“Safety Classification of Structures, Systems and Components in Nuclear Power Plants”
DRAFT SAFETY GUIDE DS367

COMMENTS BY REVIEWER Reviewers: Ukraine, Pakistan, USA, UK, Canada, Japan, France, Germany Korea, Poland, Finland, ENISS, IEC No. of Pages 54 Date: 11 Nov 2012				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
CAN	Title (DM,MdV)	Consider changing the title from ‘ … in Nuclear Power Plants” to “ …in Reactor Facilities”	Editorial; General principles are the same for both.		X		According to the DPP, this SG is primarily developed for NPPs. However, the proposed guidance might be applicable to other Nuclear Facilities with appropriate adaptations and verification. The proposal is to reflect this statement in the scope and to refer only to NPPs in the core text

JAP	P.3 SCOPE	Due to the lesson learned from the Fukushima Daiichi Nuclear Power Plant's accidents, it is important that external hazards (e.g. earthquake, tsunami etc.) should be considered in the classification process. However it is not clear that the classification of SSCs against external hazards is treated in this safety guide, this should be mentioned clearly in SCOPE.			X		Protection against external hazart is explicitely considered in the guideline. 3.9 dealing with "design provisions" specifies the conditions to consider the SSCs implemented to protect the plant against external hazards: *"To limit the effects of hazards considered in the plant design basis*[1] *(e.g. civil structures of buildings important to safety);"*
KOR	1.4 /5 2.1 /4 3.8 /4 etc.	On the basis of their classification, SSCs are then designed, manufactured, constructed, operated, tested, , inspected and maintained in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.	PSI and ISIs other inspections are also conducted according to safety classes.	X			
GER	1.4	Footnote No. 1: "Factors relevant for determining the safety significance of items important to safety are set out in <u>para</u> 5.34 of Ref. [2]."	Missing word.	X			
FRA	1.4	The goal of safety classification is to identify and classify the SSCs that are ~~essential~~ <u>needed</u> to protect people and environment	"Essential" SSCs are a part of SSCs needed to ensure safety. Essential SSCs should have a "high" safety class.	X			

[1] If the analysis of postulated initiating events performed according to national practice does not include hazards analysis.

FRA	1.4	On the basis of their classification, SSCs are then designed, manufactured, constructed, operated, tested and maintained in accordance with established processes that ensure the achievement of the design specifications and the ~~required level of~~ <u>expected</u> safety <u>performance</u>.	"Level of safety" is somehow unclear.	X			
POL	1.4/1-3	The goal of safety classification is to identify and classify the SSCs that are essential to protect people and environment from harmful effects of ionizing radiation, **considering** their roles in preventing accidents, or limiting the radiological consequences of accidents should they occur.	The formulation "irrespective of" is incomprehensible, as safety functions to be fulfilled by SSCs are just aimed at preventing accidents, or limiting the radiological consequences of accidents should they occur.	X			
FRA	1.5	~~The general approach and method of classification provided in this Safety Guide reflect the expectations of the regulatory body to justifying a classification. Furthermore,~~	Superfluous. The need exists also for licensees when looking at design submitted by vendors… See also 1.7	X			
CAN	1.8 (DM,MdV)	Change 'nuclear power plant' to "nuclear facility"	Editorial; Broaden scope to include any facility using a nuclear reactor.		X		See CAN 1 First application is for NPPS, but the guide might be applicable to other facilities as stated in 1.6. All text has been modified accordingly.
GER	1.8	"…to safety for all plant~~s~~ states, including all modes…"	typo	X			
POL	1.8/1	This Safety Guide applies to all SSCs important to safety for all plant types and states, including all modes of normal operation, during the lifetime of a nuclear power plant.	This Safety Guide applies both to all plant types and states and should clearly stated in the text.		X		In the scope, it will be specified that the guide is applicable to all NPP Types

CAN	1.9 (CL)	This Safety Guide is not readily applicable to OPG sites.	As indicated in section 1.7, the Guide in intended primarily for organizations designing nuclear facilities, and the approach (Section 1.9) may not be fully applicable to existing facilities built with earlier classification principles, such as OPG's.	X				As mentionned in 1.9, the Guide may not be fully applicable to existing facilities.
FRA	1.9	~~The way in which this Safety Guide would be applied to such facilities is a decision for individual States.~~ For these existing facilities, it may not be practical to mix their current classification scheme and the one recommended in this guide.	1.9			X		Conventional statement for all IAEA Standards
FRA	1.10	Locate 1.10 after 1.7	This paragraph is not really describing the scope of the guide.	X				
FRA	2.1	with sufficient quality to fulfill the functions that they <u>are expected to</u> perform and, ultimately the main safety functions	To stress the link with the design intent and safety case assumptions/conclusions	X				
FRA		The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methodologies complemented where appropriate, by probabilistic methods <u>and expert judgement</u>,	To enable expert judgment	X				

GER	2.1	Footnote No. 2: “According to the IAEA Safety Glossary [4], the formerly named ‘fundamental safety functions’ are now named ‘main safety functions’. In any quotation of IAEA safety standards, the term ‘fundamental safety function’ is to be understood as ‘main safety function’~~”~~ and is ~~are~~ identified with (*) in the text.”	Editorial.	X			
PAK	Page 7 line 1 Section 2.2	Requirement 27: Support service systems Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.	In section 2.2 “BASIS REQUIREMENTS” of the draft guide requirements for a classification are mentioned based on SSR-2/1, however, the requirement number 27 is also relevant and may be mentioned in the draft safety guide.	X			
GER	2.2	“(d) The time following a postulated initiating event … to perform a safety function.~~”~~ The design shall be …”	Editorial (deletion of unnecessary quotation mark).	X			
JAP	P.7 footnote 3	None	Confinement function, which is performed by piping system or containment, does not need an action for the function. Definition of the function should be clarified.			X	Formally, only containment isolation or confinement of radioactive materials should be used. The former refers to a function, the latter to fuel cladding, pipes, tanks, etc..
FRA	2.3	Any ~~preliminary~~ assignment of SSCs to particular safety classes should be justified using deterministic safety analysis complemented by insights from	The type of inputs don’t change whether they are used early in the project or at a		X		Since “preliminary” has been deleted, the iterative process includes the different design stages

		probabilistic safety assessment and supported by engineering judgment, recognizing that available information may change depending on the progress of detailed design and safety assessment.	confirmatory steps. However, for each type of input, more detailed or more substantiated information will be available as the project progress…				(basic, detailed, final)
GER	2.3	General note: The footnote No. 8 assigned to the term 'engineering judgement' in para 3.27 should be transferred to para 2.3.	The term 'engineering judg(e)ment' is introduced for the first time in para 2.3 and is used several times in the document (paras 2.17, 3.22 and 3.27). Consequently, it should be explained in more detail here, and not at the end of the draft document.	X			
GER	2.3	2nd sentence: "~~Any preliminary a~~Assignment of SSCs to particular safety classes should be justified using deterministic safety analysis complemented by insights from probabilistic safety assessment and supported by engineering judgement."	1) Doubling of text with para 2.17. Any assigment of SSCs to particular safety classes, whether it is final or preliminary, should be justified as described. To avoid duplication, para 2.17 should be deleted. 2) Typo		X		"Preliminary" has been deleted. Regarding deletion of 2.17, and although overlapping with 2.3 that is part of the "general recommendations", the aim of the outline of the safety classification process is to describe all the steps of the classification to support figure 1.
CAN	2.2; 2.3; 2.17; 3.22; 3.27 (HC)	The role of probabilistic methods is not clear in the document.	Technical; What is the proper way to apply probabilistic rules together with deterministic ones? Especially if there are			X	Considering both deterministic and probabilistic results gives more confidence in the classification of SSCs. In case of differences

			different results from PSA and DSA? For example, if a System is considered important to safety from the PSA results. However, from deterministic results, the same system is considered within the non-safety category. And, if this system is added to the list of systems important for safety, in witch safety category this system will be included (safety category 1, 2 or 3).				between PSA and DSA, guidance is provided in 3.27.
UK	2.2 (d) And 2.12 point 3)	(*d) The state of the transient following a postulated initiating event and in particular whether the plant has achieved a controlled state.*	Time is not the important criteria in determining whether the classification of a system can be reduced. It is the nature of transient and in particular the fact that the facility has achieved a controlled state. This can take from seconds to more than 12 hours but the time and duration is a by product of the facility's response to PIEs, it is not the prime driver.	X			Agreed, time is not the most relevant factor for classification. However it is used by some Member States and also reflects the content of SSR2/1.
FRA	2.6		• The meaning of a "design provision" is not			X	In former revisions, different proposals have

			so clear and the choices of these words to describe the concept may not be appropriate. What would be its translation in non-English languages (for example in France : “disposition de conception”, which would have a broader meaning than the one of the draft) ? • Figure 2 and Para 3.9 give a clearer understanding of what are design provisions. 3.23 also helps in understanding what accidents are to be prevented by design provisions? • The concept appears interesting but wording should be improved both to “name” the concept and to describe it…				been made. After several meetings, this wording has been considered so far has the best proposal.
JAP	Para 2.6, footnote 4	Example of the design provision should be expressed.	Para. 2.6 mentions “The design provisions may be associated with ・・・ the functions for the control and/or mitigation of AOO, DBA		X		Para 3.9 provides guidance to understand what design provisions means. Footnote 4 has been expended to make the link with section 3.9.

			and DEC ･･･ “. If the design provisions are not only SSCs for prevention function but also SSCs for mitigation function, this is inconsistent with the arrow of design provisions in Fig. 2. We need some examples of the design provisions for comprehension.				Design provisions correspond to SSCs that cannot be captured by the accident analysis, which only considers the mitigation. Examples of “design provisions” are: - Shielding for workers, - HEPA filters to reduce radiological releases, - Piping/Tanks containing radioactive materials
FRA	2.6 footnote 4		The “definition” of a “design provision” is important and should not be in a footnote. A link with Fig 2 should be made. According to this Fig 2, a design provision is “something” that decreases the frequency of an event.		X		The “definition” of “design provision” is detailed in 3.9. Footnote 4 has been expended to make the link with 3.9
FRA	2.6 footnote 4		It would be worth to put, in a footnote, some examples of “design provisions”		X		Link with 3.9 made in the footnote. 3.9 modified to include examples
FRA	2.6		It is not obvious how the “The safety classification process recommended in this			X	The direct link between DID and Safety Classification was one of the most important reason

			Safety Guide is consistent with the concept of defence in depth”				of rejection of the Safety Guide in the former version.
FRA	2.6		The way 2.6 is written could imply that functions are not necessary for the first level of DiD or to prevent AAO or accident conditions. **Considering the current and above comments on 2.6, maybe deleting 2.6 could be an option (3.9 deals more clearly with design provisions)**		X		For DID level 1 the following has been added :” *or any function needed to keep the plant within normal conditions*”
POL	2.6/2-3 and further in the text	The safety functions[3] performed at the different levels of defence in depth are considered.	The term “safety function” – as defined in the IAEA Safety Glossary 2007, and used in Draft 6.2 of this safety guide – should be used elsewhere in this document, instead of “function”. The term “safety function” is also used in the SSR-2/1 document (para. 5.34), as referred to in para. 2.2 of this document). So, the use of the term “function” **would be inconsistent** with both the SSR-2/1 document and also with para. 2.2			X	The method is aimed at identifying the functions/systems that are accomplishing the *3 main safety functions* in any plant state. At the beginning of the classification process the guideline asks for identifying all of the functions/systems involved and categorizing them according to the 4 factors. Depending on the results, the functions/systems are assigned in 1,2,3 or NC category. Thus the use of “*safety function*” is not necessary.

			of this safety guide. The safety functions should be then referred to the fundamental safety functions (as it was done in para. 3.5 of Draft 6.2). Then examples of safety functions for a LWR plant should be provided in Annex I (as it was done in Draft 6.2).				
POL	2.6/3-6	The design provisions[4] may be associated with the first level of defence in depth and the functions for the control and/or mitigation of anticipated operational occurrences, design basis accidents and design extension conditions, with the second to fifth levels of defence in depth.	This approach in safety classification consisting in using the “design provisions” in parallel with “(safety) functions” is not common one, and it was not justified in the document. Moreover the term “design provisions” and its application is not clear enough (see: comments 6 & 7 below). If this approach is accepted by Member States, then examples of these “design provisions” should be provided (at least in footnote 4) to explain better and illustrate this concept.		X		This guideline proposes to identify functions and design provisions in order to capture **all SSCs** to be classified. Footnote 4 has been expended with a link to 3.9. 3.9 will provide examples.
CAN	2.7 (SB)	Suggest deleting write up on ‘constant risk’.	Technical; Suggested since such a concept	X			

			would be difficult to implement practically. (Ref to June 2012 version)					
CAN	2.7 (DM,MdV)	Include "configuration management" as an aspect of the classification documentation.	Editorial; The basis for the classification process should consider the future needs of a configuration management program. The classification methodology should not be overly complex and ambiguous.	X				
FRA	2.7	~~If the final classification of SSCs is not available prior to granting authorization for a nuclear power plant, it should be demonstrated that a suitable design verification and change control process exists that has been independently validated by the licensee or applicant and the regulatory body.~~ It should be emphasized that not obtaining regulatory body view on final classification of SSCs early enough in the design or construction of a NPP could result in significant changes to the plant or limitations in operation.	The guide should not encourage delaying final classification of SSCs.	X				
POL	2.7/3-7		This sentence **should be deleted,** because a final safety classification has to be done and required before granting a construction permit (consent), as the safety classification determines the	X				

			engineering design and manufacturing rules for SSCs which must be specified in the safety documentation to be submitted to a regulatory body in support of an application.				
FRA	After 2.7	Add a paragraph after 2.7 "2.# To manage cases, if any, where the final classification of a SSC would be more stringent that its preliminary classification, processes should be defined and implemented to ensure that design and manufacturing have either (initially) been performed consistently with the final classification or have been (later) made consistent with the final classification, thus demonstrating that the SSC characteristics do meet the classification related requirements."	Add a paragraph to address impact of a more stringent classification that initially envisaged.			X	Design must be in accordance with the final classification of SSCs. The guide is not aimed at describing design configuration management.
ENISS	2.9 p.8	2.9. …Using information from safety assessment, such as the analysis of postulated initiating events, the functions are then categorized on the basis of their safety significance, following a ~~constant~~ risk approach as described in para. 2.12 and Section 3. The SSCs belonging to the categorized functions are then identified and classified on the basis of their role in achieving the function. The SSCs implemented as design provisions can be classified directly because the significance of their failure is direct.	The word "constant" should be deleted as it is not defined in the glossary.	X			
CAN	2.9 (DM,MdV)	Consider revising text to include "Refer to Table 1 for examples of functions."	Editorial; Suggest referring to Table 1 here			X	The Annex 1 has been added to reflect the

			as it provides examples of functions.				application of the engineering rules for systems and is not directly linked to 2.9
FRA	2.9 p.8	2.9. …Using information from safety assessment, such as the analysis of postulated initiating events, the functions are then categorized on the basis of their safety significance, following a ~~constant~~ risk approach as described in para. 2.12 and Section 3. The SSCs belonging to the categorized functions are then identified and classified on the basis of their role in achieving the function. The SSCs implemented as design provisions can be classified directly because the significance of their failure is direct.	The word "constant" should be deleted as it is not defined in the glossary.	X			
FRA	2.9	Using information from safety assessment, such as the analysis of postulated initiating events, the functions are then categorized on the basis of their safety significance, following ~~a constant risk~~ <u>the</u> approach as described in para. 2.12 and Section 3.	No need to introduce the concept of "constant risk approach". Fig 2 and 2.12 (as modified – see further comment) are enough		X		"*Constant*" has been deleted
FRA	2.9	The SSCs implemented as design provisions can be classified directly because the significance of their failure is direct.	Wording should be improved (directly direct…)		X		New text proposed: "*A SSC implemented as design provision can be directly classified because the significance of its failure is .sufficient enough to assign it to a*

							safety class."
POL	2.9/Fig. 1	Description in the top left block: "Identification of design provisions important for safety necessary to prevent accidents or to protect workers, the public and the environment against radiological risks in operational states[2], design basis accidents and design extension conditions"	This description must be consistent with the explanation provided in para. 2.6: "The design provisions[4] may be associated with the first level of defence in depth and the functions for the control and/or mitigation of anticipated operational occurrences, design basis accidents and design extension conditions, with the second to fifth levels of defence in depth."		X		2.6 takes into consideration "design provisions" and "functions". And is a general section. Footnote 4 which explains what "design provision" are has been expended to include operational conditions, in order to be consistent with the figure and 3.9.
POL	2.6, 2.9/Fig. 1, 2.13, 3.23	Consider bringing back the classification approach and flowchart Fig. 1 from the document Draft 6.2.	The classification process based entirely on analyses of safety functions for all the SSCs seems to be more consistent and logical than that proposed in Draft 6.5 (with "design provisions" not categorized in parallel).			X	Version 6.2 was not accepted by NUSSC
WNA	2.9/line 3	"…this information, the functions and design provisions required to fulfill…"	The definition of "design provisions" is not clearly specified. The term is simply stated without a clear definition in the safety guide		X		Design provision is defined in footnote 4. The definition has also been expended in order to consider other similar

[2] Normal operation and anticipated operational occurrences (see: IAEA Safety Glossary 2007, "plant states", p. 144).

							comments.
WNA	2.10/line 5 Grammatical error	• The frequency of occurrence of the postulated initiating events, as considered in the design basis of the facility, should be taken into account.	There are currently two bullets, but the last sentence about frequency of occurrence of postulated initiating events looks like perhaps it should be a stand-alone bullet. Please confirm	X			
UKR	2.12	This item is not needed for function categorization	Does not influence on safety significance			X	Comment not understood. 2.12 provides the factors to determine the safety significance
UK	2.12 add footnote	Add the following footnote to the description of the constant risk figure: *One member state complements the use of constant risk approach with that of the unmitigated hazard. Using this technique, the importance of a safety function is determined by assuming it is not present following the postulated initiating event and then directly computing the radiological consequences without any SSC mitigation or prevention. High, medium and low consequences are specified in terms of offsite and onsite doses from the unmitigated hazards and these complement constant risk based approaches in order to determine the category of a safety function. Such an approach is also deemed to meet the principles of this guide.*	The constant risk approach is often very complex and cannot be readily applied early in the design process. Whereas the unmitigated hazard is consistent with early design principles where there is good knowledge on the radiological hazard and the main safety functions but there is a lot of uncertainty about many aspects of the design of SSCs and the contribution they make to reducing risks.		X		According to similar comments from other Member States, the notion of "*constant risk*" has been deleted because too difficult to be demonstrated. However the notion of "*risk approach*" is kept because consistent with SSR 2/1 asking for screening both the consequences and the probability. Thus it is not considered necessary to add a footnote.
ENISS	2.12 p.10	2.12. The functions should then be categorized into a limited number of categories on the basis of their safety significance, using a ~~constant~~ risk approach, with account taken of the three following factors:	Idem	X			

CAN	2.12 (SX)	Consider revising "The constant risk approach is based on the principle that the more likely the event, the lesser its consequences"	Technical; This section tells what the constant risk is. However, it does not tell how to use the constant risk to do classification.		X		According to similar comments from other Member States, the notion of "*constant risk*" has been deleted because too difficult to be demonstrated. However the notion of "*risk approach*" is kept because consistent with SSR 2/1 asking for screening both the consequences and the probability.
CAN	2.12 (HC)	In section 2, clarify the role of the constant risk approach figure and the three factors to be consistent with section 3 descriptions	Technical; An inconsistency is noticed between the figure 2 (page 10) and the text of the section 2.12. The text indicates that "The functions should then be categorized on the basis of their safety significance, using a constant risk approach, with account taken of three factors. However, the figure 2 shows that the constant risk approach is depending of only two factors.		X		Time (3rd factor) is of less importance in the classification process and might be not considered at all. However it is used by some MS and is also identified in SSR2/1
CAN	2.12, 3.13 (HC)	The use of constant risk should be reviewed.	Technical; Since the Fukushima accident the 'constant risk' concept has proved risky.	X			According to similar comments from other Member States, the notion of "*constant risk*" has been deleted because too difficult to be

							demonstrated. However the notion of "*risk approach*" is kept because consistent with SSR 2/1 asking for screening both the consequences and the probability.
FRA	Fig 1	Identification of postulated initiating events considered in the design ~~basis~~ for the plant	To avoid confusion with DBA (and include DEC)		X		Modified in "*Plant Design Basis*" in the whole text
FRA	Fig 1	Categorization of the functions ~~based on a constant risk approach~~ according to their safety significance	Avoid the use of "constant risk approach" (see previous comment)	X			
FRA	Fig 1	Identification of design provisions ~~important for safety~~ necessary to prevent accidents or to protect workers, the public and the environment against radiological risks in operational conditions	Superfluous	X			
FRA	Fig 1	Design, ~~and~~ manufacturing and other engineering requirements for SSCs as well as operation requirements	To be more consistent with 1.4 and 2.1		X		To be consistent with section 4, same formulation as in title is proposed ("*applicable engineering design rules for SSCs*")
ENISS	FIG 1 p.9	Delete in the flowchart indicating the classification process the word "constant"	Idem	X			
US	Fig 1	Add a convergence criterion or question to the decision diamond, and "yes"/"no" labels to the output paths. The convergence criterion or question could be "Have all the events, functions, and design provisions been identified, and all the required SSCs been classified?"	Clarity		X		Proposal replaced by "Completeness and Correctness"
US	Fig 1	Delete the box indicating "Iterative process	Not necessary		X		Not totally necessary but

		and modification”					consistent with the text
GER	FIG. 1	• Split Fig. 1 into two separate figures for both processes: o An iterative process to identify and classify SSCs to control PIE (left branch of Fig. 1) and o a sequence for classification of SSC implemented as design provisions (right branch without feedback and without the step to identify PIEs). • As “design provision” is a new term in the IAEA safety standards, a definition shall be provided in this guide and an implementation in the IAEA Safety Glossary shall be considered.	The left branch in Fig.1 describes the requirements to control PIEs. Safety functions to control PIEs as well as necessary SSCs will be identified. The identified SSCs will be classified according to its safety significance. This part of the process is properly described. The right branch addresses SSCs implemented as design provisions (according to para. 3.9) which are necessary • to eliminate events, where no SSCs to control those events are provided in the design (e.g. failure of the reactor pressure vessel), • to limit consequences on reactor safety due to internal and external hazards or		X	X (bullet 1)	In both cases, the assessment of the consequences needs a safety assessment. Footnote 4 of 2.6 has been expended with a link to 3.9 which provides further explanations and examples

			• to practically eliminate early and large releases supplementary to the control of PIEs. In contrast to the process shown in Fig. 1 the right branch is indeed not based on a safety analysis of PIEs. Thus, two separate processes have to be considered: • Process 1: to control PIEs • Process 2: practical elimination of events not controlled or considered in the design. Here, no safety analysis is performed and no feedback (iterative process) is needed				
CAN	Figure 1 (DM,MdV)	After prevent add 'and mitigate'	Technical; Should mitigation be included in design provision identification box?			X	Basically "design provisions" are aimed at preventing accidents or limiting effects/propagation of

							accident/hazards. Mitigation is restricted to core or radiological consequences
CAN	Figure 1 (DM,MdV)	Add text to decision box.	Editorial; No text for a question in decision box	X			
CAN	Figure 1 (DM,MdV)	Add more explanation so application of constant risk approach can be understood by a new process user. Also refer to section 3.13	Technical; More detail is required for constant risk approach.		X		"*Constant Risk*" Approach has been deleted
CAN	Figure 1 (HC)	Add reference to section numbers to the boxes in the figure.	Editorial; Figure could reference sections for quick reference			X	
IEC	Figure 1 page 9	Replace "Categorization of the functions based on a constant risk approach" by "Categorization of the functions based on their safety significance taking in particular into account a constant risk approach"	Consistency of figure 1 where categorization depends of constant risk approach (2 factors) with 2.12 where categorization depends of 3 factors. In 2.12 the text indicates that "The functions should then be categorized …, using a constant risk approach, with account taken of : 1) consequences of failure to perform the function, 2) Frequency of occurrence … 3) The time following a postulated initiating event at which …. Figure 2 of 2.12		X		"*Constant Risk*" Approach has been deleted Time (3rd factor) is of less importance in the classification process and might be not considered at all. However it is used by some MS and is also identified in SSR2/1

			indicates that the constant risk approach is depending of only two factors, namely 1) frequency of an event, 2) consequences				
FRA	2.10	The basis for the design ~~basis~~ of the plant and its inherent safety features;	To avoid confusion with DBA (and include DEC) (See SSR2-1 §5.3, 5.9,5.24 and especially 5.28)		X		Changed in Plant Design Basis
FRA	2.10 bullet list	Add a bullet "the features* that are designed for use in, or that are capable of preventing or mitigating, events considered in the design extension conditions." "footnote * See para 5.27 to 5.32 of ref [2]"	To clearly encompass SSCs used for DEC			X	According to SSR 2/1, DEC are now clearly included in the design basis. Consequently, the necessary SSCs can be identified
FRA	2.12	The ~~constant risk approach is based on the~~ principle should be that the more likely the event, the lesser its consequences, as illustrated in Fig. 2.	Avoid introduction of "constant risk approach" (consistency with 3.13)	X			
WNA	2.12 FIG. 2: Diagram indicating the constant risk approach	~~High~~ AOOs (anticipated operational occurrences) ~~Medium~~ DBA (design basis accidents) ~~Low~~ DEC (design extension conditions) Fig 2 should be portraying the "constant risk" line as a band rather than as a line.	The labeling of the vertical axis in Fig. 2 should be changed This change would more directly relate the use of Fig. 2 with the definitions of the safety categories in Section 3.15 and Table 1. Comment: While the constant risk approach follows the principle that the more		X		1 "constant risk approach" has been removed from the text upon request of several MS. Thus it is assumed that the text has been clarified. The frequency level (high, medium, low) is consistent with the frequencies of (AOO, DBA, DEC). The text just before figure 2 has been modified and follows the proposal

			likely the event, the lesser its consequences, some readers of this document may interpret this approach to mean that quantitative values of risk should be used in the safety classification process. Using quantitative values may lead to inappropriate conclusions when comparing the risks within the design basis to the design extension conditions. Fig 2 should be portraying the "constant risk" line as a band rather than as a line. Another way to communicate the constant risk approach is to simply state that the principle is that normal operation has the lowest consequences, followed by AOOs, DBAs and design extension conditions with the highest consequences.				suggested in the last part of the comment.
KOR	2.12 3.13	Use of 'constant risk' concept must be re-considered. Lowering the level of safety by using the 'constant risk' must not be considered. Especially, the sentence within the parenthesis of para.3.13 must be deleted. ~~(e.g. for functions dedicated to mitigation of the consequences of severe accidents, the engineering rules to be applied are less stringent than those applied for functions for mitigation of the consequences of~~	According to para.5.34 of SSR-2/1 and para.2.3 and 2.17 of this document, assignment of SSC to particular safety classes should be justified using '<u>deterministic</u>' safety analysis '<u>complemented by' probabilistic</u> safety assessment.			X	At the moment the best practices in MS is to classify SSCs for DEC but with less stringent requirements. This guide is aimed at reflecting the best practices in MS and thus the parenthesis of par 3.13 cannot be deleted

		~~design basis accidents , because the probability of the severe accident is lower).~~	But, the DIRECT use of 'constant risk' concept in this document is not the way of 'complemented by probabilistic safety assessment.' Moreover, 'constant risk' concept has been proven to be 'risky' by the example of 'Fukushima'.				
CAN	Figure 2 (DM,MdV)	There is not enough explanation to complement the figure.	Technical			X	Figure 2 appears to be self standing
ENISS	FIG. 2 p.10	FIG. 2: Diagram indicating the ~~constant~~ risk approach	Idem	X			
FRA	Fig 2	Delete diagonal line and "constant risk"	Avoid introduction of "constant risk approach"		X		A common basic principle commonly agreed in safety is that the more likely the event, the lesser its consequences. This principle is also named "constant risk approach. Although this wording is now no longer used in the core text , keeping it in a figure reflects the general approach.
CAN	2.13 (DM,MdV)	Consider adding a clear definition of design provisions?	Editorial; Is there a clear definition for this?	X			Yes, Footnote 4 has been expended and 3.9 provides principles and examples
FRA	2.13	~~Categorization of the~~ As safety significance of design provisions ~~is not necessary because their safety significance~~ is directly linked to the consequences of their failure.,	To avoid a potential misunderstanding.		X		First part maintained, last part maintained

		Design provisions ~~are~~ can be directly assigned to a safety class.					
FRA	2.13	Inset 2.13 at the beginning of 2.15	2.13 and 2.15 could be merged as both address "design provisions"			X	2.14 and 2.15 are respectively addressing 1/the SSCs that part of a function that has been categorized. 2/ SSCs implemented as design provisions. Thus both paragraphs are needed to keep the logic
CAN	2.14 (DM,MdV)	Add short statement such as 'Safety categories are typically separated into high, medium and low safety"and refer to Table 1	Editorial; At this point it is not clear what types of safety classes there are			X	Chapter 2 presents the General Approach. Chapter 3 presents in detail the classification process. The response to this comment is in para 3.17 through 3.23.
WNA	2.15/line 1 Grammatical error	"…implemented as, or designed with, design…"	The single comma after "as" is confusing without a second comma. Add a comma as indicated	X			
CAN	2.16 (SX)	More clarity is needed in "In this Safety Guide three safety categories for functions and three safety classes for SSCs are recommended, based on the experience of the Member States. However, a larger or smaller number of categories and classes may be used if desired."	Editorial; Three safety classes cover SSCs important to safety only, not all SSCs. Actually, four classes are used for all SSCs, which are Classes 1, 2, 3, and Class not important to safety. It is recommended that "important to safety" be added after "SSCs" to avoid confusion.	X			

FRA	2.17	Delete 2.17	Duplicates 2.3		X		Regarding deletion of 2.17, and although overlapping with 2.3 that is part of the "general recommendations", the aim of the outline of the safety classification process is to describe all the steps of the classification to support figure 1.
GER	2.17	Delete this para.	See comment to para 2.3.		X		Regarding deletion of 2.17, and although overlapping with 2.3 that is part of the "general recommendations", the aim of the outline of the safety classification process is to describe all the steps of the classification to support figure 1.
JAP	2.17/L2	Add "final" in front of "assignment". Final assignment of SSCs to particular safety classes ・・・ .	Para. 2.17 is almost same as para. 2.3. Para. 2.3 is for preliminary assignment of SSCs. Para. 2.17 is for final assignment of SSCs.		X		In 2.3, "preliminary" has been deleted and there is no need to now introduce "final". Regarding deletion of 2.17, and although overlapping with 2.3 that is part of the "general recommendations", the aim of the outline of the safety classification process is to describe all the steps of the classification to support figure 1.
FRA	After 3.1	Add a paragraph, "The safety classification is the last step of a 3 steps process:	Clarification (to highlight difference in words : categorization			X	All of these steps are clearly separated in the flowchart (figure 1)

		1. identification of safety functions and design provisions; 2. categorization of safety functions and design provisions; 3. classification of SSCs performing the safety functions or design provisions."	⇆ classification)				
JAP	3.2	For the purposes of simplification, the term 'function' designates the primary function that is performed by front-line system or any supporting function that is expected・・・.	It is supposed that the primary function is one performed by front-line system.		X		Text has been modified: "*includes* the primary function *and* any supporting function"
FRA	3.3	The functions to be categorized are those functions required to achieve the main safety functions for the different plant states (~~,~~ including all modes of normal operation).	Clarification (normal operation is within plant states)	X			
WNA	3.5/line 3 & 3.15/line 25	"…and/or **engineered safety features** in the event of deviation…"	"Engineered safety features" is not defined anywhere in this document or in the IAEA Safety Glossary. The usage appears consistent with the NRC definition. It should be clearly defined.			X	Terminology already used in SSR 2/1
CAN	3.6 (DM,MdV)	Not sure text '(a design basis accident or design extension conditions) is required. Consider removing.	Editorial	X			
FRA	3.6	Owing to their importance to safety, monitoring for providing the ~~operator~~ plant staff and off-site emergency response organization with a sufficient set of reliable relevant information in the event of an accident	To avoid misunderstanding (operator may be understood as control room operator) as TEPCO Fukushima	X			

			accident highlighted the need for adequate information on plant status not only in the main control room…				
WNA	3.7/line 3 Grammatical error	"…, or to mitigate the consequences of a severe accident, are…"	Add a comma after "…severe accident..," for proper sentence construction.	X			
ENISS	3.7 p.12	3.7. Functions credited in the safety analysis either to prevent some sequences resulting from ~~multiple~~ credible independent failures from escalating to a severe accident, or to mitigate the consequences of a severe accident are designated as functions associated with design extension conditions.	The word "multiple" should be replaced by "credible" because all multiple failures should not be taken into account.		X		To be consistent with SSR 2/1, "multiple" is replaced by "additional" (see SSR 2/1 Requirement 20)
FRA	3.8	In addition to the functions identified, design provisions are implemented to prevent accident. In particular, these provisions ensure that the main safety functions are fulfilled under all modes of normal operation.	See previous comments on design provisions. Does that mean that all systems used to ensure the safety function in normal operation are to be safety classified (ex: condenser cooling water in a PWR ?). The current wording might go further than what is described in Fig 2 and footnote 4. What consistency with 3.9 ? As an option, 3.8 might be deleted (keeping 3.9 would be enough and 3.23 clarified which			X	The response is No. The classification is requested only if required from the screening of the factors used to assess the safety significance

			accidents are the ones of interest for design provisions)				
POL	3.8/1-2	In addition to the functions identified, design provisions are implemented to ensure that the main safety functions are fulfilled under modes of normal operation, **anticipated operational occurrences, design basis accidents and design extension conditions.**	This sentence should be consistent with provisions of para. 2.6 (3rd sentence).			X	Mitigation of PIEs is performed by functions (not by design provisions). See Flowchart (figure 1), 3.8, 3.9, footnote 4 have been made consistent.
FIN	3.8 and 3.9	The concept of design provisions is not understandable.				X	According to 2.2, SSCs accomplishing one of the three main safety functions during normal operation must be considered. These SSCs cannot be captured with the accident analysis. Thus it is necessary to identify which SSCs used in normal operation must be classified, this is the aim of the concept of "design provisions". An example is the SSCs for the planned releases.
FRA	3.9	To prevent the occurrence of situations* ~~the failure of an SSC~~ not considered in the design ~~basis~~ for the plant *footnote : this is the case of some situations which are "practically" eliminated, as described in para 2.11, 4.3, 5.27 of ref [2]	As initially written, this bullet is focused on avoiding failure of SSC, but not on situations to be avoided (e.g. heterogeneous boron dilutions, core melt in spent fuel pool, bypass of the confinement…). New wording enable: - to clearly encompass SSCs used for DEC and			X	"*situation*" is not used in SSR 2/1. The prevention of situations not considered in the design of the plant relies on either dedicated functions (e.g RPV depressurization) or on a very high reliability of the component (e.g. RPV and Polar Crane). The latest corresponds to the

			to have a wider scope : events not considered in the design (which may be broader than failure of SSC) - a clearer like with situation to be practically eliminated				implementation of design provisions.
POL	3.9	Design provisions are implemented in particular for the following reasons: • ~~To protect people (workers and the public) and the environment from harmful effects of radiation (direct radiation, airborne activity and releases of radioactive material);~~	The list in para. 3.9 was internally inconsistent, as the first bullet is in fact the fundamental safety objective (acc. to SF-1) – and there is no need to state it here, while the other ones are certain specific "reasons".			X	Indeed in the first bullet operational condition was missing as it appeared in the flowchart. The shielding necessary to protect the workers in normal conditions required by SF-1 cannot be captured by the functions implemented to mitigate PIEs. Thus, especially for design provision under normal operation. This bullet is essential.
WNA	3.9	Design provisions are mainly implemented for the following reasons - To protect people (workers and the public) and the environment from harmful effects of radiation (direct radiation, airborne activity and releases of radioactive material); - To prevent the failure of an SSC not considered in the design basis for the plant (e.g. rupture of the reactor pressure vessel for LWR - To reduce the frequency of failure of SSCs that may cause an accident; - To **limit the effects of hazards considered in the design basis for the plant** ;	Needs clarification, if necessary also examples and a definition of "design provision". In some instances it is not clear if something is a **function or a design provision** 1. For example we understand that a lifting device designed not to collapse under load is a design provision. However, the I&C function		X		1/ & 2/It is agreed that prevention may rely on both design provisions and functions. Examples have been added in 3.9. Definition of "design provision" has been expended in footnote 4, 2.12 and 3.9.

		- To prevent a postulated initiating event from developing into a more serious sequence without the occurrence of another independent failure.	actuating the breaks of the lifting device is a function. 2. The rules for classification of design provisions limiting the effects for internal hazards (see Section 3.15) do not allow a straight forward classification of those SSCs. Presently these devices would be assigned to F2 (class 3). Assessment of the radiological consequences in case of failure of such provisions would be complex and could represent a huge amount of studies. It is also unclear whether it is necessary to differentiate between SSCs implemented as design provisions and SSCs classified on the basis of their role in achieving the function. For example, in order to prevent a postulated initating event from developing into a more serious sequence, SSCs that perform monitoring and communications for providing the operator with a sufficient set of reliable information in the event of an accident could be directly assigned a safety				3/ Basically, an hazard should not result in an accident. This is why <u>mitigation</u> of consequences is not addressed. However, by design and for the safety of the plant, it is needed to <u>limit</u> the effect of hazards. For the hazards which could directly result in radiological consequences (e.g. fuel assembly drop in the fuel building), an assessment of the radiological consequences in anyway required. In 3.15, monitoring devices are assigned in category 3 (deterministic approach) Finally 3.11 has been expended to facilitate the classification of design provisions for hazards.

			class.				
POL	3.9/Footnote 6	[6] If the analysis of postulated initiating events performed according to national practice does not include hazards analysis.	Obvious correction.	X			
WNA	Footnote 6/pg 13	"[6] If the analysis of postulated initiating…"	The word "If" is miss spelled	X			
KOR	3.9 / the second bullet point	To prevent the failure of a n SSC not considered in the design basis for the plant (e.g. rupture of the reactor pressure vessel for LWR);	erratum	X			
GER	3.9	"… pressure vessel for LWR);"	Typo, Close Bracket	X			
JAP	3.9 4th bullet	To limit the effect of hazards (internal and external hazards) considered in the design basis for the plant;	Clarification				
FRA	3.9	(e.g. rupture of the reactor pressure vessel for LWR)	Typo	X			
GER	Footnote 6	"…if the analysis of …"	Typo, add letter	X			
FRA	3.9 footnote 6	Delete footnote 6	The rationale for footnote 6 and its implications are not clear. The importance of taking due account of external hazards is highlighted by TEPCO Fukushima accident…			X	The aim of this footnote is precisely that if hazards are not addressed in the PIE analysis (that is the case in some MS), they should be addressed separately
FRA	3.10	The functions required for fulfilling the	Clarifications	X			

		main safety functions in all plant states~~,~~ (including modes of normal operation) should be categorized on the basis of their safety significance.					
FRA	3.11 Low severity	Add an additional bullet: “ • Cause the values of key physical parameters to exceed the specified design limits for normal operation, but remain within the specified design limits for anticipated operational occurrences.”	For parallelism with the “medium severity” and “high severity” lists			X	Deviation from normal operation ranges within the limits of AOOs is not a sufficient justification to require the safety classification of an SSC.
CAN	3.11 (GB)	Add to the text: “For levels of severity designated as ‘high”, the assessment of the consequences of failure of the function should be made assuming that the functions belonging to the subsequent level of defence in depth does not respond as designed and in due time [for example, if class IV is lost, next defence in depth is class III power; for “High” consequence, Class III power is also considered failed].”	Technical; For greater clarity and completeness.			X	Considering the writing of the guidance for “medium” and “low” severity, that clearly specifies that “subsequent level of DID should be considered” it is clear that this not applicable for “high” severity
CAN	3.11 (GB)	For HIGH section Add to the text: "...Lead directly to an off-site release of radioactive material"	Editorial			X	Why focusing only on off-site release? A regulator may also have requirements for on-site releases. The initial proposal covered both off-site and on-site.
POL	3.11/3-4	• Lead directly to an **off-site** release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body; or	Off-site releases of radioactive material are concerned here.			X	Why focusing only on off-site release? A regulator may also have requirements for on-site releases. The initial proposal covered both off-site and on-site.
POL	3.11/7-9	~~For levels of severity designated as ‘medium’ and ‘low’, the assessment of the consequences of failure of the function~~	This sentence is unclear: what does “the subsequent level of		X		Text has been modified for better clarity :

		~~should be made assuming that the functions belonging to the subsequent level of defence in depth respond as designed and in due time~~	defence" exactly mean here? which defence levels are concerned? Moreover, this sentence is inconsistent with the subject of para. 3.11 which contains definitions of the severity levels.				*"(...) should be made assuming the correct response in due time of all other any independent functions"*
POL	3.11/11-13	• Lead to an **off-site** release of radioactive material below the limits for design basis accidents accepted by the regulatory body but higher than those established for anticipated operational occurrences; or	Off-site releases of radioactive material are concerned here, and this should be clearly stated.			X	Why focusing only on off-site release? A regulator may also have requirements for on-site releases. The initial proposal covered both off-site and on-site.
CAN	3.11 Foot note 6 (GB)	Ch2ange "f" to "If"	Editorial	X			
POL	3.11/21-	• **Cause the values of key physical parameters to exceed the specified design limits for normal operation, but remain within the specified design limits for anticipated operational occurrences.**	The second bullet should be added in the definition of "low severity"– through bringing back the 2nd bullet from Draft 6.2 (p. 16), as the reason of its deleting is unclear.			X	Deviation from normal operation ranges within the limits of AOOs was not a sufficient justification to require the safety classification of an SSC.
CAN	3.11 (GB)	For MEDIUM section Add to the text: "...Lead directly to an off-site release of radioactive material"	Editorial			X	Same explanation as for "high"
CAN	3.11 (GB)	LOW section: Modify the text: "Not exceeding the design limits for AOO, but could lead to doses to workers above the authorized limits." Delete: "authorized for normal 21plant operation"	Technical	X			

ENISS	3.11
	p.13
		3.11. The three levels of severity should be defined as follows:
		• The severity should be considered 'high' if failure of the function could:
		  • Lead directly to a release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body; or
		  • Cause the values of key physical parameters ~~to challenge or~~ exceed acceptance criteria for design basis accidents7.
			There is only an issue when parameters are exceeded. To be in line with Requirement 19 of SSR-2/1 (Safety of NPPs: design): *Design basis accidents*
			A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.
				X			

CAN	3.12 (GB)	Consider using 'Probability of failure' or consider rewording "...failure of the function will be achieved...”;	Editorial; The meaning of this sentence is not clear		X		Text modified as follows: “*However, it should be verified that the failure rate at the demand claimed for the function*”
UK	Add to the last sentence of para 3.12	*Generally it is expected that probabilistic criteria for safety functions should match those derived deterministically. For example high reliability requirements derived from the PSA should match that of the high functional category derived deterministically. In cases where high reliability is derived from the PSA for low category safety functions derived deterministically then that should be viewed as a matter of concern and reviews should be undertaken of the validity of*	The current text does not give sufficient weight to the PSA. PSA in particular is used to ensure that the there is a balance of risks and it is also a powerful but independent check of the validity of the deterministic methods. This text opposite is deigned to give that		X		If the concern is understood correctly, this is addressed in 3.27. Following your comment, 3.27 has been modified as follows: “*Consistency between these approaches will provide confidence that the safety classification is correct. Generally it is expected that probabilistic*

		both the deterministic and probabilistic analyses.	balance.				*<u>criteria for safety functions should match those derived deterministically</u>."*
ENISS	p.15	<u>Safety category 2</u> Any delayed function required to reach and maintain a ~~stable and durable~~ safe state and whose failure, when challenged, would result in consequences of 'high' severity; or	Stable and durable to be deleted as pleonasm. See the definition of safe state in SSR-2/1 (Safety of NPPs: design): *Safe state* *Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.*		X		Text has been modified as follows: "Any delayed function required to reach and maintain **<u>for a long time</u>** a safe state"
CAN	3.13 (SX)	It is unclear that what this section and Figure 2 try to tell for the purpose of classification. The example seems to tell that a low frequent accident requires a low reliable safety function; a high frequent accident requires a high reliable function. If it is what this section means, the idea is not right because, generally speaking, a function for DBAs should be more reliable than a function for NOs or SAs while DBAs are less frequent than NOs, but more frequent than SAs.	Technical; For the purposes of classification, the greatest importance should be given to maintaining constant the risk resulting from the combination of likelihood and consequences (e.g. for functions dedicated to mitigation of the consequences of severe accidents, the engineering rules to be applied are less stringent than those applied for functions for		X		The text has been modified by replacing "probability" by "risk" because classification is driven by the risk (probability x consequence)

			mitigation of the consequences of design basis accidents, because the probability of the severe accident is lower). Figure 2 illustrates this approach.				
FRA	3.13	~~However, for the purposes of classification, the greatest importance should be given to maintain constant the risk resulting from the combination of likelihood and consequences (e.g. for functions dedicated to mitigation of the consequences of severe accidents, the engineering rules to be applied are less stringent than those applied for functions for mitigation of the consequences of design basis accidents, because the probability of the severe accident is lower).~~	Fukushima accident show the need to have qualified equipment to handle DEC. Stringent measures may be needed for some key equipments enabling to avoid a catastrophic event. There is probably a need to differentiate function categorization for DEC (where full redundancy and diversity may not have the same extent) and safety class of equipment sued for this function (equipment may need a high safety class) If this paragraph was to be kept, at least, the following modification should be made ("for functions dedicated to mitigation of the		X		The guidance expressed in 3.13 is consistent with the common practice in MS for new reactors and consistent with WENRA approach. In addition, this guide explicitly requires classification of SSCs for DEC. Text is kept, suggested modification to replace "are" by "may" is accepted

			consequences of severe accidents, the engineering rules to be applied ~~are~~ <u>may be</u> less more stringent than those applied…)				
CAN	3.13 (GB)	Consider rewording: "...the engineering rules applied to functions dedicated to mitigate severe accidents are less stringent than those applied to functions that mitigate design basis accidents, because the probability of occurrence of severe accidents [for example 1/1000000] is lower that the probability of occurrence of design basis accidents [for example 1/10000]."	Editorial		X		"*Probability*" has been replaced by "*Risk*"
JAP	3.13	3.13. With consideration of factors 1 and 2, this approach ・・・ the most significant consequences have the lowest ~~probability~~ <u>frequency</u> of occurrence. ・・・ because the ~~probability~~ <u>frequency</u> of the severe accident is lower)	As same as Fig. 2, "probability" should be changed to "frequency".	X			
JAP	3.13	None	**Clarification** Para. 3.13 describes that the frequency of the severe accident is lower than that of the design basis accidents as an example of the constant risk approach. How about the difference between the consequences in the case of the failure of measures against the			X	If understood correctly, the consequences of the failure of measures against DBAs or DEC (without core melt) is a core melt accident with radiological releases that are still "acceptable" (for new plants). The consequences of measures against severe accidents (DEC) are no longer acceptable.

			design basis accidents and that against the design extension conditions?				
UKR	3.14	This item is not needed for function categorization	If performance of a function is delayed, any evidence that there is sufficient time for this function to be recovered, can't guarantee that it will be actually done.			X	This section addresses the long term part of the accident during which some functions may be called upon within a certain time, but not at the beginning of the transient. Thus, the controlled state has already been reached, and it is expected that sufficient time would be available for the operator to reach the safe shutdown.
UK	3.14	*Factor 3 (see para 2.12) reflects the status and stability of the facility following a postulated initiating event for which a function will be required to perform. The disturbance to the facility should be considered in various phases during the evolution of the postulated initiating event: some functions are required to be performed immediately after the accident to bring the reactor under control, while others are necessary for reaching and maintaining a stable and durable state. Where performance of a function may be delayed, provided evidence that there is sufficient time for this function to be established, this should not be used as a criterion for downgrading the Category of*	This comment lines up with that in comment 1. Time is not a criterion for downgrading a safety function. What time does allow is much greater flexibility in the use of operators to respond to the evolving situation. Recent events have shown us that despite long time periods unless the total integrity of the system matches the safety function then major core damage and a		X		This guideline reflects the practice of MS. However, in order to take in consideration this comment to make the approach less systematic, the text has been modified as follows: "*Where performance of a function may be delayed, provided evidence that there is sufficient time for this function to be established, <u>it might be acceptable</u> <u>to allow</u> a lower category (…)*"

		the safety function required but does allow greater flexibility in the use of operator actions in order to fulfill the safety requirements. Generally, it is only acceptable to credit operator actions to establish a safety function after a sufficient time delay enabling detection of the postulated initiating event and diagnosis and completion of the actions by the operator.	large release can occur.				
FRA	3.14	Where performance of a function may be delayed, provided evidence that there is sufficient time for this function to be established, the proposed approach is to ~~assign it to~~ <u>allow</u> a lower category than a function of equal importance that is required to be performed immediately.	Fukushima accident show the need to have qualified equipment to handle DEC. Stringent measures may be needed for some key equipments enabling to avoid a catastrophic event. To enable flexibility		X		Text has been modified as follows: "*Where performance of a function may be delayed, provided evidence that there is sufficient time for this function to be established, <u>it might be acceptable</u> <u>to allow</u> a lower category (…)*"
POL	3.14/2-5	The time factor should be considered in the various phases during the evolution of a postulated initiating event: some functions are required to be performed immediately after the accident to bring the reactor under control, while others are necessary for reaching and maintaining a ~~stable and durable~~ safe state.	The term "stable and durable safe state" was not defined. Its meaning is probably the same as "safe shutdown state" – the term used in Table 1 (column 1, row 4), and "safe state" as defined in the SSR-2/1 document (p. 60). This also corresponds to the term "safe shutdown		X		Text has been modified as follows: "*while others are necessary for reaching and maintaining <u>for a long time</u> a safe state*". This proposal is to be consistent with the modification made in 3.15 (Category 2).

			state" defined in the "EUR" document[3] (Vol. 1, App. B).				
POL	3.14/5-8	Where performance of a function may be delayed, provided evidence **exists** that there is sufficient time for this function to be established, the proposed approach is to assign it to a lower category than a function of equal importance that is required to be performed immediately.	Editorial correction to make the text more comprehensible.	X			
KOR	3.15 vs. 3.23	Safety categorization and safety classification should be consistent. The relation between safety classification of para.3.23, safety function categorization of prar.3.15 and level of severity of para.3.11 shall be mentioned.	According to para.3.20 of this document, SSCs identified from the functions should be assigned to the safety class corresponding to the safety category of the function to which they belong. However, the safety categorization of para.3.15 and safety classification of prar.3.23 does not consistent. The relation between safety classification, safety function categorization and level of severity shall be mentioned.			X	Regarding the classification of SSCs belonging to functions, 3.20 and 3.15 are consistent. 3.23 deals with the classification of SSCs implemented as design provisions.
UK	3.15	<u>Safety Category 1</u> Any function required to control or mitigate the consequences of an anticipated operational occurrence or a	The point here is removal of the words 'respond immediately' from the definition of		X		Text has been modified "immediate" has been replaced by "automatic"

[3] European Utility Requirements for LWR Nuclear Power Plants. Revision C. April 2001.

		design basis accident and whose failure, when challenged, would result in consequences of ‘high’ severity. Safety Category 2 Any function required to control an anticipated operational occurrence or design basis accident and whose failure, when challenged, would result in consequences of ‘medium’ severity.	both main clauses for the categorization Safety Category 1 and Safety Category 2 and lines up with ONR’s concerns about the potential to reduce the safety category on arbitrary and difficult to judge concepts such as immediate.				which is no longer an arbitrary concept (see modifications in the text)
FRA	3.15	Monitoring for providing the plant staff and off-site emergency services with a sufficient set of reliable relevant information in the event of an accident	See previous comment	X			
POL	3.15/11-12	Any delayed function required to reach and maintain a safe state and whose failure, when challenged, would result in consequences of ‘high’ severity; or	Same as for comment 15. The term “stable and durable safe state” was not defined. Its meaning is probably the same as “safe shutdown state” – the term used in Table 1 (column 1, row 4), and “safe state” as defined in the SSR-2/1 document (p. 60). This also corresponds to the term “safe shutdown state” defined in the “EUR” document (Vol. 1, App. B).		X		See previous comment
POL	3.15/19-20	Any delayed function required to reach and maintain a safe state and whose failure, when challenged, would result in consequences of ‘medium’ severity; or	Same as for comment above		X		See previous comment

CAN	3.15 (DM,MdV)	Clarify the use of the term "immediately".	Editorial; What does this mean and is the precise definition set by each regulator.		X		Text has been modified "immediate" has been replaced by "automatic" which is no longer an arbitrary concept (see modifications in the text)
CAN	3.15 (GB)	Add to the text: "In each bin identified by Section 3.2 to 3.7, list the systems/components required to perform specific function. Then, assign a safety category to each system/component listed in each bin."	Editorial; Flow of decision is not sufficiently captured by the document.			X	Text kept as it is for simplification
CAN	3.15 (GB)	More description/definition/details are needed for this section.	Editorial; "NON-SAFETY-Category" here is the only place in document that introduced the notion of "non-safety-category".	X			Now considered in 3.16
GER	3.15 Safety Category 1	"…performed immediately to control ~~or mitigate~~ the consequences…"	Clarification in consistency with SSR-2.1 §2.13 (1)-(4)			X	There is no clear consensus on the correct use of "*control/mitigate*" for AOOs and DBAs
GER	3.15 Safety category 2	"…to ~~control~~ mitigate an anticipated operational occurrence or design basis accident …"	Clarification in consistency with SSR-2.1 §2.13 (1)-(4)			X	There is no clear consensus on the correct use of "*control/mitigate*" for AOOs and DBAs
WNA	3.15 Safety category 2/ line 6	Safety category 2: …. Any function designed to provide a backup of a function categorized in safety category 1 and required to control design extension conditions without core melt. Medium/long-term functions such as a diverse heat sink to reach an adequate final state can remain in Cat. 3	Example of such SSCs: Extraborating System (in case of ATWS), Primary Depressurization Lines used in case of CCF of Secondary Side Heat Removal Systems, Diverse Actuation System, SBO			X	Such request has only been made by WNA.

			Diesel Generators				
WNA	3.15 Safety category 3/line 1	Safety category 3: Any function actuated in the event of an anticipated operational occurrence or design basis accident and whose failure when challenged would result in consequences of ’low’ severity;	Requirement is stated clear but there are not many practical examples from our point of view. On the other hand wrong interpretation of this rule could open room to classify everything that might be beneficial for safety into Cat. 3/class 3 (operational systems in the turbine island for example). Radiological consequences calculations showing if DBC acceptance criteria can be met without the function are normally not available.			X	Definition of “low severity” has been improved. This should clarify the concern.
WNA	3.15 Safety category 3/line 7	Safety category 3: ... Any function specifically required to mitigate the consequences of design extension conditions,	Control functions and functions specifically implemented with the objective to reduce the actuation frequency of SCRAM or ESFAS. Operational functions which also help to reduce the actuation frequency (main steam bypass, start-up and shutdown feedwater pump, etc.) are not meant here. We would prefer to rephrase the rule with the word specifically.			X	Adding “specifically” appears to be useless. Either the function is specific to mitigate the consequences of DEC and thus should be categorized accordingly (i.e. Category 3 if not assigned in Category 2), or this functions is also necessary for other accidents conditions, and thus the assigned safety category should be of the higher category of the two cases.
WNA	3.15 Safety category 3/line 7	Safety category 3: ... “Any function…unless already required to be	It is not clear in the safety guide what safety category is to be used for design			X	DEC with core melt is assigned to Category 3.

		categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity; or…" Functions necessary to mitigate severe accidents as well as medium/long term functions necessary to reach an adequate final state in complex sequences or…	extension conditions WITH core melt. Example of such Functions: Core Melt Stabilization System, Containment Heat Removal System, diverse heat sink				The other examples provided could be in category 2 or 3 depending on the potential use for DEC without core melt.
WNA	3.15 Safety category 3/line 9	**Safety category 3:** ... Any function specifically designed to reduce the actuation frequency of the reactor scram or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant;	Control functions and functions specifically implemented with the objective to reduce the actuation frequency of SCRAM or ESFAS. Operational functions which also help to reduce the actuation frequency (main steam bypass, start-up and shutdown feedwater pump, etc.) are not meant here. We would prefer to rephrase the rule into "Any function **specifically** designed to reduce the actuation frequency of the reactor scram or engineered safety features..."			X	See response for 3.15 line 7
WNA	3.15 Safety category 3/line 13	**Safety category 3:** ... Monitoring for providing the operator with a sufficient set of reliable information in the event of an accident (design basis accident or design extension conditions), including monitoring and communication means as part of the emergency response plan, unless already assigned to a higher category;	Information necessary to reach the safe state following a DBA (Post-accident monitoring) needs to be assigned to Cat. 2. Thus, this requirement would mainly refer to monitoring/communication functions necessary to mitigate design extension conditions and information necessary to communicate			X	The guidance provided corresponds to a minimum requirement. There is no distinction made between the DBA post-accident monitoring and the monitoring in emergency conditions.

			with the Emergency Response Team.				
POL	3.16/Table 1, column 1, row 4	Functions for the control of design basis accidents after a controlled state is reached (for bringing the plant to a safe ~~shutdown~~ state)	Ensuring consistency with the SSR-2/1 document where the term "safe state" is defined and used.	X			
FRA	Table 1	In the last line (functions for the mitigation of consequences of a design extension condition), in the 2 right-end columns, replace "Usually not implemented, or non-safety-category" by "case by case decision"	French regulations states that equipment used to demonstrate safety (thus including for DEC) should be properly qualified (it therefore implies some safety classification). Current wording "usually not implemented" may be understood as encouraging no safety classification. From the point of view of the consequences of an accident (except on the workers), situations which would result in "low" consequences would probably not selected as DEC. This is less clear for events with "medium" consequences… See also comment			X	The consequences of the failure, when challenged, of any specific DEC function cannot be "medium" or "low".

GER	Table 1 2nd line, 1st column	"…Immediate functions for the control~~/mitigation~~ of consequences…"	Table 1 should be consistent with para 3.15.			X	See corresponding resolution on 3.15
JAP	Table 1 Column 2, row 5	Change safety category 2 or 3 including category 1.	The demand frequency of sever accident measures may be low. However, their failure results in consequence of higher severity than "high". Then the safety category should include safety category 1 in addition to safety category 2 or 3			X	In this guideline the classification does not only consider the severity of consequences but also the probability of the accident to occur (risk approach)
CAN	Table 1 (SX)	It is recommended that class 3 be eliminated for the DBA functions.	It is hard to believe that the consequence of the failure of a function for DBAs could be low, and the function could be classified as class 3. In reality, it is rare for functions for DBAs to be classified as less than Class 1.			X	The guidance provides a general method for all types of reactors. For some of them, it might be possible that Category 3 does not exist for DBAs.
CAN	Table 1 (SX)	Reconsider use of the term "Usually not implemented, or non-safety-category".	Editorial; Do not create more unnecessary terms. Use term "not important to safety" which is defined in the IAEA glossary, and widely used.		X		"Usually not implemented" has been removed from the core of the table
CAN	Table 1 (DM,MdV)	It is recommended that class 3 be eliminated for the DBA functions.	It is hard to believe that the consequence of the failure of a function for DBAs could be low, and			X	See previous resolution

			the function could be classified as class 3. In reality, it is rare for functions for DBAs to be classified as less than Class 1.				
CAN	Table 1 (CL)		This Table is the core of the Guide: it categorizes the SSCs into Safety Category 1, 2 or 3 (and one non-safety class) depending on the immediate functions for the control/mitigation of the consequences of AOOs and severity of the consequences of the failure of the function.	X			
US	Table 1/ Row 2/ Column 4	Add “Note (c)” in the table, and add, below the table – (c) Some AOOs do not produce serious consequences, or even require a safety function. For example, the inadvertent opening of a small secondary system valve, in a PWR, would result in a small increase in steam load and continued operation at a higher power level, with no demand for a reactor trip. SSCs for this scenario would be classed in the lowest safety category of any categorization scheme. In this document, that would be Safety Category 3.	Notes and examples are added to illustrate how the table might be applied.			X	According to the definition of “low” the inadvertent opening of a small secondary system valve does not match any criteria for “low” category and would then be Non Categorized.
US	Table 1/ Row 3/ Column 2	Add “Note (d)” in the table, and add, below the table – (d) For some DBAs, the automatic reactor trip may not be the sufficient or	Notes and examples are added to illustrate how the table might be applied.			X	Technically, the comment is correct as a LOCA+ loss of ECCS is definitely a DEC sequence, should it

		relevant safety function for mitigation. If a DBA involves a breach in the RCS, it may be necessary to actuate an emergency core cooling system (ECCS). If a DBA requires core cooling from an ECCS, and it is not provided, then the resulting scenario is even more unlikely than an ATWS (due to the lower probability of the initiating event). Such a DBA would also be in the Design Extension Conditions category, since it is the result of more than one failure. In this case, "high consequences" could be extremely high fuel clad temperature and core damage that could jeopardize the ability to cool the core.					occurred. In that case, only the LOCA is postulated and the methodology proposed requires assuming the failure of the emergency core cooling from ECCS to assess its safety significance. In addition, adding so many notes to the table would be confusing because not relevant.
US	Table 1/ Row 3/ Column 3	Add "Note (e)" in the table, and add, below the table – (e) A PIE is designated as a DBA if it is used to set the performance requirements for specified mitigation equipment. If a PIE produces medium consequences if a required Safety Category 2 function is not performed, then it is reasonable to question whether the PIE should be a DBA. A conservative analysis of the PIE, assuming that the Safety Category 2 function is not available, would show that adequate protection is provided by the Safety Category 1 function. PIE/DBA analyses usually credit only the Safety Category 1 functions.	Notes and examples are added to illustrate how the table might be applied.			X	PIEs include <u>all</u> events (and not only DBAs) likely to occur in the plant life time. In the document, "consequences" is used as the consequence of the failure of the function designed to respond to the PIE (and not the consequences of the PIE itself). In addition, adding so many notes to the table would be confusing because not relevant.
US	Table 1/ Row 3/ Column 4	Add "Note (f)" in the table, and add, below the table – (f) A PIE that produces low consequences if a required Safety Category 3 function is not performed is not likely to be a DBA. A conservative analysis of the	Notes and examples are added to illustrate how the table might be applied.				In case of DBA, the fulfillment of the acceptance criteria is achieved by functions of category 1. However, the method

		PIE, assuming that the Safety Category 2 or 3 functions are not available, would show that adequate protection is provided by the Safety Category 1 function.					proposes to assign in a Category 3 a system whose failure would lead to low consequences following a DBA. Usually, such systems are not modeled by experienced designers for the DBA plant response. In addition, adding so many notes to the table would be confusing because not relevant.
US	Table 1/ Row 4/ Column 2	Add “Note (g)” in the table, and add, below the table – (g) Functions that are required after a controlled state is reached are not immediate (i.e., automatic) functions. Therefore, they are not higher than Safety Category 2. For example, with a steam generator tube rupture (SGTR), it is important to specify equipment that can depressurize the RCS to a pressure below the SG shell pressure, and thereby prevent flow from exiting the RCS, through the ruptured tube, and passing into the atmosphere through the steam relief valves. This function could be in a mid-level safety category, since it is not needed immediately, and it is generally backed up by other functions, also in a mid-level safety category, that perform similar functions. For example, the RCS can be depressurized by opening a power-operated relief valve (PORV), or by using pressurizer spray.	Notes and examples are added to illustrate how the table might be applied.			X	The control of the pressure of the affected SG (to prevent its over pressurization) is accident management dependent. Should it be justified that this action could be delayed and made the operator, then it would be Category 2. In addition, adding so many notes to the table would be confusing The guidance cannot be reactor type or accident management dependent.
US	Table 1/	Add “Note (h)” in the table, and add, below	Notes and examples are		X		Agreed. The categorization

	Row 5/ Column 2	the table – (h) An event in the design extension condition category could be a PIE that has experienced another, independent failure, or it could be a scenario that is not part of the design basis. In either case, the SSCs specified for mitigation might not be sufficient. Therefore, it is preferred to use different SSCs, which are independent of SSCs that are normally specified for the PIE. For example, if the PIE becomes an ATWS, due to failure of the Safety Category 1 (reactor trip) function, and attributed to a common cause failure in the actuation logic or hardware, then mitigation for the design extension condition event (ATWS) should be provided by another SSC that does not rely upon the same actuating logic or hardware. If the failure is a Safety Category 1 function, which is an immediate function, it could be necessary to specify the use of another immediate function (e.g., a diverse scram system), which does not have to meet all the Safety Category 1 requirements, due to the unlikelihood of the design extension condition event. This would be, as indicated, a Category 2 function, since it would be a function that is designed to provide a backup of a function categorized in Safety Category 1 (para 3.15) to control design extension conditions.	added to illustrate how the table might be applied.				of back-up functions is already specified in 2.15 (see Category 2 for this example). Core text is sufficient without adding any note.
WNA	Table 1/last row	"Safety category 2 or 3 (see para. ~~3.14~~ 3.15)…"	Reference to Paragraph 3.14 looks like it should refer to Paragraph 3.15.	X			
CAN	3.19 (SX)	Suggest using "class not important to safety" rather than "non safety –class."	Editorial; see Section 3.13 above			X	Terminology is MS dependent

CAN	3.19 (GB)	Correct typo "one non safety-class one non safety class."	Editorial	X			
ENISS	3.19 p.17	3.19 The approach to safety classification recommended in this Safety Guide is based on three safety classes and one non safety-class ~~one non safety class.~~	Typo error	X			
JAP	3.19	3.19. ・・・ and ~~one non safety-class~~ one non safety class.	**Editorial** Duplication	X			
GER	3.19	"…and one non safety-class ~~one non safety class~~."	Doubling of words	X			
KOR	3.19 /2	The approach to safety classification recommended in this Safety Guide is based on three safety classes and ~~one non safety-class~~ one non safety class .	erratum	X			
CAN	3.22 (HC)	Guidance should be given to clarify the classification of individual SSCs. The text is not clear.	Technical; After the classification of a system for example, how to classify components in that system. The text in section 3.22 indicates that "The initially assigned safety class of some individual SSCs may be modified, if justified by appropriate analysis"; If some individual SSCs (such as a component) will be classified in different safety classes, what are the conditions and the guidance for that?		X		Agreed. Text has been slightly modified to improve comprehensiveness. The guidance proposes to perform a detailed functional analysis (or PSA) evaluating the consequence of the failure of a component with regard to the full performance of the function.
POL	3.23/5-7	Any SSC whose failure would directly lead,	To clarify classification		X		Agreed but original text is

		from normal operation, to an accident not considered a design basis accident (design extension conditions **or a beyond design basis accident more severe than design extension conditions).**	of accidents in terms of their severity.				correct to reflect that for new plants, the plant design basis includes both DBAs and DEC. Beyond plant design basis has the same meaning as the proposal
IEC	3.23	"Safety class 1 … to an accident not considered **as** a design basis …"	Editorial "as" missing.	X			
WNA	3.23 from line 4	Safety class 1 Any SSC whose failure would directly lead, from normal operation, to an accident with "high" radiological consequences not considered a design basis accident (design extension conditions or an accident not considered in the design basis); or Any SSC required to respond immediately to control or mitigate the consequences of an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'high' severity.	The proposals should be added to use equivalent criteria for directly classification of SSC`s, e.g. design provisions, as for the categorization of functions.			X	For Safety Class 1, the guideline proposes a deterministic criterion: to reduce the probability of a DEC, any SSC whose failure would result in A DEC should be assigned in Class 1. For clarity, 3.18 and 3.19 have been switched. Now 3.19 through 3.22 are addressing the classification of SSCs participating to a function, and 3.23 id dedicated to SCCs implemented as design provision.
WNA	3.23 form line 8	**Safety class 2:** Any SSC whose failure, ~~postulated from normal operation,~~ would directly lead, from normal operation, to "medium" radiological consequences~~ result in consequences of 'medium' severity,~~ as defined in para. 3.11. or Any SSC required to reach and maintain a stable and durable safe state and whose failure, when challenged, would result in consequences of 'high' severity;	The proposals should be added to use equivalent criteria for directly classification of SSC`s, e.g. design provisions, as for the categorization of functions.			X	For clarity, 3.18 and 3.19 have been switched. Now 3.19 through 3.22 are addressing the classification of SSCs participating to a function, and 3.23 id dedicated to SCCs implemented as design provision.

		or Any SSC designed to provide a backup of a function categorized in safety class 1 and required to control design extension conditions without core melt.					
WNA	3.23 from line 11	**Safety class 3:** ~~Any SSC whose failure, postulated from normal operation, would directly result in consequences of 'low' severity, as defined in para. 3.11~~. Any SSC whose failure would directly lead, from normal operation, to "low" radiological consequences, as defined in para. 3.11; or Any SSC required to function to reach and maintain a stable and durable safe state and whose failure, when challenged, would result in consequences of 'medium' severity; or Any SSC required to mitigate the consequences of design extension conditions, unless already required to be classified in safety class 2, and whose failure, when challenged, would result in consequences of 'high' severity; or Any SSC whose failure, would deprive the operator of a sufficient set of reliable information in the event of an accident (design basis accident or design extension conditions), including monitoring and communication means as part of the emergency response plan, unless already assigned to a higher safety class.	The proposals should be added to use equivalent criteria for directly classification of SSC`s, e.g. design provisions, as for the categorization of functions.			X	For clarity, 3.18 and 3.19 have been switched. Now 3.19 through 3.22 are addressing the classification of SSCs participating to a function, and 3.23 id dedicated to SCCs implemented as design provision.
FRA	3.23	As explained in para. 2.9, the design provisions ~~are not categorized and the corresponding SSCs may~~ can be directly classified according to the severity of consequences of their failure:	Superfluous	X			
GER	3.23	1st bullet point (Safety Class 1): "Any SSC whose failure would directly lead, from normal operation, to an accident not	Missing word.	X			

		considered as a design basis accident …”					
KOR	3.24 /1	Any SSC that is ~~independent of~~ not directly contribute to a particular function but whose failure could adversely affect that function …	Not logical. Independent of something cannot adversely affect that.		X		Modified as follows; “Any SSC that does not contribute to…)
WNA	3.24	Any SSC that is independent of a particular function but whose failure could adversely affect that function (if this cannot be precluded by design or prevented by an adequate interface or barrier) should be classified appropriately in order to avoid an unacceptable impact of the failure of the function.	The idea of this rule is correct but its application may lead to discussions. Failure of class 2 pipework must not affect the integrity of class 1 pipe work as this may directly lead to 'severe consequences'. Impact from the class 2 pipe on the class 1 pipe must either be prevented by an adequate interface (e.g. fixed point) or the class 2 pipe must be upgraded to class 1. On the other hand a water-carrying line routed in a class 1 battery room must not be assigned to class 1: The failure of the line would only affect one redundancy of the power supply system. With respect to seismic-induced common mode potential the line must, however, be at least seismically qualified.			X	Comment is correct but “prevention by interface or barrier” is included in “precluded by design”

US	Para. 3.26	Replace as follows: "3.26. By assigning each SSC to a safety class together with its safety function category, a set of engineering, design and manufacturing rules can be identified and applied to the SSC to achieve the appropriate quality and reliability. Recommendations on assigning engineering design rules are provided in Section 4."	Both the safety class and safety function category should be considered in establishing the engineering design rules for SSCs.			X	The proposed approach is a top-down process (see 2.9). Categorization is only an intermediate step, but once the functions have been categorized, only the classification of SSCs is considered to determine the appropriate engineering rules
WNA	3.27	3.27. The adequacy of the safety classification should be verified using deterministic safety analysis, which should be complemented by insights from probabilistic safety assessment and/or supported by engineering judgement4. Consistency between these approaches will provide confidence that the safety classification is correct. If there are differences, further assessment should be performed and a final class should be assigned provided an appropriate justification.	Further guidance have to be given, e.g. in a TecDoc: It is understood that it would be necessary to provide a report checking the (determinstically assigned) safety class against PSA risk-importance measures.	X			No impact on the document.
GER	4.1	"Once the safety class of SSCs is established, corresponding engineering design rules should be specified and applied, in accordance with the basic concept that the plant is to be designed such that • the most frequent occurrences yield little or no adverse consequences to the public~~,~~; • ~~such that the improbable~~ extreme ~~situations~~ events, having the potential for the greatest consequences to the public, have ~~a low~~ the lowest probability of occurrence."	1) To improve the comprehensibility of the sentence, introduce structuring in two parts. 2) To avoid a tautology ("… the improbable extreme situations … have a low probability of occurrence"), modify the wording of the second part. Compare with the text in para 3.13.		X		Modified as follows: *"…to the public, such that the extreme events, having the potential for the greatest consequences to the public, have the lowest probability of occurrence."*

4 Expert groups providing engineering judgement should include knowledgeable personnel from the operating organization of the plant, and personnel with skills and expertise in probabilistic safety assessment, safety analysis, plant operation, design engineering and systems engineering.

JAP	4.2	4.2. Engineering design rules are related to the three characteristics of capability, dependability and robustness: a) Capability ・・・required, ~~with account taken of uncertainties~~; b) Dependability ・・・ c) Robustness ・・・. These abilities should take into account uncertainties.	Taking into account uncertainties is only in a) capability. All these three abilities (capability, dependability and robustness) should take into account uncertainties.	X			
US	Para. 4.3 Line 4	Replace "additional" with "specific"	DS367 should indicate that the regulatory body might apply a different set of engineering design rules for SSCs.		X		Text has been modified as follows according to FRA 4.3 proposal: *"These rules should take due account of regulatory requirements relevant to safety classified SSCs."*
ENISS	4.3 p.19	4.3. A complete set of engineering design and manufacturing rules should be specified for safety classified SSCs. These engineering rules should ensure that the SSCs possess all the design features necessary to achieve the required levels of capability, dependability and robustness. The regulatory body might establish additional requirements for SSCs that are safety classified.	Is the sentence in red useful?				Text has been modified as follows according to FRA 4.3 proposal: *"These rules should take due account of regulatory requirements relevant to safety classified SSCs."*
FRA	4.3	~~The regulatory body might establish additional requirements for SSCs that are safety classified.~~ These rules should take due account of regulatory requirements relevant to safety classified SSCs.	Alternate wording to better incorporate regulator' input.	X			
ENISS	4.2; 4.3; 4.7 p.19 & p.20	capability, dependability and robustness	Terms not defined in the glossary		X		Definitions are given in 4.2. These could be included in the glossary as necessary.
WNA	4.4/line 3	"- Such design requirements applied at the system function level can include e.g. single failure criteria, independence of redundancies,	Bullet 1 talks about applying single failure criteria at the system level.			X	Design requirements are established for systems.

		diversity, testability, etc."	While this can be done, it is different than postulating a single failure somewhere within a safety function, because the function could credit other systems to make up for a single failure in one specific system. Suggest Paragraph 4.4 address the single failure criterion mostly from a functional, rather than system, basis.				
GER	4.4	2nd bullet point: "Such design requirements applied ~~for~~ to individual ~~SSCs~~ structures and components can include …"	Consistency with the introductory statement which distinguishes between the system level and individual structures and components.	X			
IEC	4.4	Replace "Such design requirements applied for individual SSCs can include e.g. environment and seismic qualification …" by "Such design requirements applied to individual structures and components"	Modify to be consistent with the beginning of the paragraph and because the first S of SSC stands for system. We understood that the individual structures and components are for I&C also what is named "equipment".	X			
IEC	4.4	Suppress "quality assurance procedures" or requalify those procedures to better target them for example by using "manufacturing quality assurance procedures"	As we understood that the individual structures and components are for I&C also what is named "equipment". Concerning quality assurance procedures it's true we apply such requirements during all	X 1/			

			the life cycle of the equipment, but we also have quality assurance procedures to be applied at system level for individual I&C systems and even we have quality assurance procedures to be applied for the overall I&C.				
		Suppress or reformulate to better target "They are typically expressed by specifying the code or standard that applies"	Same thing for the codes and standards in IEC/SC45A we have a dozen of standards to cover the overall I&C and individual I&C systems, so the use of codes and standards to specify is not limited and specific to the individual SCs.			X 2/	In 2.6, it is stated : "*The engineering design rules for items important to safety at a nuclear facility shall be* ***<u>specified</u>*** *and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology (SSR 2/1 Requirement 18)*" The wording "specifying" is consistent with SSR2/1. In addition, para 4.5 states : "*The licensee or applicant should provide and justify the correspondence between the safety class and the set of engineering design and manufacturing rules, including the codes or*

							standard that applies."
GER	4.5	"The licensee or applicant should provide and justify the correspondence … including the code~~s~~ or standard that applies."	Editorial.	X			
CAN	Glossary (SB)	There needs to be a clear definition of terms, such as Design Extension Conditions, as document includes discussion on severe accidents, DEC with core melt, DEC without core melt.	Editorial; It should be consistent with those defined in SSR 2/1, referred to in this guide.		X		Terminology used in this guide is consistent with SSR 2/1. Should it be any need to include definitions in the Glossary, this should come from SSR 2/1
GER	List of References	Delete Ref. [5].	Ref. [5] is not cited in the draft document.	X			
IEC	References	Suppress the reference [5] and maybe depending of the IAEA rules of reference also reference [4]	[5] does not appear in the text of the safety guide and [4] only in a foot note (according to the IEC rules we would have in our document to suppress it).	X			
WNA	Reference [5]	~~"AMERICAN NATIONAL STANDARDS INSTITUTE, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors Plants, ANSI N18.2-1973, ANSI, Washington DC (1973).~~"	Reference [5] doesn't appear to be called out anywhere, and as far as I can tell it was replaced long ago by ANS 51.1 (for PWRs) and ANS 52.1 (for BWRs). Suggest it be deleted.	X			
US	Annex I Rows: Category 3	Add the following general Note to the Table: "SSCs performing Category 1, 2, and 3 functions that respond to design-basis accidents must meet the Redundancy Requirement, Independence of redundant trains, Physical separation of redundant trains, Periodic testing, Qualification to environmental conditions, and nuclear	Table 1 in DS367 indicates that control or mitigation of design-basis accidents can be considered Safety Categories 1, 2 or 3. Paragraph 3.20 indicates that SSCs are initially assigned to the safety class			X	Systems Class 1 and Class 2 are credited in the DBA accident analysis. The former to fulfill the acceptance criteria, the latter to reach the safe state. The design requirements specified in the table are correct and for class 2 requirements for

		grade quality assurance requirements.”	corresponding to the safety category of the function. Annex I should not allow Class 2 and Class 3 systems to be excluded from requirements for redundancy, independence, physical separation, environmental qualification, or nuclear grade quality assurance, where those systems are used in response to design-basis accidents. In addition, safety systems that mitigate design-basis accidents must meet nuclear grade quality assurance requirements (not simply commercial grade provisions).				redundancy, independence, etc. are required. Class 3 includes essential systems for the mitigation of severe accident, but also systems only related to safety. Thus, requirements cannot be generic for the whole Class 3. Regarding essential systems for the mitigation of severe accident , the current practice in the MS is not totally fixed yet and it is difficult to require the same requirements as for Class 1 systems.
CAN	ANNEX II ASME/RCC-M Level 3 (DM,MdV)	Consider removing the statement “Any pressure retaining component not already classified in safety class 1 or 2, for which leakage or breakage could lead to doses to workers above authorized limits” from the ANNEX II ASME table.	Technical; Per section 3.11, leakage or breakage that could lead to doses to workers above authorized limits is considered ‘low” consequence. Pressure boundary components with this kind of consequence would be DS367 class 3. Now, per this table, DS 367		X		According to UK comments (see below), Annex II has been deleted

			Class 1, Class 2 and Class 3 pressure boundary components need to meet at least ASME Class 3 requirements. Remember, ASME Class 3 is a nuclear grade. In other words, all pressure boundary components important to safety (DS 367 Class 1, Class 2 and Class 3) require nuclear grades, which is far away from the existing practice.				
US	Annex II	Delete text in Note 1 beginning with "Therefore…" Delete Note 2.	The ASME *Boiler & Pressure Vessel Code* (B&PV Code) provides specific engineering rules for each Code Class. U.S. NRC Regulatory Guide 1.26 provides guidance for the application of each ASME B&PV Code Class to specific nuclear power plant systems and components. Annex II allows less stringent design and manufacturing criteria to be applied to ASME B&PV Code Classes based on probabilistic analysis without specific acceptance criteria.		X		According to UK comments (see below), Annex II has been deleted

UK	Annex II	Delete table.	Our judgment is that greater thought needs to be given on this complex process of integrating Structural Integrity requirements with that of Systems Classification and should be the included in a tecdoc.	X			
WNA	Annex II/item 3/line 1	• "Any pressure retaining component in safety class 2	Annex II seems to require a lot of equipment that we previously designed to ASME Section VIII to be designed to ASME Section III Part ND by including "any pressure retaining component in safety class 2" under ASME/RCC-M level 3. Was this intended?		X		According to UK comments (see below), Annex II has been deleted
GER	Annex II	1st row, 2nd column of the Table: "If required by regulations (e.g. for ~~RCPB~~ reactor coolant pressure boundary)"	The abbreviation "RCPB" has not been introduced elsewhere in the document. Therefore, its usage should be avoided here.		X		According to UK comments (see below), Annex II has been deleted
POL	Annexes	Annex I. Safety functions for LWRs Annex II. Example of a set of engineering rules for systems performing functions of different safety categories Annex III. Example of a set of engineering	Annex I from the Draft 6.2 should be brought back. More examples (in rows) should be provided in the table, including for instance: reactor coolant system pressure boundary,			X	List provided in the former version and coming from NS-R-1 was questionable and actually removed from SSR 2/1.

		rules for design and manufacturing of pressure retaining components of different safety classes	reactor protection system, primary containment, etc.				
UKR	General	It is proposed to specify somewhere in the document that the classification criteria identified in this Guide may be specified and detailed for individual systems and components in line with the classification principles established in these documents. Components can also be classified by other attributes established in respective documents.	Document 367 (Draft 6.5) contains common requirements and applies to all NPP structures, systems and components. There may be specifics for some categories of components. For example, for instrumentation and control systems that were commissioned earlier and have been in operation for a long time, the safety classification established in Standard 61226 “NPP–Instrumentation and Control Systems Important to Safety–Classification” of the International Electrotechnical Commission (IEC) is used. This IEC standard is accepted in most European countries as a national one. After 2000, IEC issued editions 1, 2 and 3 of this standard. All IEC standards related to		X		While developping the document, a special attention has been given to I&C issues, in order to make sure that the guiddance provided in DS 367 would be consisten with the regulations/guidance/codes and standards applicable to I&C. IEC reviewed DS 367, make comments and supports this document (see below)

			I&C systems are based on this standard. IEC 61226 takes into account the specific features of I&C, which, in the first place, are associated with the necessity to cope with common-cause failures (e. g., failures caused by software failures). DS 367 should take into account peculiarities of I&C and experience in the development and use of IEC 61226 in order to avoid the application of lower requirements for I&C (because of lower requirements for redundant components).				
FIN	General	The safety guide has developed which is good. The Finnish support the main line of French comments		X			
KOR	Throughout the document	‘Safety category’ vs. ‘Safety function category’	Both terminology ‘Safety category’ and ‘Safety function category’ are interchangeably used throughout the document. One terminology needs to be used to avoid any confusion.	X			Checked. The only wording used is “ Safety Category”

FRA	General		Was the review by Technical Editors performed (as this document is to be reviewed by NUSSC for transmission to CSS) ?	X			Yes
FRA	General		There is much improvements compared with the draft sent to MS consultations. During NUSSC, the benefits and the need of a new MS consultation should be discussed. To support this discussion, a version in revision mode showing the differences between the most recent draft and the draft sent to MS would be useful…	X			A version showing that all of the guidance of this draft was already in the former version has been uploaded on the NUSCC web-site.
FRA	General		The differences between the concept of “design provision” (to decrease frequency of event) and “functions” (to decrease consequences of event) may be discussed at NUSSC (see also comments on 2.6). The concept of “constant risk approach” and the need to use it in the guide	X			The logic of “**constant**” risk has been removed from the text

			could also be discussed in NUSSC.				
CAN	General (SC)		Comment: Overall the document is much improved over earlier versions.	X			
CAN	General (CL)		Comment: In summary, the guide is good advice if you are designing a new nuclear power plant. The proposed approach to categorize the SSCs is reasonable and sound; the Guide provides advice of how to proceed and resolve apparent conflicts (SSCs belonging to more than one Safety Category, etc.).	X			
WNA	General	The recommended procedure in DS367 v6.5 has been specified on the established requirements in SSR-2/1, provides a systematic approach for classification of all relevant mechanical and electrical/electronical SSC´s including a practicable interface to engineering design rules.		X			
WNA	General	In general the performed test runs of DS367 v6.5 showed that the recommended classification procedure is headed in the right direction and is less sensitive to user interpretations than the previous versions.		X			
WNA	General	Most of the comments given in the following discuss recommendations of DS367 for which some more guidance would be helpful for the practice. This		X			

		guidance could be given in a TecDoc as proposed in the previous discussions.					
WNA	General	It should be noted that in some countries an approved safety classification methodology is established that differentiates between the classification of the pressure boundary on the one hand and all the other mechanical and electrical / electronical SSC´s on the other hand. The following proposed supplements support also the recommended classification procedure of DS367 to provide sufficient flexibility and to fulfill the superior safety classification requirements of SSR2/1 adequately.		X			
IEC	General		IEC/SC45A supports this new draft which integrates important modifications compared to the versions previously submitted for comments. Some experts taking regularly part to IEC/SC45A activities, in particular to the development of the standard IEC 61226 (classification of I&C functions) participated actively to the last technical meetings of this project. In the coming months after finalization of this	X			

			draft of safety guide, IEC/SC45A will review the current version of IEC 61226 to define the scope and principles of a revision of IEC 61226 for the future published revision be consistent with this safety guide. Furthermore this revision of IEC 61226 will consider also impact of lessons learned during the Fukushima event.				