DS414, Safety of Nuclear Power Plants: Design, 03 April 2009 Draft

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 1 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	1.2	[Modify this paragraph as follows] It is now recognized that the designs of many existing nuclear power plants, as well as the design bases of many new plants have been extended to include additional measures to mitigate the consequences of more complex sequences involving multiple failures, and some severe accidents. Complementary systems and capabilities have been added to many existing plants to aid in severe accident prevention and mitigation. Most existing nuclear power plants have implemented severe accident mitigation guidance. The design of new nuclear power plants in Generation III and Generation III+ explicitly include consideration of severe accident scenarios in design.	§1.2 states, "*It is now recognised that the design bases of many new plants have been extended to include additional measures to mitigate the consequences of more complex sequences involving multiple failures, and some severe accidents.*" This is not only the case with many new plants. Many existing plants have been backfitted to cope with severe accidents to one degree or another with complementary systems aimed at severe accident prevention and mitigation, and nearly all plants have implemented symptom-oriented EOPs and severe accident management (SAM) procedures or guidelines. New plants in Generation III and III+ are explicitly designed for severe accidents in an effort to prevent containment bypass and containment failure. In Europe, most PWRs have been backfitted with hydrogen management systems based on severe accident hydrogen production rates, backfitted with filtered containment venting systems, and backfitted with bunkered emergency systems.		Reference to Gen III deleted.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 2 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
2	1.3	[Modify the text of §1.3 as follows] When considering ~~both old and new~~ existing nuclear power plants it ~~is~~ may be convenient to continue to maintain the distinction between design basis, which includes all planned normal operational modes of the plant and design basis accidents, and beyond design basis events that include severe accidents. For nuclear power plants of Generation III and Generation III+, such a distinction may be less useful since such designs explicitly incorporate severe accidents within the plant design basis. Under such circumstances, it may be counterproductive to try to distinguish between design basis accidents and accidents beyond the design basis.	§1.3 states, "*When considering both old and new plants it is convenient to continue to maintain the distinction between design basis, which includes all planned normal operational modes of the plant and design basis accidents, and beyond design basis events that include severe accidents.*" In fact, it is not convenient at all for Generation III and Generation III+ designs which explicitly include severe accidents within the design basis. The design of these plants incorporates features explicitly for attempting to avoid or control accident progression to avert containment bypass or failure. With these plants, it is counterproductive to try to distinguish between DBAs and BDBAs.		Amended to remove reference to Gen III		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 3 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
3	1.3	[Modify the text of §1.3 as follows] It is accepted that it may not be reasonably practicable to apply all the requirements of this new publication to existing designs that are already in operation. For such designs, it is expected that a comparison will be made against the latest or current standards as part of the periodic safety review of the plant to determine whether any reasonably practicable safety improvements can be implemented. For existing plants without a periodic safety review process, there should nonetheless be a process in place within the safety organization to periodically examine whether there are any such safety improvements that can be implemented. This is in keeping with the "high standard of safety" set forth in SF-1 (Ref. 1).	§1.3 also states, "*It is accepted that it may not be reasonably practicable to apply all the requirements of this new publication to existing designs that are already in operation. For such designs, it is expected that a comparison will be made against the latest or current standards as part of the periodic safety review of the plant to determine whether any reasonably practicable safety improvements can be implemented.*" It has to be recognized that not nearly all reactors are covered by PSRs. Certainly the 104 NPPs in the United States are not covered by PSRs, and there are probably some other countries that don't require PSRs (e.g. Russian Federation). For plants not covered by a PSR, this standard recommends nothing – why?		Final sentence not required.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 4 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
4	1.5	[Modify Para. 1.5 as follows] This publication is intended for use by organizations designing, manufacturing, constructing, ~~and~~ operating, modifying, maintaining, analyzing, verifying, and reviewing nuclear power plants, as well as by regulatory bodies	§1.5 states, "*This publication is intended for use by organizations designing, manufacturing, constructing and operating nuclear power plants as well as by regulatory bodies.*" This list should also include those organizations engaged in maintaining, modifying, analyzing, verifying, reviewing, etc. nuclear power plants. The Paks fuel damage event is a good example of why this should be the case.			Y	The intent of this is covered by the concept of 'Design Entity'.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 5 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
5	1.7	Delete the first bullet under §1.7.	§1.7 states that this publication does not address requirements that are specifically covered by other publications in the new IAEA Safety Series documents. This is not correct. Indeed, NS-R-1 is the over-arching nuclear power plant safety requirements document – it must *by definition* cover these requirements, even if not in detail. Lower echelon documents can elaborate on how to meet the requirements, but Safety Guides cannot *by definition* establish requirements themselves. This must be done by NS-R-1.			Y	Clarification added that other 'requirements' documents are intended.

DS414, Safety of Nuclear Power Plants: Design, 03 April 2009 Draft

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 6 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
6	1.7	Modify the last bullet under §1.7 to refer to the IAEA Nuclear Security Series publications.	Since NS-R-1 does not cover security requirements, it should then refer to the documents that do cover such requirements instead of leaving the reader or user of the standard in the dark.	Y			

COMMENTS BY REVIEWER Reviewer: Steven C. Sholly Page 7 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
7	2.1	[Combine §2.1 and §2.2 as follows] The Fundamental Safety Principles publication [1] establishes the findamental safety objective and ten principles. The fundamental safety objective and the ten principles have to be met without unduly limiting the operation of facilities or the conduct of activities that give risk to radiation risks. Facilities and activities that give risk to radiation risks must yield an overall benefit, and protection must be optimized to provide the highest level of safety that can reasonably be achieved. To ensure that facilities are operated and activities conducted so as to achieve the higehst standards of safety that can reasonably be achieved, measures have to be taken: (a) To control the radiation exposure of people and the release of radioactive material to the environment; (b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation; and (c) To mitigate the consequences of such events if they were to occur.	The principle that facilities and activities must yield an overall benefit, and that protection must be optimized to provide the highest level of safety that can reasonably be achieved are essential and should not be left unstated here. These are the reasons why measures have to be undertaken. If these statements are not to be included, the reader should simply be referred to SF-1 instead of the heavily abridged version contained in the draft.		The fundamental safety objective and the ten principles have to be achieved without unduly….. 3rd proposed sentence is not necessary since the reader is already referred to the SF-1 document.		

Comment [NN1]: Au7 amended

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 8 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
8	2.9	[Modify the first sentence of §2.9 as follows] To achieve safety in design of the plant, it is necessary to achieve the highest level of safety that can reasonably be achieved ~~take all reasonably practicable measures~~ to prevent accidents having harmful consequences resulting from loss of control over the reactor core and other sources of radiation, and to mitigate their consequences should they occur; …	§2.9 states, "*To achieve safety in design of the plant, it is necessary to take all reasonably practicable measures to prevent accidents … and to mitigate their consequences …*". But this is not what SF-1 says. Principle 5 states, "*Protection must be optimized to provide the highest level of safety that can reasonably be achieved.*" It doesn't say "reasonably practicable", and a requirements documents should not be reinterpreting SF-1. In addition, the phrase "reasonably practicable" is not defined in the IAEA Safety Glossary, and this means it can be interpreted to mean whatever the user wants it to mean. NS-R-1 should repeat the precise language of SF-1 or reference it – it should not be interpreting it in such a way as to lead to a lower standard of safety. The phrase "reasonably practicable" is not in SF-1, and it cannot appear here.		To achieve the highest level of safety that can reasonably be achieved in the design of the plant, it is necessary to take measures to prevent…..		

Comment [NN2]: Au 8

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 9 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
9	2.9 2.10 2.12 2.15 4.5 4.8 5.6 5.12	Replace all occurrences of the phrases "*very low probability*" (§2.9, §5.6), "*extremely low*" (§2.10), "*very low probability (likelihood) of occurrence*" (§2.12), "*very low probability of occurrence*" (§2.15, §4.8)with the phrase "less than 10^{-7} per year". Replace the phrase "*likely to occur during the service lifetime of the nuclear power plant*" (§4.5) with the phrase "having an estimated mean frequency of 10^{-2} per year or higher". Replace the word "*credible*" (§5.12) by the phrase "*having an estimated mean frequency of occurrence of at least 10^{-6} per year, provided that failure of safety systems in response to the initiating event results in a severe accident scenario frequency of less than 10^{-7} per year.* " [This is consistent with the 10^{-7} per year standard above.]	This is the first example in this document of a statement (and related statements) that appear periodically throughout the document. If IAEA wants to use phrases like "*very low probability*" (§2.9, §5.6), "*extremely low*" (§2.10), "*very low probability (likelihood) of occurrence*" (§2.12), "*very low probability of occurrence*" (§2.15, §4.8), "*likely to occur during the service lifetime of the nuclear power plant*" (§4.5), and "*credible*" (§5.12). These terms and expressions are not defined in the IAEA Safety Glossary, so they need to be defined here. If IAEA can't say quantitatively what it means by such terms and phrases in 2009, then it has no business using them. Undefined, these terms can be chosen by the user to mean whatever they want them to mean, and are therefore essentially useless in a standard since they require a value judgment from the user that inherently varies from user to user (depending on their degree of risk aversity, their familiarity with probabilistic concepts, and their notion of			Y	It is not IAEA policy to include numerical targets.

			what is "low").				

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 10 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
10	2.11	The Secretariat needs to define robustness, preferably quantitatively. Robustness without a definition is not acceptable in a safety standard.	§2.11 uses the word "*robustness*". Neither "robust" nor "robustness" are defined in the IAEA Safety Glossary. Robust in what manner? To what extent? Based on comparison with what standard? Does "robustness" mean a 10^{-3} conditional failure probability per challenge? Or 10^{-4}, 10^{-5}, 10^{-6}, 10^{-7}, or some other value? The word "robustness" as used here has no meaning, and can therefore be interpreted by the IAEA or a safety authority or a nuclear facility operator to mean whatever they want it to mean. Such semantically null words and phrases have no place in a nuclear safety standard – most especially in a requirements document.			Y	This section is explanatory background.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 11 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
11	2.12	[Reword the 2nd and 3rd sentences of §2.12 as follows] Measures are therefore taken to ensure that the radiological consequences are mitigated. Such measures include: engineered safety features; on-site accident management procedures established by the operating organization; <u>complementary measures and accident management (Level 4 of defense-in-depth) [4 and INSAG-12];</u> and possibly off-site intervention measures established by appropriate authorities in order to mitigate radiation exposure if an accident has occurred.	§2.12 discusses measures taken to ensure that the radiological consequences of accidents are mitigated. There is no mention here of "complementary measures" which are part of Level 4 of defense-in-depth (INSAG-10, INSAG-12). Note that complementary measures are more than just accident management, since INSAG-10 and INSAG-12 distinguish the two terms, referring to "complementary measures and accident management" (see INSAG-10, page 6; and INSAG-12, pages 18 & 86).		….features; complementary measures; and accident management.…		

COMMENTS BY REVIEWER Reviewer: Steven C. Sholly Page 12 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
12	2.16 3.19	[Revise the 3rd sentence of §2.16 as follows] For a nuclear power plant this will be the plant owner or the plant operating organization (if different from, and contracted to the plant owner). [Revise 3.19 accordingly]	§2.16 (§3.19 is similar) states, "*The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks. For a nuclear power plant this will be the operating organization.*" This is not necessarily true – the holder of the operating license has primary responsibility, whether the holder of the license is the owner or an organization contracted by the owner to operate the facility. The responsible organization is the one holding the operating authorization from the regulatory authority.		2.16 revised to read "….be the plant owner or the plant operating organization if different from and contracted to the plant owner." No change proposed to 3.19.		

Comment [NN3]: Au12

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 13 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
13	3.5	[Reword §3.5 as follows] The design for a nuclear power plant shall ensure that the structures, systems and components important to safety have the appropriate characteristics, specifications and material composition so that the safety functions can be performed and the plant can operate safely with the required reliability for the full duration of its design life, ~~with accident prevention and protection of site personnel, the public and the environment as prime objectives.~~in accordance with the Fundamental Safety Objective [1].	§3.5 attempts to restate the principal safety objective of SF-1. It cannot by definition do this. Instead, it should refer directly to the appropriate sections of SF-1. It is not appropriate for a requirements document to try to redefine the principal safety objective – that objective is fully stated and explained in SF-1.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 14 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
14		[Reword the first sentence of §3.6 as follows] The design ensures that the requirements of the owner and the operating organization, the requirements of the regulatory authority, and the requirements of national nuclear safety legislation (as well as applicable national and international standards) are met and that due account is taken of the human capabilities and limitations.	§3.6 states, "*The design ensures that the requirements of the operating organization are met and that due account is taken of the human capabilities and limitations*." The design should also ensure that the requirements of the regulatory authority, the requirements of nuclear legislation and rules, and the applicable national and international standards are met. Further, the operating organization may not be the same organization that owns and is responsible for the design of the plant.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 15 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
15	3.7	Delete the word "operational" from the text of §3.7.	§3.7 states, "*The design takes due account of relevant operational experience that has been gained in operating plants and of the results of relevant research programmes.*" The word "operational" can be deleted without losing the meaning. Operational and experience in "operating plants" is redundant.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 16 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
16		[Reword §3.11 as follows] SSCs important to safety are preferably of a design proven in previous equivalent applications, and are selected to be ~~consistent with the plant reliability target of the systems.~~consistent with the Fundamental Safety Objective and Principle 5 in that protection must be optimized to provide the highest level of safety that can reasonably be achieved [1].	§3.11 states, "*SSCs important to safety are preferably of a design proven in previous equivalent applications, and are selected to be consistent with the plant reliability target of the systems.*" Why not choose a design that is better than the reliability target if it is available? Why simply fall back on a more-or-less arbitrary reliability target if a better alternative is reasonably available? The statement as written encourages mediocrity, not the "highest level of safety that an reasonably be achieved" (SF-1, Principle 5, "Optimization of Protection").	Y			

COMMENTS BY REVIEWER Reviewer: Steven C. Sholly Page 17 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
17	3.16	[Reword the first sentence of §3.16 as follows] "~~A c~~Comprehensive deterministic and probabilistic safety assesments shall be carried out …"	§3.16 refers only to a "comprehensive safety assessment". It should refer to both deterministic and probabilistic assessments as these two types of assessments are complementary.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 18 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
18	3.22	[Reword the 6th bullet of §3.22 as follows] • the safety impact of ~~individual~~ design changes~~, or multiple changes that may have significant interdependencies,~~ have been properly assessed and understood (both individually and collectively by deterministic and probabalistic means) and …	§3.22, 6th bullet, states, "The formally designated entity ensures that … the safety impact of individual design chagnes, or multiple changes that may have significant interdependencies, have been properly assessed and understood". The cumulative effect of design changes has to be properly assessed and understood. It is not enough to assess design changes in isolation or in selected groups. The assessor cannot be certain that earlier aggregated evaluations have properly considered subsequent design changes. A cumulative assessment is a must, both deterministically and probabilistically.		Reference to probabilistic, etc not needed.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 19 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
19	3.22	Insert the word "all" at the beginning of the 7th bullet of §3.22	There should be no doubt that this requirement refers to <u>all</u> design changes.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 20 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
20	Following 4.4	The numbering of the paragraphs is erroneous in the draft. The numbering goes from 4.1 to 4.4, and then starts over again at 4.1 under "Requirements for Defence in Depth". The numbering should be sequential.	One cannot have two different paragraphs with the same number.	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 21 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
21	4.4	[Reword §4.4 as follows] Monitoring of plant status is provided to ensure that the required safety functions are achieved, and to ensure that in the event of their actuation in the course of accident management, complementary functions are achieved as well.	§4.4 states, "*Monitoring of plant status is provided to ensure that the required safety functions are achieved.*" Monitoring is also provided to ensure that in the event of their actuation in the course of accident management, complementary fuctions are achieved as well.		, and that in the event of their actuation in the course of accident management, complementary functions are also achieved.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 22 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
22	4.3 (which should be 4.7; see Comment Nr. 20, above)	[Reword the 2nd bullet under §4.3, which should be 4.7, as follows] The design therefore … is conservative, and the construction is of high quality, so as to provide confidence that plant failures and deviations from normal operations are minimized; accidents are prevented as far as practicable; ~~and~~that the activation of safety systems is minimized; and that there are no cliff-edge effects introduced into plant response to accidents.	§4.3 (which should be 4.7), 2nd bullet, states, "*The design therefore … is conservative, and the construction is of high quality, so as to provide confidence that plant failures and deviations from normal operations are minimized; accidents are prevented as far as practicable; and the activation of safety systems is minimized.*" The design also has to assure that there are no cliff-edge effects. This phrase is defined in the IAEA Safety Glossary.	Y			

COMMENTS BY REVIEWER Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 23 of 43 Date: 29 May	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
23	4.4 (Which should be 4.8, see Comment Nr. 20, above)	[Reword §4.4, which should be 4.8, as follows] To ensure that the overall safety concept of defence in depth is maintained, the design is such as to prevent as far as practicable challenges to the integrity of physical barriers, failure of a barrier when challenged, and failure of a barrier as a consequence of failure of another barrier. Insofar as light water cooled and moderated reactors are concerned, it has to be noted that the occurrence of unmitigated severe core damage can simultaneously or nearly simultaneously challenge multiple physical barriers (the integrity of ceramic fuel pellets, the integrity of fuel cladding, the integrity of the reactor pressure vessel, and the integrity of the containment).	§4.4 (which should be 4.8) states, "*To ensure that the overall safety concept of defence in depth is maintained, the design is such as to prevent as far as practicable challenges to the integrity of physical barriers, failure of a barrier when challenged, and failure of a barrier as a consequence of failure of another barrier.*" While this is correct, for LWRs it has to be noted that severe core damage can simultaneously or nearly simultaneously challenge multiple physical barriers (the integrity of ceramic fuel pellets, the integrity of fuel cladding, the integrity of the RPV, and the integrity of the containment. This is one of the key lessons of the TMI-2 and Chornobyl-4 severe accidents, as well as various experiments conducted since then.		Added to 2nd bullet: '…….failure of one or more barriers when challenged;'		

Comment [NN4]: Au 23 amended.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 24 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
24	5.3	[Add the following sentence to the end of §5.3] The means of addressing and quantifying uncertainties must also be included in the design basis.	§5.3 states, "*The design basis includes specification for normal operation, plant states rsulting from the postulated initiating events (PIEs), the safety classification, reliability, important assumptions,and the particular methods of analysis*." What about uncertainties – how are they addressed and quantified? How are uncertainties dealt with in the design?		'is', not 'must'.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 25 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
25	5.11	[Reword §5.11 as follows] The PIEs include all credible failures of plant systems, structures and components; human errors during operation; and internal and external initiated events. The PIEs should also include human errors during shutdown and refueling modes, as well as human errors during testing, surveillance, maintenance, and modifications irrespective of operating mode at which these activities take place.	§5.11 states, "*The PIEs include all credible failures of plant systems, structures and components; human errors during operation; and internal and external initiated events.*" This should also include human errors during shutdown and refueling. It should also include human errors during testing, maintenance, and modifications irrespective of whether these activities take place during operation or not.	Y	See revised text.		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 26 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
26	5.15	[Add the followng to the end of §5.15] A cumulative probabilistic assessment of all such exclusions shall be made to ensure that they do not collectively contribute significantly to the frequency of severe accidents and their consequences. A bounding analysis using conservative assumptions will probably suffice for most such exclusions, and where this is not the case a more detailed analysis is required.	§5.15 states, "A justification shall be provided for the exclusion of any rare initiating events, sequences or situations for which it is not realistic to set up provisions for the management of their consequences." To this should be added, "A cumulative probabilistic assessment of all such exclusions shall be made to ensure that they do not collectively contribute significantly to the frequency of severe accidents and their consequences. A bounding analysis using conservative assumptions will probably suffice for most such exclusions, and where this is not the case a more detailed analysis is required."			Y	PSA is addressed by GS-R-4

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 27 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
27		[Reword §5.23 as follows] Where prompt action (within 30 minutes or less) in response to a PIE is not necessary, manual initation of systems or other operator actions is permitted. This is acceptable if the time interval between the detection of the abnormal event and the required action is large enough and adequate procedures (such as administrative, operational and emergency procedures) are defined to ensure the reliability of such actions. Further, the instrumentation required to alert the operators to the need for the manual action must be reliable. Where such manual actions are planned, they should be periodically practiced on the plant simulator to ensure that plant design and procedural changes do not invalidate the conclusion that the manual actions are acceptable.	§5.23 states, "*Where prompt action in response to a PIE is not necessary, manual initation of systems or other operator actions is permitted. This is acceptable if the time interval between the detection of the abnormal event and the required action is large enough and adequate procedures (such as administrative, operational and emergency procedures) are defined to ensure the reliability of such actions.*" How large a time interval is "large enough" – is it 5 minutes, 10, 20, 30, 60 or what? Moreover, it is not enough to conclude that sufficient time is available and whether procedures exist. Where are the instruments that let the operators know the action is needed – are the instruments visible from normal working stations? What is the reliability of these instruments? What about uncertainties? What about time of day considerations? What about task loading – suppose the need arises during a complex sequence of events where the operators are heavily task loaded?			Y	1) Specific numerical targets are not included in a requirements document. 2) 2nd proposal is more appropriate for a guidance document.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 28 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
28	5.28	[Reword §5.28 as follows] Severe accident sequences for which it is not reasonably practicable to implement mitigatory measures ~~are~~<u>can be</u> excluded from the design basis with proper justification.<u> Where such scenarios are excluded from the design basis, a cumulative probabilistic analysis should be performed to demonstrate that these scenarios are not significant contributors to the frequency of severe accidents or to risk.</u>	§5.28 states, "*Severe accident sequences for which it is not reasonably practicable to implement mitigatory measures are excluded from the design basis with proper justification.*" Should read "can be", not "are excluded". In Generation III and III+ designs, they are not excluded – rather, all severe accidents are considered explicitly both deterministically and probabilistically in the design. Where severe accidents are excluded, there should be a cumulative probabilistic justification to demonstrate that in total these scenarios are not significant contributors to CDF or to risk.			Y	Assessment issue appropriate to GS-R-4.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 29 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
29	5.31	No proposed change; comment only.	§5.31 states, "*All internal and external hazards that have the potential to directly or indirectly affect the safety of the plant shall be identified and used as events that could lead to postulated initiating events to be considered in the design basis of SSCs. The assessment of the consequences of such event shall also be included in the analysis.*" Does IAEA really, literally mean what this statement says? If so, then, for example, one would have to include as possible PIEs random reactor pressure vessel rupture and propagating steam generator shell rupture for PWRs. In fact, these two possible initiators have been excluded in all PWR safety analyses that I have ever seen (the total running into the dozens).		Noted		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 30 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
30	5.50	[Reword §5.50 as follows] The single failure criterion shall be applied to each safety group incorporated in the plant desgin to perform all actions necessary in response to a particular PIE. The single failure criterion as applied here shall reflect one train out of service for test and maintenance, and a single failure in another train, and yet still provide sufficient redundancy to perform the safety function.	§5.50 states, "*The single failure criterion shall be applied to each safety group incorporated in the plant desgin to perform all actions necessary in response to a particular PIE.*" This is not enough of a description. The single failure criterion should reflect one train out of service for test & maintenance, and a single failure in another train, and yet still be able to perform the safety function. This would exclude a 2-train design. Modern designs (EPR, for example) have 3 or 4 trains for this very reason. And in EPR and AP1000, the trains are physically separated for protection against external hazards like aircraft crash. The description in the text would allow a reverting to 2-train designs. This is not acceptable. Of course, current 2-train plants could not comply with it – but so what? We should not be writing standards for the least common denominator plants.			Y	This is covered by para 5.53

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 31 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
31	5.54	[Reword §5.54 as follows] Compliance with the single failure critieron for all PIEs and DBAs is mandatory.	§5.54 states, "Non-compliance with the single failure criterion is exceptional, and is clearly justified in the safety analysis." Nonsense – non compliance with the single failure criterion is not permitted for PIEs and DBAs at all. Of course, if RPV rupture is included as a DBA, then the single failure criterion either doesn't apply, or you need a second vessel or the vessel needs to be in a cavity that (a) cannot fail even in case of RPV rupture, and (b) contains sufficient fluid to maintain core coverage in case of RPV rupture.			Y	This para is intended to cover very rare PIEs etc for which the SFC is not practical to apply.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 32 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
32	5.82 and 5.83	Delete §5.83.	§5.82 states, "Structures, systems and components important to safety shall not be shared between two or more reactors in nuclear power plants." Fine – except the very next paragraph contradicts this! "In exceptional cases where structures, systems and components important to safety are shared between two or more reactors, it is demonstrated that all safety requirements are met for the all reactors under all operational states (including maintenance) and in design basis accidents." You can't have it both ways – either there is no sharing or there is not. The standard need not be written so that all existing NPPs can comply with it – rather the standard should be forward looking. §5.83 should be deleted.			Y	Para 5.82 & 5.83 have been amended (US comment no 28), since the option for sharing should not be completely dismissed.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 33 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
33	5.87	[Reword §5.87 as follows] The design incorporates appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste. Consideration is given to access to facilities and lifting and packaging capabilities. Travel paths for heavy loads are designed so that they do not pass over safety related SSCs, or the design of the intervening structures is such that heavy load drop from the highest point can be accommodated with sufficient margin to preclude failure.	§5.87 is incomplete as written. "*The design incorporates appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste. Consideration is given to access to facilities and lifting and packaging capabilities.*" What about control of heavy loads (spent fuel casks)? It must be assured that heavy loads are not lifted over safety-related SSCs or that the design of the SSCs is such that it can take the drop of the heaviest load from the highest point of lift.			Y	This is a specific aspect of PIEs that would be covered under the hazard analysis, and in a safety guide. Note also that this para has been moved to follow para 6.103 (Fr comment 58)

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 34 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
34	5.92	[Reword §5.92 as follows] The plant shall be isolated from the surroundings by suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, provision shall be made in the design of the buildings and the layout of the site for personnel and/or equipment for the control of access, and attention shall be paid to guarding against the unauthorized entry of persons and goods to the plant. The goods to be considered shall include explosive, incendiary, and combustible materials, whatever their physical form. In addition, positive control of vehicles is required at a setback distance sufficient to preclude accident initiation by detonation of a vehicle bomb.	§5.92 states, "*The plant shall be isolated from the surroundings by suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, provision shall be made in the design of the buildings and the layout of the site for personnel and/or equipment for the control of access, and attention shall be paid to guarding against the unauthorized entry of persons and goods to the plant.*" This is not enough – "goods" should be expanded to explicitly include fluids, gases, explosives, etc. Control of vehicles is also required to prevent "car bombs".			Y	1) Examples should be covered by the associated guidance document. 2) Security requirements covered by other IAEA documentation.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 35 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
35	5.96	[Reword §5.96 as follows] In the analysis, account is taken not only of physical interconnections, but also of the possible effects of one system's operation, maloperation or failure on the physical environment of other essential systems, in order to ensure that changes in the environment do not affect the reliability of system components in functioning as intended. Effects to be considered shall include seismic, fire, smoke, fire suppression system actuation (whether in response to fire or as a result of spurious actuation or deliberate maloperation). Spatial interactions shall be considered.	§5.96 is incomplete. It should include explicit consideration of common cause failures resulting from the PIEs (seismic, fire, smoke, etc.) and the response to systems to the PIE (including inadvertent actuation, as in fire suppression system actuation). Spatial interactions must also be considered.			Y	Covered by the hazard analysis.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 36 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
36	5.106	[Reword §5.106 as follows] The design takes account of the probabilistic safety analysis of the plant in all modes of operation (e.g., full power, low power, cold shutdown, hot standby, refueling) and under all other plant states (test, surveillance, maintenance evolutions) with particular reference: • To establish that a balanced design has been achieved such that no particular feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety; and • To provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behavior ('cliff edge effects') will be prevented.	§5.106 should specify that the probabilistic analysis takes account of all plant states (normal operation, low power operation, cold shut down, hot standby, refueling, and any other plant state (test, surveillance, and maintenance evolutions, for example).		…..' plant in all modes of operation and plant states, with…'		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 37 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
37	6.3	[Reword §6.3 as follows] The possibility of a recriticality or a reactivity excursion following a PIE is precluded by design.	§6.3 states, "*The possibility of a recriticality or a reactivity excursion following a PIE is minimized.*" It should state that these things should be excluded. Minimization is how we wound up with the RBMK and the Chornobyl-4 accident. There is no reason to accept recriticality or a reactivity excursion in a nuclear power plant design in response to a PIE – this is contrary to SF-1.	Y	The possibility of a recriticality or a reactivity excursion that results in exceeding fuel design limits following a PIE is excluded by design.		

Comment [NN5]: USA 30

Comment [NN6]: Au 37

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 38 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
38	6.18	[Reword §6.18 as follows] Pipework connected to the reactor coolant boundary is equipped with adequate isolation devices to limit any loss of radioactive fluid. At least two isolation devices in series shall be provided, with suitable leak detection provided between these two devices as well as after the last of the devices. Detection of isolation device position or functioning shall be safety-related and highly reliable. The man-machine interface (including alarms, instrumentation, controls, and procedures) shall be such that operator attention is immediately directed to possible symptoms of an interfacing systems LOCA.	§6.18 states, "*Pipework connected to the reactor coolant boundary is equipped with adequate isolation devices to limit any loss of radioactive fluid.*" This should be expanded. The goal is also to suppress the frequency of interfacing systems LOCAs, which are often identified in PSAs as leading contributors to risk for LWRs. At least two isolation devices in series should be used, and there should be safety-related and highly reliable leak detection provided for the space between the isolation devices as well as after the last isolation device. Detection of isolation device position or functioning should also be safety-related and highly reliable. The man-machine interface design and procedures should be such that operator attention is immediately directed to interfacing LOCA situations.			Y	6.20 covers the intent of LBB arguments. The other proposed wording is more appropriate for guidance. HF aspects are addressed separately.

COMMENTS BY REVIEWER Reviewer: Steven C. Sholly Page 39 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
39	6.32	No change proposed; comment only.	§6.32 appears to require containments. No exclusion possibility is offered. So what will MAGNOX, AGR, and VVER-440 units do? What about LMRs? What about GT-MHR and PBMR? I have no problem with requiring a containment for all nuclear power plants irrespective of design as a matter of prudent risk management.				The document is looking to future designs, not those that will be phased out. See also new wording proposed in paras 1.6 & 1.8

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Page 40 of 43 Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna Date: 29 May 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
40	6.67	[Reword §6.67 as follows] Appropriate measures are taken and adequate information is provided to safeguard the occupants of the control room against hazards, such as high radiation levels resulting from an accident condition or the release of radioactive material, or explosive or toxic gases, which could hinder necessary actions by the operator. Windows shall not be present in either the main or emergency (alternate) control rooms.	§6.67 states, "*Appropriate measures are taken and adequate information is provided to safeguard the occupants of the control room against hazards, such as high radiation levels resulting from an accident condition or the release of radioactive material, or explosive or toxic gases, which could hinder necessary actions by the operator.*" This should be expanded to explicitly preclude the presence of windows of any type in the control room. This absolute exclusion is necessary to protect the operators from high radiation doses in the case of a severe accident at the site, and to protect them against combustible or toxic gas release, from ingestion of smoke in case of an onsite fire, and for physical protection reasons. Maintenance of a positive control room pressure or provision of safety glass is no substitute for the absolute exclusion of windows.			Y	This is a detail of design more appropriate to a guide.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 41 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
41	6.89	[Reword §6.89 as follows] Adequate lighting shall be provided to facilitate safe opeation in normal operation and accident conditions in all operational areas. The adequacy of lighting shall consider fire, smoke, seismic initiating events, and all other PIEs. The purpose of lighting includes facilitation of access and egress as required for protection of plant personnel in the event of an accident, and also includes security considerations.	§6.89 states, "*Adequate lighting shall be provided to facilitate safe operation in normal opeation and accident conditions in all operational areas.*" This should be expanded to include all conditions, including fires (and the resulting smoke), and the purpose of lighting should also be to facilitate access and egress as need be.				'Accident conditions' should cover the events suggested. Purpose of lighting is covered by 'facilitate safe operation.'

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna 2009			Page 42 of 43 Date: 29 May				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
42	6.90	[Reword §6.90 as follows] Effective means of communication shall be provided throughout the plant to facilitate safe operation in all modes of operation (full power, low power, hot standby, cold shutdown, refueling) and following all PIEs and DBAs.	§6.90 states, "*Effective means of communication shall be provided throughout the plant to facilitate safe operation.*" This has to be expanded to include all possible modes of operation (refueling, shutdown, etc.) and include consideration of all PIEs and DBAs at a minimum.		'…safe operation in all modes of operation and following all PIEs and DBAs.' Note thayt this para has now been moved to precede para 5.90 (Fr comment 75)		

Comment [J7]: Fr 75; Au 42

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Steven C. Sholly Country/Organization: Austria/Institute of Risk Research, Univ. of Vienna			Page 43 of 43 Date: 29 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
43	6.97	[Reword §6.97 as follows] Measures are provided to minimise any interaction between buildings containing safety-related SSCs (including power and control cabling) and any other plant structure ~~the turbine building and the reactor building~~ resulting from external events such as earthquake and high winds (e.g., tornado, hurricane, etc.).	§6.97 states, "*Measures are provided to minimise any interaction between the turbine building and the reactor building resulting from external events such as earthquake.*" This should not be limited to the reactor building, but should also include any other structure containing safety related systems or components (including power and control cables).	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: F. Féron Country/Organization: France/ASN			Page Date: 14 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.			Need to better take into account severe accidents in the "initial" design of the most recent NPP (like EPR under construction)		See new wording in para 1.3		

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
2.			A few world should be added to clarify how these requirement apply to existing plant, taking into account that theses requirements should primarily be applicable to "new" plant		See new wording in para 1.2.		
3.			General remark : the terms explained in the AIEA safety glossary and the glossary at the end of this guide should be marked in the text when first used.		For final editing		
4.	1.3/8	Add "and should" before "implemented"	"Can" is not enough. Implementation is expected.	Y			
5.	2.2/ (a)	Replace "to restrict the likelihood of" by "to prevent"	Initial wording may be understood as PSA oriented	Y			
6.	2.7	At the end of 2.7, add "should they occur"	Clarification	Y			
7.	2.8/3	Replace "limited" by "some"	Alternate wording as "limited" may be not understood as ALARA			Y	"some" may also not be understood as ALARA.
8.	2.8/6	Replace "with operational limits and radiation protection standards" by "with regulatory and operational limits as well as radiation protection standards"	To include regulatory limits	Y			
9.	2.9	At the end of 2.9, add "and that radiological consequences of such accidents are dealt with (see 2.7 and 2.12)"	Consistency within the guide	Y			
10.	2.10/1st bullet	At the end, add a footnote "including new and spent fuel in storage"	Clarification	Y			
11.	2.12/7	After "appropriate authorities", add "and supported as required by the operating organization"	The operator has to contribute to some of the off-site actions (survey…)	Y			
12.	2.12/10	Add "high" before "radioactive releases"	Clarification	Y			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
13.	2.12/13	Replace “may” by “should”	This is the goal to pursue, not an option	Y			
14.	2.14/4)	Delete “although very unlikely”	Too qualitative			Y	The escalation to this level should be very unlikely, it is difficult to describe it otherwise.
15.	2.14		The text should precise what kinds of situations are addressed at this level. In France, beyond design basis accidents without core degradation are addressed at the third level : the fourth level concerns only severe accidents			Y	Bdbas are included in design basis considerations.
16.	2.16/11	After “decommissioning”, add “(see 3.19)”	Clarification	Y			
17.	2.16/12	Delete “For the purposes of the present document, it is intended that similar approach should be adopted at the design stage for eventual incorporation into the arrangements of the operating organization.”	Duplicates 2.17	Y			
18.	2.17/6	Replace “Pre-licensing” by “Before a plant is ordered by a customer”	Clarification		Prior to a plant being ordered,		
19.	3.2/2	Replace “of the design” by “its design, as well as overall plant design”	Clarification to ensure overall quality (balance design, interfaces between SSC…)	Y			
20.	3.9/1	Replace “is kept” by “and radioactive discharges are”	To include radioactive discharges has both have to be minimized (not one versus the other)	Y			

Comment [J8]: Fr 18 amended

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
21.	3.12/3	Replace "necessary safety function" by "safety function"	Clarification		'necessary' replaced by 'appropriate'		
22.	3.14/3	Replace "has to be expected and accommodated" by "can not be excluded"	Unless failure is excluded, management of the failure consequences has to be managed.	Y			
23.	3.22/1st bullet	"Code of conduct of engineering"	Not easily understandable in French		definition of engineering standards		
24.	4.1	Replace 4.1 by "The design and the design process shall incorporate the concept of defence in depth"	As written, the meaning of 4.1 is unclear.Is it on the plant design itself or on the plant design process ?	Y			
25.	4.3/6th bullet	Delete "i.e……releases"	Duplicate 4.2	Y			
26.	4.8/2	Add "high" before "radioactive releases"	Clarification	Y			
27.	4.9/1	At the beginning of 4.1, add "In addition to the objective of reducing radiation doses as low as reasonably achievable,"	To insist on ALARA, even if acceptance criteria are set.	Y			
28.	5.1/3	Before "internal", add "conditions generated by"	Clarification	Y			
29.	5.2/1	Delete "normal"	Superfluous	Y			
30.	5.3/1	Replace "normal operation….(PIEs)" by "all operational states and accident conditions"	Consistency with 5.4	Y			
31.	5.5	At the end, add "as well as relevant regulatory requirements"	Regulations have to be considered	Y			
32.	5.8/4th bullet	Replace "in which … accidents)" by "including severe accidents"	Consistency with IAEA safety glossary	Y			
33.	5.11		The definition is not fully consistent with IAEA safety glossary…				

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
34.	5.12	Replace "both for serious consequences and significant probability have been anticipated and addressed to achieve the safety objective." By "for serious consequences or of significant probability have been anticipated and addressed to achieve the safety objective. Specific attention should be paid to ensure that events with the potential both for serious consequences and significant probability have been anticipated and addressed to achieve the safety objective."	The PIE should also include high probability events (leading to AOO…)			Y	1st sentence modified as proposed, 2nd sentence adds nothing since it repeats most of the 1st.
35.	5.15/2	Delete "for which it… consequences"	The second part of the sentence is too vague….			Y	Not a good reason for removal.
36.	5.16	Replace 5.16 by "The engineering design rules for structures, systems and components shall be specified and shall comply with the appropriate accepted international or national standard and standard engineering practices, taking into account their relevancy for a nuclear installation (see para. 3.6)."	Alternate wording		… with the appropriate accepted national or international standard engineering practices (see para. 3.6), taking into account their relevance to a nuclear installation and whose use is also accepted by the national regulatory body.		

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
37.	5.17/3	After "design basis accident", add a footnote "see para 5.29 for beyond design basis accident"	What about beyond design basis accidents (including severe accident) which are now considered at the design stage ? (see comment 1)	Y	Agreement is dependent on IAEA policy to cross referencing to other paragraphs.		
38.	5.21/1	Delete "basis" in "design basis for the safety system"	Severe accident are to take into account in the design (see comment 2)			Y	The safety system has a design basis.
39.	5.21/3	Before "control and mitigate", add "prevent those accidents and"	Prevention is not to be forgotten		'…prevent, or control…..'		
40.	5.25/1		Is "accident management" appropriate considering the meaning in the IAEA safety glossary		To be reviewed		
41.	5.25/1	Replace "procedures" by "provisions, including procedures,"		Y			
42.	5.26/3	Add "safe" before "human access"	Clarification	Y			
43.	5.27/5	Replace "identify and to implement those reasonably practicable provisions for their prevention and mitigation" by "identify the possible provisions for their prevention and mitigation and justify those not to be implemented"	Prevention and mitigation should be encouraged.		Final part of sentence is best covered by retaining 5.28.		
44.	5.28	Delete 5.28	See proposal in comment 43			Y	*See response to comment 43 above.*
45.	5.31/3	Delete "basis" in "basis for the safety system"	See comment 38				*See response to comment 38*
46.	5.32/4	Replace "The capability for shutdown, residual heat removal, confinement of radioactive material" by "Achieving the fundamental safety functions (see 4.2)"	Consistency within the guide	Y			
47.	5.33/5	Delete "nuclear"	Consistency with SF-1	Y			
48.	5.39/2	Replace "may" by "are"		Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: F. Féron Country/Organization: France/ASN			Page Date: 14 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
49.		After "The method for classifying the safety significance of a structure, system or component is primarily based on the potential consequences associated with the failure to perform their safety function(s),", add "estimated on a deterministic way complemented where appropriate by probabilistic methods"	The mention of the method of classification which figured in the previous version has been deleted. However, the method of classification used in DS 367 uses first a deterministic approach based on the safety role during PIEs, complemented if appropriate by a probabilistic approach.	Y			
50.	5.46/2	After "lower class", add "(less stringent requirements)" and, after "higher class", add "(more stringent requirements)"	Clarification	Y			
51.	5.48	Add the end of 5.48 add "and their expected performance".		Y			
52.			Paragraph 5.6 of the current NS-R-1 has been deleted in the current version. We wonder why. This paragraph is developed at the paragraph 5.29 but should have been kept in the 5.6			Y	The 'old' para 5.6 becomes part of the new 'key' principle 5.31, and is developed in 5.29
53.	5.65/2	Replace "item" by "SSC"			SSCs replaces 'items important to safety'		
54.	5.66/2	Before "normal operation", add "the ambient conditions (temperature, irradiation, humidity, vibrations…)"	To clarify what are environmental conditions.		The examples are given in the next sentence.		
55.	5.66/2	After "design basis accident", add "and where appropriate beyond design basis accident including severe accidents (see 5.68)"	See comment 1	Y			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
56.	5.68/3	Before "a justifiable extrapolation program", add "A qualification program or"	A qualification program (not an extrapolation from design basis accidents) is used for equipment required during beyond design basis accidents in French NPPs and also for equipment required during severe accidents for French EPR.	Y			
57.	5.85/3rd bullet	At the end, add "and beyond design basis accidents"	See comment 1			Y	This is specific to storage systems.
58.	5.87	Transfer 5.87 before 6.103	Logical order as 6.103 deals with handling…		Moved to *follow* 6.103		
59.	5.104	Add a bullet "- assessment of beyond design basis accident (including severe accidents) and resulting radiological consequences."	See comment 1			Y	Assessment is now addressed by GS-R-4
60.	6.1		What about beyond design accident ? See comment 1		Changed to include reference to accident conditions		
61.	6.6/1	Replace "permissible" by "tolerable"	Integrity of the first barrier should be the rule….			Y	Permissible is intended to indicate a specified limit.
62.	6.31	At the end, add "In beyond design accidents, such transfer should be maintained as far as possible".	What about beyond design accident ? See comment 1				The intention of the document is to encompass bdbas without continual repeat references.
63.	6.33/2	Replace "would" by "will"			'would be' replaced by 'is' to comply with IAEA style.		

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
64.	6.36	Locate 6.36 after 6.34	To address confinement in all operational states and accidents conditions.	Y	Note simplified text of 6.36		
65.	6.37/2	After "design basis accidents" add ", and as low as possible in beyond design basis accidents"	What about beyond design accident ? See comment 1	Y			
66.	6.46		What about beyond design accident ? See comment 1			Y	Point covered by para 5.30
67.	6.47/2nd bullet	Delete "design basis"	See comment 1	Y			
68.	6.51/2	Replace "sense unsafe conditions and automatically initiate the operation of the appropriate systems required for achieving and maintaining a safe condition." By "automatically initiate the operation of the appropriate systems required for achieving and maintaining a safe condition before variables mentioned in 6.49 reach a safety limit."	Alternate wording			Y	Proposed wording is no clearer than the existing.
69.	6.51	Locate 6.51 after 6.53	To have 6.51 and 6.54 together as both deal with the protection system.	Y			
70.	6.59/2	Replace "6.82" by "6.57"	Inadequate cross reference	Y			
71.	6.71/2	Replace "room" by "centre"	Consistency with 6.70	Y			
72.	6.84/1	Replace "and" by "."	Shorter sentence	Y			
73.	6.85/1	Replace "provided with alarm systems" by "designed"	Consistency with the way requirements are stated in the guide. (More goal oriented that means oriented)	Y			
74.	6.88	Delete 6.88	Although true, it is not really a design feature (scope of the document)	Y			
75.	6.89	Transfer 6.89 at the end of 5.80 "In particular, adequate lighting…"	Same topic			Y	5.80 is not dealing with lighting.

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
76.	6.90	Combine 6.90 with 5.90	Same topic (communication)	Y			
77.	6.92/1st bullet	Delete "in normal operation and design basis accident conditions"	Superfluous (or add beyond design basis accident – see comment 1)	Y			
78.	6.98	Replace ". The ALARA principle shall be applied" by "and ALARA."	Alternate wording	Y			
79.	6.99/3	Delete "on the site"	Superfluous			Y	Indicates a need for safe on-site storage.
80.	6.104 and 6.105		Check consistency of bullet lists and bullet list wording. (some bullets of 6.105 seem appropriate for 6.104)		Some additional points added to the storage of fresh fuel.		
81.	6.107	Delete 6.107	Duplicates 4.6			Y	4.6 deals with reactor design, 6.107 et seq is intended to address protection of personnel.
82.	6.111	Locate 6.111 before 6.108	Logical order		More logical to *follow* 6.108		
83.	6.113	Locate 6.113 after 6.99	Deals with waste/effluent treatment systems	Y			
84.	6.122		Although true, it is not really a design feature (scope of the document)				Recommended to retain
85.	Glossary	Complex sequence	This word is only used once in the document (1.2), is it worth defining it in a glossary ?	Y			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 14 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
86.	Glossary	Severe plant condition	The word "beyond design basis" was quite true for existing NPP for which PSA lead to consider additional accidents. It is very less true for "new" NPP as such accidents are considered. Assessment methods and hypothesis, as well as acceptance criteria, are however differents…. See comment 1	Y			
87.	Glossary		IAEA should confirm that the safety glossary will be update to take into account the additional definitions.		The glossary is updated periodically		
88.	/						

TITLE: Safety of Nuclear Power Plants: design, DS414
Revision of the Safety Standards Series No. NS-R-1

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	General remarks: • Some Requirements are formulated in the „shall"form (or comparable), most of the others are not. This should be harmonized. • It is proposed to omit Appendix I (which describes the PIE concept in more details). These details should nevertheless not be omitted completely. • It is proposed to omit para. 5.20 (which addresses combinations of events in more detail). These details should nevertheless not be omitted completely.					Y Y Y	Only 'key' requirements state 'shall'. It is not stated which parts

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	• It is proposed to omit para. 5.25 (which addresses events in low power and shutdown states). These aspects should nevertheless not be omitted completely. • The global term to be used should be "structures, systems and components (SSCs)". It should be systematically checked if the use of "system" or "component" alone is correct or if "SSCs" would not be the correct term (e.g. para. 2.14 (1)). • The application of the term "safety related item" is not necessary and not useful (what would be the meaning of "item" in relation to "SSCs" or "procedures"?) • The statements of para. 6.53 of the current NS-R-1 are missing in the present draft DS414:" 6.53 If resilient seals (such as elastomeric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have the capability for leak testing at the containment design pressure, independent of the determination of the leak rate of the containment as a whole, to demonstrate their continued integrity over the lifetime of the plant." and should be contained in the revised requirements. In the statements of this para. the requirements for the repeated examination of the leak tightness of the penetrations of the containment are defined. Separate examinations of the leak tightness during the operating stage or during the outages are reasonable • The statements of para. 6.60 of the current NS-R-1 are missing in the present draft DS414:"6.60. The design shall provide for ample flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in design basis accidents do not result in damage to the pressure bearing structure or to other systems of importance in limiting the effects of design basis accidents." An important aspect for the safety of components (e.g. pumps, engineered safety features) is the structural integrity of the walls in case of pressure differentials during incidents/accidents within the containment. By an appropriate design of the openings the impacts can be reduced.			Final editing check. Para restored with amended wording.	Y Y Y	Reasoning not clear. See glossary definition. Text has been amended in response to comment Ge 24
2.	1.4	This publication establishes design requirements for structures, systems and components as well as procedures and organizational processes important to safety that ….	Completeness: NS-R-1 addresses not only SSCs.	Y			
3.	1.6	It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled	The last sentence of this para. is not well			Y	This is setting out the scope.

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). ~~In the development of the requirements for design, account is taken of postulated initiating events (PIEs), which include many factors that, singly or in combination, may affect safety.~~	placed here and should be deleted. The subject of PIEs is better dealt with in the chapter on defence in depth.				
4.	2.3	Para. 2.3 is missing.	editorial			Y	For final editing of para numbering.
5.	2.11 / 4	In order to achieve the fundamental safety objective in the design of a nuclear power plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate radiation doses that could be received by workers at the installation and the public, as well as potential effects on the environment (see para. 4.7) as a result of the operation of the plant.	Refer to para. 4.7 [4.9] (identification of radiation sources) instead of para. 4.9 (radiological radiation criteria).	Y			
6.	2.14 (1)	The aim of the first level of defence is to prevent deviations from normal operation, and to prevent system failures. This leads to the requirement that the plant be soundly and conservatively ~~sited,~~ designed, constructed ..	Plant siting is not able to prevent deviations form normal operation.			Y	Siting takes account of external hazards that may lead to system failures.
7.	2.17	It remains unclear if the positions from INSAG 19 are adopted in NS-R-1 or not.	clarification		No change to the text required.		
8.	3.5	The term “safety function” should be defined (against “Fundamental Safety Function”).	clarification	Y	See amendment Au 13.		
9.	3.30	Para. 3.20 is missing	editorial	Y	For final editing.		
10.	3.22	Second bullet, second line insert “operational”: ….taking into account operational experience….	editorial	Y			
11.	4.1 – 4.4	These numbers are duplicated.	editorial	Y	For final editing.		
12.	4.3	… provides multiple physical barriers to the uncontrolled release of radioactive materials to the environment, adequate protection of these barriers, and assurance of their	editorial / completeness	Y			

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		effectiveness by the use of passive and/or active features;					
13.	4.3 (new after para. 4.2)	The design shall take into account the fact that the existence of multiple levels of defence is not a sufficient basis for continued power operation in the absence of one level of defence. All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.	Number 4.4 of the current NS-R-1 shall not be omitted because this is also a design (not only operational) issue.	Y			
14.	5.21	The Design Basis Accidents are used to define the design basis for the safety systems ~~and for the design of all other structures, systems and components important to safety~~ that are necessary to control and mitigate the consequences of these accidents.	This para. mixes up requirements resulting from design basis accidents with regard to the safety systems (systems necessary to control the DBA) with other SSCs. This is not consistent.			Y	Systems important to safety are a relevant consideration.
15.	5.25	The term "accident management procedure" should not be used as well for design basis accidents as for beyond design basis accidents.	"accident management procedure" should only be used for beyond design basis accidents		Text amended by Fr comment 41 & Ja comment 19.		
16.	5.30 a (new)	The message of para. 5.31 (8) from current NS-R-1 should be added (Accident management procedures shall be established, taking into account representative and dominant severe accident scenarios.)	completeness	Y	'are', not 'shall be'		
17.	5.49	The potential for common cause failures of items important to safety shall be considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the required ~~assumed~~ reliability.	Correct wording: necessary requirement	Y			
18.	5.62	The design ensures that reasonable on-line maintenance and testing of systems important to safety can be conducted without the necessity to shut down the plant.	What is the safety reason for demanding on-line			Y	Sound and established practice

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			maintenance?				
19.	5.105	The applicability of the analytical assumptions, methods and degree of conservatism used are verified. The safety analysis of the plant design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and shall be consistent with the current or 'as built' state.	The added sentence (from current NS-R-1 5.72) should not be omitted.	Y			
20.	6.1 a	The reactor core and associated internal components located within the reactor vessel shall be designed and mounted in such a way that they will withstand the static and dynamic loading expected in operational states, design basis accidents and external events to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure cooling of the core.	Para. 6.2 from current NS-R-1 shall not be omitted.	Y			
21.	new para. 6.19a	Inspection of the components of the reactor coolant system is addressed in 6.19. The inspection of the reactor core (para. 6.5 of current NS-R-1) should also be added.	completeness			Y	Covered generically under key requirement 5.59.
22.	6.11 a	At least one of the two systems is capable of quickly rendering the nuclear reactor subcritical by an adequate margin from normal power operational states, in anticipated operational occurrences and in design basis accidents, on the assumption of a single failure.	Para. 6.15 of current NS-R-1 shall not be omitted.			Y	Specific requirements for SFC have been withdrawn from the draft, as they are covered generically.
23.	6.33 and 6.37	Instead of "prescribed limits" for radioactive releases "allowed / nationally defined limits" or "as low as technically achievable limits" should be required	The application of the wording "prescribed limits" seems to be too weak			Y	'Prescribed' is intended to cover national/international limits.

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
24.	6.38	Para. 6.51 of the current NS-R-1 substantiates the requirements relating to the enhancement of the leak tightness of the containment. These aspects should be mentioned in para. 6.38	completeness		Para 6.40 amended to read: 'The number of penetrations through the containment is kept to a practical minimum, and all penetrations meet the same……'		
25.	6.66. [6.71] last line 6.67. [6.71] 3rd line 6.71. [6.87] last line	… state after the onset of anticipated operational occurrences, ~~or~~ accident or severe accident conditions. … resulting from an accident or severe accident condition ~~or~~ respectively the release of radioactive material, or explosive or … … resulting from accident or severe accident conditions	It is not clear if "accident conditions" includes the severe accident conditions as well. Since in the document "severe accidents" are separately mentioned, these paragraphs should be precise			Y	See glossary definition of 'accident conditions.
26.	new 6.69a new 6.69b	Same text as modified 6.66 [6.71] but with regard to the supplementary control room. Same text as modified 6.67 [6.72] but with regard to the supplementary control room.	The supplementary control room must allow to take the same actions as in the control room as well under all expected environmental conditions..	Y Y	Minor word change.		
27.	new	… The actuation of accident management procedures should	It is recommended to			Y	Existing text

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	6.66 and 6.69	be possible from the control room. … from the supplementary control room.	add a sentence to 6.66 and 6.69 with regard to the operation of accident management procedures in both types of control rooms.				addresses the issue.
28.	6.76	"severe accidents" should be added.	completeness			Y	See glossary.
29.	6.90	"normal power operational states, in anticipated operational occurrences and in design basis accidents" should be added.	completeness	Y	Note that the para has been moved to precede 5.90 & reworded.		
30.	6.92 (1)	measures are provided to prevent the lifting of ~~unacceptable, or~~ excessive loads ~~in normal operation and design basis accident conditions~~.	Better wording		Covered by comment Fr 77.		
31.	6.92 (2)	… highly reliable ~~conservative~~ design measures are applied to practically exclude ~~minimize the likelihood of~~ an uncontrolled load drop, and …	Clarification, better wording			Y	Existing wording is adequate.
32.	6.115. [6.105(1)] / 2	Stationary dose rate meters are provided for monitoring the local radiation dose rate at places routinely accessible by operating personnel and where the changes in radiation levels in normal operation or anticipated operational occurrences may be such that access is limited for certain specified periods of time.	The more general formulation allows for some places with access limitation that might not be routinely occupied by the personnel.	Y			
33.	6.117. [6.105(3)] / 1	Stationary monitors are provided for continuously measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by personnel and where the levels of airborne activity may on occasion be expected to be such as to necessitate protective measures. These systems provide an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected.	The 2nd sentence implies a stationary monitoring device with continuous measurement.	Y			
34.	6.122.	Arrangements are also made to determine the radiological	A general specification	Y	'…by		

COMMENTS BY REVIEWER Country/Organization: Germany / Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) Date: May 2009				RESOLUTION			
Comment No.	Para No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	[6.106] / 2	impact, if any, in the vicinity of the plant by surveillance of radioactivity concentrations and contaminations and dose and dose rate in accordance with standards and principles used internationally and accepted by the national regulatory body, with particular reference to:	of the methods to be applied would be helpful.		surveillance of radioactivity concentrations and contaminations and dose and dose rates with…'		

DS 414 Safety of Nuclear Power Plants: Design

COMMENTS BY REVIEWER Reviewer: G. BAVA Page 1 of 3 Country/Organization: ITALY/ISPRA Date: May 12 2009							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	2.14	Merge sub items n. 1 and 2	Sub item 2 alone does not represent a level of defense.	Y			
2	4.3	…. to fulfill the ~~fundamental~~ safety functions ….	The original text implies that there are additional safety functions different from the fundamental ones. This concept should not be dismissed.			Y	The fundamental safety functions are defined in 4.2
3	5.15	A **technically supported** justification shall be provided for the exclusion of any rare events, sequences or situations for which it is not ~~realistic~~ **reasonable** to set up provisions for the management of their consequences.	It should be clarified that technical background is needed. The adjective realistic seems to have a meaning more appropriate for the evaluation methods	Y			

			rather than for the measures.				
4	5.27	……., ~~from which event sequences can be selected~~ to identify and to implement those reasonably practicable provisions for their prevention and mitigation.	For clarity.			Y	Not all event sequences will be selected.
5	5.31 e segg.		The difference between the "hazards" and the other accidents/events has to be clarified. Hazards are stated to be "used as events". So, if defined in such a way, it is not clear why to introduce this term.				Point accepted, but the wording is adequate.
6	5.47	….. is classified at the highest level of the functions, systems, and equipment ~~from which it is not independent~~ which are depending from it.	For clarity			Y	Existing text is correct.
7	5.85	… shall be designed to: - **prevent the occurrence of events that can lead to releases to the environment** - **…..** - **…..** of design basis accidents **and the protection against other internal or external events**	The preventive actions should be underlined, the external events should be considered.		1st amendment agreed. 2nd proposal *not agreed* since hazards are considered under the PIEs analysis.		
8	5.99	…account is taken in the design of: - …. - ..the facilities necessary for storing radioactive waste generated in ~~both~~ operation and **the programs to accommodate the waste generated** in decommissioning of the plant.	In order to clarify that the storage capabilities for decommissioning are not required to be in place since the start up of the plant.	Y			
9	5.100 title.	SAFETY ASSESSMENT	Consider to change the title on the basis of the contents and taking the new definitions and GS R 4 into account.			Y	Title has been agreed within IAEA.
10	6.10	**The design of the core shall**	This sentence in previous			Y	The issue is covered

		sufficiently reduce the demands made on the control system for maintaining flux shapes, levels and stability within specified limits in all operational states.	6.13 section should be maintained.				in 6.8
11	Former 6.17	**In judging the adequacy of the means of shutdown, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or could result in a common cause failure.**	This sentence is missing in the present draft. The statement is of great importance for design purposes.		Reworded: "Failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or could result in a common cause failure are considered."		
12	6.81		See also comment 2: clarify that not only items for fundamental safety functions have to be served by HVAC.			Y	HVAC is not a fundamental requirement.
13	Former 5.10		Consider reinserting former 5.10 paragraph that clarifies the approach to fire protection with a DiD philosophy.			Y	5.10 is covered in the associated IAEA guide on fire protection
14	6.105	The handling and storage systems for irradiated fuel are designed: • …. • **to accommodate all the fuel discharged from the reactor according to the foreseen core management strategy and the full core, with adequate margins.** • …..	Add the sentence in order to specify that the irradiated fuel storage capabilities are appropriate with margins is a relevant design input..	Y			
15	7.	Internal hazards…..	See comment				No change required

Comment [J9]: It 11 amended

COMMENTS BY REVIEWER Reviewer: H. Tezuka, T. Matsumoto, Z. Ogiso, K. Maki Page 1 of 8 Country/Organization : Japan/ JNES, NSRA Date: 25 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text/ Comment	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	General	The draft of DS414 is very well prepared in reviewing the NS-R-1; redundant texts have been improved and required messages become clearer. We recommend to submitting this draft to the MSs for review. However, we see that there are paragraphs some of which seem to be important have been deleted. We recommend reconsideration of maintaining some of deleted paragraphs mentioned in below comments.					
2	1.6/ 3	The draft limits the use of this publication to only water cooled reactors while para.1.3 of NS-R-1 states that it is recognized that in the case of other reactor types, including innovative developments in future systems, some of the requirements may not be applicable, or may need some judgment in their interpretation. The reason of the use of limitation should be justified.	This document is useful also other reactor types than water cooled reactors. Clarification of the deleted part.		See additional text in paras 1.6 & 1.8		
3	2.2~2.5	Delete the paragraphs quoted from SF1 and refer the relevant part of SF1 if necessary.	Editorial				Retained for ease of reference.
4	2.13	'This concept is applied to all safety activities, whether organizational, behavioural or design related, to ensure that they are subject to layers of	Editorial; 'Defence in depth' denotes the practice of having multiple, redundant, and <u>independent</u> layers of safety systems to reduce the risk.	Y			

		overlapping provisions' →'This concept is applied to all safety activities, whether organizational, behavioural or design related, to ensure that they are subject to **independent** layers of provisions.'					
5	2.14, 1)/4	Insert behind "engineering practices" the following wording of [2.10] of NS-R-1 for user friendly; such as application of redundancy, independence and diversity,	For User friendly and better understanding.	Y			
6	2.14, 5)/1, 8 2.14, 6)/3	"severe accidents" is replaced with "severe plant conditions" in only para. 2.14. The reason of the replacement should be clarified.	Clarification of the replaced wording.				Severe plant do not necessarily lead to an significant core melt.
7	3.10/1	Delete 'and' placed after '… shall be'.	typo	Y			
8	3.16-3.17	[3.13] of NS-R-1; Independent verification of the safety assessment has bee deleted. The reason of the deleting should be clarified.	Clarification of the deleted part.				Assessment is now covered under GS-R-4
9	Heading of 3.19~3.22	Change the heading to "Responsibility of the Operating Organization"	Current heading; INTEGRITY OF THE DESIGN THROUGH ITS LIFE does not fit the content of paras. 3.19~3.22.	Y			
10	3.19~3.22	Move paras. 3.19~3.22 and the heading to the top of the Section 3.	As for the management of safety design, responsible person/organization should be stated first.	Y			
11	4.2[4.6]/ 4	Change "fuel" to "core".	Maintain the word of para.4.6 of TS-R-1. Heat removal is needed from not only "fuel" but also core internals such as fuel	Y			

			cladding, control rods, etc.				
12	4.3[4.7]/ 2	It is unclear what inherent features can be identified from a systematic approach. "inherent features" mentioned here need to be clarified.	Clarification			Y	Example not required, but inherent features are intended to include for example negative reactivity coefficient.
13	4.4, p11	Move this para. to Section 6 and place behind 6.49 for example.	Section 6 is more suitable. See the comment No. 29.		Is this para really necessary? 6.49 covers the requirement. Propose to delete.		
14	4.3[4.1]/ 2nd bullet/ 2	Change ';' to 'and' to read '…are minimized and accidents are prevented…'	Typo		; changed to ,		
15	4.3[4.1]/ 2nd bullet/ 3	Delete the last part of wordings that are; and the activation of safety systems is minimized.	It is not relevant directly to safety. Do we need this message?				It is relevant, since unnecessary activation places undue demands on the SSs.
16	4.3[4.1]/ 6th bullet/ 3	Change fuel to core.	Core heat removal is more general to fuel heat removal. See the comment on para. 4.2.		Alternative wording provided in comment Fr25		
17	5.9	Replace this para with the following relevant text in NS-R-1; In the design of the plant, it is recognized that challenges, that stem from the PIEs, to all levels of defence in depth may occur and design measures shall be provided to ensure that the necessary safety functions are accomplished and the safety objectives can be met.	The current text is difficult to understand. Relevant part of [5.8] of NS-R-1 is more comprehensive.			Y	The point is covered by para 4.3.
18	5.19 1st & 3rd bullet	Need to clarify the difference between safety limits (bullet 1) and limits for normal operation (bullet 3).	Clarification			Y	Covered in NS-R-2

19	5.25	Change "the accident management procedures" to "the management procedures of design basis accidents" to read; The design specifies the management procedures of design basis accidents required to provide the means for regaining control over the plant in the event of a loss of control and for mitigating any harmful consequences.	Editorial		This para. has been subject to revised wording under Fr comment 41.		
20	5.32	The following deleted part should be maintained as follows; The fundamental design concepts of fire protection are: (1) to prevent fires from starting; (2) to detect and extinguish quickly those fires which do start, thus limiting the damage; (3) to prevent the spread of those fires which have not been extinguished, thus minimizing their effects on essential plant functions.	Confirmation Important aspects to implement the requirement.			Y	These concepts are covered in NS-G-1.7.
21	5.38	'For multiple-unit plant sites, the potential simultaneous impact of specific hazards on several plants on the site is taken into account in the design.' Should be deleted.	In the design, the safety provisions for a unit are independent from those of other unit.			Y	It is important that such potential impact is not overlooked.
22	6.3bis	The para. [6.5] of NS-R-1 should be maintained as follows; The reactor core and associated coolant, control and	Design needs to take into account the inspection and testing.			Y	Para 5.59 addresses maintenance, etc. so it is not necessary to repeat the requirement for each system.

		protection systems are designed to enable adequate inspection and testing throughout the service lifetime of the plant.					
23	6.10	Change “and in external events“ to “and in external events within design basis”.	External events here should be limited to in those of design basis in order to exclude the events that lead to sever accidents.	Y			
24	6.10	Add “, on the assumption of a single failure” at the end of the text.	Single failure criterion has been deleted, maybe, by mistake.				Single failure is covered by para 5.50, so is not repeated subsequently.
25	6.22bis1	Maintain the content of paras [6.27] of NS-R-1 as follows; Heading; In-service inspection of the reactor coolant pressure boundary New para. The components of the reactor coolant pressure boundary are designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the boundary.	It is important that the design permit inspection and test. In-service inspection [6.27] of NS-R-1 is missing.				See response to comment 22 above. Para 5.59 – 5.61 address maintenance, etc. so it is not necessary to repeat the requirement for each system and component.
26	6.26bis	Maintain the content of paras [6.34] of NS-R-1 as follows; In residual heat removal systems, adequate isolation capabilities are provided with sufficient reliability, on the assumptions of a single failure and the loss of off-site power.	NS-R-1 [6.34] In residual heat removal systems, adequate isolation capability should be clearly mentioned in order to retain the reactor coolant boundary.				See response to comment 22 above.
27	6.29 bis	Maintain the 1st sentence of [6.38] ; The emergency core cooling	It is important that the design permit inspection and test for SSCs important to safety.				See response to comment 22 above.

		system is designed to permit appropriate periodic inspection of important components and to permit appropriate periodic testing.					
28	6.32 bullet No.3	"external natural event", that appears only in this paragraph, may need definition.	Clarification	Y	Changed to 'hazards'.		
29	6.49 to 6.68 (instrumentation and control systems)	Clarification in documented basis is needed for the reason of deletion of the word "shall" in many paras. (6.52, 8.53, 6.54, 6.55, 6.57, 6.58, 6.61, 6.62, 6.67, 6,68)	This document provides fundamental requirements for the safety, change in the level of requirements shall be clearly understood by every users without any miss interpretations.			Y	The style follows the new IAEA approach.
30	6.49bis	Insert 4.4 of page 11.	Monitoring of plant state is an important function of I&C.		New para 4.4a added.		
31	6.51 and 6.54	Requirements for the protection system should be integrated into single para.	There are no para regarding the protection system without 6.51 and 6.54. So, these short paras should be integrated into a set of requirements for the protection system as previous 6.80 for better understanding.		See rewording proposed by Fr comment 69 & Swe comment 14.		
32	6.54/ bullet No.2	• To initiate the appropriate safety systems for falling a safe condition	Editorial		See rewording proposed by ENISS comment 24.		
33	6.55bis	Maintain [6.79] of NS-R-1 as follows; Various safety actions shall be automated so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or design basis accidents. In addition, appropriate information shall be available	Automatic control has been deleted. It should be maintained.		See revised text		

		to the operator to monitor the effects of the automatic actions.					
34	6.56	Change "I&C" to "instrumentation and control".	Editorial; This abbreviation is not needed because this is the only place where this word is used.	Y			
35	6.58	……when the reactor is **in operation**, including the possibility of testing channels independently…… →……when the reactor is **in service**, including the possibility of testing channels independently…	Some sensors can't be tested in operation. For example, RCS temperature, RCS flow.	Y			
36	6.59	Change "6.82" to "6.58".	typo	Y	6.57, not 6.82.		

TITLE: DS 414 Safety of nuclear power plants: design - Rev 14 April 2009

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Anders Hallman, Erik Jende Country/Organization: Sweden/SSM			Page.1 of 5 Date: 27 May 2009				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	General	The structure of the document has become very unclear and in fact has weakened the earlier document NS-R-1. It is basically the same document but in the new draft some of the requirements have been promoted to key requirements in bald printing and the other requirements reduced to descriptions (without shall statements). It is now difficult to see what is actually required. If a new structure is preferred, it is better to use the structure of the					The style is in compliance with the new IAEA approach.

2	General	revised GS-R-1 where there are numbered requirements (shall statements) and supplementary text (have to/has to statements) on what is required in order to meet the basic requirements. This is much more clear. To rework DS 414 in this way will require substantial work since additional aspects may need to be addressed under each key requirement in order to give a more complete picture about what needs to be done to fulfil the requirement. However, DS 414 is maybe the most important document of the Agency with regard to reactor safety and quality is more important than a short revision time. It also seems essential for the IAEA to use the same structure for all requirements documents. It is mentioned in 1.1 and 1.2 that DS 414 is intended to reflect the present consensus on design requirements for reactors and that the design bases of many new plants have been extended to handle more complex sequences including some severe accidents. This is not consistently reflected in the proposal. In general it is difficult to see on what points the requirements have been increased to reflect the state of the art. See specific comments below. The language needs a lot of polishing and structural considerations. For instance in para 2.14 the numbering does not correspond to the levels of the defence in depth. Paras 4.1- 4.4 are		Y	Wording has been revised.		

3	General	doubled. Some additional management items should be included such as taking into account a future safe decommissioning and requirements on documentation of the design (PSAR, SAR),		Y			
4	Section 3	Last part of the last sentence should be more specific about beyond design basis events. Should be added: **Highly unlikely** severe accident sequences for which it is not reasonably practicable to		Y			
5	Para 4.1	implement mitigatory measures are excluded from the design basis with proper justification.	Compare the wording of para 5.9 and 5.27.				Current wording is adequate.
6	Para 5.28	The main categories should be internal and external events and distinction made between initiating events and consequential events. 5.33 should be in bald printing (shall statement).	We are here talking about mitigatory measures and not preventive ones.				See Fr comment 43, which proposes deletion of para 5.28.
7	Paras 5.31-5.36	More adequate to say: The potential for CCF shall be taken into account.	These paras could be more clear and better structured. Now the distinction between events and hazards are unclear.		See amended structure.		
8	Para 5.49	The worst permissible configuration, capacity level and time should be considered. SSCs important to safety in new designs should be able to be tested, inspected and monitored to the extent	Isn´t that a too low ambition for the current state of the art to say: "The potential for common cause failures shall be considered."	Y			

		desirable.					
9	Para 5.53	This notion could be further developed.		Y			
			This para also shows a too low ambition.				This para is intended for those parts of the plant where best practices are not possible.
10	Para 5.61						
			There seems to be a consensus that PSA should play a more active role in the design of new plants, not only as a verification instrument. The earlier NS-R-1 also provide more objectives for PSA which are still relevant.				PSA is addressed under the recently published GS-R-4.
11	Para 5.106	The system to control instabilities should be automatic.					
		Accident conditions need to be specified: BDB-events including selected severe accidents, or all severe accidents except those justified according to 5.28? This formulation need to be in line with 6.36. What is					Point is covered under revised para 6.51 (Fr comment 69). Accident conditions are defined in the glossary. Specific events such as airplane crash are not addressed in NS-R-1.
12	Para 6.8	required with regard to a major air plane crash?					
13	Para 6.32	It should be specified if the requirements for instrumentation also cover severe accidents. Compare 6.53 which is not a shall statement. 6.49 could be merged with 6.53.			See revised para 6.36 (Fr comment 64)		
		Accident conditions should be specified.					Accident conditions are defined in the glossary.
14	Paras 6.49	Accident conditions should be specified.					See para 6.67
		Replace “is reduced ALARA” with “is kept ALARA”	Compare earlier NS-R-1, 6.71.				

15 16 17 18	Para 6.66 Para 6.72 Para 6.107 -6.113 Appendices	The appendices in earlier NS-R-1 are important for the understanding of the requirements. We recommend that updated versions are included in the new NS-R-1.					Appendices removed as agreed via the DPP process

DS 414, Rev. 14, 03 Apr 2009

COMMENTS BY REVIEWER Reviewers: C. Ryser, B. Stegmaier Country/Organization: Switzerland / ENSI			Page 1 of 1 Date: 2009-06-02	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	3.10.	Structures, systems and components (SSCs) important to safety shall be designed according…	"and" in the orgininal text ("shall be and designed") is superfluous	Y	Text revised by other MS comments to read 'Structures, systems and components (SSCs) important to safety shall be designed according to the latest, currently applicable		

Comment [J10]: Ja 7

Comment [J11]: ENISS5

					standards.		
2	5.72	The systematic consideration of human factors in the design process is supported by a formal programme that specifies how human factors principles and methodologies are applied throughout the design process. Particular attention is given to a user centred approach in the design of the working systems with active involvement of the users (or user representatives) in the design process in an iterative way in order to make sure that the user needs are adequately considered.	I suggest that a new paragraph is added after 5.72. In paragraph 5.72. it is said that HF shall be considered *systematically* and throughout the entire *design process*. This statement suggests the development and application of a HF Engineering programme. I strongly support this view and would welcome to make this aspect more clear by adding some additional considerations (all the other parapraphs with exception of 5.81. are focused on the *product* of the design process).		The users (or user representatives) are actively involved in the design process in an iterative way in order to ensure that their needs are adequately considered.		
3	4.2	To be added: The example of a detailed subdivision of these three fundamental safety functions is given in the annex	In the actual NS-R-1 in para 4.6 this connection is made. Why should the example for safety functions be left out?			Y	To be covered in a guide.
4	5.73.	The design is aimed at supporting plant personnel (users) in the fulfillment of their tasks and responsibilities. It is aimed at limiting the effects of human errors that can impact upon safety and at supporting human strengths and capabilities.	The text should also include the need for a user/human-centred design that supports human capabilities.		'…at supporting plant personnel (users) in the fulfillment of their tasks and responsibilities, and at limiting…'		
5	5.73/line 2	Attention is paid to plant layout and procedures (…), including maintenance and inspection, in order to facilitate the interface between personnel and the plant. Attention is also given to the interaction between human,	- New paragraph: Paragraph 5.73. touches two different issues. - "operating personnel" is too restrictive. All user categories shall be in the		1st part accepted, second part is considered to be covered by the subsequent paras.		

Comment [NN12]: Sw 02 amended

		technological and organisational aspects, for instance to the impact of chosen technologies on individual and collective personnel tasks.	focus of design efforts. - A socio-technical view should be fostered. It is important to consider that human, technological and organisational aspects impact each other. Examples: computerised procedures have big impact on communication within the shift crew; number and organisation of shift crew can have an impact on the design of the control room; maintenance and outage organisation can have an impact on the design of the man-machine-systems (e.g. if maintenance has to be done during normal operation, maintenance and shift personnel might need separate systems to work on and appropriate communication tools) etc.				

DS 414 Safety of Nuclear Power Plants: Design (NS-R-1 Rev 14 03 April 2009)

COMMENTS BY REVIEWER Reviewer: Country/Organization: UK (NUSSC) / HSE (ND) Date: 29 May 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	General		We support the progress of the current version of this document. It provides significantly more substance in the areas of Design Intent, and Defence in Depth, as				

			addressed in design.				
2	General		From the onset, the document uses the term "Nuclear Power Plant". Then, even by the third page, terms such as "all facilities and activities" and "nuclear installations" are being used. The ambiguity should be removed. According to the scope of DS 414, this document will be used primarily for land based stationary nuclear power plants with water-cooled reactors.				"all facilities and activities" is a direct quote from SF-1, so does not need to be changed. Other refs. to nuclear installations have now been amended
3	General		It is not clear what the paragraph numbers in square brackets refer to. If they indicate a change in paragraph numbering between different drafts of the document, this should be made clear.		The square brackets indicate a numbering change between different drafts, but will be removed at the final editing.		
4	Para 2.14 (2), 3rd sentence	The last sentence should be extended to read: "The whole process is supported by a detailed analysis which determines the operational and maintenance requirements for the plant **and the quality control requirements of operational and maintenance**	For completeness	Y			

		practices."					
5	Para 2.17, 5th sentence	Modify to read: "This balance will change when the plant is put into service since much of the detailed knowledge will be transferred to the **operating organisation's intelligent customer at the NPP and its design authority in the operating organisation's technical offices or the offices of the partnering responsible designers.**"	For completeness and clarity		'…operating organization's design entity in the operating organisation's technical offices or the offices of the partnering responsible designers, through…..' Note that "Intelligent customer"reference is not recognized in many member states		
6	Para 3.22, 5th bullet		This bullet states *"the necessary engineering and scientific skills and knowledge are maintained either within the operating organisation or other internal sources or by responsible designers or other sources"*. We do not agree with the words underlined. This seems to be contrary to the "intelligent customer" requirement. It is also inconsistent with current UK guidance; Paragraph 56 of the NIIs Safety Assessment Principles (SAPs) states "*An*		See proposed amendments to the *second* and 5th bullets which make it clear that the knowledge is held by the operating organisation.		

Comment [J13]: UK 5 amended

			'intelligent customer' capability should be maintained …….A capable organisation requires the retention and use of knowledge to understand nuclear safety requirements and to control risks throughout all activities, including those undertaken by contractors."				
7	Para 5.12	Consider modifying to read: "The PIEs are selected on the basis of **a combination of engineering analysis plus deterministic and probabilistic techniques.**"	For clarity	Y			
8	Para 5.34		There needs to be an explanation of where this may exist. Perhaps an example may be sufficient to do this.			Y	This is a well established practice.
9	Paras 5.59 and 5.61		Paragraph 5.59 states "*Structures, systems and components important to safety shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability to meet the required reliability over the lifetime of the nuclear power plant*". However, paragraph 5.61 states "*If the structures,*		See amended para 5.61 which strengthens the requirement.		

			systems and components important to safety are not designed to be able to be tested, inspected or monitored to the extent desirable, then the following approach is followed:..." For new designs of plant, paragraph 5.61 should require a robust justification for why the design requirements in paragraph 5.59 cannot be met. This justification is needed before proposing alternative approaches.				
10	Para 5.60	Insert the following sentences at the end of this paragraph to read: "~~Some sub-~~*Where* systems *structures* or components ~~may~~ need to be withdrawn from the reactor for calibration, test, maintenance or refurbishment~~.~~ ~~The~~ *the* facilities for doing such tasks ~~need to~~ have standards of quality assurance and quality control for components, practices and environment commensurate with the importance of the safety function of the items requiring calibration, test, maintenance or refurbishment."	The additional sentences suggested are needed to address omissions in the current draft.		Amended as shown		
11	Para 5.82		The wording in this paragraph, ie *"5.82 [5.57] Structures, systems and components*		See rewording of this requirement proposed by USA comment 28: "Structures,		

			important to safety shall not be shared between two or more reactors in nuclear power plants." will not allow the requirements contained in paragraph 5.83, ie *"5.83. [5.57] In exceptional cases where structures, systems and components important to safety are shared between two or more reactors, it is demonstrated that all safety requirements are met for all reactors under all operational states (including maintenance) and in design basis accidents."* to be met. This is because shall is an imperative and does not allow for exceptional circumstances. The original wording in NS-R-1 gave room for manouevre.		systems and components important to safety shall not be shared between two or more reactors in nuclear power plants unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and removal of residual heat from the remaining units".		
12	Para 6.59		This paragraph contains a reference to paragraph 6.82, which is not correct for here. It seems likely that paragraph 6.57 [6.82] should be	Y			

Comment [NN14]: USA 28

			referenced here.				
13	Paras 6.101 – 6.102 (Sub-section Control of airborne radioactive materials)	Suggest modifying this sub-section to read: **Control of airborne radioactive material** 6.101 Ventilation systems, with appropriate levels of cleanup are required in nuclear power plant to: ▪ **Support containment** – the building layout and ventilation system work together to provide containment and minimise the spread of contamination for normal /abnormal operations and in the event of an incident. This function ensures the correct area conditions appropriate to the radiological classification of the area. ▪ **Provide adequate cleanup** of the offgas/extract streams, commensurate with the level of challenge (under normal and incident conditions) and the aerial effluent discharge limits of the facility. ▪ **Provide adequate dilution** of noxious/asphyxiant/ explosive atmospheres arising within the facility to ensure operator safety.	This whole section appears to be asking too much from a significant process area, which would appear to be a single system, whereas there may be a number of systems. Following consultation with the UK National Nuclear Ventilation Forum, the proposed text is suggested.	Y	*Minor amendments to existing text only* to clarify that reference is being made to building ventilation systems. *Existing bullet points retained.*		

		6.102 These systems should include appropriate cleanup equipment that must be reliable and able to be tested. The offgas/extract stream cleanup equipment must provide the necessary retention factor to meet the discharge limits."					

Comments on IAEA Draft Safety Guide "Safety of Nuclear Power Plants: Design" (DS414) Draft 14

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	Various	The term 'guarantee' and 'confidence' are not used correctly in regulatory applications. Adherence to regulatory criteria or various standards does not guarantee safety. Similarly applicants do not need to provide confidence that safety is achieved. Recommend using the term 'provide assurance' or 'provides reasonable assurance.'	Improve clarity.		Noted for final editing.		
2	1.6 / 5	"…(PIEs), which include many factors that, ~~singly or in combination~~ themselves or in combination with others, may affect safety."	Adds clarity	Y			
3	1.7 / 8	"• nuclear security requirements, with exceptions for cyber security	Section 1.7, last bullet, states that nuclear		Note that cyber security		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	& 5 [or 6]	as outlined in Section 5 [or 6]" To be consistent with the above modification, add the following statement in Section 5 [or 6]: "Consideration of cyber security included in the design process at an early stage and continue throughout the entire process."	security is not considered in the scope of the document. While t is easier to separate physical security & administrative security controls from NPP design, cyber security is integrated and must be considered at the design stage. In our current global security environment, cyber security must be considered in plant safety. Design features of an instrumentation and control system play a major part in addressing cyber security and administrative or physical security measures alone are most likely not sufficient. For example, the way data is transmitted between instrumentation and control systems can largely affect the		can be inferred from para 5.93 which states: *"Unauthorized access to, or interference for any reason with, structures, systems and components important to safety, including computer software and hardware, shall be prevented."*		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			vulnerability of that system to a cyber attack. Today, many regulatory frameworks do not adequately address cyber security requirements or guidance; yet is a major, credible threat.				
4	2.1	Too much emphasis is placed on severe accidents. Need to include a new paragraph placing emphasis on anticipated operational occurrences and the detection and interception of operational deviations that often occur with releases of radioactive materials, characterized by high probability of occurrence, low risk consequences to the public with doses hovering at about or just over established limits, and significant volumes of liquid or gaseous wastes discharged into the environment.	Current discussion does not reflect recent past and current operational experience.			Y	The point is covered in the discussion on defence in depth, para 2.14 (2)
5	2.13	The 'Concept of Defense in Depth' should include a discussion of emergency preparedness.				Y	This is briefly addressed in the discussion on defence in depth, para 2.14 (5)

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
6	3	"MANAGEMENT SYSTEM PROCESSES[1] 3.#. The management process ensures that the design, fabrication, procurement, and installation of the liquid and gaseous radioactive waste processing systems and effluent radiation monitoring system are implemented in accordance with the requirements of an established QA program.	Silent on QA aspects. Generic observation, here and throughout.			Y	Reference to QA is generally minimised, since the reader is referred to QA aspects under ref 6 relating to Management Systems.
7	3.2 / 2	"…the quality of the design is ensured at all times, which includes the means for identification and correction of design deficiencies, checking adequacy of design, and control of design changes."		Y			
8	3.7 / 2	"…gained in operating plants and of the results of relevant research programmes. 3.#. The design takes due account of relevant experience related to construction failure experience and construction deviation data that has been gained in similar plants."	Construction defect-induced risk could result in increased cost to owner utilities. USA utilities [e.g., Diablo canyon, Columbia-2] experienced significant construction bond expenses due to significant construction schedule delays.		As written, this appears to be a commercial, rather than safety issue. However, para 3.7 has been amended to include a		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			Collection and documentation of construction deviation data and defect data for structures, systems, and components could be made readily available to architect companies for their timely budgetary and schedule management activities.		reference to the issue.		
9	3.10 / 2	"...designed according to the latest or currently applicable standards (see para. 5.16)."	The applicable standards are clarified in 5.16			Y	Generally, it is not IAEA practice to refer to subsequent paras.
10	3.13 / 3	"…supporting research programmes, performance tests with specific acceptance criteria, or by examination of operational experience from…"	For non-standard components, established- research facilities are finding programmatic needs and funding needs for additional verification/validation tests and performance tests to be conducted. Professional engineering societies [e.g. American Society of Mechanical Engineers] require	Y			

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			performance tests to be conducted in order to certify critical components for safe operation of operating plants and new nuclear plants to be built in Euro nations and USA.				
11	3.18 / 2-3	"…manufactured, assembled and erected according to established processes that ~~guarantee~~ ensure the achievement of the requested performance and reliability defined in the design…"	No process can guarantee success	Y			
12	3.22 /	"…of the plant is available and maintained up to date taking into account ~~of~~ past experience…"	Adds clarity	Y			
13	4.2 – 4.5	Consider incorporating the concept of "diverse and redundant" in discussing Defense-in-Depth.	The concept of defense-in-depth includes diverse and redundant.		This is covered in para 5.49		
14	5 & 6	The single failure criteria are inconsistently applied in on a system basis in section 6, however, a broad single failure criterion is applied in section 5.50 (for example ECCS and Containment specifically require consideration of a single failure but RHR and service water do not). Recommend that single	Improve clarity			Y	Some examples have been retained where it is considered that the need for compliance may not be clear.

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		failure discussion in Chapter 6 be removed given that it is already captured in Chapter 5.					
15	5.8 / 5-7	"• design basis accidents; ~~and~~ • beyond design basis accidents in which there is the potential for considerable core damage (severe accidents)~~.~~; and • avoid the cross-contamination of non-radioactive systems; and • avoid unmonitored and uncontrolled radioactive releases to the environment;"	Need to address such events.			Y	This is not appropriate to be included as a category of plant state.
16	5.16 / 3	"…practices ~~(see para. 3.6)~~, or those standards or practices already used internationally or ..."	Clarity to ensure that all acceptable standards are included, not just those from organizations that IAEA supports.		Para ref retained, but wording amended as proposed in Fr comment 36		
17	5.19 / 12	"• action statements and completion of timely milestones addressing deviations from the defined operating limits and conditions."	Discusses actions but does not mention that some actions have to be completed within a specific time frame.	Y	…including completion times for actions…		
18	5.26 / 2	"…the most suitable location to	Adds clarity and removes	Y			

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		ensure its ~~ready~~ availability at the time of need and to allow…"	redundancy				
19	5.32 / 5	"…and monitoring of the state of the plant shall be maintained. 5.## In considering design features of Offgas systems, the design should address component features and equipment malfunction analyses in determining whether the OGS is designed to withstand internal effects of H_2/O_2 detonations or is provided with instrumentation and analyzers to preclude the formation of explosive gas mixtures."	Need to address such events.			Y	This is a design detail more appropriate to a safety guide.
20	5.47	Note that this precludes the presence of "nonsafety" software to be executed on a safety processor, regardless of software function. Safety processors must not be subject to stalling or other misoperation due to software that has not been subjected to full safety-grade controls and verifications.			Point accepted, but is adequately covered in the existing text.		
21	5.49	This includes consideration of software-related common-cause failures			Software is addressed in 6.60		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
22	5.50	Address whether single failure is intended to mean “active” and “passive” failures or not.	Operating experience shows there are significant differences in “active” versus “passive” failures and whether single failure means one or both.				Point is covered in 5.55
23	5.56	In some cases, the “safe state” may depend upon current conditions and may therefore not be reliably predicted in advance. Such cases must be noted and analyzed, and the selected approach to this “safe state” design must be documented and justified.			Point noted, and it is argued that the safety analysis would address this.		
24	5.59	Removal from service must not impact compliance with the single-failure criterion.				Y	Para 5.53 is intended to address the issue.
25	5.61	Note that I&C MUST be designed to be suitably tended and monitored. These provisions will therefore not apply to I&C.			Requirements for testing I&C are covered in 6.56		
26	5.65 5.69	Equipment must be able to withstand PIE and accident conditions when they are at the end of their normal lifetimes, after lifetime exposure to limiting “normal” conditions.			Existing text covers the issue.		
27	5.72	Safety-related HMI must be				Y	Considered to be

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		provided for all necessary manual functions and for monitoring plant conditions as needed. If SR-HMI is different from the HMI used in normal operation, then it must be demonstrated that the time required for the operator to determine that transition from normal to SR HMI is necessary and for that transition to be completed is sufficiently short. It must also be shown that the use of the less familiar equipment will have no negative effect upon the performance of the operator.					covered by para5.78
28	5.82 and 5.83	5.82 prohibit sharing systems. 5.83 permits sharing systems in exceptional cases where it can be demonstrated that all safety requirements are met. Recommend striking 5.82 or replacing both with a requirement similar to GDC 5 – "*Sharing of structures, systems, and components*. Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions,	5.82 and 5.83 are inconsistent and could be improved.	Y	'removal of residual heat', not 'cooldown'.		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units."					
29	5.101	The Safety analyses must be coordinated with the I&C design: • Assumed actuation points must be consistent with instrument channel setpoints in consideration of setpoint uncertainty. • Assumed human response times must be consistent with HMI and I&C design. • The safety analyses must account for all credible conditions that might be caused or augmented by the nonsafety digital control system or the safety-related control and protection system, such as multiple spurious actuations. Misoperation of the nonsafety control system must not place the plant in a condition that is inconsistent with the safety analysis assumptions.		Y	Minor word changes for editorial consistency.		
30	6.3	Precluding recriticality following an	The safety concern is	Y			

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		event is not needed. Not exceeding fuel design limits is needed. Recommend inserting 'that results in exceeding fuel design limits' after 'excursion.'	with exceeding fuel design limits not with recriticality.				
31	6.4 / 1-4	"Fuel elements and assemblies shall be designed to ~~be mechanically robust and to withstand satisfactorily the anticipated irradiation and environmental conditions in the reactor core in combination with all processes of deterioration that can occur in normal operation, anticipated operational occurrences and design basis accidents~~ <u>return their structural integrity following the design basis seismic event over the range of burn-up conditions for their design lifetime</u>."	It is not clear that paragraph 6.5 static and dynamic loading includes seismic vibratory motion. Seismic vibratory response is important if fuel assemblies do not have appropriate ductility and assembly stiffness. This is especially important if spent fuel assemblies are stored in a water pool. This sentence should be added to section 6.5		Fuel elements and assemblies shall be designed to *maintain their structural integrity* and ……. and in anticipated operational occurrences *and PIEs*		
32	6.17 / 2	"…devices, even in design basis accidents, will <u>protect the RCS pressure boundary from overpressure and will</u> not lead to unacceptable releases of…"	The plant design includes adequate protection of the RCS pressure boundary against overpressure events.	Y			
33	6.47	Combustible gas control provisions only apply to design basis events. By and large, you do not have a combustible gas control problem for	Needed for safety.	Y	Para 6.47 amended to read 'accident conditions'		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		design basis events because there is no substantial fuel failure. Recommend adding 'beyond design basis events' to the combustible gas control requirement.					
34	6.51	Operation of the protection system must be consistent with the safety analyses, including consideration of measurement and setpoint uncertainty and including consideration of credible misoperation.				Y	Already covered by comment 29
35	6.54	"The protection system is designed: • to be capable of overriding unsafe actions of the control system; ~~and~~ • to fail to a safe condition; and • to be channalized and meet the single-failure criterion."				Y	SFC is a general requirement.
36	6.55	The design should also minimize the need for operator action in response to any accident or PIE, and should provide for timely action consistent with the safety analyses when operator action is needed.		Y	Added as a bullet point.		
37	6.57	"Design techniques such as testability, ~~including a self-checking~~	With the introduction of computer-based safety			Y	This discussion is more appropriate for

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~capability where necessary,~~ fail-safe behavior, functional diversity and diversity in component design or principles of operation are used to the extent practicable to prevent loss of a protection safety function. Features that increase the reliability of computer-based safety systems (such as self-testing and signal comparison) are balanced against the level of complexity added to the systems. The increased reliability from the feature and the potential unreliability from the increased complexity are justified. Features that do not sufficiently improve reliability or perform a safety function are not included on the computer-based safety system."	systems, many new features and capabilities can be added. In some cases, the new features increase reliability of the system, while others do not add much reliability but are added for convenience. In either case, the features increase the complexity of the computer-based safety systems. For example, regulators are seeing computer-based safety systems that have dozens of microprocessors to accomplish relatively simple safety functions that are reliably accomplished by relays and other analog components in many operating nuclear power plants. Most of the complexity arises from the increased communication between				a safety guide.

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			the independent divisions of the safety system or between the safety system and less important systems. There is a balance between the increase functions to improve reliability and the complexity (potential unreliability) it introduces. Therefore, there should be an assessment and justification for any features/functionality beyond the safety function. Finally, simplicity is a fundamental principle in safety system design.				
38	6.58	The safety system should perform its safety function with one channel removed from service for testing, coincident with one unobserved single failure.				Y	Para 5.53 covers the issue.
39	6.60 6.62	The possibility of software-based common-cause failures must be taken into consideration. Protection			Cyber security to be addressed		

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		from deliberate or accidental interference with system operation must be provided (cybersecurity).			separately, but note response to comment 3 above which draws attention to para 5.93		
40	6.62	There are several instances of nonspecific requirements here (e.g. “very high quality”). These should be defined here, or referenced to some lower-level document.			Point noted. Such requirements are normally expanded in the associated safety guide.		
41	6.63	Safety systems must be fully independent of all systems, equipment, and software of lower classification, and also of the same classification but other division. There must be no sharing of information or resources among divisions or from a lower classification up to a higher classification.				Y	Covered by 6.63.
42	6.64	The signal source must be classified as part of the higher-class system.		Y			

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
43	6.67	Also protect the control room and safe-shutdown locations from excessive heat or cold and from noxious fumes or any other conditions that might interfere with operator performance.				Y	Examples do not need to cover every possibility
44	6.69	All locations must be accessible under all plant conditions, including PIE and accident conditions.				Y	Some locations may not be accessible for all accident conditions.
45	6.71	Communications must not be hindered by PIE or by accident conditions, including loss of power.				Y	Addressed by requirement 6.72.
46	6.81	HVAC for the control room should be safety-grade.			Noted - the requirement would be derived from the classification process.		
47	6.98 / 3	"The ALARA principle shall be applied. 6.## The system should include provisions addressing operational interfaces with plant systems in determining and setting alarm/trip set-points for activating alarms and terminating effluent releases or	New paragraphs suggested, because the topics are not addressed elsewhere.			Y	This level of detail should be included in a safety guide.

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		isolating processes. This aspect should address the placement of detectors in plant systems such that the activation of an alarm and termination of a release or isolation of a process stream occurs before systems/environs located downstream of the detector are affected. 6.##. System calibration should consider whether instrumentation response is expected to change given that radionuclide distributions may vary with the operational status of the plant (i.e., normal operation, anticipated operational occurrences, and accident conditions). 6.##. Process and effluent systems design should address associated sampling equipment used to extract and condition (e.g., pressure, temperature, and humidity) process and effluent streams being monitored. 6.##. System design process					

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		should include a provision to develop, review, verify, validate, and audit digital computer software used in radiation monitoring and sampling equipment, including features used to terminate or divert process and effluent streams. 6.##. All effluent discharge points are defined as the discharge path beginning with interfaces with plant primary systems and terminating at the point of controlled discharge to the environment."					
48	6.117	Monitors may also be appropriate in locations not subject to contamination under normal conditions but possibly subject to contamination as a result of equipment failure or other unusual circumstances.		Y	Monitors are also located in areas possibly subject to contamination as a result of equipment failure or other unusual circumstances.		
49	7. / 9	"…meteorological conditions (extreme winds, tornadoes, snow loads, severe lightning events), biological phenomena,..."				Y	Examples only are indicative, not comprehensive.

Comment [NN15]: USA 48 amended

COMMENTS BY REVIEWER Reviewer: United States of America Country/Organization: United States of America/ NUSSC Date: June 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		"…explosions external to the site (from other industrial installations and transportation accidents), asphyxiant and toxic gases,…"					

DS 414 Safety of Nuclear Power Plants: Design

COMMENTS BY REVIEWER Reviewer: Page 1 of 2 Country/Organization EC Date: 20 April 2009				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text/ Comment	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	General	The draft DS is **very well** prepared and the revisions introduced to the NS-R-1 are well identified; which facilitates a lot the NUSSC members review. The revision is well done and the document might be submitted to the MS. Some editorial comments are provided bellow for possible consideration.					
2	1.3	Is there general agreement on this subject? It is suggested to bring this issue to the	Clarification			Y	See revised wording

		attention of the NUSSC members in June 2009 meeting and see whether there is consensus.					
3	1.7	Delete first bullet	If there are requirements related to the design in some other IAEA SS they shall be cited. Requirements in the IAEA SS not relevant to the design are not of interest to this document.				This bullet is intended to draw attention to the ongoing process of revisions to IAEA publications, for example GS-R-4, the implications of which remove the need for detailed reference in NS-R-1 to assessment.
4	2.1&2.7	Reference is made once to FUNDAMENTAL safety principles once only to safety principles. Make the text consistent	Consistency	Y			
5	2.17&2.18	May be these para could be deleted	Better clarity. The subject covered by 2.17&2.18 is better defined in 3.19-3.22				These paras. are intended to explain the concept, not the specific requirements.
6	5.7	Replace "Initiating events" with "Event sequences" or "PIE"	Otherwise it is not clear what is meant by just initiating events	Y			
7	5.13	Delete "numerical design and"	A slang is introduced which does not bring much added value but may confuse the translations in other languages		'numerical' replaced by 'the'		
8	5.16	Please check reference to para 3.6	Seems to be a mistake		Should be 3.10		
9	5.31 – 5.36		The text is somewhat not systematically presented here. E.g. 5.31 mentions Hazards(external and internal) then Fires and explosions are caused by external events than suddenly we have OTHER (		This section has been revised and restructured..		

			comparing with what??) internal events and again External events that are supposed to be different external hazards already addressed in 5.31?? Any streamlining of the text here may help to improve the clarity				
10	6.60 – 6.62	May be ”computer based systems” could be replaced with “computer based equipment”?	To avoid tautology	Y			

TITLE:
IAEA SAFETY STANDARDS: Safety of Nuclear Power Plants: Design, Draft Safety Requirements DS 414
NS-R-1, revision 14, 03 April 09

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
General comments		This draft underwent significant improvements since the last known version. The restructuring of the text along IAEA guidance is very welcome: this reduces the number of “shall” and provides clarity in the document making clear distinctions between real requirements and explanatory statements. Some simplification has also been provided, as suggested by ENISS, and most of our previous comments have been considered. Thanks to the technical officer. However, we think that the first part of chapter 5 should be restructured to make clearer the distinction between design basis accidents, beyond design basis events and those events that could be excluded and for each of them the corresponding design rules. All these elements are presented in the text of this draft but in a bit confusing order. For example, 5.16 and 5.17 should be placed between 5.20 and 5.26 and 5.15 should be after 5.30. Para 5.18 and 5.19 could be moved just after 5.58. We have noticed that the sections related to the respective role of the deterministic and probabilistic approach have been drastically simplified and we offer some comments to reinforce the role of PSA in the design. We continue to think that the concept of “safety group” in the implementation of the Single Failure Criteria which has been scarcely used since the first version of NSR-1 brings more confusion than clarity and should be replaced by “safety functional group”.			Highlighted part will be addressed in final editing.		

COMMENTS BY REVIEWER Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		The items under 5.23 to 5.26 which deal with operator action could be simplified and its details would be more useful in a guide. In the original draft considered at the TM May 2008 there was a comment in the "Background" section referring to the application to design types other than LWRs. This has now been omitted and the scope is not entirely clear. Although it is recognised that the principle applications will be to LWRs, it would be useful to indicate that some of the basic principles have wider applicability. Some further comments are provided below.					
1	1.8	This Safety Requirements publication follows the relationship between principles and objectives for safety, and safety requirements and criteria. Section 2 elaborates on the safety ~~principles,~~ objectives, principles and concepts which form the basis for deriving the safety requirements that must be met in the design of the plant.	To be in line with the title of chapter 2.	Y			
2	2.3		Paragraph 2.3 is missing		Renumbering will be in final editing.		
3	2.14		Paragraph 2.14 contents description of Defence in depth. There are 6 items, but actually there are 5 levels of defence – that is confusing. Point 2 describes no level in defence in depth and the character is informative only. Suggestion: take of the Nr 2 and to let separate article without numbering.	Y			
4	2.17	Pre-licensing the responsibilities for the design will rest with the design entity organizations but once the plant	For clarification	Y			

Formatted: Font: (Default) Arial, Complex Script Font: Arial

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		is ordered the ultimate responsibility will lie with the <u>license holder</u> ~~customer~~, however, the detailed knowledge will rest with the responsible designers.					
5	3.10	Structures, systems and components (SSCs) important to safety shall be and designed according to the latest, ~~or~~ currently applicable standards.	The criterion should be the latest standard which is applicable rather than their being a choice	Y			
6	4.1	The design shall provide adequate means to maintain the plant in a normal operational state; to ensure the proper short term response immediately following a PIE; and to facilitate the management of the plant in and following any design basis accident, and ~~following those plant states~~ <u>those accidents</u> beyond the design basis that are considered <u>in the design</u>.	To improve clarity		Note that this requirement has been deleted and replaced by 4.2		
7	4.1 to 4.4		Paragraph numbering is not correct. These paragraph numbers appear under FUNDAMENTAL SAFETY FUNCTIONS and REQUIREMENTS FOR DEFENCE IN DEPTH		Noted for final editing		
8	4.4	FUNDAMENTAL SAFETY FUNCTIONS Monitoring of plant status is provided to ensure that the required safety functions are <u>available and</u> achieved	The availability of the safety functions is important to be monitored.	Y	New para 4.4a added		
9	5.6		This would be better placed after 5.8. Otherwise it is not clear why you want to define	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			these categories. It is so you can apply different acceptance criteria as part of the graded approach.				
10	5.16	The engineering design rules […] shall comply with ~~the appropriate accepted national standard engineering practices, or those~~ standards or practices already used internationally ~~or established in another country~~, and whose …	National standards in non industrial countries could be insufficient for the design of NPPs. International standards should be used to facilitate standardisation.		See revised wording provided in Fr comment 36.		
11	5.27	…. to implement those reasonably practicable provisions for their prevention and mitigation and to provide additional margin to the overall safety objective of the plant	Without this addition, the requirement may impose measures or modifications that have little safety benefit. This will be more in line with a risk-informed approach			Y	See revised wording provided in Fr comment 43 & 44.
12	5.46	The design ensures that any failure of structures, systems and components in system classified in a lower class will not propagate to a system classified in a higher class. Any non compliance should be clearly justified in the safety analysis.	This statement might be difficult to implement on some components of existing plants such as cable. Exception should be allowed under proper justification (using for instance functional analysis)			Y	The existing wording is well established
13	5.48	….And such that their quality ~~and reliability~~ is commensurate with their safety classification	Classification is linked with safety and quality, not with reliability.	Y			
14	5.50	The single failure criterion shall be applied to each safety functional group incorporated in the plant design to perform all actions necessary in response to a particular PIE.	The term “Safety Group” was created by the fathers of the NS-R-1 but had been very scarcely used. It introduced a concept not easy to understand and to discriminate from the concept of “function”. The SFC has to be applied to a set of equipments which are grouped to achieve a safety function. The wording “safety functional group” convey better	Y			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			this idea than the wording “safety group”				
15	5.59	….their functional capability to meet the ~~required~~ reliability <u>target</u> over the lifetime.…	Reliability is a performance objective not a safety requirement. The term “reliability target” used in previous version was more correct.	Y			
16	5.69	… so as to take into account relevant ageing, <u>neutron induced embrittlement</u> and wear-out mechanisms and potential age related degradation, ….	Neutron induced embrittlement is a very specific nuclear ageing mechanism that should be mentioned here	Y			
17	5.71	Provision is made for monitoring, testing, sampling, and inspection, to asses ageing mechanisms predicted at the design stage and to identify unanticipated behaviour or degradation that may occur in service. <u>Potential exceptions are justified according to 5.61</u>	Potential exceptions on 5.59 are provided in 5.61. Similar exception should be provided here.	Y			
18	5.89	The escape routes meet the relevant ~~national~~ international requirements for […]	To be consistent with comment on 5.16.			Y	National requirements may be more onerous
19	5.104	In first bullet point replace “design basis” by “design envelop”	Design bases are defined for individual SSSCs. The analysis confirms that for the plant as a whole this envelops all design basis accidents.	Y	‘….design bases for all SSCs important to safety; Note that the expression ‘design envelope’ may not be		

COMMENTS BY REVIEWER Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					readily understood in all MSs		
20	5.104 and 5.105	The deterministic safety analysis mainly provides: ….	These 2 paragraphs have been simplified and perhaps over simplified for the respective interest of deterministic and probabilistic approaches. (ie PRA is used to identify and justify selection of PIEs)	Y			
21	5.106	To add as a second bullet: • To identify any additional PIEs and especially the one belonging to Beyond Design Basis that have to be considered	To be consistent with 5.27			Y	Covered by para 5.27
22	6.4 and 6.7	6.4 Fuel elements and assemblies shall be designed to be mechanically robust and to withstand satisfactorily the anticipated irradiation and environmental conditions in the reactor core in combination with all processes of deterioration that can occur in normal operation and in anticipated operational occurrences ~~and design basis accident.~~	There is a contradiction between the requirement of 6.4 that asks for the fuel elements and assemblies to be robust under design basis accident and 6.7 that describes the present situation of fuel elements behaviour under LOCA. We suggest deleting reference to deign basis accident in 6.4 and transforming 6.7 in a requirement and not an explanation and moving it just after 6.4	Y			
23	6.33	[…] associated systems for the control of pressures, temperatures and moistures; and features […]	Keeping water content in the air at an acceptable level for personnel and equipment See also 6.81.		…and moisture levels…		
24	6.54	The protection system is designed: • To be capable of overriding unsafe actions of the control system; ~~and~~ •	The objective of the protection system is not to fail		'achieve', not 'meet'		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Dr. W. Zaiss Country/Organization: ENISS			No Pages: 6 Date: 28/05/09				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~To fail to a safe condition~~ to meet safe condition in case of failure					
25	6.106	For reactors using a water pool system for fuel storage, the design ~~shall~~ is provided with the following:	This is not a requirement. To be consistent with 6.105 the word "shall" should be deleted.	Y			
26	Glossary	Definition of terms ***Severe plant conditions*** (*Event, or sequence, with a very low frequency of occurrence, with consequences that are beyond the design basis, and against which mitigating measures have been provided in the design*) and ***Complex sequence*** (*Event, or sequence with a low frequency of occurrence, with consequences that are beyond the design basis, and against which mitigating measure have been provided in the design*) is identical with the small difference – word "*very*". It should be better to use one term (Complex sequence), which is included in more documents.			To be considered in final drafting		