Review of Safety Guide on Deterministic Safety Analysis for NPPs (DS491)

Step 11 – Second review of the draft Safety Guide by the review Committees (after comments by Member States)
(Step 11b – Comments about the resolutions provided to Member States' comments. (**Deadline 16 May**))

# Resolutions to comments provided by NUSSC (second review)

**Comments provided by review Committees representatives:** Finland (1), France (8), UK (5), Canada (8)
After deadline: Germany (7 new comments, 23 May); Russian Federation (5 comments, 29 May)
**Unsolicited comments provided:** ENISS/Observer (10)

*6 June 2017*

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| **Section 1** | | | | | | | |
| Russia-1 | 1.7 | Add footnote: "The concept of "design extension conditions" established in IAEA safety standard SSR-2/1 is not accepted in all countries. For example, in Russia the former concept of "beyond design basis accidents" is in use, which means that representative set of all possible accident scenarios are analyzed irrespective of their probability". | The concept of "design extension conditions" established in the standard of IAEA of SSR-2/1 is not accepted in all countries. For example, in Russian Federation this concept is not accepted, and the former concept of "beyond design basis accidents" continues still in use. | | | X | *As it is indicated in the comment, this request relates to SSR-2/1 (Rev. 1) and is out of the scope of this Safety Guide. On the other hand the Safety Standards are not binding on Member States.*<br>*Reminder of the resolution provided in the previous step (April):*<br>"This Safety Guide does not describe whether or how the States apply the safety requirements from SSR-2/1 (Rev.1) |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | | | | | or other requirements [*regarding Deterministic Safety Analysis*]. It provides guidance on how the [*applicable*] requirements of SSR-2/1 (Rev.1) can be fulfilled. "Design extension conditions" is the term currently used in IAEA Safety Standards." |
| **Section 2** | | | | | | | |
| Russia-2 | 2.1 Line 4 | Add new sentence after the first sentence: "The second objective of deterministic safety analysis for nuclear power plants is to determine and justify operator actions in case of breach of NPP normal operation, including accidents". | In this para it is established that the objective of the deterministic safety analysis for NPP is confirmation that safety functions and necessary systems, structures and components in combination with operator actions where necessary are capable and effective to keep the radiological consequences in the acceptable limits. This objective seems being not sufficient, since accident management operator actions also have to be | | | X | *Focus of this Safety Guide is not safety systems design but demonstration that [design] meets applicable safety requirements. Operator's actions and procedures are inputs used to demonstrate meeting the safety objective. In procedures, conservatism is not applied to its preparation but to its implementation. Section 7 covers how operator's actions should be considered in* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | specified and proved by deterministic analyses. This applies not only to actions aimed to limit radiological consequences, but also to other accident management actions (aimed to restore controllability of NPP – e.g. manual borating in case of ATWS if failed does not lead to any radiological consequences, but prevent restore controllability of NPP; or aimed to reduce radiological release or probability of radiological release even in case when release is lower limit value or in case when operator actions results in release reduction but not to the value which is lower than limit value). | | | | *the analysis and the existing wording of para. 2.1 seem consistent with such treatment.* |
| Russia-3 | 2.1 | Add footnote: "The concept of "practically eliminated" events, established in IAEA safety standard SSR-2/1, is not accepted in all member states. For example, in Russia this concept which was called earlier as the concept of | Footnote is necessary since "practically eliminated" concept is not applied in all IAEA member states. | | | X | *As it is indicated in the comment, this request relates to SSR-2/1 (Rev. 1) and is out of the scope of this Safety Guide. On the other hand the Safety Standards are not binding on Member* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | "hypothetical accidents" was rejected after Chernobyl accident". | | | | | *States.*<br>*Reminder of the resolution provided in the previous step (April):*<br>"[This Safety Guide does not describe whether or how the States apply the safety requirements. It provides guidance on how the requirements can be fulfilled.] Practical elimination is treated in, but not limited to, the IAEA Safety Glossary, SSR-2/1 (Rev.1) and TECDOC 1791 |
| Germany-2 (relev. 3) | Tables in Section 2 | *Change Heading format of tables* | Heading and text are difficult to distinguish in the tables, perhaps usage of classic table style, see SSG-2(2009) | | *Final format used in the Safety Guide (including headings) will be adapted to the IAEA Guidelines (SPESS C)* | | |
| Germany-1<br><br>(relev 3) | 2.4 | *Move to footnote or to chapter 5* | Does not fit in "OBJECTIVES OF DETERMINISTIC SAFETY ANALYSIS", it has the character of an annotation, calculated curves are the means to fulfill the objectives, not an objective in itself | | | X | *Chapter 2 is explanatory, no guidance is provided. It seems better not to distinguish objectives and means. It doesn't fit with the guidance provided in Section 5. The comment is **new** and **unique,** after the long review process.* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| Germany-3 (relev. 2) | 2.12 Line 2 Sentence 3 | *reformulate* | Not understood: [..] taking into account the very low probability that all parameters would be at their most detrimental value at the same time. | | *For clarification, sentence 3 will be modified as follows:* 2.12. Option 3 is so called BE plus uncertainty approach. This allows the use of BE computer codes together with more realistic hypotheses. A mixture of ~~B~~best estimate and partially unfavourable initial and boundary conditions … | | |
| ENISS-1 (Observer) | 2.15 Line 5 | 2.15. Option 4 allows the use of best estimate code modelling, system availability assumptions and initial and boundary conditions. Option 4 may be appropriate for realistic analysis of anticipated operational occurrences aimed at assessment of control system capability (paras 7.17 to 7.44) and in general for best estimate analysis of design extension conditions (paras 7.45 to 7.67) as well as for the realistic analysis that support PSA modelling, in particular the ones which aim to justify ~~with the purpose of justification of~~ operator actions. | Realistic TH/N calculations carried out to support PSA modeling (either to define minimal system configuration requirements, or to evaluate grace period before operator action is required) should also be mentioned. It is proposed to add these types of realistic analysis. | | | X | *Analytical support for PSA is not considered as deterministic safety analysis, as explained in the Annex; there are no acceptance criteria used for such application.* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | **Section 3** | | | | |
| ENISS-2 (Observer) | 3.4 | 3.4. The deterministic safety analysis should address postulated initiating events that can occur in all modes of normal operation. Initial conditions should consider a ~~controlled plant mode~~ stationary state with normal operation equipment operating prior to the initiating event. | ENISS believes that the original text (i.e. *"stationary state"*) is more appropriate than the new one (i.e. *"controlled plant mode"*). The original one states the pragmatic convention that is used to define the initial conditions for plant transients, as it would not be reasonable to perform multiple analyses for a given PIE considering any possible control systems configuration to describe the initial plant state. Instead, the new one is rather obviousness as, by definition, before the initiating event, the plant is controlled (normal state). | X | *[This change was incorporated in the last version of the draft (April). Former formulation will be used]*. | | |
| ENISS-3 (Observer) | 3.14 Line 2 | 3.14. The set of postulated initiating events should be defined in such a way that it covers all credible failures, including | Editorial proposal. | X | | | |
| ENISS-4 (Observer) | 3.15 Bullet 3 | "For internal hazards such as fire or flood ~~or external hazards such as earthquakes~~ the definition of the induced postulated initiating event should include failure of all the equipment that is neither designed to withstand the effects of the event nor protected from it. | In case of external hazards, it is common practice to use a load case approach. This approach is decoupled from the identification of hazard induced PIEs. It rather relies on the protection and sizing of protection and safeguard | | *Dash 3 will be modified as follows:*<br><br>"For internal hazards such as fire or flood or for failures caused by external hazards such as earthquakes | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | systems that may be needed in case of a potential PIE. Therefore, ENISS suggests limiting the last bullet to internal hazards. | | the definition of the…” | | |
| ENISS-5 (Observer) | 3.16 | 3.16. Additional failures are assumed in deterministic safety analysis for conservatism (e.g. single failure criterion in design basis accidents) or for the purpose of defence in depth (e.g. common cause failure). Distinction should be made between these additional failures and failures that are part of, or directly caused by, the postulated initiating event. Further failures may be added to bound a set of similar events, so as to limit ~~limiting~~ the number of analyses. | Editorial proposal. Meaning is kept unchanged. | X | | | |
| ENISS-6 (Observer) | 3.26 Line 5 | “… ~~Moreover, large bypass accidents do not allow much time for taking action to protect the public in the vicinity of the plant~~.” | Accidents without severe core damage (e.g. core kept covered), even with containment opened (i.e. equipment hatch and/or personal hatch opened) do not lead to large consequences non-compatible with the time delay to protect the public in the vicinity of the plant. ENISS believes that the previous sentence is sufficient to require special attention to accidents with potential containment bypass and suggest removing this last sentence. | X | | | |
| Canada-1 | 3.27 and Table 2 | Delete last sentence of 3.27 and Table 2. | Canada [23] commented on the previous draft that the | | | X | *It seems convenient and generally acceptable to* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | Reason continued:<br><br>Czech Republic made a similar comment (Czech Rep 3). The comment suggested deleting the table or removing the new category of events between $10^{-4}$ and $10^{-6}$/yr. A comment from France (France 3) asked to remove the lower bound of $10^{-6}$/year; making it open ended.<br><br>IAEA only dispositioned France 3, and referred Canada 23 and Czech Republic 3 comment dispositions to France 3 disposition. Since the intent of Czech Republic 3 and Canada 3 are quite opposite of that of France 3, they should be dispositioned separately. | table should be deleted as the classification scheme used here is not known outside the countries of origin and the frequency range is too severe.<br><br>The lower frequency limit of $10^{-6}$ is two orders of magnitude more stringent than the values given in SSG-2 Rev 0. Such increased severity is not justified by changes to high-level documents such as GSR Part 4 or SSR-2/1. SSR-2/1 added requirements for DEC but did not require that DBA regime should be more restrictive. No changes to SSR-2/1 Requirement 19 (5.24 to 5.26) were recommended in DPP466, *Fukushima Omnibus*.<br><br>The older plants, and even the newer ones, will not be able to cope with this event frequency. Consider seismic events as an example. Likely no plant in the world will survive a severe seismic event with an intensity that corresponds to 1 occurrence in 1 million years. | | | | *keep this kind of table in this Safety Guide. It doesn't represent an strict application of requirements from SSR-2/1 and GSR Part 4 but clearly indicated that it is an* ***example*** *and thinking in* ***new*** *NPPs. From both points of view (example and new NPPs) it seems convenient to use figures encouraging further responsibility and enhanced levels of safety. It seems not a relevant issue of the Safety Guide.* |
| ENISS-7 (Observer) | 3.28 Dash 5 | ...~~wrong positioning of a fuel assembly~~… | Thanks to organizational preventive features, the wrong positioning of one fuel | | | X | *This is a new and unique comment received after the long* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | assembly should not appear as an AOO but rather as a DBA. | | | | *review process* |
| Germany-4<br>(relev. 3) | 3.30<br>Dash 2 | Remove “feedwater line breaks“ in bullet 2 | Depending on specific design it could lead also to increased heat removal | | *Dash 2 will be modified as follows: Decrease in reactor heat removal:*<br>“loss of feedwater ~~line breaks~~” | | |
| Germany-5<br>(relev. 2) | 3.35<br>(b) | Reformulate, e.g. reactivity increase | Not understood: “Reactivity anomalies;” | | *Bullet (b) will be modified as follows:*<br>“(b) Reactivity increase ~~and power distribution anomalies~~ in the fresh or spent fuel;” | | |
| [UK-11] | [Written:]<br>*3.41*<br>*Bullet 2*<br><br>[It seems it should be:]<br>**3.40**<br>**Bullet 1**<br>**Line 2** | [Written:]<br>Delete:<br>“… multiple tube rupture.”<br>Insert:<br>“…multiple tube rupture; beyond the design-basis assumptions.”<br><br>*[Corresponding interpretation:]*<br>• Initiating events that could lead to situations beyond the capability of safety systems that are designed for design basis accidents. A typical example is the multiple tube rupture beyond the design-basis assumptions in a steam generator of a pressurized water reactor | Historical evidence on the condition of steam-generator tubes does not support the asserting that this is a lower frequency event. In some cases, an inspection has revealed that 10% of the tubes are defective. In my experience all plants run with defective tubes at some time in their design life.<br><br>Designers of new plant are always convinced that they have fixed the problems, but nature tends to find new ones.<br><br>The author should consider whether judgements on sequence frequency should be made in this document. | X | | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment Nr | Para / Line Nr. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| [UK-13] | 3.41<br>Bullet 1<br>Dash 1 | Delete:<br>• ~~*uncontrolled heterogeneous boron dilution (PWR);*~~<br>A better example is:<br>• *Fracture of high-integrity pipework*; | This boron dilution is not a lower-frequency event.<br><br>It occurred in France some years ago. As I recall, It was only good fortune which prevented a criticality.<br><br>In most plants the event is only avoided by good administrative control.<br><br>It is also a potential consequence of near-frequent small LOCA. This fault is close to being an AAO and needs to be assessed as DBA to confirm all reasonable protection/prevention measures are taken.<br><br>The author should consider whether judgements on sequence frequency should be made in this document. | | *Dash 1 from bullet 1 will be deleted:*<br><br>• ~~*uncontrolled heterogeneous boron dilution (PWR);*~~ | | *It seems better not to incorporate the replacement example suggested (*"Fracture of high integrity pipework*") as it is considered a DBA in many States.* |
| Germany-6 (relev. 2) | 3.41<br>Bullet 3<br>Dash 4 | *reformulate* | Not understood: "Loss of normal access to the ultimate heat sink.", what does normal access to ultimate heat sink mean and what is an "abnormal" access? | | | X | *According to the Safety Glossary, the* "ultimate heat sink (UHS) is a medium into which the transferred residual heat can always be accepted, even if all other means of removing the heat have been lost or are insufficient. (i:<br>This medium is |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | | | | | normally a body of water or the atmosphere)". *Few reactors use more than one UHS. Loss of a river or the atmosphere is not considered a DEC but loss of access to the UHS can be a problem. Consideration of this DEC points out using diverse UHS or alternate access to a single UHS.* |
| ENISS-8 (Observer) | 3.48 Bullet 1 | • Loss of core cooling capability, such as an extended loss of off-site power with partial or total loss of on-site AC power sources ~~(exact sequence is design dependent)~~, or/and the loss of the normal access to the ultimate heat sink (exact sequence is design dependent); | LUHS resulting in a severe accident consequence is also dependent on the plant design. An UHS sufficiently diversified from the normal UHS can allow to prevent core damage in case of LUHS. Therefore, ENISS suggests moving "(exact sequence is design dependent)" at the end of the sentence. | X | | | |
| [UK-21] | 3.49 Line 1 | Change: "3.49 The low frequency of occurrence…" To "3.49 The low estimates of the frequency of occurrence…" | The only thing that we know about these frequency estimates is that they are wrong. If these estimates were reliable, then there would be no case for doing the analysis. | X | | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | The actual frequency is likely to be dominated by residual risk. | | | | |
| Canada-2 | 3.50 Last sentence | "… The analysis of these sequences should provide the environmental conditions to be taken into account in ~~the assessment~~ assessing[8] ~~on~~ whether the equipment used in severe accidents ~~are~~ is capable of performing ~~their~~ its intended functions when necessary (see Requirement 30 from SSR-2/1 (Rev.1) [1]). | The resolution of the comment Canada [31] is acceptable but has introduced typographical errors. | X | | | |
| France-1 | 3.51 | 3.51. Determination of postulated initiating events should consider effects and loads from events caused by relevant site specific internal and external hazards and their combinations (SSR-2/1 (Rev.1), Requirement 17, paras 5.15A to 5.21A) [1] | Combinations of hazards is a crucial issue and should appear in DS491 (see Fukushima Dai-ichi lessons) for consistency with requirement 16 of SSR-2/1 ("all foreseeable PIE") | X | | | |
| Germany-7 (relev. 2) | 3.53 Bullet 2 | • The nuclear power plant design is robust enough to prevent any transition from the load resulting from the hazard into an initiating event; or | Clarify what "load" exactly refers to | | *Bullet 2 will be modified as follows :* «… to prevent any transition from the load caused by the hazard into an initiating event; ' | | |
| France-2 | 3.56 | The event sequences requiring specific demonstration of their 'practical elimination' should be classified as follows:<br>1) Events that could lead to prompt reactor core damage and consequent early containment failure, such as:<br>a. Failure of a large pressure-retaining component in the reactor coolant system;<br>b. Uncontrolled reactivity accidents; | | X | *A footnote will be added:*<br><br>"*Footnote*: These conditions should be analyzed during the identification of event sequences to be practically eliminated. Nevertheless, | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment Nr | Para / Line Nr. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | 2) Severe accident sequences that could lead to early containment failure, such as:<br>a. Highly energetic direct containment heating;<br>b. Large steam explosion;<br>c. Explosion of combustible gases, including hydrogen and carbon monoxide;<br>3) Severe accident sequences that could lead to late containment failure[FOOTNOTE]:<br>a. Basemat penetration or containment bypass during molten core concrete interaction (MCCI);<br>b. Long term loss of containment heat removal;<br>c. Explosion of combustible gases, including hydrogen and carbon monoxide;<br>4) Severe accident with containment bypass;<br>FOOTNOTE: These conditions should be analyzed during the identification of situations to practically eliminate. Nevertheless, their consequences could generally be mitigated with implementation of reasonable technical means. | France supports the deletion of bullet 3 (in these cases mitigation provisions should be implemented).<br><br>**Nevertheless, if needed, in order to achieve a consensus**, France proposes another option: adding the same footnote as the one added in DS482 (*These conditions should be analyzed during the identification of situations to practically eliminate. Nevertheless, their consequences could generally be mitigated with implementation of reasonable technical means.*) | | consequences from “a” and “b” could generally be mitigated with the implementation of reasonable technical means. | | |
| France-3 | 3.56 point 5 | 5) ~~Significant fuel degradation in a storage fuel pool and uncontrolled releases~~ | Point 5 should be deleted: the choice to implement or not mitigations provisions for a fuel melt in the storage fuel pool should be left to the vendors (cf. WENRA O3, footnote 35, Safety of new NPP designs). | | | X | *Taking into account the current state-of-the-art there are no feasible mitigation measures to prevent large releases, in particular when the SFP is outside the containment. When considering DEC in SSR-2/1 (Rev.1),* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | | | | | *distinction is made of DEC without significant fuel degradation for not giving credit to the mitigation.* |
| France-4 | 3.56 point 6 | 6) ~~In-vessel and ex-vessel re-criticality after core melting~~. | Point 6 is not related to practical elimination and demonstration could be challenging. If it is relevant for a very specific kind of reactor, it has to be specified only in a footnote for example and the kind of reactor should be quoted | X | | | |
| Russia-4 | 3.57 Line 2 | Rewrite the first sentence as follows: “Consequences of event sequences that may be considered to have been “practically eliminated” are not part of the deterministic safety analysis if they are physically impossible. Those low likelihood “practically eliminated” event sequences which are physically possible are subject for deterministic analysis with the only objective to justify operator actions and accident management strategy”. | Even for low likelihood “practically eliminated” sequences of events personnel shall know how to accomplish accident management and therefore such sequences of events are subject to deterministic analysis. | | | X | *Appropriate operator actions and accident management strategies may be a component of the practical elimination. The para indicates that once the practical elimination is demonstrated, consequences are not to be determined, since it is clear that it would mean that the NPP has been already destroyed.* |
| **Section 4** | | | | | | | |
| | | | | | | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| **Section 5** | | | | | | | |
| Canada-3 | 5.5 item (b) | (b) The users (or their supervisors) are sufficiently experienced in the use of the code and appropriately understand its uses and limitations for the application case (e.g. loss of coolant accident); | The reason given for rejecting Canada [38] to add "*or their supervisors*" is inadequate:<br>"*A new analyst should be experienced by training before being involved into analysis work.*"<br>But training is in 5.5 (a) so "experience" in 5.5 (b) presumably means hands-on experience of using the code to develop a safety case. If an analyst must already have this experience before working on a safety case, then it is impossible to introduce new analysts.<br>*[Note by Technical Officer: Canada-38 is the comment made about 5.5 in the previous step]* | X | | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| Canada-4 | 5.9<br>line 3 | 5.9. To minimize human errors in code development, only properly qualified or supervised personnel should be involved in the development, verification and validation of the code. Similarly, in user organizations, only suitably qualified or supervised personnel should use the code. | Same as the resolution of Canada [38], if only experienced analysts are allowed to perform analysis, it is impossible to employ a new analyst.<br>Note that supervision is accepted in the first sentence. It should also be accepted in the second.<br>Please reconsider this resolution.<br>*[Note by Technical Officer: Canada-38 is the comment made about 5.5 in the previous step]* | X | | | |
| Finland-1 | 5.25 | The validation should ideally include comparisons of code outputs with four different types of test:<br>(1) Basic tests. Basic tests are simple test cases that may not be directly related to a nuclear power plant. These tests may have analytical solutions or may use correlations or data derived from experiments;<br>(2) Separate effect tests. Separate effect tests address specific phenomena that may occur at a nuclear power plant but do not address other phenomena that may occur at the same time. Separate effect tests should ideally be performed at full scale. If not, appropriate attention should be | The code to code validations should be limited to rare cased where there is no means to acquire appropriate test data. | X | *Last para. will be modified as follows:*<br><br>"The validation against test data is the primary means of validation. However, in cases where no means to achieve appropriate data for validation are available ~~F~~for (2), (3) and (4) above, ~~in the absence of relevant experimental data~~ it is possible to enhance confidence on results by means of code to code comparison or | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment Nr | Para / Line Nr. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | paid to possible scaling effects (see paras 5.29 to 5.31);<br>(3) Integral effect tests. Integral tests are test cases that are directly related to a nuclear power plant. All or most of the relevant physical processes are represented. However, these tests may be carried out at a reduced scale, may use substitute materials or may be performed at different boundary conditions;<br>(4) Nuclear power plant level tests and operational transients. Nuclear power plant level tests are performed on an actual nuclear power plant, for example during the commissioning phase. Validation through operational transients together with nuclear power plant tests are important means of qualifying the plant model.<br>The validation against test data is the primary means of validation. However in cases where is no means to achieve appropriate data for validation ~~F~~for (2), (3) and (4) above, ~~in the absence of relevant experimental data~~ it is possible to enhance confidence on results by means of code to code comparison or bounding engineering judgement, to cover deficiencies in the full validation. The approach and the use of the code should be well justified. | | | bounding engineering judgement, to cover deficiencies in the full validation. The approach and the use of the code should be justified.” | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | **Section 6** | | | | |
| ENISS-9 (Observer) | 6.20 | | This requirement appears redundant with 3.7 and may be suppressed. | | | X | There are differences between 3.7 and 6.20, mainly related to PIE assumed conditions |
| | | | **Section 7** | | | | |
| Canada-5 | 7.30 | 7.30. For conservative analysis of anticipated operational occurrences the technical acceptance criteria related to fuel integrity and radiological acceptance criteria should, in principle, be the same as presented above for realistic analysis ~~of anticipated operational occurrences~~ design basis accidents. | Using the same acceptance criteria in conservative AOO analyses as in realistic AOO analysis is overly conservative. | | | X | *Demonstration of fuel clad integrity is strictly required in AOO [only]. If it is achieved based on non-classified means (as authorized in realistic analysis), it means that there would be no requirement to design any classified protection aiming at ensuring fuel clad integrity (1st barrier).* |
| Canada-6 | 7.37<br><br>First and last sentences | 7.37. For conservative safety analysis, credit should not be taken for operator diagnosis of the event and for starting the actions until after a conservative delay time. The corresponding timing claimed should be justified and validated for specific reactor design; for example earlier than in 15 minutes if performed in the control room, or 30 minutes for ~~the~~ field actions<br><br>*[Note from Technical Officer: This* | First sentence is incomplete. As currently worded, no credit may be taken for operator action <u>ever</u>.<br><br>Final sentence, editorial. Delete “the”. | | *[This comment is treated together with ENISS-10 and this resolution covers both].*<br><br>*Paragraph 7.37 will be modified as follows:*<br>“7.37. For conservative safety analysis, credit | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| Comment Nr | Para / Line Nr. | Proposed new text | Reason | Accepted | Accepted, but modified as follows | Rejected | Reason for modification/rejection |
| | | *comment seems not to use the last version of para. 7.37, which is provided below]:*<br><br>*7* .37. For conservative safety analysis, credit should not be taken for operator diagnosis of the event and for initiating the necessary actions until after a conservative delay time. | | | should not be taken for operator diagnosis of the event and for starting the actions until after a conservative specified time. The corresponding timing claimed should be justified and validated for specific reactor design; for example, the minimal specified time may be ~~earlier than in~~ 30 minutes ~~if performed in the~~ for control room actions, or 60 minutes for ~~the~~ field actions." | | |
| ENISS-10 (Observer) | 7.37 | 7.37. For conservative safety analysis, credit should not be taken for operator diagnosis of the event and for initiating the necessary actions before a minimal time delay following the initiating event. The corresponding timing claimed should be justified and validated for specific reactor design; for example, the minimal time delay may be ~~earlier than in~~ 30 minutes if the action is performed ~~in~~ from the control room, or 60 minutes for the field actions. | Editorial proposal. Meaning is kept unchanged whilst clarifying. | | *Suggested changes were considered together with those made in Canada-6 (See the common Resolution in Canada 6)* | | |
| Canada-7 | 7.45 | No change to SSG-2 suggested.<br><br>NUSSC should note this problem and | Canada recognizes that SSG-2 must use the plant terminology | n/a | *n/a* | n/a | n/a |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | address it in the next revision of SSR-2/1. | defined in SSR-2/1 so we do not expect a change to SSG-2. However, we would like to repeat that classification of plant states based on <u>outcome</u> is illogical. It effectively sets a criterion, "*DEC without fuel melting shall not result in fuel melting*" which is clearly circular. | | | | |
| UK comment to para. 7.49.<br>- First raw is reminding the comment made in December 2016 (in that moment it was para. 7.55) and the resolution provided with an observation (see below "Former UK-18").<br>- The raw after is a new formulation of the comment/proposal (see below "new UK-18" and the interpretation of the comment) | | | | | | | |
| ["Former"] UK-18<br><br>*[UK comment from previous step]* | 7.55 Line 2<br><br>*[Former para. 7.55, became 7.49 after MS changes]* | *Change final sentence to*<br>"…Furthermore, unavailability of a system or component due to maintenance may ~~does~~ not need to be considered" | In the UK our initial expectation would be that a diverse safety system would remain operable during a plant maintenance condition on a single train of the system since this is a planned state that will definitely be entered into. In exceptional circumstances it might be possible to argue that it is not reasonably practicable to ensure availability during the maintenance condition but this would need to be demonstrated. For example it is quite easy to incorporate redundancy into a C&I system during the design phase for a | | | *Resolution provided:*<br>X | *Resolution provided: "Current formulation seems adequate. The aim of DEC-A analysis is not necessarily to cover any possible initial plant state as they are meant to prove that core melt frequency is acceptably low."*<br><br>*[New observation:]* "UK wants this decision to be reconsidered. The aim of DEC-A should be to ensure that the risk of core melt is reduced as low as reasonably |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | new power plant. | | | | practicable." |
| [New UK-18] | [Written:] 7.48 line 1<br><br>*Note: The comment refers to 7.49* | [Written]:<br>Change:<br>"*For design extension conditions without significant fuel degradation, the single failure criterion does not need to be applied. Furthermore, unavailability of a system or component due to maintenance does not need to be considered"*<br>To:<br>*"For design extension conditions without significant fuel degradation, the analysis should make reasonable assumptions about the availability of safety systems. However, the single failure criterion does not need to be applied to low-frequency fault sequences. Furthermore, unavailability of a system or component due to maintenance may not need to be considered"*<br><br>(See below)<br><br>*Interpretation of the proposal:*<br>7.49. For design extension conditions without significant fuel degradation, the analysis should make reasonable assumptions about the availability of safety systems. However, the single failure | In the UK we take a risk-informed view.<br><br>Experience suggests that it is not prudent to design protection systems on the assumption that they will free from defects and fully available:<br><br>In the UK alone, we have approximately 300 reportable events per year where maintenance errors compromise safety systems or induce faults.<br><br>As written, this will lead to bad design.<br><br>Some of the complex events listed as design extension events are really rather frequent (approaching AAOs). It would not be acceptable to omit adequate protection of these events in maintenance states. | | | X | *The proposal seems confusing. DEC analysis doesn't consider safety systems. This para has been generally accepted.* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | criterion does not need to be applied to low-frequency fault sequences. Furthermore, unavailability of ~~safety features for this category of design extension conditions~~ a system or component due to maintenance does not need to be considered | | | | | |
| [UK-22] | 7.51 | *7.51. Non-permanent equipment should not be considered for demonstration of adequacy of the nuclear power plant design*<br><br>Propose to append:<br><br>*although it may be used to justify maintenance operations.* | | | | X | |
| Canada-8 | 7.63 First sentence | 7.63. For design extension conditions with core melting, the single failure criterion does not need to be applied. … | Editorial. Add "the". | X | | | |
| France-5 | 7.63 | For design extension conditions with core melting, single failure criterion does not need to be applied. Furthermore, unavailability of a system or component due to maintenance does not need to be considered in the deterministic safety analysis. Appropriate rules for testing and maintenance of system or component needed for design extension conditions shall be defined to guaranty their availability. | It is important to remind that, even if the single failure criteria is not applied, the availability of DEC SSCs shall be high. | X | *Last sentence will be modified as follows:*<br>"… due to maintenance does not need to be considered in the deterministic safety analysis. Appropriate rules for testing and maintenance of systems or components needed for design extension conditions should be | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | | | defined to ensure their availability | | |
| France-6 | 7.64 | 7.64. Non-permanent equipment should not be considered for demonstration of adequacy of the nuclear power plant design. For some design extension conditions, ~~S~~such equipment may be ~~is typically~~ considered to operate for long-term sequence and may be ~~is~~ considered available in accordance with the emergency operating procedures or accident management guidelines. The time claimed for availability of non-permanent equipment should be justified. | 7.64 is not clear on the meaning of "nuclear power design". | | *Paragraph 7.64 will be modified as follows:*<br>7.64. Non-permanent equipment should not be considered for demonstration of adequacy of the nuclear power plant design. For some design extension conditions, ~~S~~such equipment is typically considered to operate for long-term sequence and is considered available …" | | |
| France-8 | 7.70 | 7.70. Demonstration of 'practical elimination' of the possibility of certain conditions arising should include, where appropriate, the following steps:<br>• Identification of undesired conditions (challenges) potentially endangering the containment integrity or by-passing the containment, resulting in an early radioactive release or a large radioactive release;<br>• ~~Challenges should be addressed by implementing design and operational provisions in order to 'practically eliminate' the possibility of those conditions arising;~~ | Step2 : If challenges are addressed the situations are not practically eliminated (e.g. if the loads following a steam explosion are addressed implementing design provisions, this accidental conditions does not need anymore to be practically eliminated). The previous formulation is much more clear: (Challenges should be addressed; in case this is not possible, design and operational provisions should be implemented in order to | | *Paragraph 7.70 will be modified as follows:*<br>7.70. Demonstration of 'practical elimination' of the possibility of certain conditions arising should include, where appropriate, the following steps:<br>• *[1st bullet: No changes];*<br>• *[2nd bullet will be deleted and replaced by]:* | | |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | • Challenges should be addressed; in case this is not possible, design and operational provisions should be implemented in order to 'practically eliminate' the possibility of those conditions arising;<br>• ~~Sensitivity studies to provide assurance that sufficient margins exist to address uncertainties regarding the demonstration with high level confidence that the possibility of the referred conditions has been 'practically eliminated';~~<br>• Final confirmation of the adequacy of the provisions by deterministic safety analysis, complemented by probabilistic safety assessment and engineering judgment. | 'practically eliminate' the possibility of those conditions arising;)<br><br>Step 3: during the identification phase, the "threshold values" which should not be exceeded to avoid cliff-edge effects are identified (e.g. the value of the reactivity insertion which can lead to prompt criticality). Once these values are determined, the reactor is designed such to guarantee those margins. Here the object of the sensitivity studies is not understandable here.<br>Clarification is necessary or consider full deletion | | Implementation of design and operational provisions in order to 'practically eliminate' the possibility of those conditions arising; the design of those provisions should include sufficient margins to cope with uncertainties;<br>• *[Existing 3rd bullet: to be deleted];*<br>• *[4th bullet: No changes].* | | |
| Russia-5 | Section 7 | Add new subsection "DETERMINISTIC SAFETY ANALYSIS FOR JUSTIFICATION OF THE OPERATOR ACTIONS" | To supplement section 7 with special subsection, containing recommendations about implementation of realistic analyses for justification of the operator actions. This subsection has to reflect the same issues, as other subsections of this | | | X | *See resolution to Russia-2 about para. 2.1* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | | section, namely:<br>• Specific objectives of the analysis.<br>• Acceptance criteria.<br>• Availability of systems.<br>• Operator actions.<br>• Analysis assumptions and treatment of uncertainties<br>(see also our proposal to supplement p.2.1). | | | | |
| **Section 8** | | | | | | | |
| | | | | | | | |
| **Section 9** | | | | | | | |
| | | | | | | | |
| **Annex** | | | | | | | |
| France-7 | A-28 | A-28 Deterministic safety analysis has an important role in support of the probabilistic safety assessment by determining so called success criteria. Deterministic safety analysis is typically used to identify challenges to the integrity of the physical barriers, to determine the | | X | *Last sentence will be modified as follows:*<br><br>"…The deterministic analysis is to be performed in a realistic way ~~but~~ | | "Shall/should" *sentences are not used in Annex* |

| COMMENTS BY REVIEWER | | | | RESOLUTION | | | |
|---|---|---|---|---|---|---|---|
| **Comment Nr** | **Para / Line Nr.** | **Proposed new text** | **Reason** | **Accepted** | **Accepted, but modified as follows** | **Rejected** | **Reason for modification/rejection** |
| | | failure mode of a barrier when challenged and to determine whether an accident scenario may challenge several barriers. By means of the analysis it is to be determined whether an event sequence, for various combinations of equipment failures and human errors, can prevent nuclear fuel degradation. The deterministic analysis is to be performed in a realistic way but uncertainties shall be quantified where needed | For PSA, the preferred approach should be "realistic" + "uncertainties". If uncertainties are high, the PSA results are not meaningful. | | although uncertainties are ~~shall be~~ quantified where it is necessary ~~needed~~ | | |
| | | | | | | | |