived from the hazard evaluation for the site ~~the original design basis~~, as it is addressed in Section 5 for non-permanent equippment, is ~~a part of the safety reassessment of existing nuclear power~~ to be considered for identifcation of design provisions to enable their use. ~~While for new nuclear power plants the mitigation of design extension conditions is expected to be accomplished by permanent design features, and the use of non-permanent equipment is intended for very unlikely external events of a magnitude exceeding the original design basis,~~ for existing nuclear power plants the use of non-permanent equipment with adequate connection features can be the only reasonable improvement in some cases. Relying on non-permanent equipment may be adequate provided there is a justification to show ~~demonstrate~~ that the coping time to prevent the loss of the safety function that the equipment is intended to fulfil is long enough to connect and put into service the equipment under the conditions associated with the accident. The recommendations in this regard provided in Section 5 would be relevant. Non-permanent equipment ~~that would be necessary to minimize the consequences of events that cannot be mitigated by the installed plant capabilities~~ needs to be stored and protected to ensure its timely availability when necessary, with account taken of possible restricted access due to external events (e.g. flooding, damaged roads). | "Original design" is a new notion To be consistent with the SS nR-2/1 and section 5 (non permanent equipment is not considered in safety demonstration)<br><br>This statement/recommendation is not justified, not editorially consistent with SSR-2/1 and not relevant for this annex which is not related to new NPP<br><br>That could be interpreted as use of non permanent equipment for pratical elimination of event sequence that would lead to early releases, which is obviously not appropriate due to lack ot time | y | | Partially implemented<br><br>There are no recommendations here, as an Annex. It is expected that some explanations would be then provided | | |

# ssgDS508 "Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants" (Draft dated 18 September 2020)
## Status: STEP 7

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modifi-cation/rejection |
| | | General | Germany notices the very strong improvements made in this guide discussing important aspects of assessing implementation of defence in depth as well as practical elimination. This guide will provide valuable guidance to member states. We would like to emphasize and acknowledge the effort made for drafting this guide. Based on the strong improvements further comments aim to further enhance and improve the draft. | | N.A.<br><br>Thanks | | | |

Relevanz: 1 – Essentials | 2 – Clarification | 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Relevanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | 1. | 1.1 | Over the latest decades, IAEA safety standards for nuclear power plant design have been enhanced several times with the aim of providing confidence that the successive generations of nuclear power plants are designed so as to operate efficiently at the highest levels of safety that can be reasonably achieved considering the state of the art practices and techniques in science and technology and taking into account the feedback gained from the nuclear events ~~and~~, operational experience and insight from safety research. | Insights from (safety) research in nuclear science is an important driver for improving nuclear safety. | Yes | I wanted to respect the agreement reached by the WG of NUSSC and so far the text is maintained but the Technical Editor has already anticipated that this kind of paragraph is not usual and needs to be removed | | |
| 3 | 2. | 1.3<br>1st sentence | IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment of Facilities and Activities, also revised after the Fukushima Dai-ichi accident [2], establishes requirements for safety assessment covering the whole lifetime of all types of f~~acility~~ facilities and ~~activity~~ activities. | Change singular to plural. | | | x | I would agree with your comment but this was a change by the technical editor and I need to acknowledge that I don't have the same level of English |
| 2 | 3. | 1.3<br>last sentence | …. However, specific requirements for safety assessment and safety analysis of nuclear power plants are established in SSR-2/1 (Rev. 1) [1] as well as in the specific safety guides SSG-2 (Rev. 1) [8], SSG-3 [9] and SSG-4 [10], and | SSG-2 Rev.1, SSG-3 and SSG-4 are substantiating the overarching safety requirements and are specific for NPPs. We propose to add these guides | | Safety guide don't provide requirements. Therefore, it is better to clarify the relation with them later on when they | | |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modifi-cation/rejection |
| | | | these need to be considered to address specific aspects of relevance for nuclear power plant design. | here. | | are introduced. , i.e. 1.10<br><br>Making this change in the short time available would also require to renumber all references in the guide | | |
| 3 | 4. | 1.6<br>3rd sen-tence | … As described in para. 2.13 of SSR-2/1(Rev.1) [1], the implementation of defence in depth at nuclear power plants comprises 5 levels. Safety features for DEC as well as other safety features that underpin the demonstration of practical elimination of event sequences that can lead to early radioactive releases or large radioactive releases correspond to one or more levels of defence in depth. | Typo | Yes | | | |
| 2 | 5. | 1.6<br>last sen-tence | … Therefore, this Safety Guide addresses the assessment of the implementation ~~or assessment~~ of defence in depth in relation to these aspects. | It should be clear what this safety guide addresses. Therefore, we propose to avoid the “or” and suggest rephrasing the last sentence. We think it is also better aligned to the title the NUSSC WG agreed upon. | Y | Changed to imple-mentation starting in 3.1 “ **and “** assess-ment starting in 3.31 | | |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Relevanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 2 | 6. | 3.19<br>1st sentence | Since the objective in DBA and in DEC without significant fuel degradation is the same, namely to prevent core damage or damage to the fuel in the irradiated fuel storage, the primary difference between these two accidental conditions is the use of different ~~or~~ acceptance criteria, different design requirements ~~for design~~ ~~or~~ and different approaches for performing safety ~~assessment~~ analyses to ~~achieve~~ demonstrate this objective. Thus, in design extension conditions the following apply: | To clarify that for DBA and DEC different acceptance criteria can be applied and the different approaches for safety analysis can be utilized (see also SSG-2 Rev.1). | Yes | Considering also some changes requested by others | | |
| 2 | 7. | Add new para after 3.25 | Fuel melting in the irradiated fuel storage leading to large or early releases should be practically eliminated and are excluded in the category of DEC with core melting. | To clarify, the only severe accidents involving core melting is considered here. Consequently, fuel melting in the spent fuel pool needs to be practically eliminated. | Yes | Added to this paragraph for now to prevent wrong cross references from one paragraph to another | | |
| 1 | 8. | 3.28 | The challenges to plant safety presented by DEC with core melting, and the extent to which the design may be reasonably expected to mitigate their consequences should be considered in establishing procedures and guidelines ~~the severe accident management guidelines or guides~~. Recommendations in this regard are provided in IAEA Safety Standards Series No. | We are still convinced that the range of EOPs should be slightly extended to DEC with core melting. For example, the successful implementation of the in-vessel retention (IVR) strategy requires a flooding of the reactor cavity at the right | yes | | | |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | | SSG-54, Accident Management Programmes for Nuclear Power Plants [14]. | point in time. A too late flooding would hamper the success of IVR. Therefore, clear procedures and criteria are necessary to initiate the right steps at the right point in time. | | | | |
| 1 | 9. | New para below 3.45 | <u>It should be demonstrated that the reliability of engineered safety features for DBA and safety features for DEC is not limited by the reliability of its support systems.</u> | This is not an aspect of independence of DiD and should be also emphasized here and not only in para 3.64. Usually, safety systems for DBAs or safety features for DEC depend on support systems. It is important to assess that the reliability of the support systems will not determine the reliability of the safety systems or safety features. | Yes | Added after 3.48 | | |
| 1 | 10. | 4.5 last sentence | … In such cases, it may be necessary to demonstrate practical elimination by showing with a high degree of confidence that such severe accidents would be extremely unlikely <u>or physically impossible</u>. | In accordance with paras 4.2 and 4.32 physical impossibility is the second way of demonstrating practical elimination and should be added here. In case demonstration by physical impossibility is | | | x | It is about situations of limited confinement, for example in accidents involving fuel storage or when the containment is open |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modifi-cation/rejection |
| | | | | not possible, demonstration by extremely unlikely with a high degree of confidence would be possible. | | | | and cannot be closed in time<br><br>In such case we cannot say that a severe accident would be physically impossible.<br><br>It is clear in other paragraphs that in general there are two alternatives |
| 1 | 11. | 4.6 first sentence | SSR-2/1 (Rev. 1) [1] does not provide quantitative acceptance criteria for the radiological consequences of accident conditions, or for the magnitude of what is to be considered ~~an early~~ a large radioactive release. An early release should be defined site specific ~~(which is site specific as it considers~~ considering the time restrictions to implement off-site protective measures~~), or a large radioactive release~~. | First, it has to be clarified what is considered as a large release. An early release is also a large release, but with insufficient time to implement off-site countermeasures. For that reason, we propose to reformulate the first sentence of para 4.6. | y | It could be mostly the case for some sequences that releases would be at the same time large and early. This would be the worst. There could be also large and late.<br><br>My understanding is that early releases (as defined in SSR 2/1) could be smaller than the threshold of large releases, i.e. not | | |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | | | | | sufficient to contaminate a large area, but requiring protective measures that cannot be timely implemented<br><br>The changes proposed don't contradict this view | | |
| 1 | 12. | 4.10 | As part of the overall safety approach, the 'practical elimination' concept should be applied to a new nuclear power plant at the earliest design stage~~, when it's more practicable to design and implement additional[3] safety features~~. The incorporation of ~~such~~ <u>safety</u> features <u>for DEC</u> is <u>part of</u> an iterative <u>design</u> process using insights from engineering experience, and from deterministic safety analyses and probabilistic safety analyses in a complementary manner.<br><br>~~[3] 'Additional' is intended here to describe any design provision that is implemented following practical elimination assessment to support the demonstration of 'practical elimination' of~~ | To align para 4.10 with the terminology of the IAEA Safety Glossary. In the Safety Glossary it is clearly distinguished between *safety systems* and *safety features for DEC*. and to avoid confusion by introducing a new term. We understand *additional safety features* for DEC-A as safety features which compensate the unavailability of a safety system provided to control DBA and consider *complementary safety features* for accidents with core melt (DEC-C), which have | | | | Safety features is a general term (not exclusive for DEC), see it use ion SSR 2/1<br><br>Safety systems are designed for DBAs<br><br>In relation to DEC it is therefore said safety features, but specifically DEC.<br><br>In any case, the safety features |

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | | ~~some accident sequences, considering that some design provisions already implemented to support other safety objectives and analyses can participate in the demonstration.~~ | completely different phenomena than DBA and DEC-A. This understanding is also supported by WENRA's Safety Objectives for New NPPs.<br><br>The two main messages still remain: Start implementation in an early design stage and reconsider practical elimination during the iterative design process. | | | | here cannot be associated to DEC.<br><br>The reactivity coefficients of the reactor for instance are an intrinsic safety feature relevant to practical elimination not associated to DEC<br><br>There is also the more the more philosophical question that DEC are conditions for which the plant is design, but not for the conditions practically eliminated and it would cause some problems of interpretation |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

| | COMMENTS BY REVIEWER<br>Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Pages: 7<br>Country/Organization: **Germany** Date: 30.10.2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|---|
| Rele-vanz | Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 2 | 13. | 4.12 (c) (i) | Basemat penetration ~~or containment bypass during~~ due to molten core concrete interaction; | Containment bypass phenomena are addressed in item (d). | | | x | In order to keep alignment with SSG-2<br><br>Although the basemat is likely to be the point of the containment breach, in some reactor may be another boundary point of the containment the point of attack. |
| 3 | 14. | 4.14 first sentence | The approach described in paras 4.12 and 4.13~~)~~ combines, when relevant, the following: | Typo. | Yes | | | |

Relevanz: 1 – Essentials 2 – Clarification 3 – Wording/Editorial

**Japan NUSSC comments on DS508 "Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants"**

| COMMENTS BY REVIEWER<br>Reviewer: Japan NUSSC Member<br>Pages: 4<br>Country/Organization: Japan / Nuclear Regulation Authority (NRA)<br>Date: 30 October, 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | 3.11./Line 3 | Design basis accidents are postulated events that are not expected to occur during the lifetime of the plant. The most frequent events categorized as DBAs should have an expected frequency typically below $10^{-2}$ per reactor-year. | The frequency is typical value used in the Member States and it is already stated in para. 3.7. in "usually" value. Also, this word is used in the fourth sentence in this para. | Yes | | | |
| 2. | 3.17./Line 1 | Design extension conditions without significant fuel ~~damage~~ degradation are to a large extent technology and design dependent, but they can be classified in three types [8], as follows: | To keep a consistency with the definition used in SSR-2/1 (Rev. 1). | Yes | | | |
| 3. | 3.19./Line 3 | Since the objective in DBA and in DEC without significant fuel degradation is the same, namely to prevent core damage or damage to the fuel in the irradiated fuel storage, the primary difference between these two accidental conditions is the use of different ~~or~~ criteria for design or safety assessment to achieve this objective. | Editorial. | Yes | | | |
| 4. | 3.19./Line 9 | (b) Less conservative assumtions and criteria than for DBA, or best estimate methods, are acceptable for the safety analysis." | Specify the reference for "less conservative". It misleads less severe condition than nominal one. | Yes | | | |

| COMMENTS BY REVIEWER<br>Reviewer: Japan NUSSC Member<br>Pages: 4<br>Country/Organization: Japan / Nuclear Regulation Authority (NRA)<br>Date: 30 October, 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| 5. | 3.20./ Line 3-6 | The use of available safety systems, when possible, in DEC without significant fuel degradation has the important advantage that safety systems are designed with very stringent reliability criteria. In such cases, the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result (in particular regarding the prevention of cliff edge effects) that cannot be simply achieved by best estimate calculations. If the rules were the same, there would not be a need for differentiation between DBA and DEC. | It is difficult to understand the second sentence, so it is desirable to revise it. | Yes | Changed considering also other comments | | |
| 6. | 3.21./Line 4 | Therefore, for the conditions described in para. ~~3.12~~ 3.19 (a) it may be possible to show that some safety systems would be capable of (and be qualified for) mitigating the event under consideration, based on best estimate analyses and less conservative assumptions. | Wrong para number. | Yes | Changed | | |
| 7. | 3.24. /Line 3-4 | As some safety systems are designed to cope with various DBAs (e.g. the emergency core cooling system is designed for several sizes and locations of loss of ~~cooling~~ coolant accidents or main steam line breaks), safety features for DEC can help to reinforce the capability of the plant for specific sequences improving and balancing the risk profile applying less stringent design or safety assessment criteria than for DBA conditions. | Use appropriate technical wordings. | Yes | “systems are”<br><br>“coolant” | | |

| COMMENTS BY REVIEWER<br>Reviewer: Japan NUSSC Member<br>Pages: 4<br>Country/Organization: Japan / Nuclear Regulation Authority (NRA)<br>Date: 30 October, 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| 8. | 3.29./Line 2 | Radioactive releases due to leakage from the containment in a severe accident should ~~remain below the design leakage rate limit~~ be low enough for sufficient time to allow implementation of emergency measures. Beyond this time, containment leakages could exceed this limit but still be well below the criterion for a large radioactive release. This may be achieved by provision of adequate filtered containment venting or other design features or alternative measures that could be included in an overall demonstration of adequacy of the containment function. | The design leakage rate limit would not necessarily be maintained under severe accident conditions. | Yes | The containment is designed for DEC<br><br>Changed to well below the safety limit leak rate. This is accordance with SSG-53 par. 4.100 | | |
| 9. | 3.30. | A safety assessment of the design should be performed with consideration of the progression of severe accident phenomena and their consequences, and addressing applicable topical issues such as the following:<br>− ~~Corium~~ Molten core stratification and criticality;<br>− Thermal-chemical interaction between ~~corium~~ moletn core, steel components and vessel;<br>− Heat transfer from corium to vessel or end-shield;<br>− Combustion of hydrogen and other gases;<br>− Steam explosion due to molten fuel-coolant interaction; | 1) Terminology should be unified with used in para 4.12 (c) (i) and others as “molten core”.<br>The same terminology should be replaced in Annex I-11, I-16, I-17 and so on.<br><br>2) Completeness. | yes | Corium changed to core melt<br><br>Corium is used in SSG-2, also<br><br>These are examples of severe accident phenomena to be considered, no neeed to be exhaustive. | | |

| COMMENTS BY REVIEWER<br>Reviewer: Japan NUSSC Member<br>Pages: 4<br>Country/Organization: Japan / Nuclear Regulation Authority (NRA)<br>Date: 30 October, 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| | | − ~~Corium~~ Molten core -concrete interaction;<br>− Containment over pressurization<br>− Containment overtemperature<br>− Direct containment heating<br>− Direct contact with a containment (shell attack)<br>More detailed information is provided in para. 7.66. of SSG-2 (Rev. 1) [8]. | Beside the listed topical issues, DCH (Direct Containment Heating) and shell attack are evaluated in safety assessments for DEC with core melting.<br>3) Specify relevant para in SSG-2 (Rev. 1). | | in DECs is a list of example<br>SSG-2 par 7.66 is about analysis assumptions and treatment of uncertainties. Not everything there is relevant for the purpose of this paragraph | | |
| 10. | 3.34./Line 7 from the top of page 11 | It should demonstrate that, for each credible initiating event, the risk has been reduced as low as reasonably practicable, considering also internal hazards and/or external hazards that could cause the event. The assessment should consider insights from engineering analyses and from deterministic and probabilistic safety analysis, as appropriate for the different plant states. | Clarify “engineering analysis” taking examples. | y | Changed to assessment of engineering aspects | | |
| 11. | 3.39./Line 2 | The performance of safety provisions at each level of defence in depth is assessed through engineering assessment and deterministic analysis involving the use of validated and verified analysis codes and models to demonstrate that acceptance criteria are met with sufficient margins. | Clarify “engineering assessment” taking examples. | y | Changed to assessment of engineering aspects | | |

# DS508 - Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants

| COMMENTS BY REVIEWER<br>Reviewer: Page…. of….<br>Country/Organization: Russian Federation/SEC NRS Date: November 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | 2.8 | In addition, the design should be such that no cliff edge effect ~~**in the radiological consequences**~~ is expected for accidents slightly exceeding the plant design basis **that can lead to a sudden large variation in radiological consequences**. | i. 4.9 SSR-2/1 | y | Changed with the comment of other country<br><br>i. 4.9 SSR-2/1<br><br>is not related to this | | |
| 2. | 3.36d | For barriers considered as ultimately necessary to prevent early or large radioactive release, margins to failure should be assessed to determine if these are adequate to withstand loads caused by **external** hazards of a severity exceeding that considered for design | In our opinion, we are talking **not only about natural impacts**, but about all impacts that are external to the barrier | | | | Only for natural hazards margins are required. In 5.21A SSR 2/1<br><br>Natural hazards of a higher severity than the design basis are in general possible. It is a matter or probability<br><br>If we speak about man made, water dam failure or aircraft crash, it is for what it is designed. You |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | cannot design for a Cesna and expect to have margins for a B747 |
| 3. | 3.12 | … For the same reason, containment isolation provisions in case of DBAs should also be designed to meet very high reliability requirements for ensuring that limits for radiological consequences are not exceeded and sufficient coolant inventory can be maintained. ~~Severe accidents with an open containment constitute one of the plant conditions to be practically eliminated that are addressed in section 4~~ | This last sentence should be removed as the section deals with design basis accidents | yes | It has been removed, but I disagree.<br><br>I only say that if the mitigation of the DBA fails it results into a severe accident and with the containment open, this is a case for treatment in chapter 4 for practical elimination refer that | | |
| 4. | 3.19 | (a) Less stringent design requirements than for DBA can be applied, for example …, equipment can have a lower safety class and **less** rigorous reliability measures are allowed | Mistake | yes | | | |
| 5. | 3.26 | The accident conditions chosen (**in containment)** should be justified based on engineering judgement and insights from the probabilistic safety analyses: see SSG-53 [5]. | Because the link for SSG-53 means that it's said only about containment | y | NO.<br><br>The conditions are of the plant | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | Safety features fror DEC-B are mostly containment systems (and support systems)<br><br>SSG-2 has been added<br><br>You can check SSG-2 3.45 a 3.50 and SSG-53 3.38 a 3.45 (they are not consistent) and decide which ones are more useful | | |
| 6. | 3.52 | For example, a failure, whether equipment failure or human error, at one level of defence ~~**or even combinations of failures at two levels of defence**~~, should not propagate to jeopardise defence in depth at the subsequent levels. | See 2.13 SSR-2/1 and Paragraph 3.31 of the Fundamental Safety Principles.<br>Also it isn't clear that the "subsequent levels" will be in case of "combinations of failures at two levels of defence" – may be some example is needed here? | Y | If we want to stick to the wording of SF-1 and SSR 2/1 we are not going to have any progress.<br>Failure at one level should not affect a subsequent level, this is the idea, but it is also said that the levels should be independent to the extent possible<br><br>The mere recognition that the can be some dependencies between the levels difficult to eliminate implies that there are going to be dependent failures of two levels, but perhaps this is enough. Some example can be placed (the guide | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | mentions for instance the sharing of systems between two levels of DiD) but tendency of some countries are about staying just with recommendations. Therefore, I delete it | | |
| 7. | 3.56 | “…. it should be ensured that within the sequence of events that may follow a postulated initiating event, a system credited to respond in a given plant condition should not have been needed for a preceding condition. This is especially important when safety systems are credited for the mitigation of DEC. Thus, complementary safety features designed to mitigate the consequences of DEC without significant fuel degradation should be independent from SSCs postulated as already failed in the sequence. ~~This is especially important when safety systems are credited for the mitigation of DEC.~~ <br>. | It proposed to swap sentences (without any changes in words), because it is not clear what “This is” refers to? | Yes | | | |
| 8. | 3.60 | … (e.g. an alternate power supply for DEC **without significant fuel degradation** ~~with core melting~~ could be connected if necessary to equipment for DEC **with core melting** ~~without significant fuel degradation~~) | As a rule alternate power supply envisaged in design for SBO and also used in case the SBO developed to severe accident | y | I understand the point, but I suggest to remove alternate. The change would be otherwise wrong, because the idea that you could with a good reason use something for DEC B in DEC A is this will prevent core damage<br>Nobody says that in DEC B there is only one source (and supply and source is different, between supply, e.g. bus bar/cabinet and source, eg. Diesel / battery there are transformer s inverters, chargers etc, that can be the reason of the power loss and a different reconnection can be established. ) | | |
| 9. | 4.8 | “The first step for demonstrating the | It’s proposed to provide | | | | The approach to |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | practical elimination of plant conditions that can lead to an early radioactive release or a large radioactive release is the identification of severe accident sequences having the potential to give rise to 'unacceptable radioactive releases'. This identification process is expected to result in a list of accident sequences that could be grouped into a small set of plant conditions. The identification process should be justified and supported by relevant information [1)]."<br><br>**1) This list of accident sequences shall be based on the list accident sequences for DEC with core melt initially presented in design (as a rule reflected in chapter 15 and/or chapter 19 of SAR), but shall take into account phenomena that lead to unacceptable radioactive releases and additional safety features that proposed to mitigate their consequences. The result of this analysis shall be presented in SAR separately from analysis of DEC** | some footnote to clarify the issue of "list of accident sequences that could be grouped into a small set of plant conditions".<br>The question to solve by this footnote is where regulatory body can see and review implementation of practical elimination | | | | elaborate such list is later on in 4.12 paragraphs<br><br>I cannot put such a foot note, shall is not allowed in SGs, not even should in footnotes. Not all sequences go through DEC-B and what and where is presented in the SAR belongs to the SG on the SAR, SSG-61, approved for publication<br><br>As an example, all sequences that start from a PIE and progress to core damage (there are more than 100 in a PSA level 1) and continue through the level 2, where there would be an event to be analysed, namely $H_2$ explosion need to be demonstrated that have been practically eliminated |
| 10. | 4.12 a(ii) | Prompt neutron reactor runaway | Because not any fast | y | It depends how | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | accident<br>(instead *fast reactivity insertion accident*) | insertion of reactivity leads to subsequent failure of the containment and a large radioactive release | | fast. Normally this can be called also reactivity excursion<br>The term propose is not common<br>Others suggested rapid instead of fast<br><br>I am changing to<br><br>Uncontrolled reactivity accidents<br><br>Used in SSG-2 | | |
| 11. | 4.12 e<br>Ref.5 | Significant fuel degradation in the spent fuel pool when located outside the containment. Where a fuel pool is located within a containment, it should be justified that appropriate technical and organizational measures to prevent and mitigate severe accidents in the fuel pool are considered in the design. | Replacement is proposed because the original text does not addresses the case with the fuel pool located inside the containment.<br>(in case the suggestions is acceptable, ref. 5 can be excluded) | | | | It would be at most a matter of changing the foot note.<br><br>For the case that the SFP is in the containment, is there any plant designed to cool the fuel if the SFP once it is damaged and not before?<br>Is there any design to avoid penetration |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | of the SFP liner or hold the molten fuel? Are there $H_2$ recombiners dimensioned for the $H_2$ that can be generated in the pool ? etc.<br>I don't think this is the case.<br>The design would always be oriented to the P.E. versus the mitigation. |
| 12. | 4.19 | (a) The state of the art in nuclear science and technology, **including the industry experience from the operation of NPP and accidents, that happened previously;** | Text enhancement | y | I am including it, but don't you thing that the state of the art in any field does consider the experience from the past?<br>The experience and the accidents always belong to the past | | |
| 13. | 4.26 | … or be tolerant to the loss of support functions **(for example balanced combination of active and passive safety systems allow to use passive systems in case when support systems are failed. Safety functions can be provided** | It's proposed to add this text as example of technical design for diverse safety systems used in different plant state.<br>Its should be noted that | | | | Using active or passive systems or a combination of them is a design choice<br>Passive systems can be used for DBA, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | **both by active systems and passive systems independently of each other in different plant states).** | the issue of using passive systems as a diverse features to manage DEC isn't clearly describe in DS508. But this type of systems allow in new design provide independence beetwen layers of DiD and claim that some sequnces are practicaly eleminated (may be some lincs to IAEA TECDOC will be useful in this case) | | | | for DEC or for both.<br>They have to be designed with the corresponding requirements.<br><br>Here, "*Where design provisions and operational provisions rely on support functions* …"<br>It is implicit that we speak about active systems. This was a paragraph that other country requested and it is not wrong<br><br>The issue of passive systems is not well described because countries don't agree on the guide advocating for a design option. |
| 14. | 5.1 | 5.1 …, but it is possible, although very unlikely for a well designed nuclear power plant, that some conditions arise that exceed the margins of the design of some | Please clarify as it looks like here some contradictions?<br>How to ensure sufficient margins if, according to | y | There are margins in the design from different sources ( in the safety analysis, by using design codes, etc.)<br>Do margins ensure that safety limits would never be | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | <u>SSCs</u>, thus impairing the fulfilment of safety functions. … Par. 5.21 and 5.21.A of SSR 2/1, rev. 1 [1] require the need to <u>ensure sufficient margins against external hazards for such cases in the design</u>. | the statement, they have already been exceeded | | exceeded? Not always. In some cases it is possible, but sufficiently unlikely if margins are well established.<br><br>Which one is a relevant case emphasized explicitly in SSR 2/1 after the Fukushima Daiichi accident?<br><br>External hazards | | |
| 15. | II-3. | It is important to note however, that an accident condition commonly considered as a design extension condition in new nuclear power plants (e.g. station blackout or anticipated transients without scram), is only such if safety features have been introduced in the design to mitigate its consequences. **~~Otherwise, it would remain a beyond design basis accident.~~** | It's proposed to **delete or clarify this conception** because it's not clear what does it mean "remain a beyond design basis accident"<br>It's misleading sentence as:<br>- IAEA glossary said <u>***"beyond design basis accident.*** Postulated *accident* with *accident conditions* more severe than those of a *design basis accident"*</u> so it means it can be DEC;<br>- in Russia and some other countries the conception of DEC isn't applied so the **BDBA=DEC** (it's the same) | | | | Exactly not <u>***"beyond design basis accident.*** Postulated *accident* with *accident conditions* more severe than those of a *design basis accident"*</u><br><br>Not all beyond design basis accidents are DEC, only if the plant is design for them<br>Notice the difference between SSR 2/1 and SSR 2/1 rev. 1 in the definitions at the end |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| COMMENTS BY REVIEWER<br>Country/Organization: **WNA / CORDEL**<br>Date: October 28, 2020<br>pages | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1. | | General comment on terminology and definitions<br>Careful attention should be given to harmonizing the wording<br>For example :<br>• "supporting systems", "support system", "support service system" are being used<br>It may be advisable to include a section with Definitions at the end of the document (as is done at the end of SSR-2/1), for example to differentiate the terminology used for provisions whether they aim at mitigating AOOs, DBAs or DECs, for example :<br>• "Safety provisions for AOOs" : features required/credited for AOO mitigation (some of them can be "safety systems" if reliable enough to cover AOO+DBA)<br>• "Safety systems for DBAs" = Engineered safety features required/credited for DBA mitigation.<br>"Safety features for DECs" = safety features required/credited for DEC mitigation (some of them can be "safety systems" if availability and efficiency can be justified)<br><br>To greatly facilitate reading, it is also suggested to introduce and use abbreviations for design extension conditions without significant fuel degradation (=> DEC A is proposed) and for design extension with core melting (=> DEC B is proposed) | | Y | I would agree if the countries agree<br><br>As for the abbreviations perhaps<br><br>DEC w.s.f.d and DEC w.c.m<br>Because some countries have DEC A, B, C or 1,2 …<br><br>also P.E.? for practical elimination der | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2. | 1.10 | This Safety Guide does not consider the specific safety analyses to be carried out for different plant states, as this is addressed in IAEA Safety Standards Series Nos SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [8], SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [9], and SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [10], as appropriate. **One objective of this guide is not only to provide guidance for assessing whether the consequences of Design extension conditions (DECs) comply with the acceptance criteria but to provide guidance for assessing whether the method implemented to establish the list of DECs and the rules adopted for their analyses are appropriate.** | The list of DECs should not be established by doing cherry picking but should result from the implementation of a systematic method and a clear set of rules for their analyses should be established beforehand. The guidance provided currently in DS508 on these aspects is not sufficient to enlighten stakeholders unfamiliar with the concept of DECs. | | | | This Sg doesn't provide this guidance.<br><br>The verification that the selection is appropriate and the rules are corrected is part of SSG-2, as it is for AOOs and DBAs |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3. | 2.6 | 2.6 The requirements in paras 2.3–2.5 establish the safety approach for the design and specifically establish the need for radiological consequences of accident conditions to be not only below acceptable limits but to be as low as reasonably achievable (ALARA). ~~In addition, it needs to be demonstrated in the design that plant states that could lead to high radiation doses …~~ ~~…~~ ~~"The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures" (para. 5.31A of SSR 2/1 (Rev. 1) [1] in relation to DEC).~~ | Keep only the beginning of 2.6<br>The rest is redundant with 2.8 and 2.8 is more clear | | | | I am quoting the requirements on which this safety guide is based |
| 4. | 2.7 | This safety guide is focused on the protection of the public and the environment in accident conditions, which should be assessed ~~to~~ by verifying compliance with a number of requirements in SSR 2/1 Rev.1[1] ~~on~~ pertaining to the general plant design and particularly on its capability to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures, ~~as those indicated above,~~ as well as other requirements for plant specific systems, for instance those related to the containment structure and its systems. | Editorial modification to clarify the fact that the objective is the protection of the public and the environment, not the compliance with the requirements per se => The objective is ensured by verifying compliance with the requirements.<br>In the scope of the safety guide, the focus is put on DEC and practical elimination, which are covered by overarching requirement 20 and more specifically by the text added in red. | y | I can leave with this There is already other comment affecting it<br><br>I don't think it is necessary to make it unnecessarily complicated. I hope it doesn't become reason to keep deleting paragraphs | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5. | | In accordance with Requirement 5 of SSR-2/2 (Rev. 1) [1], radioactive releases in accident conditions are required to be below acceptable limits and be as low as reasonably achievable. In addition, the purpose of the fourth level of defence in depth is that off-site contamination is avoided or minimized. To this aim, a limit for the release of radioactive materials or on acceptable limit on effective dose should be specified for each category of accident conditions, and compliance with these limits should be verified. For accidents without significant fuel degradation, the releases are required to be minimized such that off-site protective measures (e.g. sheltering, evacuation) are not necessary. For accident with core melting, the releases are required to be such that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'. The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release. In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis | The last two sentences could be kept but moved at the end of 2.10. | | | | I don't move there I would be separating criteria for the different types of DEC |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6. | 2.10 | ~~Harmful radiological consequences to the public can only arise from the occurrence of accidents.~~ The most harmful (radiological) consequences arising from facilities and activities have come from inter alia the loss of control over a nuclear reactor core.<br>Therefore, the following chapters are devoted to the implementation and assessment of defence in depth and the complementary need for demonstration of practical elimination of accident sequences that can lead to early or large radioactive releases.<br>The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release. In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis. | "Harmful radiological consequences to the public can only arise from the occurrence of accidents."=> There may not be a consensus on this formulation. It is suggested to reformulate, using the wording from SF-1<br><br>The last two sentences are moved from 2.8 | Y | Text has been moved considering other comments too<br><br>Are we here only to copy SF-1 or requirements?<br><br>Now we would have the most harmful consequences and loss of control over the reactor core?. What this would be ?<br><br>Can it be interpreted as something leading to reactor scram ?<br><br>From SSR 2/1:<br>— "A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions" (para. 5.25 of SSR-2/1 (Rev. 1) [1] in relation to design basis accidents).<br><br>Would you admit that an AOO can have hamful consequences on the public? | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7. | 2.11 | ~~Recommendations on radiation protection in design of nuclear power plants are provided in IAEA Safety Standards Series No. NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants [12], and recommendations for protection of the public are provided in IAEA Safety Standards Series No. GSG-8, Radiation Protection of the Public and the Environment [13].~~ | This is out of the scope of the document. It may be moved to chapter 1 where paragraph 1.9 already states what this guide is not intended to provide. | | | | NO<br><br>The subject is not treated in the guide. It is legitimate to say at this place<br><br>This is happening constantly that at some point one guide refers to another for some subject. |
| 8. | 3.2 | … will lead to no or little harm to the public. **The systematic consideration of failures acknowledges for the fact that the understanding of the failure modes of the SSCs credited in the analysis may be incomplete (due to insufficient operating or tests feedback, unexpected phenomena during transient…) and therefore it is a safe design principle to implement several independent lines of defense able to perform the same safety function. On this basis, systematic failure of SSCs should be postulated in principle, though, as exceptions, some exclusion of failure could be claimed, in particular on probabilistic grounds.** | Proposed additional sentence because this is the main driving idea in defense in depth:<br>• Design high quality SSCs<br>• In spite of the quality of SSCs, postulate their failure<br>• Implement alternative means to limit the consequences of failures<br>Recalling these principles helps to understand the further recommendations | | I | | find the wording complicated and that it can be challenged<br>I don't think this is really needed |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9. | 3.3 | **(d) The analysis rules associated to each level of DID that specify in particular: the SSCs that can be credited in the analysis, the level of conservatism expected in analysis belonging to a given level, the derived safety criteria that bound the acceptable level of degradation of the barriers associated to each level.** | Propose to add a 4th aspect because the set of analysis rule is of major importance to assess the performances of the safety provisions. Depending on the level of conservatism and the safety criteria selected, a given provision may or may not fit within a level of DID. | | | | I agree on the topic, but this is very complicated for the purpose here<br><br>It is not only the analysis rules but also the design rules. They affect the reliability |
| 10. | 3.6 | **Anticipated Operational Occurrences** | It is suggested to add a title just before 3.6 (as it is done with DBA just before 3.8 and DEC just before 3.13) | | | | We are not singling out AOO from normal operation<br><br>It was the decision in February to cut the specific parts on NO and AOO |
| 11. | 3.7 | **Anticipated Operational Occurrences (AOOs) and Design Basis Accidents (DBAs) are single postulated initiating events or single representative event sequences corresponding to different frequency ranges.**<br><br>Consistent with the highest frequency of postulated initiating events for design basis accidents (usually lower than $10^{-2}$ per reactor-year), the reliability of safety provisions for anticipated operational occurrences should be such that the frequency of transition into an accident condition is significantly lower than this value. | It is important to make it clear that AOOs (as well as DBAs) are single postulated initiating events, as opposed to most DECs which are the combination of multiple failures.<br>“single representative event sequence” is a wording used in SSG-2 | | | | What is the result of the failure in the control of an AOO?<br>It would be normally a DBA condition?<br><br>single postulated initiating events doesn’t exist in SSG-2 and the term single representative event sequence is later not used after definition. What should the purpose here? It makes things more complicated? |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 12. | 3.11 | Design basis accidents are postulated events that are not expected to occur during the lifetime of the plant. The most frequent events categorized as DBAs should have an expected frequency below $10^{-2}$ per reactor-year**. DBAs should include both rare single initiating events and also frequent single initiating events that failed to be controlled in the second level of DiD.** The operation of safety systems designed to control DBAs should **in principle preferably** rely on automatic actuation**. However, actuation of safety systems or operator intervention should be acceptable unless sufficient time, information and conditions necessary for detection, diagnosis, decision making and for performing the required actions with a high level of confidence are not available.** ~~and should not involve human intervention for a sufficiently long period of time and their~~ **Safety systems**~~-~~reliability should be very high. **Their performance should be ensured despite the occurrence of the most penalizing single failure affecting them at the most penalizing time.** | It helps to understand why some DBAs implicitly combine a single initiating event with the failure of control or limitation systems.<br><br>If the required conditions are available to allow reliable human action with a high level of confidence, this should not be ruled out.<br><br>SFC implies identifying the most penalizing single failure and the corresponding time. | y | I can implement the 1st part<br><br>The rest is not aligned with SSR 2/1 4.11, 5.11, 5.57, etc. and goes in details that are not wanted in this guide | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13. | 3.11 continued | Safety systems should be designed to ensure their reliable operation under postulated external hazards and prevailing environmental conditions. The reliability of safety systems should be such that ~~(to the extent possible)~~ the collective contribution to the core damage ~~frequency of failing to mitigate DBAs~~ does not exceed the safety goals of the plant (for new nuclear power plants typically below $10^{-5}$ per reactor-year). If this is not the case, ~~DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate to achieve such goal~~s. **safety features for DEC-A should be implemented in the design, in addition to the safety systems, to prevent core melt in the most frequent sequences [DBAs + failure of safety systems] and in accident conditions not covered by DBAs such as events involving multiple failures not covered by DBAs, up to the extend needed to meet the safety goal of core damage frequency.** | The probabilistic target for CDF does not only rely on safety systems involved in DBA mitigation but on control systems for normal operation, safety provisions for AOO mitigation …<br><br>clarification | Y | Partially<br><br>If to the extent possible is removed, there is no need to design for DEC-A<br><br>the collective contribution to the core damage refers that it is not just because of the safety systems for DBA<br><br>The last part it is better to include it in the section on DEC | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14. | 3.12 | ~~If the design of the containment is such that in the case of the most limiting DBAs the intervention of cooling or pressure reduction systems (e.g. containment spray) is necessary to ensure the integrity of the containment boundary, such systems should be designed, constructed and maintained to ensure a very high reliability, since their failure would not only lead to a severe accident but also jeopardize the subsequent measures for its mitigation.~~ **Because the integrity of the containment can be challenged by certain DBAs (DiD level 3a), certain DEC-A (DiD level 3b) and by DEC-B (level 4) independent and diversified features should be implemented in the design to remove heat from the containment in case of DBA with failure of the safety systems challenging the integrity of the containment, so that the hability to remove heat from the containment would not be jeopardized in case of escalation up to an accident condition with core melt.** ~~For the same reason, c~~Containment isolation provisions in case of DBAs should ~~also~~ be designed to have very high reliability for ensuring that acceptable limits for radiological consequences are not exceeded and sufficient coolant inventory can be maintained. Severe accidents with an open containment constitute one of the plant conditions to be practically eliminated that are addressed in Section 4. | Failure of pressure reduction system won't cause a severe accident<br>This statement implicitly assumes that containment cooling function cannot be diversified and ensured by independent means. It should rather be recommended that independent and diversified means exist to remove heat from containment, so that the failure of the safety system does not jeopardize the capability to limit the consequences in DEC. | | | | If a system like containment spray is needed for some DBAs to protect the containment, then if the cooling fails and the core is damaged we have a severe accident with an open containment<br><br>Cooling the core with a failed containment is also challenging because there will be a loss of cooling inventory<br><br>I don't know which are are DEC-As challenging the containment, but all DEC-B will<br><br>This is a text already revised with other comments |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 15. | 3.16 | Design extension conditions without significant fuel degradation **(also referred to as DEC-A)** should be considered for unlikely yet credible single or multiple failures with the potential for exceeding the capabilities of safety systems designed for the mitigation of DBAs. **The DEC-A approach is intended to consider events not covered by the DBA approach, for which mitigation is required to meet the core damage frequency target. Those events impair this probabilistic safety target because the frequency of occurrence resulting from the combination of some postulated single initiating event frequency and multiple-failures probability is insufficiently low. Addressing DEC-A in the plant design and in the plant safety assessment in a deterministic way allows to identify and justify the presence of the needed mitigation features and their performance level. In particular, the DEC-A events should cover the AOO events and the most frequent DBA events experiencing a common cause failure on their mitigation means (incl. safety systems), with a resulting probability of occurrence higher than the target for core damage frequency. Additional or different mitigation features should therefore be implemented for those DEC-A events to prevent core melt, while they are not covered by the DBA approach.** | The additional text is proposed to provide the reason for having a DEC-A approach in addition to the DBA one.<br>This additional text can replace 3.22 and 3.23 which can then be deleted. It is more logical to insert this text at the beginning of the section dealing with DEC-A rather than almost at the end of the DEC-A section.<br><br>It is important mentioning that DEC-A consider the combination of common cause failures to AOOs and the most frequent DBAs only. | Y | I can agree that it would be good to provide this approach at the beginning<br><br>The new text is fine as a concept but the text needs improvement and cannot be implemented immediately<br><br>Although CCFs could be the most likely cause of system failures, we should be careful not to refer exclusively to CCFs.<br>SFC criterion is also not required for AOOs/level 2. | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16. | 3.17 | A postulated initiating event associated with the **complete** failure of a safety system used for normal operation, e.g. a support system, and is required for the control of the initiating event. **In practice the potential consequences of failure of every safety function should be reviewed in order to build the list of relevant DEC w/o significant fuel degradation** | A single failure in a support system should not lead to a DEC | y | No need for "complete"<br><br>The failure of the system means that it cannot perform its intended function | | |
| 17. | 3.18 | ~~In general, the mitigation of DEC without significant fuel degradation should be accomplished by specific safety features designed for such conditions. Alternatively, they can be mitigated by available safety systems that have not been affected by the events that led to the DEC under consideration~~. **The mitigation of DEC-A should be accomplished either by specific safety features designed for such conditions, or by available safety systems that have not been affected by the events that led to the DEC-A under consideration. In the 2nd case, complementary design requirements related to the safety function they have to perform under the considered DEC-A, may be added to the initial design requirements related to the DBA one (e.g. qualification, reliability).** | Both approaches are acceptable. It is important to explain that if safety systems, not affected by the initiating event, are used in DEC-A, it may be necessary to take into account additional design requirements for these safety systems | y | The 1st part of you change is purely editorial<br><br>The 2nd part can be misleading because the environmental conditions for qualification are not more demanding for DEC-A and reliability requirements for DEC-A are not higher than for DBA.<br><br>In fact we say that rules for design and safety assessment are more relaxed | | |
| 18. | 3.19 | Since the objective in DBA and in DEC without significant fuel degradation is the same, namely to prevent core damage or damage to the fuel in the irradiated fuel storage, the primary difference between these two accidental conditions is the use of different **rules** or criteria for … | Addition of a missing word | y | Changed with other comments | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 19. | 3.20 | ~~The use of available safety systems, when possible, in DEC without significant fuel degradation has the important advantage that safety systems are designed with very stringent reliability criteria.~~<br>~~In such cases, t~~ **T**he rules for **DEC without significant fuel degradation (DEC-A)** safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result (in particular regarding the prevention of cliff edge effects) that cannot be simply achieved by best estimate calculations. ~~If the rules were the same, there would not be a need for differentiation between DBA and DEC.~~ **Using less conservative rules for DEC-A analyses compared to DBA analyses is justified by the reliability level to be covered considering the multiple failures already considered in the definition of DEC-A sequences.** | Use of safety system sis already covered by 3.18. The first part of 3.20 does not add new recommendation<br><br>It is worth explaining why the rules can be less conservative. | y | There is no need for the deletion because it emphasizes why the use of available safety systems is of advantage<br><br>The last part explaining why it is justified can be added (this is also not providing a recommendation)<br><br>I keep the last part that you want to delete to clarify that if everything is done in the same way (design and safety analysis) DBA and DEC-A can be merged | | |
| 20. | 3.22 | ~~Design extension conditions should be considered for failures of safety systems designed both to cope with anticipated operational occurrences and DBAs.~~ | See modification proposed for 3.16. The new text proposed for 3.16 combines 3.22 and 3.23 and it is more logical to give the reason why the DEC-A analyses are implemented in addition to DBA analyses, at the beginning of the section. | y | The explanation that you proposed can be considered at the beginning, but here you are deleting the recommendations on which there are comments by others and this needs to be taken into account | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 21. | 3.23 | ~~Design extension conditions should also be considered to reduce the frequency of severe accidents caused by failures in the mitigation of some DBAs to acceptable levels by, if possible, the use of additional, diverse measures to cope with common cause failures of safety systems.~~ | See modification proposed for 3.16. The new text proposed for 3.16 combines 3.22 and 3.23 and it is more logical to give the reason why the DEC-A analyses are implemented in addition to DBA analyses, at the beginning of the section. | Y | The explanation that you proposed can be considered at the beginning, but here you are deleting the recommendations on which there are comments by others and this needs to be taken into account | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 22. | 3.24 | Design extension conditions without significant fuel degradation constitute a reinforcement of the design for some complex and unlikely failure sequences. As some safety systems are designed to cope with various DBAs (e.g. the emergency core cooling is designed for several sizes and locations of loss of cooling accidents or main steam line breaks), safety features for DEC can help to reinforce the capability of the plant for specific sequences improving and balancing the risk profile applying less stringent design or safety assessment criteria than for DBA conditions. ~~The reliability of safety systems should be high enough for DEC without significant fuel degradation to only be postulated exceptionally and to occur with a frequency lower than the most limiting DBAs.~~ | The last sentence is unclear, and incorrect since the frequency of occurrence of the DEC-A sequence is generally of the same order of magnitude or even higher than the one of the most limiting DBAs (e.g. AOO of 1/r.y + CCF of safety system 10-3/d lead to DEC-A event of 10-3/r/y - DBA of 10--2/r.y + CCF of safety system 10-3/d lead to DEC-A event of 10-5/r.y).<br>Indeed, even though the reliability of safety systems is high (failure ~ 10-3/r.y), the defense in depth principle recommends to assume their failure. Basically it seems safe that any safety function that is "frequently" used is diversified. Therefore, having many DEC sequences illustrates a strong design and not a poor one.<br>Some DBAs have very low frequencies, so it happens that DEC sequences may have higher frequencies than those DBAs. It would be a mistake to exclude overlapping of frequency range for DBA and DEC-A. | Y | I can agree that in the way it is written this part is controversial<br><br>This I disagree in that :AOO of 1/r.y + CCF of safety system 10-3/d lead to DEC-A event of 10-3/r/y -<br><br>In general because it means that there is no systems for AOO or is the same for AOO and DBA<br><br>The point to be made is postulated DEC-A is not an alternative for designing safety systems reliably and compensate with something of a lower class or even saving on equipment for AOOs<br><br>For the moment I leave it with a very low frequency | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 23. | 3.26 | The accident conditions chosen should be justified based on engineering judgement and insights from the probabilistic safety analyses: see SSG-53 [5]. A detailed analysis should be performed and documented to identify and characterize accidents that can lead to core damage. For new nuclear power plants accidents involving core melting ~~are~~ **should be** postulated as DEC, irrespective of the fact that the design provisions taken to prevent such conditions make the probability of core damage very low. Aspects that affect the accident progression and that influence the containment response and the source term should be taken into account in the design of the safety features, as indicated in SSG-53 [5]. | editiorial | y | I have changed It is not purely editorial<br><br>SSR 2-1 doesn't say that all accidents involving core melting should be postulated as DEC | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 24. | 3.29 | ~~Radioactive releases due to~~ **The** leakage from the containment 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 leakages could exceed this limit but **still remain below the safety limit leak rate and, as a consequence the radioactive release should** be well below the criterion for a large radioactive release. This may be achieved by provision of adequate filtered containment venting or other design features or alternative measures that could be included in an overall demonstration of adequacy of the containment function.<br>**If a containment venting system is included in the design, it should not be designed as the principal means of removing the decay heat from the containment in case of severe accident and it should be assessed whether the safety margins in containment dimensioning are such that it would not be needed in the early phases of the severe accident, to deal with the containment pressure.** | It is incorrect to compare radioactive releases with containment leakage rate.<br><br>consistency with SSG-53<br><br>This proposed new text corresponds to what was indeed meant by the second sentence of requirement 6.28A which was added during SSR-2/1 revision 1 process ! It was not written explicitly like that because some Member States did not want to see the term and even less some requirements on venting systems in SSR-2/1. Now, SSG-53 is a guide for design, not for assessment. So this aspect is covered nowhere in the suite of IAEA safety standards for the moment. DS508 is a good opportunity to fill this gap ! | y | Changed with other comments<br><br>It seems that disagreement exist about this<br><br>I would add this text preliminary but it will raise questions<br><br>It is partially addressed in SG-53 and not at all in SSG-2 | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 25. | 3.30 | A safety assessment of the design should be performed with consideration of the progression of severe accident phenomena and their consequences**, the achievement of acceptable end state conditions,** and addressing applicable topical issues such as the following:<br>— Corium stratification and criticality;<br>**— Corium stabilization and cooling;**<br>— Thermal-chemical interaction between corium, steel components and vessel;<br>… | Stabilization and cooling are important aspects which should be assessed to ensure that an acceptable end state can be reached | Y | Partially<br><br>The example list of topics covers the topic proposed considering also other changes | | |
| 26. | 3.34 | 3.34 The performance and reliability of safety provisions for different plant states should be assessed taking into consideration the **applicable set of analysis rules associated to each level of DID** ~~level of risk and their safety significance~~. Such safety provisions … | Level of risk and safety significance are reflected by the level of DID | y | It is interconnected The part removed is important for those using a risk informed approached, these aspects are considered in the safety classification<br><br>Plant states levels of DiD are equivalent | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 27. | 3.36 | (e) The number of barriers provided in the design should be justified. The assessment of defence in depth should ~~examine various barrier options and~~ demonstrate that the barriers chosen for each plant state offer **an appropriate** ~~the best~~ protection for workers and the public that may be reasonably expected | A designer cannot analyze in sufficient detail multiple design options in order to compare them in a safety analysis report. It is never possible to prove that the "best" option has been found. It is only possible to prove that it is good enough, according to established criteria. It is recommended that derived criteria (on main plant parameters, proving barrier integrity for instance) should be selected rather than mere radiological criteria | y | The first part<br><br>Best reasonably expect is appropriate | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 28. | 3.38 | 3.38 The adequacy and effectiveness of safety provisions should be assessed by performing deterministic safety analyses modelling the plant response **to a given initiating event** for different boundary conditions representative of **each level of DID**. **Each of these levels of DID should be characterized by a type of transient analysis, with associated set of analysis rules, level of conservatism and safety criteria, typically** anticipated operational occurrences, DBA, DEC without significant fuel degradation and DEC with core melting. Recommendations on conducting deterministic safety analyses for the different plant states are provided in SSG-2 (Rev.1) [8]. | In order to achieve a "readable" demonstration of DID, each level has to be clearly defined and characterized (with rules and objectives). Claiming that DID in only proved on a case by case basis for each initiating event makes it impossible to grasp as a whole. | y | Implemented with some modifications<br>3.1 The adequacy and effectiveness of safety provisions should be assessed by performing deterministic safety analyses modelling the plant response to a given initiating event for different boundary conditions representative of each plant state, operational occurrences, DBA, DEC without significant fuel degradation and DEC with core melting, which should be characterized by a type of transient analysis, with associated set of analysis rules, level of | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 29. | 3.39 | The performance of safety provisions at each level of defence in depth is assessed through engineering assessment and deterministic analysis involving the use of **analysis rules specific to the level of DID considered,** validated and verified analysis codes and models to demonstrate that acceptance criteria are met with sufficient margins. | Confidence in the margins obtained depends on the analysis rules applied (and not on a mere quantitative result). The margins are all the more large that the analysis are conservative. On the opposite, a Best Estimate analysis in some cases may falsly let to think that margins are available compared to the acceptance criteria whereas the result may be highly sensitive to small variations in some input data (cliff-edge effect). | y | Yes<br><br>But this is covered in the change made with the previous comment | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 30. | 3.43 | 3.43 Equipment for controlling anticipated operational occurrences is aimed at reducing the number of challenges to safety systems. It should be demonstrated that their reliability is such that anticipated operational occurrences only evolve into DBA conditions with a low frequency **low enough to remain consistent with the core damage frequency target** ~~well below the highest frequency of postulated initiating events categorized as DBAs~~. | The only requirement is that the frequency of the initiating event combined with the failure of provisions credited in AOO (DID level 2) is consistent with the frequency range expected for DID level 3 (DBA).<br>The DBA range typically starts at 10-2/r.y, it would not be acceptable that the frequency of AAO PIE combined with failure of AOO provisions would be greater than 10-2/r.y<br>Indeed, the DBA resulting from an AOO with failure of the safety provisions for the AOO, is correctly mitigated by the safety systems being designed for the DBA | | | | Your explanation repeats what you have deleted.<br><br>Instead the change requires meeting the CDF target.<br>This is not the specific objective of systems for AOO |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 31. | 3.44 | The combined reliability of the safety systems designed to mitigate the consequences of a DBA should be sufficient to demonstrate with high confidence, that their probability of failure under the conditions expected for each accident sequence postulated is very low. A failure probability below ~~than~~ 10-3 in order of magnitude would be consistent with the strict requirements for reliability imposed to safety systems and supported by operational experience and testing.<br>**Note : The design rule « single failure criterion » applied to any safety system contributes to meeting this reliability target.** | editorial<br><br>self explanatory | y | Editorial change<br><br>Reliability achieved is not only the result of SFC but several other requirements imposed to the design of safety systems | | |
| 32. | 3.46 | 3.46 Safety features for DEC without significant fuel degradation should be demonstrated **to be efficient enough to prevent core melt** for the accident sequences for which they are intended, **according to the applicable analysis rules, and** to be sufficiently reliable in order to contribute to ensuring a core damage frequency below the established probabilistic targets. | The first concern is to prove the efficiency of the DEC features, according to rules that guarantee acceptable margins. Reliability has to be considered in a second step. Both are necessary. | Y | I agree and I included it<br>Here however, we re are dealing with the reliability not with the DSA and engineering analysis | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 33. | 3.47 | The capacity and reliability of safety features specifically designed to mitigate the consequences of DEC with core melting should be adequate to ensure that the containment integrity will not be jeopardized during any postulated core melt sequence. ~~However, since the analysis of core melt and its impact on containment integrity is surrounded by considerable uncertainties, only a limited reliability can be attributed to those components necessary to ensure the containment integrity after a core melt accident.~~ **Since the analysis of a core melt accident and its impact on containment integrity is surrounded by considerable uncertainties, the reliability claimed for those components necessary to ensure the containment integrity after a core melt accident is to be defined cautiously with due consideration of these uncertainties.** | The last sentence is excessive, since the limited reliability resulting from important physical uncertainties does not apply to the components involved in the containment integrity function whose qualification relies on enveloping and robust severe accident conditions (e.g. containment isolation valves, whose high reliability is recommended in article 3.12). The proposed sentence seems more appropriate. | y | I implement the comment because we think the same<br><br>Qualification of several components has important limitations.<br><br>Some countries don't accept LERF/CDF to exceed a certain value | | |
| 34. | 3.48 | Consider deleting or clarify | Consider deleting or clarify because the text is difficult to understand and may be interpreted in many ways. What means "extreme scenarios"? Are we still talking about DEC-B? Non permanent equipment are not supposed to be credited in the safety analysis (DBA/DEC) | y | Clarified<br><br>Severe accidents | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 35. | 3.50 | Consider deleting | Reqt 21 of SSR-2/1 does not seem to deal with independence between level of DID but rather about independence between redundancies. Referring to it here seems inappropriate because, though physical separation, functional independence, …. could be credited to prove independence, they are not strictly required. | | | | Some general plant design requirements in SSR-2/1 (Rev. 1) [1] address aspects contributing to it.<br><br>**Interference between safety systems or between redundant elements of a system**<br><br>It is a point of reference. We are not developing the requirement in full |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 36. | 3.53 | It is recognized in the IAEA safety standards that full independence of the levels of defence in depth cannot be achieved **and it is actually not systematically needed**. This is due to several factors and constraints, such as a potential common exposure to the effects of external hazards and/or internal hazards, an unavoidable sharing of some items important to safety, as well as human factors. **Typical cases concern the containment isolation valves which, thanks to their very high reliability can be credited under accident conditions, whether DBA, DEC-A or DEC-B, or the number of diversified I&C platforms which do not need to be 5 to achieve the safety functions under normal operation + AOO + DBA + DEC-A + DEC-B. In a similar manner, I&C instrumentation needed to achieve the safety functions does not need 5 diversities of sensors.**<br>The design of a nuclear power plant should consider all potential causes of dependencies and include and implement an approach to remove them to the extent reasonably practicable. Robust independence is essential and should be implemented among systems whose simultaneous failure would result in conditions having harmful effects for people or the environment. For this reason, safety features specifically designed to mitigate the consequences of accidents with degradation or melting of the core should, as far practicable, be independent from safety systems, in accordance with paras 4.13A and 5.29 of SSR-2/1 (Rev. 1) [1] **and also from systems used in normal operation and to mitigate AOO**. | The fact that "*full independence of the levels of DiD cannot be achieved*" is insufficient to recognize it is acceptable in the NPP design. Complement should be added to indicate that this full independence is not required everywhere.<br>Examples could be given to substantiate this assertion. Knowing that the frequency of core melt is very low, it may only result from complex sequences including massive failures. There may be many paths to result in a core melt and there are only a limited number of representative sequences analysis. In order to be sure that any of these paths is adequately bounded, it is better not to credit any system belonging to a former DID level. In other words, when we analyze DEC-B, we don't know exactly how we arrived to that situation and we don't actually care to know for the safety demonstration, we postulate that everything is lost and we just rely on dedicated features. | y | What you say is not totally<br>**and it is actually not systematically needed**<br>this cannot be written<br>Second large change it is too long and I have been asked to remove several paragraphs already written on I&C<br>I have put the containment itself as something shared for different levels of DiD<br>The last part is correct, although obvious<br>I have put it | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 37. | 3.57 | The SSCs needed for each postulated initiating event should be identified, and it should be shown by means of engineering analyses that the SSCs needed for implementing any one defence in depth level are sufficiently independent from the other levels. The adequacy of the achieved independence should also be assessed by probabilistic analyses. | Independence between 2 systems is a deterministic characteristic, probabilistic assessment cannot help to assess it. Probabilistic assessment can only help to assess an overall level of risk for the plant, considering the known lacks of independence | | | | This is not true<br><br>You consider only the whole PSA integrated process aimed at calculating CDF or LERF<br><br>This doesn't prevent you from taking parts of the models to<br><br>Calculate failure probability of the ECCS<br><br>Or the combined failure probability of EFW and Feed and Bleed<br><br>Or develop simplified models for that<br>You are only looking here primarily at dependencies |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 38. | 3.58 | 3.58 The systems and components used for different plant states should be separated, within the same safety division, from one another by distance or protective structures **in order that a given hazard does not render fully unavailable two levels of DID that may be required to achieve the safety goals.** ~~if there is a possibility for consequential failures arising from a failure of a system or component for another plant state.~~ | Losing components contributing to different levels of DID may be acceptable provided that those levels are not fully lost (different redundancies in other divisions). | | I accept the intention<br><br>Separation by redundancies is clear<br><br>AOO-A AOO – B<br><br>DBA-A DBA-B<br><br>Here we speak about<br><br>AOO-A DBA- A<br>AOO-B DBA-B<br><br>The failure of AOO-A cannot cause the failure of DBA-B . This is clear<br><br>Consequential failures from another plant state doesn't mean that the other plant state would fail totally<br><br>I can make this more clear<br><br>consequential failures arising from a failure of a system or component of one safety division in the same safety division for another plant state. | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 39. | 3.59 | … For most reactor designs, the reactor trip system is designed as a safety system that is also needed for the control of accidents. In such cases, it should be shown that there is no practicable alternative to use of the safety system to cope with the anticipated operational occurrence, and that the use of the safety system for such an occurrence does not present a significant limitation on the use of the safety system to mitigate a DBA. **It should also be shown that in that case, the reliability of the protection system (safety system) covers the frequency range corresponding to AOOs and DBAs, otherwise a back-up system of the protection system should be implemented as a safety feature for DEC-A to cope with all DEC-A sequences not covered by the ATWS cases.** | additional explanation on the implication for the protection system | | | | This important aspect is not considered purely probabilistically<br><br>This is defeating the DiD and the reactor needs to be made subcritical<br><br>I cannot recommend a back up of the protection system. The failure of the control rods to insert is most likely the reactor protection system<br><br>Here I am just highlighting an important case of dependency |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40. | 3.64 | 3.64 The assessment should demonstrate that a failure of a support service system is not capable of simultaneously affecting ~~redundant~~ parts of a safety system and **parts of** ~~(or~~ a system fulfilling diverse safety functions~~)~~ and thereby compromising ~~the capability of these systems to fulfil their safety functions, or otherwise adversely affect~~ ~~the independence of safety systems or~~ independence between levels of defence. For this purpose, the assessment should provide evidence that the reliability, redundancy, diversity and independence of the support service is commensurate with the significance to safety of the system**s** being supported **and their contribution to various levels of DID**. | It is true that support systems can also compromise the redundancy of safety systems but is it not a matter of DID, it is just a matter of DBA analysis. What is important regarding DID is that systems credited in various levels of DID are not supported by a unique system which failure would compromise both levels. | Y | Changes<br><br>The topic is important but as you say no the subject of interest here but one country has commented twice and stressed that point in the virtual meeting<br><br>I will see that both aspects are covered<br><br>The assessment should demonstrate that a failure of a support service system is not capable of simultaneously affecting parts of systems for different plant states in a way that the capability to fulfil a safety function is compromised. . For this purpose, the assessment should provide evidence that the reliability, redundancy, | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 41. | 3.65 | 3.65 An assessment of independence of SSCs that **may be** ~~are~~ necessary, **in different lines of defense,** to mitigate the consequences of a single or a likely combination of external hazards on the plant should be conducted. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in ~~common cause failure between the SSCs necessary for their mitigation.~~ **the loss of an unacceptable number of levels of DID**. **In particular safety features dedicated to core melt mitigation should always remain available.** | As stated now, this is just a requirement telling that systems required to mitigate possible events initiated by hazards should remain available. Regarding DID, the requirement should be stronger: depending on the hazard frequency, a sufficient number of levels should remain available. In particular features dedicated to core melt mitigation should always remain available. | y | I agree but we are not speaking here about the magnitude (related to the frequency of the hazard)<br><br>3.653.68An assessment of independence of SSCs that may beare necessary at different levels of defence in depth to mitigate the consequences of a single or a likely combination of external hazards on the plant should be conducted. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in common cause failure between the SSCs necessary for its mitigation at different levels of defence in depth. In particular, the necessary safety features for design extension conditions for core melting should always remain available. | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 42. | 4.3 | … However, these provisions may have limited capabilities that could not reasonably cope with some specific severe accident conditions; those are the conditions that should be explicitly identified and practically eliminated. **Therefore, practical elimination should primarily focus on provisions needed to eliminate the core melt physical phenomena which could not be mitigated in a safe and reasonably practicable manner.** | additional guidance | y | I have no problem with the additional guidance but I had already to remove the preceding text because it was considered already redundant | | |
| 43. | 4.13 | The classification and grouping in para. 4.12 ~~is~~ **are** consistent with the recommendations provided in SSG-53 [5] and SSG-2 (Rev. 1) [8], highlighting some examples …<br>… is necessary. To facilitate the grouping proposed, each type of accident sequence should be analysed to identify the associated combination of failures or associated physical phenomena that are specific to the plant design, and which have the potential to lead both to severe accident sequences and 'unacceptable radioactive releases'. This analysis helps identifying accident sequences that could lead to conditions that need to be 'practically eliminated'. **It may be associated with a PSA level-2, however demonstrative justification should be provided regarding its exhaustiveness, being as close as possible to a deterministic approach.** | The last two sentences are close to describing the purpose of PSA level-2 (not said, but could be understood as met via PSA level-2). A complement should be added to underline the objective to make the analysis demonstrative with respect to its exhaustiveness concerning the physical phenomena and the accident sequences at risk whose elimination is needed | | | | Actually there is nothing probabilistic in this.<br><br>If one case I know is H2 explosion, I know that all sequences with core melting will generate it<br><br>For other cases it is not going to be so simple to make group and take the most limiting condition, but this in essence is not probabilistic, although such sequences can be found in the PSA<br><br>Th text proposed is not well elaborated and will create confusion |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 44. | 4.23A | **Design provisions for practical elimination of some severe accident conditions could require automatic actions having detrimental effects or impairing design criteria associated to previous DiD levels (e.g. opening of primary circuit depressurization valves to prevent high-pressure core melt). In that case, an assessment of the I&C failure rate (spurious actuation of the depressurization valves) should be part of the justification needed to ensure the absence of unacceptable impact on the plant safety level (e.g. additional LOCA scenarios).** | Additional guidance proposed to be added between 4.23 and 4.24 | y | Yes but I think you don't mean automatic action. This in contradiction with the text. It is a manual depressurization. You just mean the spurious actuation. This is also for the PORVs<br><br>It is better to say that the detrimental impact on safety of spurious opening should be taken into account in the design and the safety assessment | | |
| 45. | 4.41 | When the accident sequence to be 'practically eliminated' is the result of a single initiating event such as the failure of a large pressure-retaining component6 **under normal operation**, the demonstration should rely on achieving a high level of quality at all stages of the component lifetime: design, manufacturing, implementation, commissioning, operation (periodic testing and in-service monitoring, if any) to prevent the occurrence and propagation of any defect liable to cause the failure of the component. Hence, the occurrence of the initiating event (e.g. failure of a large pressure-retaining component of the facility) or the consequential event (i.e. uncontrolled reactivity accident) needs to be considered for 'practical elimination'. | The failure of a large pressure-retaining component considered under 4.41 is a failure during normal operation (or AOO transient). It does not address the failure during an overpressure transient (DBA initiating event + failure of the overpressure protective devices) which is a sequence to be considered in the demonstration of practical elimination. Complement should be added to express this fact | y | Let's then put in operational states. | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 46. | 5 | ~~MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF VERY UNLIKELY CONDITIONS EXCEEDING THE PLANT DESIGN BASIS~~<br>**IMPLEMENTATION OF DESIGN PROVITIONS FOR ENABLING THE USE OF NON-PERMANENT EQUIPMENT FOR POWER SUPPLY AND COOLING** | The title should be consistent with the information given in 1.13 | Y | I guess I will have to surrender | | |
| 47. | 5.3 | The aim of the use of such equipment is to restore safety functions that have been lost, but not to be the regular means to achieve these functions in accident conditions **within the plant design envelope (DBA and DEC)**. | additional explanation | | , i.e. in DBA and DEC<br><br>When agreed on design basis with the new definition of the Glossary<br><br>With the existing title it was crystal clear<br><br>Accident conditions comprise DBA and DEC. It is in SSR 2/1 | | |
| 48. | 5.3 | Proposal for additional footnote:<br>**Non permanent equipment can be credited in the long term of the accident management to maintain the safe state during a time period longer than the plant autonomy**. | The deterministic safety demonstration is not performed for an unlimited period of time but it is associated to a clear autonomy target (for instance 72h). For instance we have to refill the diesel generators. | | I could agree but I don't want to make it more complicated because plant autonomy can be maintained also by receiving more Diesel fuel<br><br>As for the water supplies, it is not like the fire truck is a significant additional mass of coolant | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 49. | 5.5 note 9 | The concept of **robustness** ~~practical elimination~~ is applied to external hazards within the safety analysis | Talking of practical elimination is misleading here as the methodology is very different from what is recommended in §4. It is suggested to avoid mixing the concepts | Y | I agree but some country is already using this term for this purpose<br><br>However there is a mistake in the footnote "no" was missing<br><br>I hope this solves the issue | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 50. | 5.6 | **Selected scenarios should be defined to identify and verify the existence of margin in the design of items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site. Consideration should be given to the credible combination, if any, and the level of intensity of each natural hazard contributing to the selected scenario, taking into account recommendations provided in DS490 [15] and DS498 [16].**<br>For each selected scenario the evaluation should identify limitations on the current plant response capability and should define a strategy to cope with these limitations. In the evaluation, the various coping provisions, accident management measures and equipment (fixed or non-permanent equipment stored on-site or off-site), that will be used to restore the safety functions and to reach and maintain a safe state should be identified. Such an evaluation should include the following: | Editorial : this article should not start with "For each selected scenario …". It should first be explained what the scenarios should be and for what purpose.<br><br>Additional guidance should be provided for defining the selected scenarios, e.g. regarding combination (if any ?) and intensity of natural external hazards to be considered here. At least reference should be made to DS490 and DS498 (even though the guidance provided on this aspect in DS490 and DS498 is "limited"). Furthermore, paragraph 4.4 of DS498 talks about non-permanent equipment used to fulfil (not to restore) safety functions.<br>The additional text suggested here aims at showing that the definition of scenarios is not straightforward, but is not merely sufficient. The secretariat should consider developing specific documentation on this aspect. Reference to the draft TECDOC "Experience in applying the new IAEA principles …" may be useful as well. | y | For each relevant scenario of an external hazard above the design basis ….<br><br>The comments that I received are in the direction of reducing and not overlapping with other guides. We cannot reference TECDOCs, even less one in draft | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 51. | 5.6 (a) | ~~A robustness analysis of a relevant set of items important to safety to estimate the extent to which those items would be able to withstand natural hazards exceeding their design basis;~~ | This recommendation as initially drafted goes far beyond what is required by SSR-2/1 (the requirements are reminded in 5.2 of DS508) and what is recommended by DS490 and DS498. Recommendations in DS490 and DS498 are sufficient. Bullet 5.6 (a) should be deleted | | | | This has been discussed with the experts of our section on external hazards revising those guide.<br><br>SSR 2/1 was modified after the Fukushima Daiichi accident to enable the use of non permanent equipment<br><br>Clearly external hazards was in mind The requirement is indicated in 5.1, not only 5.2<br><br>Those on the use in 5.2. don't say that the non permanent equipment is for exclusive use in case of extreme external hazards<br><br>IN case of SBO and loss of the alternate power supply for instance they could be used too Or for the pool too<br><br>Referring here to core melting is not correct |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 52. | 5.6 (b) | An assessment of the extent to which the nuclear power plant would be able to withstand a loss of the safety functions without **exceeding the limit for radiological releases defined for accidents with core melt** ~~reaching unacceptable radiological consequences for the public and the environment~~; | Pursuing this assessment beyond the limit for DEC-B would not make sense and could give rise to non-reasonably practicable requirements to further extend the plant design envelope or the design basis for specific SSCs ! | | | | See 51 |
| 53. | 5.7 | However, where applicable, specific facilities and equipment, should be considered **during** ~~at the final stage of~~ the design of new nuclear power plants **in particular regarding the connection means of the non-permanent equipment to the plant**. | Why limit to the final stage? These features should better be anticipated (specific cable or pipe routing). | y | Should have been considered at the final design | | |
| 54. | 5.9 | The coping strategies should be defined, and the associated coping provisions should be specified and designed taking into account the most unfavourable **yet still credible initial conditions and** possible scenario. | For example, not all possible initial conditions should be strictly covered by such analysis. This statement may actually refer to plant modes like shutdown or refueling where specific concerns may arise, then it should be more explicit. Regarding power operation, the aim is not to strictly cover any possible initial condition. | y | … most unfavourable possible scenario defined according to 5.4.<br><br>considering other comments | | |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 55. | 5.14 | Complement<br>**The standards usually require high design margins; however these extreme hazards are not expected to become the design basis therefore those margins could be adapted owing to the low frequency of the events considered.** | If the usual design standards were applied, it would mean that the extreme hazard would become the design basis for the concerned equipment. This is not the purpose of this approach. | | | | This refers to good quality industrial equipment<br>Appropriate standards<br><br>The equipment is not designed for SL-2, it may not be event at the plant or on wheels<br><br>It certainly it needs to be stored in a place where it would not be affected by the hazard |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 56. | 5.16 | Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for demonstration of the successful mitigation of an accident **subsequent to an extreme hazard, in order** to prevent unacceptable radiological consequences. | Let's be clear, non-permanent equipment can only be credited in the frame of extreme hazard, not in deterministic safety analysis otherwise, this would be contradicting recommendations made in previous sections of DS508, e.g. in article 5.3 ! | | Changed to<br><br>Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for accident management to prevent unacceptable radiological consequences.<br><br>This was in mind in the changes to ssr2/1 However,<br>It will be used beyond the design basis, but if we loose the SFP cooling for instance, it will be use, even if its nor because of a hazard | | |
| 57. | Annex I page 31 | Assessment of **the justification of** practical elimination of specific common cases | Editorial: The title could be misleading without the added wording. Because these situations are practically eliminated, they are not assessed (their consequences are not studied) in the safety case. It is the justification of the practical elimination which is assessed. | | | | Sorry<br><br>I don't find the place of the text commented |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58. | Annex I | Consider deletion of Annex I | Annex I is about 90% copy of annex 4 of TECDOC 1791. It brings little added value. In case it is decided to keep it, some comments are proposed below | | | | This was agreed in the DPP<br><br>We don't need to reinvent the wheel and we start from a text that NUSSC had review, not in the regular way, but still decided on the Agency publishing the TECDOC<br><br>In this way, we should minimize comments |
| 59. | Annex I | General comment for the whole of annex I : use 'should' statements rather than 'need', 'is' … | | | | | Should or shall is not allowed<br>This has been discussed with the Editors |
| 60. | Annex I § I-2 | The safety demonstration ~~needs to~~ **should** be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgement can be made for the following key ~~requirements~~ **topics**: | General comment above | | | | See 59 |
| 61. | Annex I § I-2 | 1. **An exhaustive list of transients and loads with the related occurrence numbers and the physical parameters affecting the sensitive parts of the concerned equipment, should be justified. The rules for combination of loads should be established and justified (e.g. regarding earthquake);**<br>2. The most suitable composition materials needs to be selected (**and for each weld the most suitable combination of [base and filler] materials**)<br>3. … | This is the starting point. Without such list, the subsequent bullets are meaningless.<br><br>For a each weld, it is important to consider the base and the filler materials **altogether**. | | | | About this and other topics a book can be written<br><br>We try to highlight the basis for the demonstration in terms of engineering aspects, deterministic and probabilistic analysis<br><br>We cannot provide recommendations |

**TITLE: DS 508 at STEP 7 for submittal to NUSSC**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 62. | Annex I § I.-2 bullet 5 | | **All the relevant failure modes for the concerned equipment should be identified** (~~Design provisions and suitable operation practice are in place to minimize~~ ~~thermal~~ **ageing and environmental phenomena,** fatigue, stress corrosion, embrittlement, pressurized thermal shock, over-pressurization of the primary circuit, etc.) **and sufficiently high margins should be demonstrated.** | It is important to justify that all relevant failure modes are identified, not just the most “common” ones, without justifying the exhaustiveness. Minimizing the damage by design and operation may not be enough. Sufficient margins should be demonstrated. | | | | See 61 |

**DS 508 – Assessment of the Safety Approach for Design Extension Conditions and on Application of the Practical Elimination Concept in the design of Nuclear Power Plants**
**Step 7**

| COMMENTS BY REVIEWER<br>Reviewer: Page.... of....<br>Country/Organization: Belgium<br>Date: | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | | Introductory comment: In Step 5 we communicated some (to our opinion important) comments on the Step 5 draft. These comments where (informally?) answered by IAEA and thus we will not come back in detail to these comments. However, some of the comments below are still in line with (or related to) our comments on the draft of Step 5. | | y | | | |
| 2 | 3.4 | Also, the physical phenomena in case of DBA and DEC without significant fuel degradation ~~core~~ are similar, … | Typographical correction (delete "core") | Yes | | | |
| 3 | 3.21 | … Therefore, for the conditions described in para. ~~3.12~~ 3.17 (a) it may … | Typographical correction | Yes | | | |
| 4 | 3.31 till 3.65 | Move these articles on DiD to the beginning of Chapter 3, to be followed by the Articles 3.1 till 3.30 which focus more on DEC. | In the IAEA reply to our comment 5 on the draft of Step 5, IAEA says "There is no guide on application of DiD". A first reaction could be that it is then highly time that IAEA develops a guide on this topic (DiD being applied | | | | It is not very logical to start with the assessment and implementation of DiD and the independence between the levels of DiD to continue with the |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | for so many years!). A more pragmatic proposal is that this guide fulfills (as good as possible) this role. Therefore, we recommend that the wide scope considerations on DiD in Articles 3.31 until 3.65 are brought to the beginning of Chapter 3. In that way, the overall approach to DiD is then first explained and the more specific guidance on DEC (being a sub-item of DiD) follows thereafter. This seems to us a more logic sequence than the one now existing in the present Step 7 draft. | | | | implementation of DiD, in particularly the levels related to DEC.<br><br>The current structure follows the the agreement reached after the NUSSC WG in February |
| 5 | 3.43 and 3.44 | To be deleted? | This is still an example of Articles that do not belong to this SG, given the title of the Draft SG. These articles are purely related to DBA (and not DEC, nor PE). "Repeating" articles that belong to other SGs could lead to inconsistencies and different interpretations. | | | | These articles are not a repetition of other safety guides<br><br>During the WG of NUSSC a new title for the safety guide was proposed (very long one) focused on DEC and PE. Chapter 3 in relation to DiD was importantly reduced to be focused on these topics, but the |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | assessment of DiD cannot dissociate DEC from other plant states. |
| 6 | 5.7 | Some aspects of the use of non-permanent equipment and the associated safety assessment addressed in this Safety Guide cannot be fully considered in detail at the plant design stage and should be considered in more detail during the commissioning phase ~~plant operation~~. However, where applicable, specific facilities and equipment, should be considered at the final stage of the design of new nuclear power plants. The evaluation should consider the possibility that multiple units at the same site could be simultaneously affected. | Mobile equipment's and associated strategies could/should be foreseen as soon as possible – there is no need to wait to the operational phase. | yes | detail during the commissioning and operation phases ~~plant operation~~. …<br><br>Comment understood. The change reflects the point.<br><br>However, still aspects of training, drills, etc. mentioned in this section will indeed be considered in more detail during the operational phase | | |
| 7 | Chapter 5 | Many Articles (e.g. 5.1, 5.5, 5.8, 5.11) on external hazards to be deleted? | Many Articles in Chapter 5 are clearly focusing on external hazards, while Article 1.7 is explicitly saying that external hazards are not addressed in this SG. This is inconsistent. In reply to our comment 16 on Draft Step 5, IAEA answered "The plant design basis | | | | Article 1.7 indicates that external hazards, as well as environmental factors, human factors and other aspects are not addressed in relation to independence |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | against external hazards should be adequate.": we agree fully, but there are other SGs existing dealing with external hazards. | | | | between levels of DiD<br>The focus in on functional dependencies.<br><br>DS508 is not dealing with the design/protection against external hazards or the corresponding assessment, which is the matter of other safety guides.<br><br>It is dealing with the safety features in the design for very unlikely plant conditions exceeding the plant design basis, notably because of extreme external hazards, which was the reason to include such features after the Fukushima Daiichi accident. |
| 8 | Chapter 5 | We think that this Chapter 5 is not needed and could be integrated in Chapter 3. | In fact, "conditions exceeding the plant design basis" (see title of Chapter 5) are just was is envisaged with DEC. Therefore, the guidance | | | | Design extension conditions are within the design basis |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | on such conditions could be integrated within the guidance of Chapter 3 (partim on DEC). The aspect of “minimization of the radiological consequences” (see title of Chapter 5) could be a subchapter in Chapter 3. | | | | Safety Glossary (2018):<br><br>**design basis**<br>The range of conditions and *events* taken explicitly into account in the *design* of *structures, systems and components* and equipment of a *facility*, according to established criteria, such that the *facility* can withstand them without exceeding *authorized limits*. |
| 9 | Structure of the SG | Based on the above, we would propose:<br>Chapter 3:<br>• Starting with wide scope guidance on DiD (cf. 3.31 till 3.65)<br>• To be followed by specific guidance on DEC (cf. 3.1 till 3.30)<br>• With integration of relevant articles of Chapter 5<br>Chapter 4: PE<br>Chapter 5: no longer needed | For an improvement of the accessibility of the SG. | | | | As the current structure and contents of the chapters was agreed during the NUSSC WG meeting in February, this is a major change to be implemented without the agreement of other parties and not easy to implement in the short term with consideration of |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | comments by other countries |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# Summary Comments on Draft DS508, *Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants*, 2020-09-21

## Canadian Position

Canada considers that NUSSC should reject the present draft of DS508 as it violates key requirements of SSR-2/1.

## Requirements of SSR-2/1

SSR-2/1 Rev. 1 provides the following clear requirements concerning consequences of accidents relating to design extension conditions (DEC) and 'practical elimination'.

> *5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.*
>
> *5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.*

SSR-2/1 paragraph 2.13, footnote 3 explains the meaning of early and large releases. Footnote 3 is consistent with the definitions given in the *IAEA Safety Glossary (2018)*.

> *3 An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.*

To clarify the meaning, we can rewrite 5.31 replacing "early radioactive release" and "large radioactive release" with the equivalent text from footnote 3, giving:

> *5.31. The design shall be such that the possibility of conditions arising that could lead to ~~an early radioactive release~~ a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time, or ~~a large radioactive release~~ a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment is 'practically eliminated'.*

Comparing the rewritten 5.31 with 5.31A, it is clear that the maximum release permissible in DEC and the minimum release that must be 'practically eliminated' are at the same.

> *IAEA answer: This is not correct. 5.31A implies that the design for DEC shall be such that releases would be below the minimum release considered for "practical elimination" (with consideration of the time factor for "early"), not that they have to be set just below that value. The designer needs to demonstrate that in the most limiting scenarios considering applicable combinations of loads on the containment neither its structural integrity not it leak-tightness would be impaired in a way that the resulting release exceeds some acceptance criteria.*
>
> *If a criterion for practical elimination would be 200 T-becquerels of Cs, it is not acceptable a design that would consider a release of 199 T-becquerels, or anything closer, a "successful mitigation".*
>
> *First margins are needed anyway,* [ SSR 2/1 - 5.73. *The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular*

*that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases*.]. *Second, the ALARA criterion also applies, (req. 5 and 55).*

*If such permissive acceptance criteria are used for the successful mitigation of DEC with core melting, i.e. just below limits for "practical elimination", then failures in the mitigation (taking into account the performance of the safety features for DEC ) would necessarily imply releases well above the limits for practical elimination. This means, that the cases for practical elimination (which require a special solid demonstration) would extend from the categories indicated in section 4 of DS508 to the failed mitigation of every DEC sequence. Furthermore, the additional implementation of accident management measures such as the use of non-permanent equipment would play no role for the prevention of early or large radioactive releases.*

*In addition, no difference is made between the two categories of DEC. It is clear that the criteria could not be the same for both categories. It makes no sense that the criterion for DEC without core melting could be just below the criterion for practical elimination.*

*Therefore, SSR 2/1 is not practical in relation to acceptance criteria for DEC, perhaps because of the difficulties in achieving consensus, but the interpretation in the comment is not correct. DS508 provides a meaningful recommendation.*

**Conclusion: SSR-2/1 Rev. 1 requires that consequences more severe than those permitted in DEC shall be practically eliminated.**

*This is <u>your own conclusion</u>, which would be only valid if the acceptance criterion for DEC in terms of radioactive releases is the same as the minimum release that must be practically eliminated. Accident sequences involving the failure of the mitigation of DEC with core melting (with consequences generally below the limits for practical elimination) should nevertheless be proven to be very unlikely*

The "qualitative step" described in DS508 para 4.7 (and equivalent text in para 2.8) between the maximum release permissible in DEC and the minimum release that must be practically eliminated are a violation of the requirements of SSR-2/1 Rev. 1. See **MAJOR COMMENTS** in table below.

## Major Comments on Draft DS508 Paragraphs 2.8 and 4.7

| Proposed DS508 Text | Canada Comment |
|---|---|
| 2.8 In accordance with Requirement 5 of SSR-2/2 (Rev. 1) [1], radioactive releases in accident conditions are required to be below acceptable limits and be as low as reasonably achievable. In addition, the purpose of the fourth level of defence in depth is that off-site contamination is avoided or minimized. To this aim, a limit for the release of radioactive materials or on acceptable limit on effective dose should be specified for each category of accident conditions, and compliance with these limits should be verified. For accidents without significant fuel degradation, the releases are required to be minimized such that off-site protective measures (e.g. sheltering, evacuation) are not necessary. For accident with core melting, the releases are required to be such that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'. **The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release.** In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis. | **MAJOR COMMENT**<br>**This is contrary to requirements of SSR-2/1 Rev. 1 and must be removed.** This text introduces a new category of accidents that exceed the worst permissible DEC release but are less than the proposed PE release limit.<br><br>SSR-2/1 Rev. 1 sets the same value for the maximum permissible release in DEC and the minimum release that must be 'practically eliminated.<br><br>**Answer**<br>Please see explanations provide before |
| 4.7 **When defining these radiological criteria or targets, it is necessary to acknowledge the significant difference in magnitude between the maximum radioactive release and radiological impact that can be generated in case of a successful mitigation of DEC with core melting, and the releases and impacts that are avoided as part of the application of the concept of practical elimination.** This also ensures sufficient margins to take into account the uncertainty in analysing complex severe accident phenomena and the performance of the containment. Indeed, radiological criteria for DEC with core melting are defined in order to ensure, with a safety margin, that the radioactive releases would have limited consequences in area and time for people and the environment; therefore, **there is a qualitative step between the maximum acceptable releases for DEC with core melting (i.e. in case of successful mitigation) and the magnitude of releases to be considered for the application of the concept of practical elimination.** From the probabilistic point of view, event sequences that have been practically eliminated should only represent a very low contribution to the frequency of an early radioactive release or a large radioactive release, when the demonstration can be sustained by probabilistic analysis. | **MAJOR COMMENT**<br>**This is contrary to requirements of SSR-2/1 Rev. 1 and must be removed.** Same comment as for Paragraph 2.8.<br><br>**Answer**<br>Please see explanations provide before |

**ENISS comments on**
**IAEA draft DS508 *Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants* (18 September 2020) – Step 7**

| COMMENTS BY REVIEWER<br>Reviewer: ENISS Page 1 of 32<br>Country/Organization: ENISS Date: 30 October 2020 | | | | RESOLUTION -<br>ENISS | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| General comment | | | | | | | |
| 1 | Overall | Align the vocabulary to IAEA safety glossary and SSR-2/1. | SSR-2/1 is using the wording of the IAEA safety Glossary. To progress towards next steps, the future SSG is expected to be aligned to the IAEA safety glossary wording. | | This is the intention Misalignments are exceptions. We will try to fix it, unless there are some deficiencies in the Glossary | | |
| 2 | Overall | There is a need for more consistency in the wording across the document. | We appreciate to see several contributions from different sources gathered in a unique document, showing the implication of different IAEA Member States. However, please ensure to use the same wording for the same meaning all along the document.<br>Examples:<br>DEC wsfd and DEC wcm.<br>DEC wsfd: use DEC without significant fuel degradation but not ~~DEC without core melt~~<br>"Severe accident" may be used but the link to "DEC with core melting" should be explained somewhere (are they the same or the expression of a different meaning?).<br>"fuel degradation" may be preferred to "core melt/damage", when the spent | | Again this was the intention in relation to DEC<br><br>All DEC wcm are severe accident, the reverse is not true | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | fuel is considered, but ensure this is always the case.<br>"fuel degradation" should be preferred to "fuel damage"/ | | | | |
| 3 | Overall | No Change.<br>Just a thank you for the clarification of the structure and objective of the document, aligned to the main changes of SSR-2/1 | Revision 1 of SSR-2/1 incorporates modification relating to the main following areas:<br>• Prevention of severe accidents by strengthening the design basis for the plant;<br>• Prevention of unacceptable radiological consequences of a severe accident for the public and the environment;<br>• Mitigation of the consequences of a severe accident to avoid or to minimize radioactive contamination off the site. | | | | |
| 4 | Overall | DS508 seems to take as a reference some development issued from TECDOC-1791 "*Considerations on the Application of the IAEA Safety Requirements for the Design of NPPs*" (published in 2016, in parallel of SSR-2/1 revision).<br>SSR-2/1 should be preferred and at least should be referred first. For example, different approaches for the implementation of DEC within DiD should not be as detailed as provided in section 3 (see also below comment on 3.4 and Table1). | TECDOC-1791 is not a document consensually validated by all Member States. | | TECDOC-1791 is not a reference used in DS508.<br>Text of TECDOC-1791has been used in SSG-2<br><br>We may use parts of TECDOC-1791 as a starting point.<br><br>If agreed with the necessary changes, then it will be consensus | | |
| 5 | 1.1 | Over the latest decades, IAEA safety standards for nuclear power plant design have been enhanced several times with the aim of providing confidence that the successive generations of nuclear power plants are designed | One of the fundamental principles of ensuring safety is the optimization of protection in which social and economic factors must also be taken into account | | I see your point as representatives of the industry. I don't | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | so as to operate efficiently at the highest levels of safety that can be reasonably achieved considering the economic and social factors, the state of the art practices and techniques in science and technology and taking into account the feedback gained from the nuclear events and operational experience | (see Principle 5 and paragraph 3.23 of SF-1)<br><br>This should be reflected from the beginning. | | know if this is imbedded in be reasonably achieved<br><br>The technical editor has already anticipated that this and other paragraphs will have to be deleted. Not standard I didn't do it for now to avoid discussions on terms agreed by the WG of NUSSC | | |
| 6 | 1.3 | IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment of Facilities and Activities, also revised ~~after the Fukushima Dai-Ici accident~~ in 2016[…] | For consistency with §1.2 on SSR-2/1 Revision 1 (Fukushima Dai-ichi accident is not referenced in § 1.2 for SSR-2/1). | OK | | | |
| 7 | 1.3 | Requirements for safety assessment of the design ~~in this publication are not sufficiently detailed for nuclear power plants. However~~ are completing specific requirements for safety assessment and safety analysis of nuclear power plants ~~are~~ established in SSR-2/1 (Rev. 1) [1]~~, and these~~. All those requirements need to be considered to address specific aspects of relevance for nuclear power plant design. | A safety guide may not be the right place to discuss the relevance/level of details of IAEA requirements.<br><br>It's difficult to understand why GSR part 4 is introduced, because the conclusion is only on req. from SSR-2/1. Consider removal of GSR part 4 for simplification or consider the suggestion to link GSR part 4 and SSR-2/1. | | It is actually the other way round<br><br>SSR 2/1 is most useful in terms of the requirements for safety assessment/analysis<br><br>To be considered together with other comments by other NUSSC members | | |
| 8 | 1.4 | The objective of this Safety Guide is to provide recommendations to new NPPs on the implementation […] | This new SG should not apply directly to existing reactors. | Y | | | |
| 9 | 1.7 | Add this at the beginning of 1.7:<br>In addition to AOO and DBA, DEC without significant fuel degradation and DEC with core melting are part of the implementation | An introduction with an extended perspective on DEC without significant fuel degradation and DEC with core melting is missing. | y | Preliminarily included | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | of the concept of Defence in Depth. In terms of deterministic safety analyses methods, rules and assumptions to be followed, the IAEA safety guide SSG2 is already providing relevant guidance. However there is a need to develop guidance about the integration of DEC within the overall implementation of Defence in Depth, as well as guidance on the identification of DEC conditions to be studied. | | | Guidance on conditions to be included exist also in SSG-2, SSG-53 (not consistent) and partially in others<br><br>Let's see what will be done, because it is repetitive of 1.11<br><br>This entails renumbering of references. Not done now | | |
| 10 | 1.7 | 1.7 A key ~~issue~~ requirement is the independence between levels of defence in depth and in particular in relation to safety features for DEC (especially features for mitigating the consequences of accidents involving the melting of fuel). | "Requirement" in reference to req 7 of SSR-2/1 seems more appropriate. | Y | Implemented but I believe too strong at this point | | |
| 11 | 1.7 | 1.7 A key requirement ~~issue~~ is the independence, as far as is practicable, between levels of defence in depth and in particular in relation to safety features for DEC (especially features for mitigating the consequences of accidents involving the melting of fuel). | Intensive discussions took place to add "as far as practicable" in relation to SSR-2/1 requirement 7 of DiD levels independence.<br>Without this part of the text, SSR-2/1 requirement is not properly reflected.<br>Consider revision as suggested. | Y | Same<br>Implemented but I believe too strong at this point | | |
| 12 | 1.13 | This safety guide comprises five sections and ~~two~~ one annex~~es~~. …. | This text was agreed by the NUSSC Working Group based on a suggestion by Greg Rzentkowski, who said that the question of application to existing reactor would be discussed as part of the IAEA guide on Periodic Safety Review. | | | | We had a discussion about this being an appendix or an annex and we agreed on an Annex<br>The proposal came from Austria<br>I remember a discussion about being able to have it in time for the NUSSC meeting.<br>I remember that at least Germany wanted to have it . |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | The annex has been developed. If NUSSC agrees it would be deleted. I cannot accept your comment |
| 13 | 1.14 | Annex I provides information on the demonstration of a commonly recognized set of events or plant conditions that need to be demonstrated to have been practically eliminated. ~~Annex II provides some considerations for the application of this Safety Guide to nuclear power plants designed to earlier standards.~~ | Idem as 1.13 | | | | See previous comment |
| 14 | 2.6 | Further requirements in relation to acceptable limits for categories of plant states and more specifically for accident conditions are also specified by SSR-2/1 (Rev. 1) [1], | Missing preposition | yes | | | |
| 15 | 2.6 | Further requirements in relation to acceptable limits for categories of plant states and more specifically for accident conditions are also specified by SSR-2/1 (Rev. 1) [1], namely:<br>**— “Plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated1 and plant event sequences with a significant frequency of occurrence must have no or only minor potential radiological consequences (para. 2.11 of SSR-2/1 (Rev. 1) [1]).**<br>— “Criteria […]<br>— “… | Reference to para. 2.11 of SSR-2/1 (Concept of Safety in Design) is missing.<br>Paras 2.3, 2.4 and 2.5 are quotation from SSR 2/1 (Req. 5 – Radiation Protection in Design) and define safety approach from the radiation perspective. However, the basis of safety in design is also in para 2.11 of SSR 2/1. | | | | I agree, and this is a summary, but in section 2.1 of SSR 2/1 there are no requirements. The message is repetitive of the paragraphs of the requirements already included |
| 16 | 2.7 | 1.4bis ~~2.7~~ This Safety Guide is focused on the protection of the public and the environment in accident conditions, which should be assessed by verifying compliance with a number of requirements in SSR-2/1 (Rev. 1) [1] pertaining to the general plant design, as | This paragraph should be part of the scope (section 1).<br><br>Make it consistent with agreed scope of section 1 and move it there (after 1.4) or consider deletion. | | It can be mentioned there but I think it is pertinent to keep this message here | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | those indicated above, as well as other requirements for plant specific systems, for instance those related to the containment structure and its systems. | | | | | |
| 17 | 2.7 | As indicated in par 2.10~~1~~ of SSR 2/1, Rev.1 [1], "Measures are required to be taken to ensure | Incorrect paragraph number used. | yes | | | |
| 18 | 2.8 – 7th sentence | ~~The amount of radioactive releases considered acceptable for DEC with core melting should be significantly lower than the amount characterizing a large release.~~ | Proposal to move this to 4.7 for consistency (see comment 4) | | | | I don't see the relation to comment 4<br><br>And section 4 is about P.E, not DEC. This message is here connected to the rest of the paragraph and there is no obvious reason for moving it |
| 19 | 2.8 | In accordance with Requirement 5 of SSR-2/1~~2~~ (Rev. 1) [1], radioactive releases | Typo wrong document number. . | Y | | | |
| 20 | 2.8 | To this aim, a limit for the release of radioactive materials or on acceptable limit on effective dose should be specified for each category of accident conditions (see acceptance criteria as defined in SSG 2 § 2.5a, 4.3-4.6 4.10/4.11), and compliance with these limits should be verified. | There is an obvious link to SSG 2. This should be mentioned here to avoid inconsistency between guides. | Y | (acceptance criteria for deterministic safety analysis is addressed in section 4 of SSG-2[8]) | | |
| 21 | 2.8 | For accidents without significant fuel degradation~~, the releases are required to be minimized such that off-site protective measures (e.g. sheltering, evacuation) are not necessary.~~ and for accident with core melting, the releases are required to be such that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. | The proposed text is requiring for DEC without significant fuel degradation more than SSR-2/1 5.31A:<br>"*The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures*".<br><br>This is aligned with the European WENRA objective O2, but an IAEA | | I think you mean<br><br>SSG-7.46.<br><br>IAEA is not defining requirements her but providing recommendations<br><br>I am against of reproducing a text that allows consequences for DEC-A to be the same then for DEC- | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | guide should not defined new, nor amend existing requirements.<br>The text should be revised as proposed.<br><br>Removal of the entire paragraph may also be considered as this is duplication from 2.6 quoting SSR-2/1 5.31A<br>Another proposal may be to refer to SSG2 7.45.<br><br>An alternative proposal is to move the text to section 3.4 and to make it as an example of an alternative applied by some MS as part of the discussion on differences between MS on DiD levels. When the. level 3a and 3b (DEC without significant fuel) scheme is followed, such as in Europe, the objective O2 may be followed. | | B. This is totally illogical<br><br>If countries cannot accept the WENRA criterion<br><br>*SSG-2 -7.46*<br>*The same or similar technical and radiological criteria as those for design basis accidents may be considered for these conditions to the extent practicable. Radioactive releases should be minimized as far as reasonably achievable.*<br><br>Should be the text to be included. I am including it | | |
| 22 | 2.9 | ~~For normal operation or anticipated operational occurrences, there is limited uncertainty on plant state frequency and radiological impact, which can be monitored and is supported by many years of operating experience of previous plant designs. For less frequent plant states, i.e. accidents, there are larger uncertainties associated with the demonstration of plant state frequency and radiological consequences.~~ | This may be misunderstood as "the demonstration of accident management is uncertain".<br><br>Better to delete this text that may create confusion. | | | | We have to clarify it<br><br>But it is correct<br><br>But since we are referring to probabilities and uncertainties in the document it should be clear that<br>We can be quite confident about the frequency and the consequences of PIEs that have happened many |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | times in the nuclear industry like the loos of condenser vacuum and much less about the frequency and consequences of LOCAs that have never occurred.<br><br>Nothing to do with accident management, where of course uncertainties exist |
| 23 | 2.10 | ~~Harmful radiological consequences to the public can only arise from the occurrence of accidents. Therefore, the f.~~ Following chapters… | This statement may not always be correct. . The radiological consequences to the public can occur for example by a human malevolent attitude (Safety glossary refers to accident as unintended event), or as a consequence of a natural hazard event.. | | | | In NPP design, it is clear what is “accident” and “accident conditions” . We examined SSR 2/1 and other requirements after 2011.<br>A malevolent event or an external hazard need to cause an accident to cause harmful consequences to the public.<br><br>A malevolent event could cause an accident not considered in the design. DBA and DEC are accident conditions (considered in the design)<br><br>This just to indicate why the guide is not focused on NO and AOOs. |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 24 | 2.11 | Recommendations on radiation protection in design of nuclear power plants are provided in IAEA Safety Standards Series No. NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants [12], and ………… | Only a reminder that the document NS-G-1.13 is currently also under revision and in the final version of DS508 the marking will need to be changed | | Of course. | | |
| 25 | 3.1 to 3.12 | Consider simplification of this part. See some suggestions below. | 3.1/3.12 seems to have the intent to provide an introduction to DEC.<br>There are 3.5 pages for 3.1 to 3.12. Then for the DEC section, there are 3 pages for 3.13 to 3.31.<br><br>A better balance is expected. See comments and proposal to extend the guide on DEC without significant fuel degradation. | | The 1st part is about the overall implementation of DiD, that is relevant to introduce DEC and later on the assessment of DiD/Independence and P.E.<br><br>It is not about the number of paragraphs. Many pages have been deleted from former versions.<br><br>We cannot add more without understanding what is wanted. There are many comments about topics being covered already by SSG-2. I am receiving comments to eliminate for instance probabilistic considerations. | | |
| 26 | 3.1 | ~~For other sources of radiation or potential releases of radioactive materials, the implementation of a defence in depth strategy will depend on the amount and isotopic composition of radionuclides, on the effectiveness~~ | This quotation from SSR-2/1 para 2.14 does not seem necessary.<br><br>Make a clear quote to SSR-2/1 or consider deletion. | | | | Why is it not necessary? |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | ~~and leak tightness of the individual confinement barriers as well as the potential challenges for the integrity of the barriers and the consequences of their failures.~~ | | | | | |
| 27 | 3.2 | ~~An overall strategy of defence in depth, when properly implemented, achieves the objective that no single technical, human or organizational failure will lead to harm to the public, and that credible combinations of events and failures will lead to no or little harm to the public.~~ | This statement may not always be correct. Credible combinations of events were the sources of accidents such as TMI, Tchernobyl, Fukushima Daichi and a long list of other events, where DiD is implemented.<br>It's not only a DiD strategy that is needed, other considerations such as siting and hazard consideration, such as safety management, respectful trained and sufficiently qualified staff….<br>The whole is required to achieve the ambitious objective, not just the DiD strategy.<br>Consider deletion of this statement that may be misleading. | | | | Examples of some of these accidents showed precisely that DiD was not correctly implemented<br><br>Check SF-1 3.31 |
| 28 | 3.3 | For the implementation of safety provisions at each level of defence in depth the following is of ~~there are three aspects of~~ importance, as follows: (a) The performance of the safety provisions implemented at a level to achieve ~~meet~~ the safety objectives assigned to this level, including successful mitigation of the PIEs part of this level ~~acceptance criteria for the integrity of the barrier(s) that should be protected~~; (b) An appropriate resilience to common cause failures to ensure that a single event can't lead to harmful consequences on people and the environment ~~The reliability of safety provisions to ensure that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level, with a sufficient level of confidence;~~ (c) Adequate (i.e. to avoid a common cause failure) independence between ~~from the~~ safety provisions | As presented, the three points may be seen as the only key point of a satisfactory DiD implementation, what is not sufficient.<br><br>Item a is focused on "barriers" that are not really defined and is narrowing the importance of a DiD level.<br>Item c should incorporate independence "as far as is practicable" in an effort to be consistent with SSR-2/1.<br><br>Consider revision. | | | | This was discussed during the WG of NUSSC.<br>The proposal is changing totally the meaning |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | from ~~implemented at the previous and~~ successive levels of defence in depth | | | | | |
| 29 | 3.4 | An association of the levels of defence in depth with plant states considered in the design is frequently undertaken for design safety and operational safety. The introduction of design extension conditions in the plant design basis has resulted in ~~two~~ a number of different interpretations by Member States regarding the correspondence between plant states considered in the design and levels of defence in depth. | The analysis of the TECDOC 1791 reported here is not shared by all MS.<br>The UK SAPs have a slightly different interpretation.<br>The Finnish Regulation has 3 levels of DECs.<br>Japan may not be fully aligned to either of those…<br>China may consider both possibilities.<br>Consider proposed clarification. | | | | Indicate with is your specific comment<br><br>IAEA has agreed on DEC without significant fuel degradation and DEC with core melting<br><br>What is the 3rd level of DEC in Finland?<br><br>Also within DBA a country can have subdivisions.<br><br>Which one is the country that it doesn't associate DEC (an accident condition) with a level of DiD different from 3 or 4?<br><br>No comment from any of the countries mentioned received in this regard |
| 30 | 3.4 (Table 1) | Consider deletion of Table 1 and associated text on the 2 different approaches from 3.4.<br><br>~~These two approaches are represented in Table 1. Approach 1 (i.e. the association of DEC~~ | Table 1 is not sufficiently shared among Member States, as there is other interpretations. This should not be part of the main text. | | | | A TECDOC is not a document of consensus.<br><br>The safety guide if approved it will be |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | ~~without core melt to level 3) has the advantage that […]~~<br>~~Also, the physical phenomena in case of DBA and DEC without significant fuel degradation core are similar, […] for safety assessment to be applied for DEC and the rules to be applied to DBA.~~<br><br>An alternative to deletion may be to move the table and text to an Annex, as an illustrative example. In that case as per comment above on 2.8, the discussion about the possible evolution of SSR-2/1 5.31A may be added. | Table 1 should be handled carefully and cannot be regarded as an IAEA consensus for the moment since TECDOC-1791 is not issued from a consensus by Member States. Introducing it in this new SG formalizes this "new" approach, even though there are still strong arguments for saying that DEC fall into both level 3 and 4 just as their frequencies overlap as indicated in Table 2 of the TECDOC. | | | | The levels of DiD are not strictly differentiated by frequency<br>It is clear that in particular DBA and DEC w.s.f.d may overlap<br><br>If you cannot agree on something like this which allows for both possibilities of interpretation, it is pointless to attempt to achieve consensus on further |
| 31 | 3.5 | Normal operation comprises a series of plant operating modes […] ~~in which no failures have taken place, and no equipment is unavailable that would prevent the intended accomplishment of the goals of the operational mode~~. | The relation to a requirement from SSR-2/1 or GSR part 4 or in relation to nuclear safety is not clear.<br>Unless not accepted by the regulation, it's possible for a licensee to operate a plant at reduced power, while some failures are under repair or some equipment under maintenance (one feedwater pump on four), especially if these are not safety related equipment. These unavailabilities may prevent the plant to reach full power, but do not require a shutdown.<br>Even failures or unavailability of some safety systems are accepted as part of the technical specifications to define what is acceptable or not in terms of nuclear safety. The goal should not only be to avoid preventing normal operation, but to avoid preventing the accomplishment of a safety function. | | | | Does every sentence in the guide to explain the link to a requirement in SSR 2/1 N and if so be a copy of the requirement?<br><br>Staring-up, hot and cold shutdown, refuelling, etc are modes of operation. It is clear that equipment may be unavailable, as indicated in Tec Specs or OLCs.<br><br>If you cannot accomplish a safety function you cannot be in normal operation |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 32 | 3.5 | ~~Normal operation comprises a series of plant operating modes […]. Their impact on the plant is the main basis for establishing the safety provisions that are necessary at each plant state., For these reasons~~ Rather than discussing different possible interpretations, this Safety Guide addresses the design safety provisions necessary for each plant state, rather than for each level ~~Level~~ of defence. In this way, the significance and importance of design extension conditions for the safety approach is emphasized. | The only purpose of this development is the conclusion: "For these reasons, this Safety Guide addresses the design safety provisions necessary for each plant state, rather than for each level Level of defence".<br><br>Consider suggestion to simplify the guide and go straight to the conclusive point. | | | | If you find statement on which agreement cannot be reached or recommendations that are not achievable or detrimental for safety, they will be taken into account. Otherwise, as the majority of the NUSSC members dons t have problems with the text, it will not be changed |
| 33 | 3.6 | the integrity of <u>the first barrier</u> | What is the rationale of focusing on the first barrier?<br>Why referring to req 4.13 and not req. 4.12?<br>Barriers are discussed in SSR-2/1 as part of req. 4.12, but there is no assignment of one barrier to a specific DiD level. | | Refrence to 4.12 will be included?<br><br>Nobody assigns barriers to a level of DiDs . For DEC w..c.m the only barrier available is the containment ?<br><br>Do you wasn't to dispute that measures in operational states? are <u>not focused</u> first in protecting the fuel and when applicable the RCPB?<br><br>design provisions for operational states should have adequate capabilities to maintain the integrity of the first barrier for the | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | confinement of radioactive materials ( i.e. the fuel cladding) and to prevent a significant release of primary coolant and an evolution to design basis accident conditions, | | |
| 34 | 3.6 | to prevent a significant release of primary coolant | A "significant release of primary coolant" through the malfunction of an effluent systems" is indeed an issue, but probably less significant than a loss of cooling of the reactor.<br><br>What is meant : "significant release" or "loss of cooling capability"?<br>Please consider clarification. | | It is a release that would make a transition into an accident condition, e.g. a PORV open or a loss that cannot be compensated by the CVCS<br><br>Text will be made more clear | | |
| 35 | 3.6 | Therefore, design provisions for operational states should have adequate capabilities to maintain the integrity of the first barrier for the confinement of radioactive materials ( i.e. the fuel cladding) and to prevent a significant release of primary coolant and an evolution to design basis accident conditions, for which the actuation of the ~~engineered safety features~~ ~~(~~safety systems~~)~~ is foreseen. | Safety systems are defined in the IAEA glossary as "*Safety systems consist of the protection system, the safety actuation systems and the safety system support features.*"<br><br>They are not "engineered safety features"<br><br>Consider alignment with the safety Glossary. | | | | Also according to the safety glossary safety systems don't cover everything needed for level 3, for instance the containment functions<br>engineered safety features is used<br>in 2.13 of SSR 2/1<br>and is the chapter 6 |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | of the SAR, see approved DS449, SSG-61 |
| 36 | 3.6 | Therefore, design provisions for operational states should have adequate capabilities to maintain the integrity of the first barrier for the confinement of radioactive materials (i.e. the fuel cladding) and to prevent a significant release of primary coolant and an evolution to design basis accident conditions, for which the actuation of the ~~engineered safety features~~ ~~(~~safety systems~~)~~ is foreseen.<br><br>Consider the following for the first DiD level:<br>The prevention of accident escalation in the first level of DiD is associated to:<br>• Quality, robust design of component to prevent leaks, failures<br>• In-operation surveillance to prevent occurrence of failures,<br>• Provision to maintain plant operation despite single failures (switch to redundant equipment)<br>• Alarms for the operator to control a deviation,<br>• Automatic correction of plant parameters to avoid triggering a reactor trip,<br>• … | The link between the loss of the first barrier and "preventing and escalation to an accident condition" (SSR-2/1 4.13) is not obvious.<br><br>All of these should also maintain the first barrier integrity, but rather indirectly.<br><br>Consider clarification on this basis or deletion. | | | | Explanations on level 1 and 2 have been requested to be reduced to the minimum<br>This sort of information existing before has been removed. |
| 37 | 3.7 | the reliability of safety provisions for anticipated operational occurrences | What is the meaning of "safety provisions for AOO" ? Do you mean safety system ?<br>IAEA Glossary : "*safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents.*" | | | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 38 | 3.7 | Consistent with the highest frequency of postulated initiating events for design basis accidents (usually lower than 10 -2 per reactor-year), the reliability of safety provisions for anticipated operational occurrences should be such that the frequency of transition into an <u>accident condition</u> is <u>significantly lower</u> than this value. | Significantly lower than 10-2 is very vague: 10-3, 10-4 ?<br>Do you mean "transition into a design basis accident"?<br><br>The proposed text could be interpreted as an AOO provision to face a 10-1/year event can fail with a conditional probability of 10-1 or 10-2. This may mean an escalation to an accident condition such as a severe accident with a frequency of occurrence of 10-2 or 10-3.<br><br>The point should not be on the frequency only, but also on the capability to manage the new situation. A sufficient independence should ensure either that an AOO is managed so that failures of safety systems would only lead to an event in the frequency range of DEC or that an AOO deriving in a DBA would be managed by safety systems not affected by the situation. | y | Yes the transition is to a DBA<br><br>I can agree on all this<br>I think we try to say the same. Any reasonable technical system doesn't fail with a probability higher than 0.01, of course not affected by the PIE.<br>If the PIE frequency would be 0.1/y the transition into a DBA would have a frequency of 0.001/y<br>The systems for AOOs are not making only sufficiently reliable for a transition into DBA with frequency of 0.01/y<br><br>Other thing is that systems for AOOs may not be credited in the DSA, but the safety systems<br><br>The capability is another subject. It should be sufficient to fulfil with margins the safety functions. If the capability is insufficient without the system failing, there is no discussion.<br><br>This is a way to show the probabilistic implications but the dependencies between system (although minimized) need to be taken into account. | | |
| 39 | 3.7 | Consistent with the highest frequency of postulated initiating events for design basis accidents (usually lower than 10 -2 per reactor-year), the reliability of safety provisions for anticipated operational occurrences should be such that the frequency of transition into an accident condition is <u>significantly lower</u> than this value. | Are we just talking about the conditional probability of the "safety provisions" or about the frequency of occurrence of a sequence "AOO + failure of safety provision"?<br>In the latter case we are talking about a multiple failure event that should be considered as part of DEC without significant fuel degradation and this is out of scope in relation to Did level 1 and 2. | | | | I disagree<br><br>Not every multiple failure is DEC<br><br>For instance a reactor trip followed by the failure of the AFW (redundant system requiring thus multiple failures) results in the intervention of the EFW (safety system)<br>This is not a DEC condition |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | Only if there is a dependency between the system for AOO and the system for DBA can such a failure lead to DEC,e.g. ATWS |
| 40 | 3.11 | ~~The operation of~~ Safety systems designed to control DBAs should be passive or rely on automatic actuation for actions requiring a quick response, where a human intervention would not be effective or may present a high risk of failure. Practically, ~~and should not involve~~ human intervention should not be required for a (justified) sufficiently long period of time. ~~and their~~ The reliability of automatic actions should be very high (i.e. performed by the protection system). | Passive safety systems are also an option to consider, and they are even preferred over active systems.<br>As per SSR-2/1 4.11d, 5.59, 5.58, 5.75f, 6.33b ("[…] *operator action is not necessary within a justified period of time*"), the need for an automatic action rather than an operator action should be based on the possibility to demonstrate the success of the action, rather that defining "a sufficiently long period of time".<br><br>Consider clarification on the meaning of "a sufficiently long period of time" and alignment to SSR-2/1. | | | | The guide cannot advocate of a given reactor concept. Safety systems are active in many designs<br><br>It is not only that the automatic actions should be highly reliable. Also the the system itself once actuated<br><br>Actuation of safety systems according to 4.11d and other paragraphs should be initiated automatically |
| 41 | 3.11 | The function performed by redundant (i.e. resilient to the single failure criterion) safety systems should be such that the DBA safety objective is achieved, including the limitation of releases as far as is practicable, as per requirement 5 quoted above. | DSA studies for DBA should achieve the safety objective they are assigned too (limit the radiological consequence…), not just try to achieve a PSA objective. Then PSA should complement this with the support of best-estimate PSA support studies. | Y | OK<br>This would go at the end of .310, is it not what is there?<br>What is the guidance provided? | | |
| 42 | 3.11 | In addition, in the PSA, the reliability of the safety systems should be such that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the PSA ~~DBA~~ | To make a link with previous suggested text. Note that the PSA safety objective may vary from one MS to another and it would be difficult to reach any consensus on a value. | | | | ~~DBA~~ is not in the original text. I don't want to confuse reliability analysis of the safety systems with |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | safety goals of the plant ~~(for new nuclear power plants typically below 10-5 per reactor-year).~~ | | | | | the PSA, that people understand as an integrated study for calculating CDF. The techniques, e.g. fault tress are similar. |
| 43 | 3.11 | ~~If this is not the case,~~ As a complement to that, DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate, see below ~~to achieve such goals~~. | As written, the last sentence may be understood as "if the DBA safety systems achieve the 10-5 safety goal, there is no need to postulate DEC without significant fuel degradation". This is not consistent with SSR-2/1 req. 20. Consider revision. Suggestion for a minimal modification. | Y | "Could" has been changed to "should" Other comments received This corrects the confusion and it is correct | | |
| 44 | 3.12 | If the design of the containment is […] is necessary to ensure the integrity of the containment boundary, the failure of such systems would have the potential to jeopardize the capability to limit radiological consequences from DBA and also subsequent DEC accidents. Therefore, they should be designed, constructed and maintained to achieve both the DBA and DEC objective of limiting radiological consequences and avoid large or early releases ~~ensure a very high reliability, since their failure would not only lead to a severe accident but also jeopardize the subsequent measures for its mitigation~~. | The proposed sentence is a bit general and not going straight to the point. Consider clarification.<br><br>Suggestion proposed as a possible clarification. | Y | I can go along with the changes At the beginning but not t the second part.<br><br>The objectives of DBA (systems for DBA) is not to avoid large or early releases. | | |
| 45 | 3.12 | For the same reason, containment isolation provisions in case of DBAs should ~~also~~ be designed accordingly ~~to have very high reliability~~ for ensuring that acceptable limits for radiological consequences are not exceeded ~~and sufficient coolant inventory can be maintained~~. | The proposed sentence is a bit general and mixing confinement and cooling fundamental safety functions, while cooling is not the main focus. Consider clarification. Suggestion proposed as a possible clarification. | Y | As in comment 45, stressing that a very high level of reliability should not be removed | | |
| 46 | 3.15 | To meet the requirements described in paras 3.13 and 3.14, as per 3.38 of SSG-2 "*two separate categories of design extension conditions should be identified: design extension* | There is obviously a quotation, this should be clarified. | | | | I don't need to use SSG-2 to indicate that there are two categories of DEC. It is in SSR 2/1 |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | *conditions without significant fuel [degradation] and design extension conditions [with] core melting* (severe accident)". | | | | | More importantly, severe accident: safety glossary:<br>***severe accident.*** *Accident* more severe than a *design basis accident* and involving significant core degradation.<br>Is not the same as DEC with core melting<br><br>Not all severe accident are DEC with core melting |
| 47 | 3.16 | Design extension conditions without significant fuel degradation should be considered for unlikely yet credible single or multiple failures with the potential for exceeding the capabilities of safety systems designed for the mitigation of DBAs. AOOs and the most frequent DBAs combined with a common cause failure on redundant equipment from a safety system are expected to provide most of such credible conditions. | From the introduction, the relationship between DEC without significant fuel degradation and common cause failure should be clarified. | Y | I can agree with this | | |
| 48 | 3.16 | The following should be added to 3.16 or to an additional para:<br>A clear process for the comprehensive identification of the design extension conditions without significant fuel degradation to be studied (and for which additional safety features may be defined), should be developed considering the following paragraphs. | The introduction to DEC without significant fuel degradation should mention the need for a clear approach that could be assessed as part of the DiD implementation assessment. | Y | I can agree with this | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 49 | 3.17c | A postulated initiating event associated with the complete loss ~~failure~~ of a safety system (i.e. the intended safety function cannot be performed) used for normal operation, e.g. a support system, and is required for the control of the initiating event. | The text is simplified in comparison to SSG2 3.40, making it unclear (partial loss or total loss ?). SSG2 3.40b states : "*AOOs or frequent DBAs combined with multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function*" SSG2 3.40c: "*Credible postulated initiating events involving multiple failures causing the loss of a safety system*" | | | | SGG-2 is unclear Failure of the system is failure I don't speak about partial or total loss<br><br>No need to talk about partial loss or total loss. |
| 50 | 3.18 | ~~In general,~~ The mitigation of a DEC without significant fuel degradation should rely on ~~be accomplished by~~ specific safety features designed for this such conditions and ~~. Alternatively, they can be mitigated~~ by all the available safety systems that have not been affected by ~~the events that led to~~ this DEC condition under consideration. | The historical practise (and current practise) on DEC without significant fuel degradation is more to add some specific safety features to take over from affected SSCs and complement non-affected SSCs, rather that defining a complete set of safety features for a DiD level. For example, there is no intent to double the containment or to add a dedicated emergency feedwater system to be able to always consider the failure of the main emergency feedwater system. | Y | Fine, but not ~~ALL THE~~ available safety systems | | |
| 51 | 3.19 | the primary difference between these two accidental conditions is the use of different ~~or~~ criteria for design or safety assessment to achieve this objective | | yess | | | |
| 52 | 3.19 | Add a sentence:<br>Further details are provided in SSG-2 7.47, 7.48, 7.49. | Consider additional quotation to SSG2 7.47, 7.48 and 7.49 to support the text dealing with the same theme. | Y | This made already in the next paragraph | | |
| 53 | 3.19 | ~~Since~~ The radiological objective in DBA and in DEC without significant fuel degradation is the same, namely to prevent core damage or damage to the fuel in the irradiated fuel storage. ~~,~~ ~~t~~The primary difference between these two accidental conditions is the application of a graded approach, which may lead to the use of different ~~or~~ criteria for design or | Editorial changes and suggestion to improve the clarity and to link to the use of a graded approach. | | Changes considering comments by other countries.<br><br>O necessary to use graded approach. This is confusing and not used in SSR 2/1 or in SSG-2 | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | safety assessment to achieve this objective. …. | | | May not correct<br>If there is no difference in the approach, there is no need to differentiate DEC from DBA | | |
| 54 | 3.19 (a) | Less stringent design requirements than for DBA can be applied, for example compliance with the single failure criterion is not required, equipment can have a lower safety class and less rigorous reliability measures are allowed; | The word "rigorous" (i.e. strict, precise, hard,) seems to be in contrast with the word "allowed" and with the statement "Less stringent design requirements than for DBA can be applied (for DEC)". | yes | | | |
| 55 | 3.20 | In such cases, the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result (in particular regarding the prevention of cliff edge effects) that cannot be simply achieved by best-estimate calculations. As per SSG-2 table 1 on the possible approaches for DSA, the combined approach or the best-estimate approach with quantification of uncertainties (best-estimate plus uncertainty) should be considered. | This is a reference to SSG-2 7.54 and 7.55.<br>This should be expanded accordingly for clarification.<br><br>See suggestion or other proposal based on SSG2. | | | | It is not the purpose here to elaborate more on DSA, referring to SSG-2 is sufficient.<br>On the same token we could elaborate on the safety class for DEC and other topics |
| 56 | 3.20 | ~~If the rules were the same, there would not be a need for differentiation between DBA and DEC~~ | This may be true, but this is too simplistic. Consider deletion or develop from quotation from SGG2 providing arguments for a difference in the approaches. | | | | This is exactly the point, if everything is the same there is no need for introducing DEC at all. |
| 57 | 3.22 | Design extension conditions without significant fuel degradation should be considered for failures of safety systems designed both to cope with anticipated operational occurrences and DBAs. These include in many designs the anticipated transients without scram and station blackout. | SBO and LUHS event should not be part of severe accident, hence the text should be limited to DEC without significant fuel degradation. | Y | It is clear in this section<br>It will be included | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 58 | 3.22/3.23 | 3.22 Design extension conditions without significant fuel degradation should be considered for multiple failures (including common cause failures) of safety systems designed both to cope with anticipated operational occurrences and DBAs. These include in many designs the anticipated transients without scram and station blackout.<br>3.23 In the definition of enhancement for design extension conditions without significant fuel degradation preventing and reducing the potential for a ~~should also be considered to reduce the frequency of~~ severe accidents ~~caused by failures in the mitigation of some DBAs to acceptable levels by~~, where ~~if~~ possible, diversity should be added ~~the use of additional, diverse measures~~ to cope with a common cause failures on ~~of~~ safety systems. | Both paragraphs 3.22/3.23 are dealing with common cause failures, because AOO and DBA are mitigated by redundant safety systems. SBO and LUHS are due to CCFs on the redundant equipment.<br>Consider simplification/clarification of the text.<br><br>Diversity should be discussed as part of enhancements, this does not always mean “additional features”. A DBC redundant system with 2 pumps may be resilient to a common cause failure if the pumps are diversified, hence no need to consider a CCF as part of DEC without significant fuel degradation. | | It is not necessary. The failure of the safety system is sufficient. Since safety systems meet the SFC, multiple failures (most likely CCFs) are needed. It is not necessary to make things more complicated<br><br>There are other comment to this paragraph .<br>It should not be made more complicated | | |
| 59 | 3.24 | The reliability of safety systems should be high enough for DEC without significant fuel degradation to only be postulated exceptionally. ~~And to occur with a frequency lower than the most limiting DBAs~~ | China raised a point at the IAEA SSR-2/1 Workshop September 2019: The LUHS frequency, depending the site configuration may be in the region of DBC4 event. Do we need to consider LUHS as a DBC4?<br>The ASN guide 22 do not define a lower limit for DBC4 frequency.<br><br>The border line between DBA and DEC may vary from one MS to another and also from one design to another. Frequencies may be in a similar region.<br><br>The driver may be more that DEC is covering credible multiple failure events and DBA single initiating events. | | Is LUHS and AOO?<br><br>An AOO followed by failure of systems for AOOs end into DBA, not into DEC (unless there are dependencies that cannot be removed)<br><br>It is not acceptable to have a DBA and an unreliable safety system to end in DEC and then use a system for DEC of a lower | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | Consider deletion or revision of the text on the basis of this rationale. | | safety class, not redundant and not analysed conservatively<br><br>The result of a DBA combined with the failure of the safety system should not be more frequent that other events consider as DBA, but I need to understand better the point | | |
| 60 | 3.25/3.26 | 3.25 For new nuclear power plants, accidents involving core melting should be postulated as DEC, irrespective of the fact that the design provisions taken to prevent such conditions make the probability of core damage very low. In accordance with para. 5.30 of SSR-2/1 (Rev. 1) [1], a set of representative accidents […] on the SSCs that fulfil the confinement function.<br>3.26 The accident conditions chosen should be justified […] core damage. ~~For new nuclear power plants, accidents involving core melting are postulated as DEC, irrespective of the fact that the design provisions taken to prevent such conditions make the probability of core damage very low.~~ Aspects that affect the accident progression […] | Suggest highlighting the need to postulate a core melt, by starting the section with that point. See proposed suggestion of moving text. | | I can move the text but you have changed "are" by "should"<br><br>SR 2/1 doesn't say that. the has to be designed for every condition involving core damage | | |
| 61 | 3.28 | The challenges to plant safety presented by DEC with core melt (situations also called severe accidents), and the extent… | Introduction of the term 'severe accident' here can be used in the following (e.g. in §3.29) | | | | All DECw.c.m. are severe accidents. The reverse is not true. |
| 62 | 3.29 | Radioactive releases due to leakage from the containment in a severe accident should remain below the ~~design leakage rate~~ limit where protective actions are required in the | Comparing a rate with an absolute value (liter/mn against liter) does not seem appropriate.<br>Consider proposal to keep the idea. | | | | This is very permissive. It basically allowing to release just |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | short term to allow for sufficient time to allow implementation of emergency measures. | | | | | before the limit of an early release.<br><br>Therefore no margin<br><br>Any failure to mitigate DEC would fall into the category of practical elimination |
| 63 | 3.29 | The radioactive releases due to leakage from the containment is generally estimated by calculations considering a main assumption: the containment leakage rate. This assumption should be justified. | May be worth to complete the point about the leakage rate of the containment. | | | | This is not so easy. The topic is complicated and it is addressed in SSG-53 |
| 64 | 3.35/36 | Add a new paragraph after 3.35 explaining how graded approach is applied to the DiD concept.<br><br>3.36 Defence in depth should be implemented with appropriate account taken of the graded approach and the fact that many radioactive sources do not qualify for all levels of defence in depth. For consistent implementation, account needs to be taken of the risk represented by the amount and type of radioactive material present in the nuclear power plant, the potential for its dispersion due to the physical and chemical nature of these products; and the possibility of nuclear, chemical or thermal reactions that could occur under normal or abnormal conditions and the kinetics of such events. These characteristics influence the required number of levels and the strength of these levels, depending on the radioactive source. | In 3.35 it is expressed that the DiD strategy "…should be applied to all radioactive sources… taking into account a graded approach."<br><br>Paragraph 3.35 provides a comprehensive list of radioactive sources for which DiD should be considered. In principle, if interpreted correctly, DiD is applicable to everything that emits ionizing radiation, without distinction between the core, spent fuel, fresh fuel, waste treatment systems, etc.<br><br>It is mentioned that DiD should be applied "… taking into account a graded approach". Considering that the primary objective of the safety guide is to provide guidance on the implementation of DiD, it is suggested that a paragraph is added explaining how a graded approach is applied in practice to DiD.<br><br>Further guidance is desired in order to avoid extreme applications of the DiD concept. For example, as described in SSR 2/1, the implementation of DiD | Y | | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modi-fied as follows | Rejected | Reason for modifica-tion/rejection |
|---|---|---|---|---|---|---|---|
| | | | comprises 5 levels. However, it is unreasonable to apply 5 levels on all radioactive sources. DiD application must be adapted to each radioactive source and risk-balanced approach.<br><br>Further insight is provided in INSAG-10, Chapter 2 "The Approach to Defence in Depth". | | | | |
| 65 | 3.36 | Consider revision and alignment, at least a link to some of the requirements of GSR part 4. | It's difficult to make a link to GSR part 4 req. 4.46/4.47/4.48/4.48A that should give the red line to be followed here.<br><br>3.36 b/c may be applied to the fuel clad, RCPB, containment, but for airborne leakage barriers, is this really appropriate?. | | Yes because GSR Part4 has not been developed with an NPP in mind<br><br>I would rather think in the recommendations are reasonable<br><br>No clear What is meant by for airborne leakage barriers | | |
| 66 | 3.36 | (c) All loads [...]. For robustness, [...] avoid a cliff edge effect when loads considered for the design are <u>slightly</u> exceeded. | This precision is required to be consistent with the Safety Glossary definition of cliff-edge effect. | Yes | | | |
| 67 | 3.39 | The performance of safety provisions at each level of defence in depth is assessed through engineering assessment and deterministic analysis involving the use of validated and verified <u>computer</u> ~~analysis~~ codes and models to demonstrate that acceptance criteria are met with sufficient margins. <u>This is further developed within section 5 of SSG 2, as a guidance on requirement 18 of GSR part 4</u>. | This refers to GSR part 4 Requirement 18 and is already developed within SSG 2 section 5. | | | | |
| 68 | 3.42 | ~~It should be verified that diversity has been implemented in the design of systems fulfilling the same fundamental safety function in different plant states if a simultaneous fail-~~ | This looks like a new requirement in comparison to SSR-2/1 req 24 and GSR part-4 req 4.21.<br>Better to stick to those.<br><br>Diversity is a relative principle. | | This needs to be discussed. The requirement is not providing guidance of when these safety measures | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | ~~ure of those systems would result in unacceptable damage to the fuel or radiological consequences.~~ As per requirement 4.21 of GSR part 4: "*In the assessment of the safety functions […] It shall be determined in the assessment whether the structures, systems and components and the barriers that are provided to perform the safety functions have an adequate level of reliability, redundancy, diversity, separation, segregation, independence and equipment qualification, as appropriate, and whether potential vulnerabilities have been identified and eliminated.*" | System A can be diversified from system B. What do you mean by implementing diversity on systems A and B? The simultaneous failure of a DEC-A fuel cooling system and a DBC cooling system is expected to lead to a core damage that are unacceptable damages to the fuel. Diversity may reduce the frequency of the situation, but would not change anything to the unacceptability of the damages. | | need to be implemented.<br><br>I think this is a valid recommendation. Not a requirement<br><br>Core damage cannot be totally prevented. It is acceptable if the frequency is very low. | | |
| 69 | 3.43 | ~~Equipment for controlling anticipated operational occurrences is aimed at reducing the number of challenges to safety systems. It should be demonstrated that their reliability is such that anticipated operational occurrences only evolve into DBA conditions with a low frequency, well below the highest frequency of postulated initiating events categorized as DBAs~~. In the management of AOO, the safety systems required should be such designed that a sufficient number of equipment from the safety systems remain available if the situation is aggravating to a DBA. | There is no systematic linear evolution from NO to AOO then DBA then DEC without significant fuel degradation and then to DEC with core melting. A good example is a LOCA going straight from NO to DBA as highlighted in IAEA SRS n°46. As per the safety glossary, safety systems are used to manage AOO. AOO are therefore naturally "challenging some safety systems".<br><br>The highest frequency for DBA has been set in this guide at 10-2. Is 10-3 well below this ?<br>As explained above the point is not just about a frequency of an AOO deviating to a DBA but a frequency and the availability of provisions. A 10-4 manageable situation maybe acceptable, A 10-4 unmanageable may be a challenge.<br>Consider revision or deletion. | | | | It is not like this<br><br>If safety systems for DBA need to intervene in AOOS there is no independence between AOO and DBA. There are some exception, but not the rule.<br><br>This should be discussed the change is not acceptable |
| 70 | 3.44 | The ~~combined~~ overall reliability of the safety systems designed to mitigate | The term "combined reliability" is not very clear. | | | | Neither overall |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 71 | 3.44 | ~~[…] A failure probability below than 10-3 in order of magnitude. [..]~~<br><br>As an implementation of requirements 23 and 25 of SSR-2/1, the design of the safety systems to mitigate the consequences of a DBA should be commensurate to their safety significance. The single failure of a component should not compromise the ability to achieve the DBA safety objectives and this should be documented. | A conditional probability of failure of 10-3 for a DBA line of defence to face a 10-2 DBA event, means that a 10-5 core damage single event is acceptable. The combination of several of such events would mean a core damage frequency of some 10-5. This may prevent to achieve the PSA safety goals.<br><br>May be better to develop something around the implementation of SSR-2/1 req. 23 and 25 (SFC). | | | | I can agree with the text you proposed but we don't go further we are rephrasing the requirement for reliability and single failure criterion.<br><br>IN the example that you put you don't achieve the safety goals. Either the safety systems should be more reliable, what it has limitations, or that would be the case to considering designing for DEC w.s.f.d |
| 72 | 3.47 | ~~However, since the analysis of core melt and its impact on containment integrity is surrounded by considerable uncertainties, only a limited reliability can be attributed to those components necessary to ensure the containment integrity after a core melt accident~~.<br>As per requirement 5.29 of SSR-2/1, the DiD assessment of DEC with core melting should ensure that there is a demonstration showing that the safety features are capable of performing their safety function in the environmental conditions they are subjected to. | The containment is used for several DiD levels and this statement is creating confusion. High reliability and resilience is expected to ensure that for NO, AOO, DBA, DECs the containment is fulfilling the confinement safety function.<br><br>This is not aligned to SSR-2/1 5.29. Consider revision | | | | First thing, capable doesn't mean reliable, and it is so simple to say that SSCs for DEC w.c.m need to be qualified for the corresponding environmental conditions.<br><br>The purpose is to say that you cannot argue that the probability of the failure of the safety features for DEC w.c.m. is very low. |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 73 | 3.48 | The assessment should include an evaluation of the adequacy and effectiveness of the different accident management strategies defined to cope with severe accidents ~~extreme scenarios~~. This evaluation should demonstrate that […] | For clarification, it should be preferable to refer to SA or DEC with core melting.<br><br>Otherwise, there is a need for a definition of "extreme scenarios" | y | See next comment | | |
| 74 | 3.48 | This evaluation should demonstrate that the likelihood of an accident having unacceptable consequences for people and the environment, and which relies on ~~both fixed and non-~~ permanent equipment to mitigate the consequences of such an accident, is extremely low. As per SSG2 7.51, after a justified period of time, the demonstration may rely on the provision of non-permanent equipment. However the time claimed for the availability of non-permanent equipment should be justified. | This is not aligned with SSG2 7.51. | | | | If you fail to mitigate DEC w.c.m. you are still in a severe accident, but beyond the design basis, now you can take credit of using non permanent equipment and other accident management measures for the safety demonstration<br><br>This is not for the safety demonstration of the design<br><br>This is why I put extreme scenarios, it could be also originated by extreme external hazards. |
| 75 | 3.52 | For example, a failure, whether equipment failure or human error, at one level of defence or even combinations of failures at two levels of defence, should not ~~propagate to~~ jeopardise the overall implemented defence in depth ~~at the subsequent levels~~. Engineering assessment, deterministic and probabilistic methods should be used to assess potential dependencies to justify that independence is implemented as far as is reasonably practicable. | The point here is more to get an overall assessment. Propagation is not so key here. A failure or credible combination of may be enough to create damages and weaken DiD. | y | Resolved considering other comments<br><br>Combination of failures at two levels removed | | |
| 76 | 3.53 | It is recognized in the IAEA safety standards that full independence of the levels of defence | It would be useful to add some examples of items (SSC) important to safety | Y | There are several items that can be | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | in depth cannot be achieved. This is due to several factors and constraints, such as a potential common exposure to the effects of external hazards and/or internal hazards, an unavoidable sharing of some items important to safety (see examples in Footnote), as well as human factors. | that use to be shared between DiD levels according to best practice in real design of NPPs. A footnote would be enough. | | listed but I spent time elaborating on dependences to realize that some countries don't want it. I put the containment as a non disputable example . | | |
| 77 | 3.56 | The sharing of systems or parts of them for executing functions for different categories of plant states should be avoided as far as is practicable (e.g. AOO and DBA share some safety systems). However, since this might not be always practical or possible, it should be ensured that within the sequence of events that may follow a postulated initiating event, a system credited to respond in a given plant condition ~~should not have been needed for a preceding condition~~ should not have failed during a preceding condition. Thus, complementary safety features designed to mitigate the consequences of DEC without significant fuel degradation should be independent from SSCs postulated as already failed in the sequence. This is especially important when the safety systems are credited for the mitigation of DEC. | As the sentence just after is tempering this statement may be worth to temper it from the beginning to avoid being misled.<br><br>Demonstration of sufficiency of the independence of DiD levels is not that easy, because a number of systems and equipment intervene at different DiD levels, typically in levels 2 and 3 (e.g. for emergency feedwater system, diesels …)<br>A feasible approach consists in recognizing a high safety level for the plant thanks to equipment reliability et diversification which guarantee accomplishment of fundamental safety functions, whatever the situation. Certain systems and equipment may pertain to many DiD levels. See the example expanded below. | | | | Changes are illogical. As far as practicable is always possible<br><br>It if has not failed in a preceeding condition it would not be needed now (we will have not progressed for instance to DEC)<br><br>It has not been demanded before is OK |
| 78 | 3.57 | ~~The SSCs needed for each postulated initiating event should be identified, and it should be shown by means of engineering analyses that the SSCs needed for implementing any one defence in depth level are sufficiently independent from the other levels.~~ The adequacy of the achieved independence should also be reflected in the development of the probabilistic analyses (identification of relevant common cause failure and consideration of appropriate provisions to limit their consequences) and ultimately confirmed ~~assessed~~ | This is duplicating 3.53 and 3.56 and too strict as written.<br><br>The meaning is unclear, as said above, there is no systematic linear evolution from NO to AOO, DBA, DEC…for any single event.<br><br>May be worth to extend the role of the PSA. | | I can add about the PSA but I don't see why to delete the sentence<br><br>I don't need a PSA to postulate CCFs , this is not a probabilistic part (it is the assignment of probabilities) | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | by the results of the probabilistic safety analyses. | | | | | |
| 79 | 3.58 | As per SSR-2/1 req 21 and 24, the redundant or diversified ~~systems and~~ components used for different plant states should be appropriately separated~~, within the same safety division,~~ from one another by distance or protective structures whenever a failure or its consequences may impair the implementation of the defence in depth concept (i.e. if there is a possibility for a credible common cause failure to fail several DiD levels ~~consequential failures arising from a failure of a system or component for another plant state.~~) | SSR-2/1 requ. 21 for separation and independence apply at element/component level. There is no need to separate the injection system and the feedwater system, but to separate equipment from redundancy A from equipment from redundancy B. Consider revision and alignment to SSR-2/1. | | | | First the equipment may be separated for other layout reasons, but if the feedwater system is for AOO it needs to be separated from the injection system for DBA I need careful analysis to consider tour comment |
| 80 | 3.60 | The systems intended for ~~controlling~~ mitigating severe accidents… | For clarification | yes | | | |
| 81 | 3.61 | For instrumentation […]. This can be achieved […] redundant functions and by design for ~~reliably~~ reliability. […] | Editorial | y | | | |
| 82 | 3.63 | the operability of the safety systems is not jeopardized by failures in systems designed for normal operation ~~or anticipated operational occurrences~~. | A failure in the reactor trip used for AOO has surely an impact on the same required reactor trip for DBA. AOO share safety systems with DBA. | Y | Agree, but these are exemptions. I need to improve the text | | |
| 83 | 3.65 | Following an internal or external event, an assessment of sufficient independence should demonstrate that despite any consequential failures (including potential common cause failures) the remaining ~~of~~ SSCs are sufficient ~~that are necessary~~ to mitigate the consequences and ensure that radiological consequences are kept below acceptable limits. ~~of a single or a likely combination of external hazards on the plant should be conducted. It should be demonstrated that the postulated initiating event and the failures induced in the plant cannot result in common cause failure between the SSCs necessary for their mitigation.~~ | It's difficult to understand the meaning. For example, it's snowing, a building is necessary to protect a DEC equipment from this snow. What should be independent from what? What sort of events should be considered ? Consider revision as suggested. | Y | I can leave with your text But nowhere I am speaking about independence I will consider it together with other comments | | |
| 84 | 4.3 | However, these provisions may have limited capabilities that could not reasonably cope | As per the IAEA safety glossary "practically eliminated" may be confusing | | | | I don't understand the point |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | with some specific severe accident conditions; those are the conditions that should be explicitly identified and demonstrated as physically impossible or extremely unlikely to occur ~~practically eliminated~~. | wording. So better to use clarified wording. | | | | This term is used in SSR 2/1 |
| 85 | 4.5 | when the containment is open and cannot be closed in time, or where ~~there~~ is a ~~an~~ containment bypass that cannot be isolated | | y | Editorial | | |
| 86 | 4.5 | In such cases, it may be necessary to demonstrate the situation as physically impossible or extremely unlikely to occur ~~practical elimination by showing~~ with a high degree ~~of confidence that such severe accidents would be extremely unlikely.~~ | As per the IAEA safety glossary "practically eliminated" may be confusing wording. So better to use clarified wording. | Y | Actually what is confusing is the glossary | | |
| 87 | 4.6 | […]<br>Therefore, acceptable limits for ~~radiation protection~~ radiological consequences should be established for the purpose of AAO, DBA, DEC and practical elimination demonstration, consistent with the regulatory requirements. In addition ~~, as well as~~ probabilistic criteria or target values for the purpose of demonstrating the low frequency of a core damage accident or accident sequences leading to radioactive releases, should be established, consistent with the regulatory requirements. | There is an unclear mix between DSA and PSA targets. | | | | What is the unclear mix?<br><br>Is in addition different from as well<br><br>There are other comments to this paragraph to consider<br><br>To talk here about other plant states is |
| 88 | 4.7 - 1st and 2nd sentences | When defining these radiological criteria or targets, it is necessary to acknowledge the significant difference in magnitude between the maximum radioactive release and radiological impact that are calculated as ~~can~~ being generated in case of a successful mitigation of DEC with core melting, and the releases and impacts that are avoided as part of the application of the concept of practical elimination. | Calculation are only (penalised) estimated value, not the real ones. | yes | | | |
| 89 | 4.9 | The concept of practical elimination' is used to confirm that all reasonably practicable design provisions have been implemented, | Just to be more general and to refer explicitly to SSR-2/1 wording. | y | | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 90 | 4.11 | The issue when trying to demonstrate that a sequence leading to an early radioactive release or a large radioactive release is physically impossible or extremely unlikely to occur ~~considering whether to practically eliminate a severe accident sequence~~ is the potential for a confinement function failure. | As per the IAEA safety glossary "practically eliminated" may be confusing wording. So better to use clarified wording. | | | | We cannot make things so complicated<br><br>The glossary is not clear to me and what is acceptable in SSR 2/1 should be in the guides<br><br>We define the meaning in the guide as in SSR 2/1, and from now on, what it means is that |
| 91 | 4.12 | To ~~help~~ ensure this demonstration ~~the assessment of practical elimination~~ is manageable, the whole set of individual accident sequences that might lead to an unacceptable radioactive release could be grouped […] | As per the IAEA safety glossary "practically eliminated" may be confusing wording. So better to use clarified wording. | Y | demonstration | | |
| 92 | 4.13 | In such cases, ~~for scenarios not retained within the scope of practical elimination,~~ evidence of the effectiveness and an appropriate reliability of the mitigation is necessary. To facilitate the grouping proposed, each type of accident | Suggest to simplify this long sentence | | | | It is better to keep it |
| 93 | 4.13 | This analysis helps identifying accident sequences leading to an early radioactive release or a large radioactive release ~~that could lead to conditions that need to be 'practically eliminated'~~. | Suggest to stick to SSR-2/1 vocabulary | y | Changed<br><br>Is it not the same? | | |
| 94 | 4.17 | Group the text with 4.13 as part of "Other classification or grouping criteria are also possible." | This may be misleading to have 2 ways to categorise the sequences in the same doc.<br>This second type of classification can be introduced as the one from WENRA as an alternative to the detailed one from SSG2. | | | | These are not 2 ways. They look at different aspects.<br><br>Why is it misleading? |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | It was included following your comment, now I have been requested to remove it |
| 95 | 4.18 | The overall objective is to assess if the design is appropriate for preventing the accident sequences identified and grouped in a short list of accident scenarios that may lead to an early radioactive release or a large radioactive release ~~for practical elimination.~~ | Better to highlight the potential consequences.<br>As per the IAEA safety glossary "practically eliminated" may be confusing wording. So better to use clarified wording. | | | | We are here in this guide to address this concept and clarify it as necessary not to make things more complicated that they are. |
| 96 | 4.35 | ~~An example could be the effect of heterogeneous boron dilution for which the main protection is provided by ensuring a negative reactivity coefficient for all possible combinations of the reactor power and coolant pressure and temperature. In this case, physical impossibility applies only to a prompt reactivity insertion accident.~~ | It's a good point to try to provide example. But this one may present some limitations.<br>Better to remove to avoid confusion. Alternatively, another example may be provided. | | I can remove it<br>We only apply it to one part<br><br>What would be the example that you propose? | | |
| 97 | 4.39 | where such a ~~as~~ target has been established by the regulatory body | | y | | | |
| 98 | 5 | MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF ~~VERY UNLIKELY~~ CONDITIONS EXCEEDING THE PLANT DESIGN BASIS<br><br>Alternatively; to stick to the scope defined as part of § 1.8, the title could simply be:<br>Reinforcement of safety functions by including features enabling the use of non-permanent equipment, in the event of natural external hazards exceeding those considered for the design basis.<br><br>Or if too long: | The title is referring to something not defined and deriving from the scope defined in 1.8.<br>What is the definition of "very unlikely" in that case?<br><br>Define "very unlikely" or consider suggested revision to stick to SSR-2/1 requirements. | Y | It can be changed if others agree<br><br>Are we going to dispute that exceeding the design basis is not very unlikely? | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | Reinforcement of safety functions by including features enabling the use of non-permanent equipment | | | | | |
| 99 | 5.1 | As per requirements 17 and 5.15A to 5.21A "all foreseeable internal and external hazards[…] shall be identified and their effects shall be evaluated". As per 5.17 "The design shall include due consideration of those natural and human induced external events that have been identified in the site evaluation process". SSR-1 is defining the requirements for such a site evaluation. As per requirement 14 of SSR-2/1, the design basis for~~of~~ items important to safety for a given ~~at~~ nuclear power plant "*shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.*" ~~s is established taking into account the most limiting conditions under which they need to operate or maintain their integrity~~. | The design basis shall consider internal and external hazards as part of SSR-2/1 requirement 17. The design basis for item important to safety is part of Requirement 14 of SSR-2/1.<br><br>Consider alignment to SSR-2/1 especially req. 14 and 17.<br><br>This is key here, indeed, before discussing the "beyond", a sound design basis should be sought. The measures for the beyond should not be there to compensate for a poor design. Note that in addition to a sound design basis, the periodical safety review of this design basis is key. Where needed the implementation of improvements to address natural hazards more severe than those considered for the plant design (climate change…) with sufficient margin to avoid cliff-edge effects. | | | | Is it wrong what it is said? Is it detrimental for safety?<br><br>When the Diesel Generator or the HPSI pump is designed are not the most limiting conditions considered from the set of scenarios in which they have to intervene?<br><br>What is the value of quoting only requirements? |
| 100 | 5.1 | In addition, the revision 1 of SSR-2/1 introduced the need to consider level of external hazard exceeding those considered for this design basis with the objective of evaluating the margins that exist in the design as well as the identification of potential cliff edge effects. | It is important to understand where is the limit to be reasonably considered for the residual risks where exceeding margins is acceptable.<br><br>This section 5 is clearly discussing the lessons learnt from the Fukushima Daichi reflected in SSR-2/1 Rev. 1.<br><br>Consider an introduction based on rev1 of SSR-2/1 (proposal on the basis of § 1.4 of DS498). | | | | This was primarily the reason.<br><br>This is why it said that it is particularly important and we explain it<br><br>Now, are you saying however that when the mitigation of DEC fails, e.g. the alternate power source fails, non permanent |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | sources should not be considered because they are only for extreme external hazards? |
| 101 | 5.1 | ~~This is particularly important for the case of natural hazards, for which the occurrence of hazards of a magnitude that exceeds the safety margin of the most vulnerable SSC important to safety is generally a matter of probability. There have been cases in which some external natural hazards, such as extreme earthquakes, floods and tsunamis have exceeded the levels considered for the design as a result from the site evaluation.~~ Paragraphs 5.21 and 5.21.A of SSR-2/1 (Rev. 1) [1] require sufficient margins in the design against external hazards for such cases ~~in the design~~. | This is already discussed in the DPP and rationale for the SSR-2/1 rev.1 update.<br><br>OPEX is interesting for the lessons learnt for the future from their analysis. Lessons learnt are introduced in previous comments making this part irrelevant. Consider deletion. | | | | Idem |
| 102 | 5.3 - Last sentence | Non-permanent equipment should not be credited in the short term after an accident in demonstrating the adequacy of the nuclear power plant design (see para. 7.51 of SSG-2 (Rev. 1) [8]) for AOOs, DBAs, DECs. If non-permanent equipment are credited in the long term, the feasibility of transport to their final position and connecting operations should be demonstrated. | To be consistent with SSG 2 as per previous comment above. | | | | This is a mésinterprétation of SSG-2<br><br>Nothing about short term and even less for AOOS, DBA<br><br>*7.51*<br>*Non-permanent equipment should not be considered in demonstrating the adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long term* |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | | | | | | *sequences and is assumed to be available ...* |
| 103 | 5.4 | In order to approach the implementation of design features for using non-permanent equipment, levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site should be considered and their consequences evaluated ~~as part of the defence in depth approach.~~ | If this was part of the defence in depth approach, this should have been reflected in section 3 as part of the assessment od DiD implementation.<br><br>As this is not the case, consider revision. | | | | Every measure, design or operational is part of the DiD<br><br>Also level 5 id DiD<br><br>It is clear what belongs to this section |
| 104 | 5.5 | ~~Particularly for external hazards, it is expected that the frequency of occurrence of a natural hazard significantly exceeding a well-established design basis derived in the operating from the site evaluation is very low. However, as such frequencies are generally associated with significant uncertainties,~~ It is ~~very~~ important to understand the behaviour of SSCs under ~~to~~ loading assumptions ~~parameters~~ resulting from levels of external hazards beyond ~~above~~ the design basis. The available margins are expected to be sufficient to avoid a cliff edge effect (defined in the safety glossary as "*An instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value.*"). | The point is about margin and cliff edge effects.<br>The text is very complicated to understand.<br>The frequency is probably not the point here but the cliff edge effect.<br><br>DS498 is using the vocabulary "beyond the design basis". It's better to be consistent with this guide to be soon released. | | | | This has been discussed with the EESS section<br><br>It seems that you have a comment for every paragraph and sentence<br><br>I cannot be debating everything<br><br>What is wrong it the text proposed to be deleted? |
| 105 | 5.5 | Footnote nb 9<br>~~The concept of practical elimination is applied to external hazards within the safety analysis due to the difficulties in providing a safety demonstration based on design features comparable to the full set of cases addressed in Section 4, and it is necessary to ensure in other terms that the risk of early radioactive releases or large radioactive releases as a result from extreme external hazards is very low.~~ In accordance with SSR-2/1 5.21A, | This is difficult to understand the meaning of this footnote.<br>There is no such requirement to apply PE to external hazards within SSR-2/1 and there is nothing about that in section 4 of DS508.<br><br>Consider revision consistent with previous comments, as suggested. | | "is NOT applied"<br><br>Word missing. This has been a text agreed with other countries | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | the provisions (safety systems, safety features, additional safety features) used for the demonstration of practical elimination should be such that there is no cliff edge in the demonstration when the level of external natural hazards is reaching the level defined in 5.4. | | | | | |
| 106 | 5.6 | General comment - Overall text to be modified, see detailed comments below. | What do you mean by limitations? Capability of the plant? Are we talking about the plant design?<br>The design process for a new NPP should avoid "limitations". Therefore it's surprising to write the text only in this direction. If the available margins are sufficient, the design should be seen as acceptable. If not and limitations are revealed, a strategy has to be developed. | | | | It is fully detailed in the items a,b,c,d following the paragraph<br><br>Can you deliver and operate equipment stored outside in the middle of a typhon if you have 1 hour to do it? This is a limitation |
| 107 | 5.6 | For each selected hazard event (hazards and levels to be defined according to 5.4), the consequential scenario should be studied. The evaluation should demonstrate that available margins are sufficient or identify potential limitations on the plant response capability. ~~and should define~~ A strategy to cope with these limitations should be defined.<br>[…]<br>, that will be used to restore the fundamental safety functions […]. | SSR-2/1 is intended for new reactors considering SSR-2/1 from the beginning and this should be reflected in the guide. | | | | It is clear that the guide is for new plants<br><br>You have so many questions about the same paragraph, that it is impossible to address them. These will require the agreement of others that have provided their comments and don't have fundamental problems |
| 108 | 5.6 a | A robustness analysis of a relevant set of items important to safety to<br>1. estimate the extent to which those items would be able to withstand the hazard event, bring the plant to a safe state and limit the radiological consequences,<br>2. identify potential limitations. ~~natural hazards exceeding their design basis~~; | Consistency with 5.6 and addition of a clear objective: reach a safe state. | | | | See. Comment 107 |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| 109 | 5.6 b | Where limitations have been identified, an assessment of the extent to which the nuclear power plant would be able to withstand a loss of the safety functions only with ~~out reaching unacceptable radiological consequences for the public and the environment~~ protective actions that are limited in terms of lengths of time and areas of application to protect the public. Sufficient time shall be available to take such measures. | There won't necessary be a loss of safety function, unless the plant is showing limitations. The radiological objective is a bit vague. The DEC objective should be considered here. | | | | See 107 |
| 110 | 5.6 c | Where limitations are leading to unacceptable radiological consequences, ~~A~~ definition of the coping strategies to limit and mitigate the consequences of the scenarios leading to a loss of ~~key~~ the fundamental safety functions. This coping strategy may rely on non-permanent equipment. | There is no need for coping strategies if the plant margin are sufficient to withstand the 5.4 hazard events. There is a need to introduce non-permanent equipment, the purpose of section 5, somewhere in this long development (see comment 5.x). | | | | See 107 |
| 110 | 5.6 d | An estimate of the necessary resources in terms of human resources, equipment, logistics and communication to confirm the feasibility of the coping strategies. | Consistency with previous text. | y | | | |
| 112 | 5.x | Whatever the results of the evaluation required by 5.6, as per the SSR-2/1 requirements recalled in 5.2, provisions should be added to the plant design to allow for the use of non-permanent equipment. They should be designed, at least to handover from some permanent equipment in the long-term development of an event. The expectations and design requirements would be at a higher level if they are part of coping strategies where limitations have been identified. | We propose to add a para to follow-up para 5.2/5.3/5.4: we need provision implemented to meet the requirements identified in para 5.2 (6.45A/6.28B/6.68). | | | | This has no relation with 5.6 or 5.2 of SSR 2/1 (6.45A/6.28B/6.68).dont talk about external hazards Recommendations for design are in the corresponding safety guides<br><br>The recommendations are also very unclear |
| 113 | 5.7 | ~~Some aspects of the use of non-permanent equipment and the associated safety assessment addressed in this Safety Guide cannot~~ | The proposed text may be understood as a possibility to postpone some of the aspects. | Y | Changes in red accepted | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
|---|---|---|---|---|---|---|---|
| | | ~~be fully considered in detail at the plant design stage and should be considered in more detail during the plant operation. However, Where applicable~~ To allow the use of non-permanent equipment, this including operating personnel protection, specific facilities and equipment, should be considered at ~~the final stage of the~~ design stage for ~~of~~ new nuclear power plants. These should be designed according to the coping strategies against a hazard event as defined in 5.4. The evaluation should consider the possibility that multiple units at the same site could be simultaneously affected. | This is a key lessons learnt part of SSR-2/1 for new reactors: do not wait the plant operation, but at design stage, think about the use of non-permanent equipment.<br><br>Consider clarification as per the suggestion. | | Not the deletion of the text. It has been the result of other comments before that some aspects of the use may be not fully clear and this point and there is no reason for this not to be true.<br><br>At the tie the plant begins operation everything needed to obtain the corresponding license will be finalized | | |
| 114 | 5.9 | The coping strategies should be defined, and the associated coping provisions should be specified and designed taking into account the most unfavourable possible scenario defined according to 5.4. | It's key to define the "scenario". | y | | | |
| 115 | 5.11 | The use of non-permanent equipment should only be credited when ~~provided that~~ the time period needed for their installation, connection and start of ~~putting~~ in service is less than the defined coping time with an additional ~~specified~~ margin for time sensitive operator actions. | Consider clarification. | y | editorial | | |
| 116 | 5.14 | To ensure the success and reliability of the strategies, the performances of the necessary coping provisions should be specified. ~~, and~~ The required equipment part of these provisions should be designed and, when relevant, qualified in accordance with appropriate standards ~~to~~ ensuring operability ~~its functionality~~ when required either during or/and after conditions caused by a hazard event such as defined in 5.4 ~~an extreme external hazard or other extreme conditions taken into consideration.~~ | The unique sentence is a bit long to understand, see suggestion.<br><br>Extreme hazard and conditions are not defined. Suggest to refer to para 5.4 to make this clear. | y | Partially<br><br>Extreme earthquake is used precisely in the guide for seismic qualification<br><br>For meteorological hazards is even in the title of the safety guides | | |

| Comment No. | Para/Line No. | Proposed new text | Reason | Ac-cepted | Accepted, but modi-fied as follows | Rejected | Reason for modifica-tion/rejection |
|---|---|---|---|---|---|---|---|
| 117 | 5.16 | Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited in the evaluation required in 5.6 above, for demonstrating ~~of~~ the successful mitigation of an accident (reaching a safe state or a) to prevent unacceptable radiological consequences. | Consistent with 5.3, the use of non-permanent equipment is limited to natural external hazard events exceeding those considered in the design basis. | | | | the use of non-permanent equipment is not limited to natural external hazard events<br><br>This can be the reason for its installation but not a limit in its use |
| 118 | Annex I:<br>I-26 | This is necessary especially in some boiling water reactors where the size of the containment is small and pressure limitation may be needed both in the DBA as well as in DEC ~~with core melt~~. | Applies also for DEC without core melt | y | Changed to particularly with core melting.<br><br>The subject here is practical elimination | | |
| 119 | Annex I:<br>I-31 | In both ~~all of these~~ approaches, | Better wording. | y | | | |
| 120 | Annex II:<br>II-8. | …………Non-permanent equipment that would be necessary to minimize the consequences of events that cannot be mitigated by the installed plant capabilities needs to be stored, its operability verified and protected to ensure its timely availability when necessary, with account taken of possible restricted access due to external events (e.g. flooding, damaged roads). | Such non-permanent equipment must be ready for deployment and use when needed.<br>See also paragraph 5.12 which prescribes testing and drills | y | Added at the end | | |

**Example completing comment on 3.56:**

EFWS (Emergency Steam generators feedwater system) system may be used either to:

- remove residual heat from the fuel during normal operation under shutdown states (via Steam Generators) = Level 1
- after reactor shutdown = Level 2
- during an accident of main feedwater tube rupture (rupture de tuyauterie d'eau alimentaire) = Level 3

This can be justified because Level 3 is made of 2 types of situations:

- DBC: accidents corresponding to single failures as initiating events (e.g. primary breaks, like DBC categories 3 and 4). For such situations, we switch directly from DiD Level 1 to Level 3, and in this situation it is acceptable to use systems also required by DiD Level 2
- DEC: accidents corresponding to multiple failures (CCF or failure of a safety system required after a single initiator). These DEC conditions correspond, in general, to the degradation of a frequent situation from DiD level 2/3. Systems needed to manage the consequences (e.g. to prevent core melt) should be independent of those which failure caused the degraded situation. For example, if the loss of the main feedwater system (Level 2 situation, requiring ASG system) degrades after an additional failure of the EFWS system failure, the situation corresponds to DiD level 3. In this case, a diversified system is needed to remove residual heat (for example feed & bleed strategy).

This is complicating the subject by combining uses from different modes of operation (normal shutdown, level 1) and others . We should not compare levels of DiD corresponding to different operation modes

In fact the loss of feed water is an AOO. If the EFW is the system to respond to it (no auxiliary feedwater or start up shutdown system used for normal operation, is this ASG system?) , in that case the failure of the EFW evolves into an accident

I would understand that loss of FW + loss of ASG (system for AOO) + loss of EFW (safety system) >>> feed and bleed (DEC)

Otherwise loss of FW + loss of EFW (safety system) >>> feed and bleed (DBA)

It seems that perhaps in this design independence between level 2 and 3 (for power operation, not mixing operation modes) is not implemented and the failure of EFW after an AOO is considered DEC, not DBA. I could understand your concerns

**DS508, Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants (New Safety Guide) (Step 7)**

| COMMENTS BY REVIEWER<br>Reviewer:<br>Page 1 of 1<br>Country/Organization: Republic of Korea / Korea Institute of Nuclear Safety (KINS)<br>Date: 26/10/2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | Contents / Line 4 | SCOPE................2 | Editorial | y | It will be changed Automatically generated by MS Word<br><br>I don't know how to do it | | |
| 2 | 1.3 / Line 2 | ... after the Fukushima Daiichi ~~Dai-ichi~~ accident ... | Standardization | y | | | |
| 3 | 1.12 / Line 3 | … (for example as part of the periodic safety review ~~reassessment~~ of the plant). | Clarification (if it means PSR) | y | | | |
| 4 | 3.5 / Line 2 | … (such as the Limiting Conditions for Operation ~~Operating Limiting Conditions~~ or …) | Clarification | y | Changed to Operational Limits and Conditions in accordance with SSR 2/1 | | |
| 5 | 4.9 / Line 1 | 'Practical elimination' is … | Editorial | y | | | |
| 6 | 4.12 (a) (II) / Line 1 | (ii) ~~Fast~~ Rapid reactivity insertion accidents. | Clarification (Also in ANNEX I, II) | y | Other proposal by RF<br>Aligned with SSG-2 | | |

**TITLE**
**DS508 (version October, 2020)**

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Reviewer: G. Delfini/Rob Jansen<br>Page 1 of 1<br>Country/Organization: ANVS – The Netherlands<br>Date: 15th October 2020 | | | | | | | |
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | General | Thanks for addressing our previous comments.<br>This draft is (again) an improvement. | | N.A. | | | |
| 2 | 3.17 | (a) an initiating event….<br>(b) …<br>(c) a postulated initiating event… | Is the difference on purpose? | This difference is made in 3.40 of SSG-2 rev.1. I received a comment to a previous version for keeping the difference.<br><br>In my opinion PIEs and in line with the safety glossary are IEs that may have not occurred but have been considered in the plant design and it safety analysis. PIEs can be bounding can be bounding cases enveloping other such events.<br><br>DECs are accident conditions considered in the design. | | | |
| 3 | 3.19 | "… use of different ~~or~~ criteria for design…" | typo | Yes | | | |
| 4 | 3.21 | Reference to 3.12(a) is not correct | Possibly 3.17 (a) | Yes | | | |
| 5 | 4.38 | Computer codes and/or analytical calculations used for calculations to support ~~When~~ 'practical elimination' of an accident sequence ~~is supported by deterministic calculations, computer codes and/or analytical calculations~~ should be validated against the specific phenomena. They should reflect….<br><br>Consider moving par 4.38 under | Computer codes should always be validated, not only in case of deterministic calculations<br><br>The content of paragraph 4.38 is generally valid, and not only for "Extremely unlikely to arise with a | | Yes<br><br>Idea captured but text improved<br><br>This part of the paragraph moved as suggested | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | subchapter “General Aspects” | high level of confidence” demonstrations (present head of subchapter). | | | | |

**Sweden comments - DS508** ***Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants*** **– Step 7**

| COMMENTS BY REVIEWER<br>Reviewer: Aino Obenius Mowitz, Ninos Garis, Björn Engström, Christian Karlsson<br>Page.... of....<br>Country/Organization: Swedish Radiation Safety Authority; SWEDEN<br>Date: 30th october 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | Ch. 2 | - | We appreciate the content of Chapter 2, and view it as important for reconnecting radiation protection and nuclear reactor safety. | N/A | | | |
| 2 | 3.2 | The concept of defence in depth for the design <u>of</u> nuclear power plants… | Typo ("of" missing). | yes | | | |
| 3 | 3.4 | Also, the physical phenomena in case of DBA and DEC without significant fuel degradation ~~core~~ are similar, although there are differences in the analysis. | Typo. | yes | | | |
| 4 | 3.11/3.44/ 3.57 | 3.11 (…) ~~The reliability of safety systems should be such that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the safety goals of the plant (for new nuclear power plants typically below $10^{-5}$ per reactor-year).~~<br>**Alt. GENERAL GUIDANCE**<br>The reliability of ~~safety systems~~ SSC:s should be such that (to the extent possible) the ~~collective contribution to the~~ core damage frequency ~~of failing to mitigate DBAs~~ does not exceed the safety goals of | The descriptions of how reliability levels should be defined and assessed (in terms of PSA) is not always consistent with PSA methodology.<br><br>Eg. The safety systems are not the only SSC:s which contribute to a sufficiently low CDF.<br><br>Paragraph 3.11 is difficult to understand, especially in relation to 3.44 that also states reliability | | There are many ways to achieve probabilistic safety goals, but the contribution of the different plant systems should be balanced. This is the key here<br><br>Probabilistic analysis is not only the full PSA in the traditional form of starting from an IE and get the minimal cut sets.<br><br>This masks a lot of things and doesn't address reliability of different levels of DiD .<br><br>It is possible to analyse the reliability of individual systems or safety functions probabilistically.<br><br>Simplified exaggerated example: A generic IE | | |

| | | | | | |
|---|---|---|---|---|---|
| | | the plant (for new nuclear power plants typically below $10^{-5}$ per reactor-year).<br><br>3.44 (…) A failure probability below than $10^{-3}$ in order of magnitude would be consistent with the strict requirements for reliability imposed to safety systems and supported by operational experience and testing.<br><br>3.57 (…) ~~The adequacy of the achieved independence should also be assessed by probabilistic analyses.~~ | requirements for the safety systems. Is *safety systems* the relevant term? Alt. could the guidance be stated on a more general level?<br><br>The event trees in the PSA starts with an initiating event (IE) followed by event sequences related to functioning or failed systems. A CDF below 10E-5 is a typical safety goal for <u>all</u> IE, <u>all</u> operating modes.<br><br>In 3.44, what is the relation to the failure probability stated in 3.11? The corresponding reliability can differ greatly, for initiating events this may give very strict reliability requirements, and for other initiating events very “flexible” reliability requirements. Could the paragraph be concept of a balanced risk profile?<br><br>Para. 3.57 implies that PSA should be used to assess independence between DiD levels. Different plant states, and SSC:s needed for implementing any one defence in depth level (3.57), are difficult to isolate in the PSA event tree, since the PSA event tree is related to IE and | | leading to a reactor scram (AOO) followed by un unreliable AFW cooling system for AOO however compensated by a feed and Bleed (accident condition) and a very reliable emergency core cooling system leading to a low CDF contribution would not be acceptable. No core damage is OK in the PSA, but a contaminated containment as a result of the bleed function and the associated impact is not. The frequency of accidents needs to be kept sufficiently low too.<br><br>0.1/y x 0.1 x 0.0001 = 1.e-06 /y contribution to CDF with 0.1/y x 0.1 = 1.e-02 /y frequency of a DBA successfully mitigated<br><br>Versus<br><br>0.1/y x 0.01 x 0.001 = 1.e-06 /y contribution to CDF with 0.1/y x 0.01 = 1.e-03 /y frequency of a DBA successfully mitigated<br><br>It is not the same<br><br>We are not recommending to develop a full scope PSA and then try to get the insights from the results.<br><br>It is possible to use probabilistic analysis (don’t call it PSA if this confuses you ) to estimate how reliable is for instance residual heat removal function (or systems) for AOO and how reliable is the residual heat removal for DBA, and if in the combined failure of both functions there are functional dependencies or CCFs of relevance.<br>If you have the fault trees of a PSA, it should not be so difficult to gain such insights<br>We are not recommending a fully detail analysis, but |

| | | | | | |
|---|---|---|---|---|---|
| | | | sequence of events, rather than specific plant states. We suggest to remove the sentence here. There are other paragraphs that give guidance to use probabilistic assessment to identify dependences which are OK. | | something providing reasonable assurances that the safety functions are reliable. |
| 5. | 3.21 | Therefore, for the conditions described in para. ~~3.12~~ 3.17 (a) it may… | Typo, wrong reference? | yes | |
| 6. | 4.12 | … (a) Events that could lead to prompt reactor core damage and consequent early containment failure, such as:<br><br>(i) Failure of a large pressure-retaining component in the reactor coolant system;<br><br>(ii) Fast reactivity insertion accidents;<br><br>(iii) Sequence of events (AOO, DBA or DEC) including loss of reactor core shutdown capability. | Loss of shutdown capability could lead to early core melt and subsequent early containment failure if not managed properly.<br><br>This is not ATWS and includes event sequences worse than HPME, at least in BWR.<br><br>Examples:<br>Station Blackout (loss of all AC without reactor shutdown)<br>Steam line break inside containment (BWR) or pressurizer break LOCA (PWR) without reactor shutdown.<br><br>The point is that event sequences without reactor shutdown are worse than event sequences with successful reactor shutdown. A sequence within DBA or DEC but | | Several things are mixed here<br><br>Pressurizer break is covered by 3 (a) (1) : Failure of a large pressure-retaining component in the reactor coolant system.<br><br>This not a PIE, because of the difficulties in demonstrating that the loads generated would not jeopardize the containment integrity. It is a case for practical elimination<br><br>I think it needs to be distinguished what is postulated in the design from what may be analyzed in a PSA<br><br>DBAs with failure of the scram are normally not DEC without core melting but beyond design basis accidents. ATWS is AOO (not DBA) + scram failure. Steam from a steam line break (BWR) in the containment, would be condensed in the suppression pool. This is a DBA. In case that the control rods are not inserted, the void coefficient reduces the reactivity and there is a stand by liquid control system for boron injection to reach subcriticality after several minutes<br><br>All sequences in which subcriticality is not reached |

| | | | | | |
|---|---|---|---|---|---|
| | | | with the added failure of shutdown could lead to both containment overpressurization and core damage. We cannot see that such unlikely but important sequences are addressed in the guide. Could it please be clarified? | | eventually lead to core damage. If this also leads to containment failure is another subject. I cannot make this judgement. Every design has it limits and there are always accident beyond the design basis (although very unlikely)<br><br>It is not clear what is for you also the failure of the reactor shutdown: The failure of the control rod insertion?, then it is possible to have an emergency boration system if it is relevant. It is not a condition for P.E. it can be mitigated.<br><br>Or is it for you the failure of the reactor shutdown the failure of all the systems that may exist for shutdown<br><br>In a core melt accident is not possible in general to ensure that the corium would not become critical, but criticality is likely to be local and not sustained. In a plant designed for DEC with core melting (i.e. compliant with SSR 2/1 ) the means to stabilized the core, e.g. spreading it in a core catcher , or in vessel melt retention, need to ensure that criticality is local and not sustained and that the heat removal systems can compensate for the energy generated.<br><br>In other words, stabilizing and cooling a molten core needs to consider issues of criticality.<br><br>Of course sequences without reactor shutdown are worse that with reactor shutdown<br><br>Under practical elimination are considered the plant conditions for which mitigation is not feasible or cannot be demonstrated.<br>It seems that criticality in a severe accident is not |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | one. |
| 7. | 4.12 | … (b) Severe accident sequences that could lead to early containment failure, such as:<br><br>(i) Highly energetic direct containment heating;<br><br>(ii) Large steam explosion;<br><br>(iii) Explosion of combustible gases, including hydrogen and carbon monoxide;<br><br>(iv) Recriticality of degraded core or corium | Recriticality in degraded core or corium could lead to early containment failure.<br><br>The suggested (iv) is slow and not as fast as the fast reactivity insertion rate in I.10 in Annex 1. Even if prompt core damage is practically excluded, containment overpressurization due to fission power might not be.<br><br>The point is that event sequences with recriticality are worse than event sequences without recriticality. An event sequence within DEC-B but with the added recricticality could lead to containment overpressurization in a way which the same event sequence without recriticality would not. We cannot see that such unlikely but important sequences are addressed in the guide. Could it please be clarified? | | See previous comment local recriticality in a molten core cannot be excluded and it needs to be considered in the design: dispersion of the corium and heat removal. Note that corium is not configured as a reactor core for adequate moderation and power generation<br><br>Having said that, I am not an expert in this matter. It was not included because it can be mitigated |
| 8. | 4.1 , whole guide | Example 4.1:<br>The concept of ~~practical elimination~~ is introduced in para. 2.11 of SSR-2/1 (Rev. 1) [1], which states that “Plant event sequences that could result in | “practical elimination” = eliminating something in a practical way (i.e. not theoretical elimination) | | I think we are coming back square one |

| | | | | | |
|---|---|---|---|---|---|
| | | high radiation doses or in a large radioactive release have to be 'practically eliminated'<br><br>The concept of practically eliminating plant event sequences is introduced in para. 2.11 of SSR-2/1 (Rev. 1) [1], which states that "Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'. | "practically eliminating" = almost, very nearly or virtually eliminating<br><br>(Oxford Advanced Learner's Dictionary)<br><br>The concept of *practical elimination*, i.e. *eliminating something in a practical way* is different from the concepts of *practically eliminating something*, i.e. para. 2.11 SSR-2/1 is not phrased with "the concept of practical elimination".<br><br>This possible difference is not addressed in the IAEA glossary 2018 where the definition of *practical elimination* is describes as practically eliminating events.<br><br>Is it possible to clarify the view on this semantic issue, if any differences in meaning are intended or not? | | Personally, the Oxford dictionary version is the idea. Trying to deep in it the definition in SSR 2/1 becomes impractical, because very few things are impossible and the second option very unlikely with high confidence…. means very sure that it is nearly impossible, however if you approach it scientifically, you are asking for estimating a very low probability with small uncertainty<br><br>This is a probabilistic in nature. When the cases are investigated in practice, probabilistic analysis have a secondary role, behind the engineering and the deterministic analyses of measures implemented in case that the subject is suitable for a probabilistic analysis that it is not expert judgement<br>In which case in addition has the result a low uncertainty?<br><br>This part in the Glossary I dont understand<br>The phrase 'practically eliminated' is misleading as it actually concerns the possible exclusion of *event* sequences from hypothetical *scenarios* rather than practicalities of *safety*. The phrase can also all too readily be misinterpreted, misrepresented or mistranslated as referring to the 'elimination' of '*accidents*' by practical measures (or else 'practically' in the sense of 'almost'). Clear drafting in natural language would be preferable |
| 9. | 4.3 | A clarification of the relationship between 1) events and sequences that are practically eliminated and 2) events and sequences considered as residual risk, is needed. | Please consider to clarify, e.g. in paragraph 4.3. E.g. figures presented at NUSSC 49 could be helpful as a complement, or more extensive explanations based on the figures. | y | As figures were not wanted, everything would have to be done with explanations<br><br>So far we have not used the term residual risk because a new term would raise questions the difference should be made<br><br>However, I receive comment from some countries or observers to remove paragraphs or parts that don't |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | provide recommendations.<br>I perceive that some concepts or terms are not understood in the same manner by different people and this also raises comments<br><br>I would be beneficial to elaborate on some topics, but I would like to have the agreement of NUSSC that this is acceptable and on which matters. |

**Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

<table>
<tr><td colspan="4">COMMENTS BY REVIEWER<br>Reviewer: Hessa AL Marzooqi Page…. of….<br>Country/Organization: UAE / FANR Date: 29 Oct. 2020</td><td colspan="4">RESOLUTION</td></tr>
<tr><td>Comment No.</td><td>Para/Line No.</td><td>Proposed new text</td><td>Reason</td><td>Accepted</td><td>Accepted, but modified as follows</td><td>Rejected</td><td>Reason for modification/rejection</td></tr>
<tr><td>1</td><td>All over the document</td><td>To add: Identification of initiator frequency table in this document.<br>(It was noticed that the frequency definitions of postulated initiating events for design basis accidents is scattered and not existing for some.)</td><td>• Maintain consistency in the IAEA document. (the table can be found in INES User's Manual)<br>• The importance to identify each frequency level before analyzing defense on depth situation</td><td></td><td></td><td></td><td>INES User manual doesn't use the same terminology<br><br>I believe that there would not be agreement on such a table</td></tr>
</table>

**DS508 Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants – Step 7**

| COMMENTS BY REVIEWER<br>Reviewer: Page.1. of..19..<br>Country/Organization: UK/ONR Date: October 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | Headline comments: The UK/ONR is supportive of the objectives set out in the guide and what are the three new aspects from SSR2/1 identified in paragraph 1.2 to be expanded upon.<br><br>The guide is generally improved over previous versions – it is now simplified and more focused, particularly in Section 3. Many of the specific comments made by the UK/ONR at Step 5 have been addressed.<br><br>On practical elimination, whilst paragraphs 4.11-4.17 are generally reasonable, parts of 4.1-4.10 (new/or modified in this version) are more problematic, notably:<br>• Paragraph 4.3 on whether practical elimination is an extension of Defence in Depth measures or whether it reinforces the demonstration of Defence in Depth.<br>• Paragraphs 4.6 & 4.7 on expectations for limits and criteria for DEC and how these relate to larger events shown to be practically eliminated.<br>It is suspected that many readers of this guide (if and when it goes out for MS comment) will still not get the clarity they seek on practical elimination. In terms of adding value to what is already included in SSR2/1 on practical elimination, it is perhaps not as helpful as WENRA's equivalent guidance on the concepts or SSG-2 on what sequences/ phenomena need analysing.<br><br>Section 5 (together with some text in earlier sections) is giving inconsistent messages on whether non-permanent equipment can be considered as part of 'the design', and a lack of clarity on whether | | | Thank you<br><br>The guide has been substantially reduced and I asked myself what is the added value.<br><br>I am bound to SSG-2 that for the purpose of DSA addresses both DEC and PE., identifying cases and indicating the assessment for which DSA is only a component<br><br>I have countries asking for further elaborations and others that don't wasn't them even when the concepts a are not really clear, as it is visible from many comments.<br><br>It is a mistake that any safety demonstration that it is not PSA is DSA. DSA is has a much narrow scope in SSG-2<br><br>DSA is just chapter 15 in the SAR | | |

| | | | | | |
|---|---|---|---|---|---|
| | | such equipment can be credited for the purposes of practical elimination and demonstrating defence in depth. | | | |
| 1 | | Review use of safety provision, and consider defining.<br><br>More generally, review of terminology: safety/design systems/measures/ features/provisions | 'Safety provision' is used throughout the guide, and it has a generally understandable common meaning. However, it does not appear in the 2018 safety glossary. The glossary identifies a host of terms under "plant equipment", and "safety measure" is defined in its own right.<br>We suggest it either needs to be defined or an alternative term used in the guide which is defined elsewhere. 'Safety Provision' is not used in SSR2/1.<br><br>Para 3.10 talks about "design provisions (safety systems)" which is different again. Are design provisions the same as safety provisions? Therefore, are safety provisions the same as safety systems?<br><br>The term 'safety features' is also used (as per the Glossary) for DEC, although 'design features' is also used in this context, e.g. 3.29. | y | Thank you for this comment. I am lacking the time for a thorough implementation now<br><br>Safety measures, which don't need to be only design, would be better than safety provisions.<br>"Design provisions" is a term broadly used in other guides, for instance SSG-53<br><br>Safety feature is a generic term used in many standards not related to NPPs and in SSR 2/1. For example:<br><br>*A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations*<br><br>Safety systems are reserved for DBA.<br><br>Hence, when it came the time to refer to DEC, the term used were "safety features for DEC", meaning those safety features specific for DEC, not that "safety feature" is a term to be used only in relation to DEC. Otherwise there is no need to say for DEC.<br><br>Safety feature is used in other standards |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 1.8 | Review sentence starting *"These features…"* to clarify if it is a statement of fact for most NPPs, a requirement of the IAEA, or an assumption made in this guide. | "*These features are <u>primarily</u> intended for preventing unacceptable radioactive releases in the event of levels of natural external hazards exceeding the magnitude considered for the design, derived from the hazard evaluation for the site*."<br><br>Is this statement a requirement, expectation or an observation? Is there any evidence to back it up? Does it apply for all reactor designs? If the PSA of a facility crediting non-permanent equipment was interrogated, would it show demands on this type of equipment overwhelmingly came from extreme external hazards or would they make a contribution to other types of events? Is the statement only true for those designs which have gone for a hardened approach, as opposed to those who have gone for a FLEX approach or tried to extend site autonomy times with passive features? | y | Good point<br><br>It was in fact introduced in SSR 2/1 as a result of the lessons learned from the Fukushima Daiichi |
| 3 | 1.8 | Suggest:<br><br>"*This Safety Guide also addresses how the demonstration of defence in depth can be reinforced by* | With regards to: "*This Safety Guide also addresses the reinforcement of safety by including design features for* | y | |

| | | | | | |
|---|---|---|---|---|---|
| | | *including design features for enabling the use of non-permanent equipment….*” | *enabling the use of non-permanent equipment…"*<br><br>Is it the connection points (as per SSR 2/1 8.28B & 6.45A) which are part of 'the design' or also the non-permanent equipment itself.<br>Overall, the guide isn't clear or is inconsistent on this.<br>For example, para 3.48 refers to non-permanent equipment as part of an evaluation of the adequacy/effectiveness of accident management strategies – presumably this is part of defence in depth and can be credited for practical elimination ?<br><br>See also comments below on conflicting statements in paras 5.3, 5.10 & 5.16 below. | | For me the connection features, what is not permanent cannot be considered part of the design.<br><br>They are part of the DiD, also level 5 is part of DiD<br><br>They cannot be credited for practical elimination ( I am thinking if perhaps it would be possible fro the SFP).<br><br>P.E refers to specific cases, see below and needs a solid demonstration. It cannot rely on equipment that can possibly be miles away from the plant |
| 4 | 2.8 | "*In addition, the design should be such that there are no cliff edge effects in radiological consequences for accidents slightly exceeding those considered in the design (including design extension conditions)*." | The final sentence as currently worded says "*In addition, the design should be such that no cliff edge effect in the radiological consequences is expected for accidents slightly exceeding the plant design basis*".<br><br>This is a reasonable statement that makes sense with a | Change made | I could explain this, if people is in agreement with including explanations and not just should statements. I receive many comments for deletion<br><br>The change mad implicitly considers it |

| | | | | | |
|---|---|---|---|---|---|
| | | | ‘modern’ interpretation of what the plant design basis is (ie what it has been designed for, including DEC-B, not just DBA). However, will it be appreciated by all readers that this is not just talking about DBAs?<br><br>Suggest explaining this in full | | |
| 5 | 2.8 | First sentence should refer to SSR-2/1 not SSR-2/2 ? | Requirement 5 is from SSR-2/1 Rev.1. | Yes | Good catch |
| 6 | 2.10 | Suggest:<br>“*In a modern NPP, good design should ensure that members of the public are never be exposed to harmful radioactive consequences due to normal operation. Therefore, the following chapters have mainly focused on the implementation and assessment of defence in depth to prevent or mitigate the consequences of accidents and the complementary need for demonstration of practical elimination of accident sequences that can lead to early radioactive releases or large radioactive releases.*” | “*Harmful radiological consequences to the public can only arise from the occurrence of accidents*”. This is only achieved through design – with poor design it might not be the case. Also what is harmful can be subjective. The point being made in this paragraph is reasonable – the safety guide has focused on accidents, although defence in depth starts with Level 1.<br><br>It is noted however that paras 3.5 and 3.6 do provide guidance on normal operation, contrary to our interpretation of this text (although much reduced discussion compared to earlier vesions). | | According to 5.25 of SSR-2/1 (Rev. 1) recalled in 2.6 for DBA shall have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions”<br><br>SSR 2/1 uses harmful effects. Everything is subjective (I though radiological consequences is better in relation to nuclear safety)<br><br>We speak about designs compliant with SSR 2/1<br><br>I don’t know how to say that I am going to be dealing only with accidents.<br><br>The few things said about level 1 and level 2 is the minimum necessary to understand the role of DEC and PE<br><br>Is there any recommendation or explanation in the guide on level 1 or 2 that is detrimental or unacceptable for safety? |
| 7 | 3.1 | Review whether the scope set out in this paragraph is consistent | In terms of scope, this states *“.....with specific focus on the* | | I think this is what means specific focus |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | with both later text (3.35) and the objectives set for the guide. | *reactor core as the main source of radioactivity".*<br><br>However, paragraph 3.35 suggests a much broader scope for consideration of defence in depth, which although valid, may be confusing given the scope of this guide. | | Is DiD not applicable to the SFP?<br><br>What is DBA, DEC for the SFP? How should P.E applied to the SFP?<br><br>This was in former versions of the draft has been totally deleted.<br><br>Is there any recommendation or explanation here that is detrimental or unacceptable for safety? | | |
| 8 | 3.3(b) | The reliability of safety provisions to ensure that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level, **should be demonstrated** with a sufficient level of confidence<br><br>Or<br><br>~~The~~ **Adequate [or maybe '*Sufficient'*]** reliability of safety provisions to ensure that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level, with a sufficient level of confidence | Sentence not clear | Yes | The reliability of safety measures to demonstrate with a sufficient level of confidence that a certain plant condition can be brought under control without needing the intervention of the safety provisions implemented for next level,; | | |
| 9 | 3.11 | Delete text " *"The reliability of safety systems should be such* | In the UK, the consideration of DBAs is principally a | | **Requirement 13: Categories of plant states Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis** | | |

| | | | | | |
|---|---|---|---|---|---|
| | | *that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the safety goals of the plant (for new nuclear power plants typically below 10- 5 per reactor-year). If this is not the case, DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate to achieve such goals."* | deterministic matter. The second half of para 3.11 changes from deterministic expectations for DBAs to PSA expectations: *"The reliability of safety systems should be such that (to the extent possible) the collective contribution to the core damage frequency of failing to mitigate DBAs does not exceed the safety goals of the plant (for new nuclear power plants typically below 10- 5 per reactor-year). If this is not the case, DEC without significant fuel degradation could be postulated for specific low frequency sequences as appropriate to achieve such goals."*<br><br>Safety systems should be very reliable, but this should be driven by deterministic rules (design codes, SSC classification etc) as well as PSA. In addition, the text above seems to suggest that if a design has very reliable safety systems, DEC-As may not need to be considered - DEC-As are only needed if a CDF target cannot be met without them. SSR2/1 (as quoted in para 3.13) states DECs should be identified on the basis of "engineering judgement, deterministic assessments and probabilistic | | **of their frequency of occurrence at the nuclear power plant.** 5.1. Plant states shall typically cover: (a) Normal operation; (b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant; (c) Design basis accidents; (d) Design extension conditions, including accidents with core melting. 5.2. Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.<br><br>PSA doesn't make any system reliable. Do way say that?<br><br>Absolutely, if a DBA is believed to have a frequency of 10-4/y , any decent safety system design with the criteria applicable to them would have a failure probability below 10-3. My car is more reliable<br>This yields a 10-7 /y contribution to CDF. Would someone design an additional diverse system for DEC in this case to reduce CDF?<br><br>For the most frequent DBAs, about 10-2/y or for systems used for both AOOs and DBAs, e.g. the reactor scram, it may not be easy to have a contribution to CDF of ATWS below 10-5/y and a feature like an emergency boration system is included.<br><br>Not every DBA+safety system failure is back up by DEC-A (you can postulate it easily if some other suitable safety system is available)<br><br>As regulator, you could also indicate that safety system to mitigate a DBA should be sufficiently reliable (install more redundancies, implement diversity, etc. and make it more reliable. End of the story) |

| | | | | | |
|---|---|---|---|---|---|
| | | | assessments". PSA is just one aspect. It seems unlikely that for any current NPP technology, safety systems for DBAs could be so reliable that DEC-As never need to be considered.<br><br>The conditions for DEC-A are set out in para 3.17, and para 3.23 talks about how DECs can reduce the frequency of severe accidents caused by failures of DBA measures. The statement at the end of para 3.24 makes a similar point but is more general ie "*The reliability of safety systems should be high enough for DEC without significant fuel degradation to only be postulated exceptionally and to occur with a frequency lower than the most limiting DBAs.*"<br><br>**Propose deleting text from 3.11 as points are covered elsewhere in a more acceptable way.** | | DEC-A features are not a substitute for unreliable safety systems. It come only into application for a limited number of cases.<br><br>3.11 is fully meaningful. It describes the design approach and fafcilitates understanding the relation between DBA and DEC-A. I would have to delete also 3.12 |
| 10 | 3.12 | Proposal is that the last sentence of 3.12 is deleted. | It is stated at the end of para 3.12 that "*Severe accidents with an open containment constitute one of the plant conditions to be practically eliminated that are addressed in Section 4.*"<br><br>This is in a section on DBA (not practical elimination). | | If you have a severe accident with an open containment, it is a fact that both a large and early release will follow<br><br>How likely is the severe accident is one thing, but the consequences cannot be mitigated if the containment is not closed |

| | | | | | |
|---|---|---|---|---|---|
| | | | For many existing NPPs, shutdown faults are a significant source of risk contribution to CDF/LRF, and do need consideration.<br><br>It is very hard to make severe accidents with an open containment physically impossible. So is the implication of this statement that safety measures for DBAs (and safety features of DEC-As, even though they are not discussed till 3.13) need to ensure that the frequency of *a* severe accident is very low (lower than that for a closed containment event)? So this means that practical elimination in this context is not through a specific process applied to those plant states not covered by DBA/DEC-A/DEC-B, nor additional engineering provision above and beyond what is provided for DBA/DEC-A/DEC-B, but is something achieved by taking credit for defence in depth measures?<br><br>It is perhaps too early to introduce this nuanced idea, as what practical elimination is has not been discussed in the guide yet. | | If during shutdown a PIE progresses to a severe accident, you better make sure that the containment can be closed first.<br>Severe accident with an open containment is a case for practical elimination. You can only work in reducing the frequency of the severe accident (similar to the SFP)<br><br>But this is not the point here<br><br><br>The point is that if I have a DBA like a large LOCA or MSLB in a design that requires a spray system or containment cooling system for maintain the integrity of the containment, then if such systems fail, there are two issues:<br>- The inventory for core cooling can be lost leading eventually to a severe accident<br>- If a severe accident happens anyway due to other failures<br>-<br>In any case, there would be a severe accident situation with a failed (open) containment<br><br>Hence the reliability of such containment systems is crucial.<br>Several modern designs don't need a spray for DBA. The containment will passive withstand any DBA, but this is not a requirement in SSR 2/1. It need to be considered<br>The same applies to containment isolation measures<br><br>We only refer to section 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | | It is noted that para 3.26 states "*For new nuclear power plants, accidents involving core melting are postulated as DEC, irrespective of the fact that the design provisions taken to prevent such conditions make the probability of core damage very low*." This statement should equally apply to closed and open containment situations. It is also true whether DECs are considered in isolation or as part of a practical elimination demonstration (so still applies if 3.11 is deleted).<br><br>Para 3.36(g) says some very sensible things about justifying changes to barriers in defence in depth assessment. Again, this expectation stands, regardless of practical elimination expectations, and there is a danger that if open containment states are claimed to be practically eliminated, they might be screened out from defence in depth demonstrations.<br><br>Para 4.5 makes a sensible and less forceful statement on a similar point "*In such cases, it may be necessary to demonstrate practical elimination by showing with a high degree of confidence* | | DEC is not part of practical elimination<br><br>The plant is not designed for conditions practically eliminated precisely because they will not occur, and these are the conditions for which is not practical to design<br><br>It is not possible to design systems that will mitigate a severe accident and prevent a large release if the integrity of the containment is lost.<br><br>3.11 has nothing to do with DEC B<br><br>What is wrong with 3.36(g)?<br><br>Open containment states is not something to be practically eliminates, it is a severe accident with an open containment<br><br>We have a problem with the understanding of the relation between DiD and PE<br><br>Would it be better for you to put an open reactor as un available barrier in refuelling?<br><br>The fact is that if you remove temporarily a barrier, it needs a justification and to ensure that the protective measures are still sufficient<br><br>I removed it, but I don't see the reason and the problem |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | *that such severe accidents would be extremely unlikely*."<br><br>Given all these other statements, it is suggested the last part of 3.12 can be deleted. | | | | |
| 11 | 3.26 | Check whether SSG-53 is the correct reference | Is SSG-53 (reactor containment design) the best reference for identifying DECs through engineering judgement and PSA? Does it have more to offer than SSR2/1 or SSG-2? | y | SSR 2/1 : 5.30. In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected by using engineering judgement and input from probabilistic safety assessments.<br><br>Do I find engineering judgement and PSA in a guide for SSG-2?<br><br>**I will include SSG-2**<br><br>You can check SSG-2 3.45 a 3.50 and SSG-53 3.38 a 3.45 (they are not consistent) and decide which one are more useful | | |
| 12 | 3.29 | Clarify or define 'emergency measures' | "*Radioactive releases due to leakage from the containment in a severe accident should remain below the design leakage rate limit for sufficient time to allow implementation of emergency measures*".<br><br>What is meant by 'emergency measures'? Footnote 3 of SSR2/1 talks about "off-site protective | y | Changed to off-site protective actions | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | actions". Is that what is meant? Does it include DEC-B features or mobile equipment? Does it include venting? | | | | |
| 13 | 3.34 | Text starting "*The correct implementation….*" is turned into a stand alone paragraph, either in its current location or perhaps around 3.57.<br><br>Consider if it is a statement about defence in depth provisions (ie design) or something to be demonstrated in the assessment. | There is an important statement included in this long paragraph "*The correct implementation of the requirements implies that the multiplicity of the levels of defence is not a justification to weaken the efficiency of some levels by relying on the efficacy of other levels. In a sound and balanced design, SSCs of each level of defence are characterized by a reliability commensurate to their function and their safety significance.*"<br><br>This is point lost in its current location and is not directly linked (as written) to earlier text on what assessment of Defence in Depth should show. It is proposed it goes into a new paragraph, and consideration given to whether this is a statement about defence in depth provision and/or something that the assessment should demonstrate.<br><br>It could also be moved to the section on "INDEPENDENCE BETWEEN LEVELS OF | y | Put as a separate paragraph<br>I don't see the fitting in the part about independence | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | DEFENCE IN DEPTH" for example, around para 3.57. | | | | |
| 14 | 3.43 & 3.44 | Consider deleting paragraphs | These paragraphs seem to be repeating advice in paras 3.7 and 3.11. Are they needed, given what has been said earlier (both 3.7/3.11 and the general paragraphs in 3.40 to 3.42)? | y | You are likely right but I had other comments in the summer to perform changes.<br>I need to thing how to proceed, not losing relevant information | | |
| 15 | 3.46 | Consider deleting paragraph | Is para 3.46 just repeating para 3.41 but specifically for DEC-B and only focusing on PSA targets, and not the other aspects set out in 3.41? Is it needed? | y | You are likely right but I had other comments in the summer to perform changes.<br>I need to thing how to proceed, not losing relevant information | | |
| 16 | 3.48 | Clarify what is meant by 'extreme', perhaps by using an alternative term. | "*The assessment should include an evaluation of the adequacy and effectiveness of the different accident management strategies defined to cope with <u>extreme</u> scenarios*."<br><br>What is meant by extreme? DEC-B? Beyond design basis external | y | This is a good point<br><br>Actually it is about accident management measures for severe accidents, | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | hazards? Situations where fixed safety features fail and need portable equipment? | | whether it is for DEC-B or more adverse conditions<br><br>Changed to severe accident scenarios | | |
| 17 | 4.2 | Review need for this paragraph. Subsequent paragraphs seem to cover the same points with more clarity. | This paragraph is not clear.<br><br>In the first sentence, why is “*With regard to design*” added at the start? The sentence makes sense without it, and it is not apparent why it would or could mean something different if it was with regard to something other than design.<br><br>The second sentence starts with “*Those accident sequences*”. Presumably this refers to those mentioned in the first sentenced “events or sequences of events leading to or involving significant fuel degradation, i.e. a ‘severe accident’, for which the confinement of radioactive materials cannot be reasonably achieved”. Severe accidents leading to or involving significant fuel degradation should be addressed through | y | Changed to those event sequences for clarity . Since they end in core damage THEY are also accident sequences<br><br>EXAMPLES<br><br>Sequence of event:<br><br>LOCA, failure of ECCS, core melting, H2 release, H2 explosion needs to be practically eliminated<br><br>Confinement cannot be reasonably achieved or demonstrated<br><br>Sequence of event:<br><br>LOCA, failure of ECCS, core melting, H2 release, H2 explosion prevented, core retained in a core catcher and heat a removed from the containment (mitigation by safety features of | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | DEC-B consideration (and defence in depth).<br><br>If the point of the paragraph is to say a) it is only the events with the potential for very severe consequences that are considered appropriate for practical elimination, and b) anything with that potential not adequately addressed through defence in depth (inc DEC-B) need to be shown to practically eliminated or shown to be extremely unlikely, then it is perhaps not needed as the subsequent paragraphs discuss this. | | DEC), controlled plant state achieved. This is a successful accident sequence<br><br>It is reasonable to confine radioactivity thanks to the safety features for DEC. It is possible to design for this scenario if H2 doesn't explode<br><br>Sequence of event:<br><br>LOCA, failure of ECCS, core melting, H2 release, H2 explosion prevented, core retained in a core catcher, failure to remove heat from the containment (failure of a safety feature for DEC B and any other additional accident management measure) leading to late containment failure<br>This should be a very unlikely sequence contributing to the residual risk (it is not a sequence for the demonstration of practical elimination) |
| 18 | 4.3 | Suggest:<br>*This is where the aim of the 'practical elimination' concept lies: to reinforce the demonstration of defence in depth in the safety analysis report with a focused assessment of the final design to show that any remaining conditions having the potential for 'unacceptable* | ONR/UK has several times asked the question if practical elimination takes credit for defence in depth measures or is addition to it. Is it about extra design features above and beyond what is provided for AOOs/DBAs/DECs or is about analysis/assessment to show the design provision is adequate? | | I have tried several times to answer this question but I don't succeed<br><br>There is no safety measure at the plant not contributing to the defence in depth.<br><br>Measures that support the demonstration of P.E. are not an additional level of DiD |

| | | | | | |
|---|---|---|---|---|---|
| | | *radioactive releases' are physical impossible or are extremely unlikely to occur with a high level of confidence*. | With regard to the following sentence:<br><br>"*This is where the aim of the 'practical elimination' concept lies: to reinforce defence in depth by a focused analysis of those conditions having the potential for 'unacceptable radioactive releases'*."<br><br>is it about physically reinforcing the depth in depth, or strengthening the defence in depth safety submission demonstration with focused analysis?<br><br>Note, para 4.9 says something like this already – UK/ONR would support para 4.9 as a concept of what practical elimination is, as opposed to a separate level of defence in depth.<br><br>Para 4.10 (and footnote 3) also provide useful clarity that this is meant to be an iterative part of the design process which may result in additional defence in depth provisions, although see comments against 4.29 below. | | Aside from the exceptional cases, like the break of the RPV which would defeat any safety measures in several levels of DiD, conditions for P.E. are associated to severe accidents that in order to occur need the failure of several levels of DiD. Thus, H2 explosions are not just demonstrated to be P.E. by installing recombiners. Several DiD levels make severe accident very unlikely already.<br><br>P.E. needs a robust demonstration that relies necessarily on design, complemented as necessary by other aspects. |

| | | | | | |
|---|---|---|---|---|---|
| 19 | 4.6 & 4.7 | Clarify in the text whether new limits and criteria are required for practical elimination (suggest not) or explain how releases in excess of DEC-B limits need to be practically eliminated, and PSA can help with this. | Perhaps relevant to comments made by Canada on this draft, when these paragraphs talk about establishing acceptable limits for radiation protection, as well as probabilistic criteria or target values for the purpose of demonstrating the low frequency of a core damage accident or accident sequences leading to radioactive releases, are these in addition to 'conventional' deterministic and probabilistic criteria on DEC-B or LRF?<br><br>Surely, it is anything with consequences higher than the limits set for DEC-B that should be shown to be either physically impossible or extremely unlikely, so no deterministic limit is needed? For PSA, are targets different from those being set for L2 PSA being established specifically for practical elimination?<br><br>Should the discussion in 4.7 be more focused on setting deterministic expectations for DEC-B which have a margin to large or early release offsite requirements, such that if they are met, large or early releases are not an issue? Failure of DEC-B features, events more | y | The failure in the mitigation of DEC B, brings the plant in a severe accident condition beyond the design basis, that if not mitigated with accident management measures, e.g. using non permanent equipment, would eventually result in releases above the acceptance criterion for DEC-B and possibly above the threshold for large releases. Such sequence of events should be also very unlikely, but it is part of the residual risk. It doesn't belong to the cases for P.E<br><br>All DEC-B conditions are severe accidents, the reverse it is not true<br><br>I would try to clarify this during the meeting<br><br>I have several hundred comments<br>I am sorry , I cannot explain here all your questions<br><br>**I can offer to have a conference call before the meeting** |

| | | | | | |
|---|---|---|---|---|---|
| | | | severe than DEC-B features are designed for, or events DEC-B features are not designed against (any of which could result in larger releases) should be very low likelihood or physically impossible. | | |
| 20 | 4.11 | Suggest:<br><br>*For a modern LWR, the safety function that needs to be preserved to prevent large or early releases is confinement. In most operational modes, this is provided by the containment structure, and therefore a key consideration for practical elimination demonstrations is ensuring severe accident sequences with the potential to fail the containment are extremely unlikely.* | Does the issue identified apply to practical elimination for open containments or spent fuel pools (which this guide already says needs to practically eliminated)? | | This is <u>for every NPP, not for a modern</u><br><br>From the 3 FSFs:<br>1. control of reactivity<br>2. Fuel cooling<br>3. Shielding / Confinement of radioactive material<br>1 and 2 are only because they are needed to ensure 3.<br>For other sources of radioactivity without fissile material, only number 3 applies<br><br><br>*For a modern LWR, the safety function that needs to be preserved to prevent large or early releases is confinement. In most operational modes, this is provided by the containment structure, and therefore a key consideration for practical elimination demonstrations is ensuring severe accident sequences with the potential to fail the containment are extremely unlikely.*<br><br>I indicate the is the potential for a confinement function failure. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | In the SFP there is no containment. The ventilation/filtering system and the building provide confinement<br><br>Do we need to make it more complicated to start? | | |
| 21 | 4.22 | Suggest:<br><br>*The design provisions considered in practical elimination assessments should be identified on a case-by-case, and, where relevant, associated to the appropriate level of defence in depth or plant state at which the sequence of events would be interrupted to prevent unacceptable consequences*. | "*The design of provisions for practical eliminations*…….". <br><br>This reads like some design provisions are to be practically eliminated. | y | | | |
| 22 | 4.24 | Suggest:<br><br>*Some design and operational provisions claimed to contribute towards the practical elimination of large or early releases could be vulnerable to potential human errors prior to the accident.* | "*Design provisions and operational provisions for "practical elimination" of some severe accident might be vulnerable to potential human errors prior to the accident*."<br><br>Again this reads like some design provisions are to be practically eliminated. | Y | Some design and operational provisions claimed to contribute towards for the "practical elimination" of some severe accident sequences could | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | be vulnerable to potential human errors prior to the accident. | | |
| 23 | 4.28 | "The measures to prevent and mitigate the event sequences…." | We are considering DEC sequences with core melt, so measures to mitigate the consequences (as well as prevent) are of interest. | | | N | Sequences to be P.E. are not mitigated .<br><br>The full sequence cannot take place |
| 24 | 4.29 | Delete paragraph and/or consider combining 4.10 (& footnote), 4.29 and 4.33 earlier in Section 4 so that there is a clear explanation of when practical elimination should be addressed, for example, it is iteratively during the design process and then (once the design has reached an appropriate level of scrutiny for regulatory review), demonstrated holistically in the safety analysis report. | There still remains some doubt when reading the guide over whether practical elimination is a process followed by the designer, or a demonstration provided in the final safety submission to regulatory authorities. It can be both, but the section "DEMONSTRATION OF 'PRACTICAL ELIMINATION'" would seem to be focused on the latter given the title.<br><br>However, para 4.29 talks about additional design provisions to be implemented. In the safety submission, the design basis will be established (via an iterative processes, no doubt) and the final design will need to demonstrate practical | Y | The design and the safety demonstration are an interactive process<br><br>para 4.29 t additional design provisions to be implemented removed | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | elimination of large or early releases (as per para 4.33).<br><br>[Earlier in Section 4 (para 4.10 and footnote 3) there is reference to practical elimination being an iterative process undertaken as part of the design – that is ok, but it is interpreted that the guide has moved on by paragraph 4.29 to what should be shown in the assessment report put forward to others]. | | | | |
| 25 | 4.30 | Delete paragraph | Para 4.30 has already been stated – delete the paragraph. | Y | I agree but I cant make this change now. The paragraphs get renumbered and I cant follow your comments and others | | |
| 26 | 5 | **Suggestion – keep text largely as it is, just remove the sentence from 5.3** "Non-permanent equipment should not be credited in demonstrating the adequacy of the nuclear power plant design". | Section 5 is now much less problematic to the UK/ONR. The expectation to have provision for connecting non-permanent equipment is a good one. | | SSG-2, 7.51<br>*Non-permanent equipment should not be considered in demonstrating the adequacy of the nuclear power plant design.* | | |

| | | | | | |
|---|---|---|---|---|---|
| | | At the end of the section (para 5.16) provide some discussion on whether non-permanent equipment can be demonstrated in defence in depth and practical elimination demonstrations, noting this depends on design choices and philosophies, and member state expectations.<br><br>If credit is taken for non-permanent equipment in any deterministic or probabilistic assessments, there needs to high confidence of timely connection and operation of equipment. | However, the text still needlessly gets into discussions on whether non-permanent equipment can be credited as part of the design basis.<br><br>Whether a design/operator/country goes for a 'hardened' approach or a FLEX approach, or something in-between is a choice, informed by a range of factors. Some reactors by design provide more time for non-permanent equipment to be connected compared to other designs. This makes a difference as to whether non-permanent equipment can be credited. Many PSA models do take credit for non-permanent equipment – does this disqualify CDF/LRF determinations from these models from informing practical elimination demonstrations?<br><br>Para 5.10 states: "*To make the coping strategies more reliable, an adequate balance between fixed equipment and non-permanent equipment should be implemented*."<br><br>This is reasonable, this can be done as part of the design. Yet para 5.3 states "*Non-permanent* | | This is, allow me to say, "beyond DEC"<br><br>The equipment or connection features need to be credited for something, otherwise they are useless, but not for the demonstration of the design<br>This is part of accident management<br><br>PSA can take credit for many things. The question is what for you are developing and using the PSA<br><br>If it is used for practical elimination, certainly it is wrong (in general, perhaps it is valid for adding water to the SFP)<br>P.E requires a very solid demonstration, that cannot be based on equipment that it is not permanent.<br><br>In section 5 we have exceeded the plant design basis, we may not be in DEC anymore<br>This is accident management. |

| | | | | | |
|---|---|---|---|---|---|
| | | | *equipment should not be credited in demonstrating the adequacy of the nuclear power plant design*", contradicting this.<br><br>This contradicted again in para 5.16 "Where there is high confidence of the timely connection and operation of non-permanent equipment, their use could be credited for demonstration of the successful mitigation of an accident to prevent unacceptable radiological consequences." | | |
| 27 | 5.5 | *Footnote 9: "The concept of practical elimination is <u>not</u> applied to external hazards…."*<br><br>Provide further clarity on expectations for externa hazards, probably early in Section 4. | As worded Footnote 9 states *"The concept of practical elimination is applied to external hazards within the safety analysis due to the difficulties in providing a safety demonstration based on design features comparable to the full set of cases addressed in Section 4, and it is necessary to ensure in other terms that the risk of early radioactive releases or large radioactive releases as a result from extreme external hazards is very low."*<br><br>Should this say *"is <u>not</u> applied"*?<br><br>Either way, there seems to be a significant statement here on the | y | This has been the result of comments pushing in one or other direction<br><br>We have 3 ways in which a large release could take place<br><br>1) One of the cases in section 4, associated with events/sequence of evets that cannot be mitigated. This needs a strong demonstration according to the definition of PE<br><br>2) Failures in the mitigation of DEC-B, which eventually could result in large releases of a similar magnitude (this is the residual risk)<br><br>3) Extreme external hazards, not limited physically in magnitude but associated |

| | | | | | |
|---|---|---|---|---|---|
| | | | scope of practical elimination for 'beyond design basis' external hazards which should be covered in Section 4 rather than left to a footnote in Section 5. Is this saying that sequences involving BDB hazards do not need to be practically eliminated (but instead treated probabilistically) – if so, that needs to be clear. | | with a frequency, that can potentially fail all safety measures at different levels of DiD. This is not treated in this safety guide. It cannot be approached in the same way, but some country says in a way the concept of P.E is applied to it. |

**DS508 "Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants"**

| COMMENTS BY REVIEWER<br>Reviewer: SSTC NRS Page. 1 of 4<br>Country/Organization: Ukraine/ SSTC NRS Date: Nov 2, 2020 | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment No. | Para/Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | 2.7 | This Safety Guide is focused on the protection of the public and the environment in accident conditions | This and several other paragraphs mention protection of the public and the environment only. Shall the protection of the workers be included? | | | | The protection of the workers is also important but this guide is not addressing it. Other aspects would be necessary that are not considered in this guide |
| 2 | 3.11, last sentence | ~~If this is not the case~~ Nevertheless, DEC without significant fuel degradation ~~could~~ must be postulated ~~for~~ to address specific low frequency sequences ~~as appropriate to achieve such goals~~. | Based on the statements provided in last two sentences of para.3.11 it may be concluded that if reliability of safety systems is high and safety goal with respect to CDF value is reached, analysis of DEC sequences in the design is not necessary. Thus one of DiD levels may be completely omitted. | y | Could changed to should<br>Must not acceptable in SGs.<br><br>DEC without significant fuel degradation is part one level of DiD<br><br>One level is never totally omitted | | |
| 3 | 3.12 | If the design of the containment is such that in the case of the most limiting DBAs the intervention of cooling or | Severe accident (as defined in IAEA glossary) involves significant core degradation. Failure of containment cooling | | | | This is exactly the case. If the containment integrity is lost, the |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | pressure reduction systems (e.g. containment spray) is necessary to ensure the integrity of the containment boundary, such systems should be designed, constructed and maintained to ensure a very high reliability, since their failure would ~~not only lead to a severe accident but also~~ jeopardize the ~~subsequent~~ measures for ~~its~~ mitigation of radiological consequences. | or pressure reduction system may compromise the integrity of the containment, but not necessary will cause significant core degradation (e.g., in the cases when coolant inventory is maintained) | | | | core coolant inventory cannot be ensured after some time. |
| 4 | 3.19 | … to prevent core damage or damage to the fuel in the ~~irradiated~~ fuel storage, the primary difference between these two accidental conditions is the use of different approaches or criteria for design or safety assessment to achieve this objective | Editorial | y | The fresh fuel storage doesn't enter in the category of conditions for DEC.<br><br>Approaches included | | |
| 5 | 3.19 | (a) … rigorous reliability measures are allowed | The meaning of this statement is not evident. Does it mean that less rigorous reliability requirements may be applied for DEC equipment? | | Yes<br><br>No need to apply single failure criterion, lower safety class, etc. | | |
| 6 | 3.20, 2nd sentence | "… the rules for safety analyses [8] use less conservative methods and assumptions but they should still ensure a high confidence in the result … that cannot be simply achieved by best | It is not evident why the best estimate calculations are not sufficient. If the intent is to indicate necessity for sensitivity and/or uncertainty analysis, it seems reasonable to indicate it explicitly | y | Changed considering other similar commnets | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | estimate calculations" | | | | | |
| 7 | 3.47 | "… only a limited reliability can be attributed to those components necessary to ensure the containment integrity after a core melt accident" | It is not clear how the "limited reliability" can support justification of practical elimination of sequences leading to early or large radioactive release. Clarification is required | y | <u>This part is not about practical elimination, but about DEC</u><br><br>Severe accidents are very serious conditions for which equipment can hardly be designed or qualified as for other conditions<br><br>Actuations are not automatic. The necessary human involvement and other aspects cannot be also as reliably<br><br>This in addition to the uncertainty involved in severe accident phenomena | | |
| 8 | 4.7, last sentence | From the probabilistic point of view, event sequences that | Para.5.31 of SSR-2/1 states that the possibility of | | | | All severe accident for instance lead to |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | have been practically eliminated should only represent a very low contribution to the frequency of ~~an early radioactive release or a large radioactive release~~ all severe accident sequences, when the demonstration can be sustained by probabilistic analysis. | conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'. This implies that the sequences leading to large or early radioactive release shall consist only from those ones that are practically eliminated. Most likely the intent of the sentence is to indicate that these sequences shall represent the tiny fraction of all severe accident sequences | | | | hydrogen generation<br><br>Hence, hydrogen explosion need s to be prevented for all sequence. It is correct the way it is. |
| 9 | 4.17 | It may be useful also to classify accident scenarios in nuclear fuel storage locations and buildings taking into account the progression from an initiating event to the consequences that need to be avoided. | Editorial. Categorization of severe accident scenarios for the reactor core is given in 4.12 of the guide | | | | This paragraph may be eventually removed as a result of other comments 4.12 is not only about the reactor core, SFP is included<br><br>The source of large early releases is the fuel. What other locations/buildings should be considered? |

**TITLE: DS508: Assessment of the Safety Approach for Design Extension Conditions and Application of the Practical Elimination Concept in the Design of Nuclear Power Plants**

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Reviewer: US Nuclear Regulatory Commission | | | | | | | |
| Country/Organization: US Nuclear Regulatory Commission | | | Date: Nov. 9, 2020 | | | | |
| Comment No. | Para/ Line No. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| 1 | Tab. Contents | Scope……………………2 | Formatting consistency | Y | I don't know how to fix it (mysteries of MS-Word) | | |
| 2 | 1.8/4 | "…in the event of natural, external hazards resulting in a damage state exceeding that considered for earlier generation NPP designs, derived…" | In the U.S., the <u>magnitude</u> of the natural hazard considered for beyond-design-basis events (i.e., DEC) does not exceed the magnitude of the design basis hazard. The projected damage state (e.g., extended loss of AC power AND loss of normal access to the ultimate heat sink), however, is beyond that considered for the original design. Also provides additional clarity that the guide is intended for new reactor designs. | | | | This guide is indeed for new plants<br><br>I cannot identify the text of your comment<br><br>This is stated in 1.8<br><br>These features are primarily intended for preventing unacceptable radioactive releases in the event of levels of natural external hazards exceeding the magnitude considered for the design, derived from the hazard evaluation for the site. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | There is no recommendation for designing beyond the design basis hazard.<br><br>I am afraid I may not understand well the comment. |
| 3 | Footnote 2 | "…belongs to the level 5 of defence in depth…" | Word is missing. | y | | | |
| 4 | 3.4/10 | "…without significant fuel degradation ~~core~~ are similar,…" | Unclear sentence with "core" included. | y | | | |
| 5 | 3.18/12 | …with a very low frequency." | The existing language specifies "the most limiting DBAs." If a large double-ended pipe break LOCA coincident with total loss of offsite power is a DBA for the NPP design, then this limitation is far too restrictive. Such a DBA may be on the order of 1E-10/year or lower by some estimates. Some new reactor designers may have eliminated this unrealistic DBA, but are we certain all new ALWR designs have done this? | | Clarification<br><br>The PIE is the LOCA<br><br>It is postulated in the design thjat during a LOCA offsite power may fail and safety systems are supplied by the emergency DG<br><br>The frequency of the PIE is the one of the LOCA alone | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | The LOCA doesn't have LOOP as a consequence | | |
| 6 | 3.44/3 | Delete sentence beginning with, "A failure probability…" | Suggest not including the $10^{-3}$ reliability target value. The level of reliability would not be necessary for very low frequency initiating events. | | | | I have comments in favor or including such figures, not as a recommendation, and other for removing them<br><br>*A failure probability below than 10-3 in order of magnitude would be consistent with the strict requirements for reliability imposed to safety systems and supported by operational experience and testing.*<br><br>Safety systems are for DBA. If a DBA has a frequency of 10-3/y and the failure of safety systems to control it is 0-3. This would result in a contribution of 10-6/y from this PIE |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | We are only saying that system designed with all the requirements imposed to safety systems are expected to have a lower failure probability.<br><br>Many safety systems are designed for the most and the less frequent DBAs |
| 7 | 3.45 | Consider clarifying or deleting. | This is a new paragraph from the previous version of the document, and it is very broad and general. Not sure of the intended message. | y | There is an example in it.<br><br>I will consider deleting it | | |
| 8 | 4.7/14 | "…when the demonstration can be supported by probabilistic…" | The word choice of "sustained" is not contextually correct here. | y | changed | | |
| 9 | 4.8/5 | After "…small set of plant conditions." Insert, "Value-impact assessment of severe accident design alternatives to potentially further reduce risk of selected scenarios may be another approach. Ultimately, the identification process…" | This approach is certainly one way of achieving the objective. There are other approaches so the proposed language is to provide examples of a process that could be used but whichever process is used, it must be technically justified. | | | | I believe the text proposed is about mitigation of DEC with core melting, not about practical elimination. Those are sequences for which it is nor possible to design |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 10 | I-8/3 | "…must be identified. These scenarios must be prevented by design provisions or demonstrated by robust analyses that they are extremely unlikely to occur or lead to significant core damage due to inherent reactivity feedback characteristics of the reactor core design." | Boron dilution may occur in certain PWR designs including ALWR and SMR light water reactors. These scenarios may be AOOs for the design safety analysis. Added text to provide additional clarification. | y | I believe that this is explained in I-9.<br><br>I will se if it can be made more clear<br><br>Reactivity insertion accidents is nothing new | | |