Comment No	Para/Line No	Proposed new text	Reason	Accepted	Accepted, but modified a.f.	Rejected	Reason for modification/rejection
GER 1	General		The terms preventive and mitigative are not used consistent with other basic IAEA documents like Safety Fundamental SF-1 (3.30 and 3.34) and Safety of nuclear power plant: Design NS-R-1 (definition of concept defence in depth 2.10). The term "preventive" is used for defence level 1 and 2 and constricted for level 3 (controlled).The term "mitigative" is used for Level 4 and 5. In DS367 preventive is only used for level 1 and mitagative for all the other levels.	PA	It has been Checked.		Consistancy with DS414 has been checked. Preventive safety function is used for Defence in depth level 1. Mitigatory safety function is used for controlling AOO, DBA to prevent further escalation of the event and for mitigating consequences for design extension conditions.
FIN 1	General	The consistency of the safety guide with the new requirements document NS-R-1 (DS414) should be reviewed after the finalization of the NS-R-1 requirements.	There are several discrepancies with the current draft DS414. As the finalization of the DS414 is in near future it is recommended that the safety classification safety guide is reviewed against finished DS414.	A			
FIN 2	General	It should be considered what design and quality assurance requirements are presented in the safety classification guide.	The role of design and quality management requirements in this guide is not clear. Also the purpose of all the appendixes is not clear.	A			
FRA 1		Delete section 4	Section 4 is not about the process of categorization but about the "requirements" related to each category. This section is quite uneven, as some topics (fire resistance, seismic resistance, I&C…) are mentioned but it does not cover the full spectrum of requirements related to the design, manufacturing, installation, commissioning and operation (including periodic tests and inspection as well as maintenance)… Furthermore, 4.1 deals with the assignment of requirements by functions, not by classes….			R	DPP contains sush a section. Section 4 gives overview of engineering rules and links for example to seismic, fire, I & C classification.
FRA 2		Delete Appendix 1	Such appendix is not useful as safety functions are not apparent, nor safety classes….	PA			May be useful?
FRA 3		Delete Annex II	See comment 1			R	It is an example
FRA 4	§2.18, 3.4, 3.8, 3.9, 3.16, 3.21, table 1	To be discussed at NUSSC: having preventive safety functions classified as important to safety	Most preventive safety functions are, up to now, not classified as important to safety. For example, the I&C only used for normal operation (e.g. regulation/automatic control – see §3.8 : to maintain paramters "within expected normal range") are not classified although these are the primary means to avoid soliciting the protection system… The exception is mostly with the main primary coolant boundary (vessel…) were preventive safety features are implemented to practically eliminate some accidents.	PA	Could be discussed during NUSSC	R	There are preventive Safety functions are classified.
UK 1	General		Arising from paras 1.4 and 4.3 (and elsewhere) – a key reason for classification of SSCs is to ensure an appropriate graded approach to control is adopted on the plant when in operation. This aspect is not addressed.			R	This is addressed in high level.

UK 2	General		Arising from para 2.18, but applies generally. The language of the text does not accurately reflect the terminology for Defence in Depth in Appendix 1. Specifically, what are called "mitigatory safety functions" in the text, relate to control and mitigation in the Appendix. Indeed Control is more prominent than Mitigation in the IAEA approach; the terminology adopted is unnecessarily confusing	A			
UK 3	General		The document does not give any advice on what might reasonably be expected by way of design (etc) standards for various classes of SSC, i.e. it only goes as far as saying what Class an SSC should be placed in and does not then say what this will mean in practice.	PA			ANNEX II gives an example. A TECDOC will be developed for more practical examples.
UK 4	General		Anthony Hart can supply further comments on typographical errors and style on request.	A			
ENISS WNA General Comment	***ENISS WNA General Comment***	ENISS appreciates the possibility to comment this draft DS367 again, because the classification of Structures, Systems and Components plays an important role in the safety of NPPs in Europe. This proposed document represents a real progress with regard to a previously examined version (in February, 2009). CORDEL appreciates the possibility to comment this draft DS367 again and recognizes a real progress of the current draft compared with a		A			

		previous version (in February, 2009). The methodology proposed is not far away from the ones described in IEC 61226 and EUR, but there is still important work ahead, before the draft can be published. The concept of safety classification described in the Draft at this stage does not represent the best practice in the member states, and two major issues are still to be addressed. 1. The concept for preventive safety functions as described in the draft (e.g. 3.7 and 3.8) does not describe actual safety functions, but functions which are necessary for normal operation ("...to keep the plant parameters within their normal range..." ; "... fundamental safety functions are fulfilled in normal operation...."). These functions are needed for DID Level 1 and should therefore not be considered as safety functions, especially as a failure of one of these functions never leads to "high" or "medium" radiological consequences (as described in Table 1). If a System for DID Level 1 fails, it should be dealt with on DID Level 2 in accordance with DS 414. The same applies to safety functions for Anticipated Operational Occurrences (which are DID Level 2), which are described as mitigatory				R	Summary of good practices To prevent RPV rupture

		safety functions (e.g. 3.11), but are still part of the operational state (see IAEA Glossary for the definition of plant states). The design of the existing plants as well as the plants of the new generation is such, that only functions needed to deal with DBAs (and DEC for new plants) are considered as safety functions. 2. The use of "mitigation" in this guide is misleading (mitigatory plant specific safety function) and doesn't comply with the IAEA Glossary. Mitigation only means the mitigation of accident consequences in terms of lowering radiation doses for workers, the public and the environment and is therefore only applicable in accidents (DiD-Level 4 and 5). The Draft is using this term for all functions above normal operation (DiD Level 1), which is not in compliance with the above IAEA definition. By combining these two points we suggest renaming "preventive and mitigative safety functions" to "preventive and mitigative functions" and to keep the term "safety functions" only for DBAs. (see examples in our comments to 3.8 - 3.12 and 3.21). The proposed system leads to a 4-level safety category classification that seems unduly complex since the				

		design codes do not use to foresee as many safety classes. Fortunately this is rather formal since shortcuts exists that could result in less categories. In these conditions we would suggest the system be simplified to a 3-level structure (also see our comments to 3.21, 3.25 and annex II). As this guide is an underlying guide to NS-R-1 requirement, it should be checked for compliance with the new NS-R-1 (DS 414) when DS 414 is published – therefore we strongly recommend approving DS 367 only after DS 414 has been published. The consistency between the IAEA glossary and this guide should also be carefully checked as in the current situation there could be some diverging interpretation as the lead document is not defined. This guide defines a new process for classification which will be difficult to fully apply to existing plants which will lead to only minimal safety benefits but significant costs. Therefore we strongly recommend that the methodology proposed in this guide is limited to new plants. In this guide there are a few articles that leave too much room for interpretation. For instance regulatory bodies have different limits on radiological consequences				

		(e.g. 3.17). This could lead to different safety categorization for the same design in different countries; that falls short of safety harmonization. As for the last revision of this draft ENISS would be glad to provide experts for further clarifying this guide before NUSSC approval.					
	Section						
UK 5	Para 1.3	Modify to read: "...relevant IAEA publications have been considered..."	Typo	A			
USA 1	1.3/1	Please explain basis for changes to this section since last revision	Section 1.3 refers to NS-R-1. IAEA guidelines, e.g., NS-R-1, classify SSCs into three categories: Safety, Safety-Related, and Not Important to Safety.	PA	New Safety standards were published recently and NS-R-1 was revised by DS414. Some referenced international publications were listed as well.		Requirement 23 of DS 414 states that "All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance". Paragraph 4.1 of Ref. [1] states that "A systematic approach shall be taken to identify the items important to safety that are necessary to fulfill the fundamental safety functions, ..., for the first four levels of defence in depth." DS367 recommends three safety classes for all items (SSCs) important to safety.
UK 6	Para 1.4	Modify to read: "This will ensure that ~~the~~ appropriate engineering design rules..."	The set of design rules adopted is not unique.	A			
ENISS 1 WNA 1	1.4	[...] This will ensure that the appropriate engineering ~~design~~ rules are determined for each safety class, so that SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to standards appropriate to their safety significance.	Rules that have to be applied don't refer **only** to design but also to manufacture, maintenance, test.	A			
UK 7	Para 1.5	Rephrase to read: "The principles and method of classification provided in this Safety Guide aim at harmonizing national practices"	This seems to go beyond IAEA's remit.			R	IAEA with the help of MSs reviewed about 20 different approaches and developed this guide.
UK 8	Para 1.5	Modify to read: "... do not invalidate classifications of SSCs achieved using other methods provided these follow similar underlying principles"	There will surely be some approaches that do not meet what the international community would consider to be good practice.	A			
USA 2 (1)	1.5/1	~~To adopt the best practices in Member States,~~ the IAEA reviewed widely the existing safety classification methodologies applied in operating nuclear power plants and for new designs.	DS367 does not represent the practice in all the Member States (for example the US), since DS367 advises the use of more safety categories than are used in the US. The NRC's goal of reducing regulatory burden implies that	A	The use of three safety classes justified in the text of the draft DS367.		

			increasing regulatory burden, by adding a safety category, should be justified by some safety benefit to be gained.				
FRA 5	1.5/1	Delete "To adopt the best practices in Member States, the IAEA reviewed widely the existing safety classification methodologies applied in operating nuclear power plants and for new designs. This Safety Guide is based on this review. The principles and method of classification provided in this Safety Guide aim at harmonizing national practices. Furthermore,"	Superfluous	PA	Modified according to UK and USA 2 comments		
USA 3	1.5 Line 8	Insert: "or the national requirements of the individual Member States" at the end of the last sentence of this paragraph.	The paragraph states that the classification principles and methods provided in the Safety Guide do not invalidate SSC classification achieved using other methods. The Safety Guide should also indicate that specific requirements issued by the regulatory body of the Member State in which the nuclear power plant is located need to be met by the user of the Safety Guide.	A			
FRA 6	1.6/3	Add "safety by meeting associated" before and "targets" after "quality and reliability", and add	Safety is the objective, quality and reliability are characteristics	A			
ENISS 2 WNA 2	1.8	[...] The approach is intended to be suitable for new designs of nuclear power plants; however it ~~may also~~ shall not be fully applied to existing	Full implementation of this guide on existing plants would be very difficult and would bring huge costs with only minor safety benefits	PA	"should" for SG		Shall statement used for Safety Requirements

		plants or designs that have already been licensed. [...] ~~For upgrading of existing plants, the use of this Safety Guide will help to classify new SSCs, and reclassify existing SSCs interfacing with new SSCs if necessary.~~	To be deleted as when making modification to existing plants priority should be given to the consistency with the original standards used.			R	"will or could help"
UK 9	Para 1.9	Rephrase to read: "This Safety Guide is applicable for SSCs at nuclear power plants, but the recommendations it provides could be extended to cover any type of nuclear facility, if the appropriate amendments are made."	This is too weak. Something needs to be said about following similar principles.	PA			
USA 4	1.9 Line 9	Insert "all" prior to "SSCs" in the last sentence of this paragraph.	The Safety Guide should indicate that the scope of the safety classification methodology includes all SSCs that perform safety-related or nonsafety-related functions at the nuclear power plant.	A			
UK 10	Para 1.10	Modify to read: "Section 2 provides the basis and general approach <u>recommended for</u> meeting the safety requirements on safety classification."	The current words are too strict for a Safety Guide.	A			
UK 11	Para 1.10	Modify to read: "Section 3 describes the steps in <u>a</u> safety classification process. Section 4 provides recommendations on determining the design rules for plant specific safety functions and SSCs on the basis of their safety categories and safety classes respectively. Appendix I provides a chart indicating how safety functions	The approach set out in this SG is an example and is not the only way to do this.	A			

		relate to the various levels of defence in depth in this approach. Appendix II provides a table indicating the different steps typically performed in classification of SSCs."					
FRA 7	1.10/3	Delete "Section 4 provides recommendations on determining the design rules for plant specific safety functions and SSCs on the basis of their safety categories and safety classes respectively."	See comment 1			R	These recommendations give direction how to link rules to safety categories and classes and this task was included into DPP
FRA 8	1.10/	Delete "Appendix I provides a chart indicating how safety functions relate to the various levels of defence in depth."	See comment 2			R	Other comments
FRA 9	1.10/8	Delete "Annex II gives examples of design rules for SSCs."	See comment 1. (Eventually, Table II-III might be kept)	PA	Better to keep see other comments		
	Section 2						
ENISS 3 WNA 3	2.1 to 2.6		Check for compliance with DS 414 after DS 414 is published and take into account the comments below, when amending DS 414	A			
FRA 10	2.1 to 2.6		Reminder: ensure consistent wording with the published version of DS414	A			
JPN E1	2.2	Paragraph 4.1 of Ref. [1] states that "A systematic approach shall be followed to identify the items important to safety that are necessary to fulfil the fundamental safety functions, and to identify the inherent features that are contributing to or affecting the fundamental safety functions, for all the levels of	Editorial	A	New quotation from new draft DS414 included.		

		defence in depth. except level 5",					
USA 5	2.3/1	Please explain basis for changes to this section since last revision	Section 2.3 refers to "items important to safety". In NS-R-1, "all items important to safety" are divided into Safety and Safety-Related SSCs. These could have different quality and reliability requirements.	A	MSs' comments were the basis for changes. ANNEX II Table II-III gives example for different quality and reliability requirements for preventive and mitigatory safety classes 1-3.		
USA 6 (2)	2.4/8	… where appropriate by probabilistic methods, with account taken of factors such as: (1) the safety function(s) to be performed by the item; (2) the consequences of failure to perform the safety function; (3) the frequency at which the item will be called upon to perform a safety function; (4) the time following a postulated initiating event at which, or the period for which, it will be called upon to operate. (5) The environment in which the item is expected to operate"	Add bullet (5). This is related to (4) the time period in which the item is expected to operate. In a hostile environment, it must be determined whether the item can perform its safety function before it fails.			R	Quotation from new draft DS414 para 5.35 "The environment in which the item is expected to operate" should be the basis for the equipment qualification (seismic or harsh/mild environment) See response to comment USA 5
ENISS 4 WNA 4	2.4	Paragraph 5.35 of Ref. [1] states that "The method for ~~classifying~~ identifying the safety significance of items important to safety shall	Only safety functions and SCC are classified.	A			

		primarily be based on deterministic methods complemented where appropriate by probabilistic methods, with account taken of factors such as: (1) the safety function(s) to be performed by the SSC's ~~item~~, (2) the consequences of failure to perform the safety function; (3) the frequency at which the SSC ~~item~~ will be called upon to perform a safety function; (4) the time following a postulated initiating event at which, or the period for which, it will be called upon to operate."	In this Guide the classification of SSC is addressed and so the term SSC has to be used here. The final text of the DS414 should be modified accordingly.				
ENISS 5 WNA 5	2.5	Requirement 22 of Ref. [1] states that "Interference between ~~safety systems of lower classification~~ systems of different safety classes or between redundant elements of systems of the same class shall be prevented by means such as physical separation, electrical isolation, functional and independence of communication (data transfer), as appropriate."	For clarification	A	Requirement 22 of Ref. [1] was deleted new 5.37 from latest DS 414 was inserted		
JPN E2	2.6/Fig.1	Definition and review --> Review and definition	Definition is performed after reviewing.	A			
JPN E3	Fig.1/ 1st line on the 2nd Box	Identification of plant specific safety functions	To be consistent with the heading in Chapter 3; Identification of plant specific safety functions	A			
FRA 11	Figure 1	In the 2nd box, before safety function, add "(eventually reactor type specific, then plant specific)"	To be consistent with 2.11, 3.4 and 3.5	A			
FRA 12	Figure 1	In the 5th box, delete "three"	There may be more than 3 classes (see 2.13 and associated comment)	A			
FRA 13	Figure 1	In the 6th box, replace "design rules" by "engineering rules for the design,	To be consistent with 1.4 and 2.14	A			

		manufacturing, installation, commissioning and operation (including periodic tests and inspection as well as maintenance)"					
FRA 14	Figure 1	Add a feedback loop (after assignment of SSC to a safety class, back to identification of SSCs/groups of SSCs to perform safety function) related to the progress of the safety assessment.	To illustrate the iterative process. See 2.16	A			
USA 7 (3)	2.6/figure	Assignment of SSCs that perform safety functions to one of three safety classes	In the US, only three classes are used, and each class is simply defined: safety-related, "highly reliable", and control grade. Only the first class is truly a safety class. The three classes of US SSCs perform the functions of Categories A, B, and C.	A	See also FRA 12 comment resolution		
USA 8	2.6/figure	Please explain basis for changes to this section since last revision	Preventive safety functions: In the US, the plant is maintained in a normal operational state by automatic control systems (not important to safety), and by operators following normal operating, maintenance, and surveillance procedures. This is basically consistent with INSAG-10.	PA	Basis for changes: Member States comments		SSCs performing safety functions during normal operation should be classified in accordance with their safety significance. DS 414 requirements. (e.g. RPV Class 1) See para 3.8, 3.9
ENISS 6 WNA 6	2.6	(3) confinement of radioactive material, ~~provision of shielding against radiation and~~ control of planned radioactive release ~~of operational discharges,~~ as well as limitation of accidental radioactive releases."	Radiological or radiation protection is not considered or assimilated to a safety function. Found hereafter the right definition in the IAEA glossary (page 175) **"safety function** A specific purpose that must be accomplished for *safety*. Reference [40] lists 19 *safety*	PA	DS 414 Rev 27a		

			functions to be fulfilled by the *design* of a nuclear power plant in order to meet three general *safety requirements*: (a) The capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate *operational states* and *accident conditions*; (b) The capability to remove *residual heat* from the reactor core after shutdown, and during and after appropriate *operational states* and *accident conditions*; (c) The capability to reduce the potential for the release of *radioactive material* and to ensure that any releases are within *prescribed limits* during and after *operational states* and within *acceptable limits* during and after *design basis accidents*. This guidance is commonly condensed into a succinct expression of three ***main safety functions*** for nuclear power plants: (a) *Control* of *reactivity*; (b) Cooling of *radioactive material*; (c) *Confinement* of *radioactive material*. In earlier *IAEA publications*, 'basic *safety function*' and 'fundamental *safety function*' were also used."				
		Delete footnote 1: 1 ~~The three fundamental safety functions also have to be performed for spent fuel storage systems. In particular, fundamental safety function (2) refers to fuel in the core and spent fuel in storage at the site.~~	The proposed text is also in line with our comments on the IAEA DS414 The scope of this guide applies to NPPs including spent fuel storage part of the NPP and not the interim spent fuel storage independent of the NPP				

UK 12	Fig 1	Expand/change title	The subject matter covered by the Figure goes beyond just classifying and into design rules.			R	These steps are similar in the referenced publications
JPN E4	2.7 At page 8 Fig.1	~~Identification of SSCs or groups of SSCs to perform safety functions~~ ->Grouping of SSCs	Term should be uniformly used between in Fig. 1 and chapter three.	PA	Modified text - More detailed (see other comments)		
JPN E5	2.7 At page 8 Fig.1	~~Identification of SSCs or groups of SSCs to perform safety functions~~ ->Classification of SSCs	Same as above	PA	Modified text - More detailed (see other comments)		
JPN E6	2.7 At page 8 Fig.1	~~Identification of design rules for classified SSCs~~ ->Verification of the safety classification	Same as above			R	This is described in Section 3 and not included into Fig.1
UK 13	Para 2.8	Modify to read: "For a specific plant, prerequisites for classifying all SSCs according to their safety significance should be based upon:"	These are very unlikely to be the only prerequisites.	A			
UK 14	Para 2.8	Modify to read: "The identification of the safety functions needed to achieve the fundamental safety functions (see para 2.6) for the different plant states."	Improves English and emphasises key importance of para 2.6 to the methodology being proposed.	A			
GER 2	2.9	Initially during the design, the postulated initiating events should be arranged in groups in which properties attributes (or features) of the initiating events are the same (or very similar) (see Ref. [1], para 5.9 and Ref. [10], para. 5.34). At least	The Postulated Initiating Events are never grouped according properties. The term properties are only used for the definition for material properties.	A			

		one significant bounding postulated initiating event should be identified in each group.					
USA 9	2.9 Line 1	Insert a footnote following "postulated initiating events" in the first sentence of this paragraph to indicate that the safety classification process should consider conditions up to and including design-basis accidents.	The Safety Guide refers to postulating initiating events in addressing the safety classifications of SSCs at nuclear power plants, but does not always indicate that conditions up to and including design-basis conditions need to also be considered. For example, the first sentence in Paragraph 4.10 indicates that environmental qualification of SSCs addresses normal operation and postulated initiating events, but does not mention design-basis accidents.	PA			See DS 414 Term of Postulated initiating events includes AOOs, DBAs and design extension conditions.
FRA 15	2.9/2	Delete "in which properties of the initiating events are the same (or very similar)"	The grouping of postulating event is better described in DS414 (§5.9)	PA	Modified text		
UK 15	Para 2.9	Replace final sentence with: "Where this simplifies the analysis, one or more PIEs should be selected from the group that bound all aspects of the event that are important to safety."	Concept of bounding PIEs is currently missing.	PA			See FRA 15 Ref [10] and [11] give definition and method for bounded/bounding events.
USA 10 (4)	2.9/3	General Comment: Add a definition of "bounding".	"Bounding" should be defined and the definition added to the IAEA Glossary. Bounded events should be identified according to the parameters of interest.	PA	The definition should be added to the IAEA Glossary		See FRA 15 DS 414 para 5.9 and Ref [10] and [11] give definition and method for "bounding".
ENISS 7	2.9	For new NPP initially during the	For existing plants this is not every	A			

WNA 7		design, the postulated initiating events should be arranged in groups in which properties of the initiating events are the same (or very similar) (see Ref. [1], para 5.9 and Ref. [10], para. 5.34). At least one significant bounding postulated initiating event should be identified in each group.	time the case.				
UK 16	Para 2.10	Modify to read: "..prevent and mitigate these postulated initiating events.."	Consistency of terminology	A			
ENISS 8 WNA 8	2.11	These plant specific safety functions (see Section 3) should then be categorized into a limited number of categories, on the basis of their safety significance (i.e. the consequences of the failure of the safety function, the frequency of occurrence of the postulated initiating events they prevent or mitigate, the timing of achieving a controlled state or safe shutdown state, as described in paragraph 3.12.	It would be consistent to use the same order (2, 3, and 4) in the criteria for categorizing the plant specific functions as in paragraph 2.4.	A			
UK 17	Para 2.11	Break up the list here into bullets initiated with a phrase like "The safety significance should take into account aspects such as:"	This paragraph contains important details that could easily be overlooked.	A			
FRA 16	2.13	At the end, add "However, a larger or smaller number of class may be used if warranted"	To be consistent with 2.19. Furthermore, table 1 includes 4 safety categories + non-safety category See also 4.7 where engineering rules may vary inside a classes to be "taylored' to the SSCs according to its roles in the safety case.	A			
UK 18	Para 2.13	Make function plural	SSCs can achieve more than one.	A			
UK 19	Para 2.13	Modify to read: "Preliminary safety classifications of SSCs should then be verified	Proposed advice is too weak.	A			

		applying an appropriate assurance process"					
USA 11 (5)	2.13/3	General Comment: Identify and define the three recommended safety classes.	Adds clarity. It is the logical extension of the statement.	PA	Modified text and more detailes in Section 3		
USA 12 (6)	2.13/4	General Comment: Add a discussion, perhaps in an appendix of the experience in member states, regarding the number and definition of safety classes used.	It would be useful to know why three classes are preferred, in this guide, to two or four.	PA	It will be included in the TECDOC		
ENISS 9 WNA 9	2.14	… The aim of safety classification is to determine the appropriate engineering ~~design~~ rules for all SSCs, to ensure that SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to standards appropriate to their safety significance (see Section 4).	See rational on 1.4	A			
UK 20	Para 2.14	Modify to read: "In the design process, the aims of safety classification are to determine the appropriate engineering design rules for all SSCs and to ensure that SSCs are then designed, manufactured, constructed …"	See earlier general comment on how class is used in operation. Other modifications suggested to improve style.	A			
USA 13	Para. 2.14 Line 5	Insert "qualified," after "designed" in the last sentence of this paragraph.	The Safety Guide should indicate that the safety classification should determine the appropriate engineering rules for qualification of SSCs, in addition to design, manufacture, construction, installation, commissioning, quality assurance, maintenance, testing and inspection listed in the Safety Guide.	A			

ENISS 10 WNA 10	2.15	~~The basis for the classification and the results of the classification should be documented in an auditable record~~	Deleted. It refers to Quality Assurance of the design process which is addressed in NSR1.			R	USA comment
UK 21	Para 2.16	Modify to read: "…using deterministic safety analysis and, where appropriate, probabilistic safety analysis."	PSA is always possible, but will not always add commensurate value.	A			
PAK 1	Para 2.16 Page 10	Safety classification is an iterative process that should be carried out throughout the design process. Any preliminary assignments of SSCs to particular safety classes should be justified using deterministic safety analysis and, where possible, probabilistic safety analysis.	Second sentence of the Para may be deleted in order to avoid repetition as the concern is already addressed in Para 2.4.			R	2.4 is the quotation from DS 414 ,2.16 is a recommendation
ENISS 11 WNA 11	2.16	…Any preliminary assignments of SSCs to particular safety classes should be justified using deterministic safety analysis, and where possible, appropriate probabilistic safety analysis. Engineering judgment could also be used at this stage.	At this preliminary stage engineering judgment could be used to define classification	A			
UK 22	Para 2.17	Change reconsidered for "reviewed"	Better technical English.	A			
FRA 17	2.18/5	Replace "consequences in excess of acceptance criteria for design basis accidents" by "design extension conditions"	To be consistent with DS414	A			
FRA 18	2.18/7	Delete "See the chart in Appendix I for further detail."	See comment 2			R	It gives an overview
	Section 3						
UK 23	Para 3.2	Modify to read: "Grouping or bounding of postulated initiating events should be	Needs to be consistent with Para 2.16.	A			

		performed and assessed during the design prior to the safety classification process using deterministic safety analysis and, where appropriate, probabilistic safety assessments"					
UK 24	Para 3.2 footnotes	Reconsider the wording here.	What value is added by these footnotes? If retained, consider re-phrasing for clarity.			R	Responces for earlier questions, comments
ENISS 12 WNA 12	3.2/ line 2	In order to establish the inputs required to start the classification process, the safety objective for the design ~~safety~~ should be analysed and the specific safety challenges associated with the specific reactor type (or technology) and …	The sentence is clearer if you state "…safety objectives of the design should…." The word safety after design is not necessary	A			
UK 25	Para 3.4	Modify to read: "…necessary to fulfil the fundamental safety functions (see para 2.6) in all plant states.."	For emphasis, as per para 2.8.	A			
UK 26	Para 3.4	Modify to read: "…the safety objectives for the design ~~safety~~.."	There will normally be more than one objective.	A			
UK 27	Para 3.4	Modify to read: "Examples of reactor type safety functions for existing designs of light water reactors are provided in Annex I."	Improve English.	A			
ENISS 13 WNA 13	3.4/Line 3	At the early stage of design, 'reactor type safety functions', which are necessary to fulfill the fundamental safety functions in all plant states, should be identified in accordance with the safety objective for the design ~~safety~~…	The sentence is clearer if you state "…safety objectives of the design these…." The word safety after design is not necessary	A			
UK 28	Para 3.5	Modify to read: "…that are required for performing	Improve clarity as original wording is unclear.	A			

		the fundamental safety functions…"					
ENISS 14 WNA 14	3.5	Safety functions should be defined to an adequate level of detail in order to allow the identification of the SSCs that are required for performing these safety functions. Therefore the reactor type safety functions should be broken down to 'plant specific safety functions', which are related to plant specific PIEs ~~which prevent or mitigate the bounding postulated initiating events.~~	See general comment	PA	Added but to keep the original in brackets.		
UK 29	Para 3.7	Modify to read: "…safety functions and immediately allocated…"	Improve English.	A			
FRA 19	3.8/6	At the end, add "provided sufficient design provisions or requirements have been implemented or respectively met"	For example, for PWRs, the failure of the main reactor vessel may be ruled out of the plant design provided the vessel is designed and manufactured according to requirements imposed by the highest safety category/class.	A			
UK 30	Para 3.8	Final sentence needs to say under what circumstances specific events can be ruled out.	The current wording is too weak. It needs to say something about the likelihood of the events of concern. It must not however undermine the defence in depth philosophy, whereby the provision in each barrier does not assume the success of the others.	A			
UK 31	Para 3.8 Footnote 5	Modify to read: "…e.g. for ceramic fuels, the material itself performs an important barrier function, e.g. in pebble bed modular reactors), the reactor coolant system boundary and the reactor containment."	Improve English.	A			

ENISS 15	3.8	The preventive plant specific ~~safety~~ functions keep the plant parameters within their expected normal range, maintain the integrity of the main confinement barriers[1] (see para. 2.12 of Ref. [1]) and prevent system failures that may cause initiating events. Failures of SSCs can originate from malfunctions, the effect of external and internal hazards or human induced events. Specific events can be ruled out of the plant design basis (for example: rupture of reactor pressure vessel for pressurized water reactors see para 2.12 Ref. [1]))	Preventive functions are not safety functions (see our general comment). Regarding the ruling out of specific events, it is important here to reference DS 414 that defines how to rule out specific events of the plant design basis.	PA	Text was modified		Preventive safety functions that are required for performing the fundamental safety functions are safety functions during normal operation (DS 414)
WNA15	3.8	The ~~preventive~~ plant specific safety functions keep the plant parameters within their expected normal range, maintain the integrity of the main confinement barriers ~~(see para. 2.12 of Ref. [1])~~ and prevent system failures that may cause initiating events. Failures of SSCs can originate from malfunctions, the effect of external and internal hazards or human induced events. Specific events can be ruled out of the plant design basis (for example: rupture of reactor pressure vessel for pressurized water reactors)~~.~~, provided sufficient design provisions or requirements have been implemented or respectively met, see para 2.12 Ref. [1]))	It is important to reference DS 414 to the major aspect here that defines how to rule out specific events of the plant design basis. For example, for PWRs, the failure of the main reactor vessel may be ruled out of the plant design provided the vessel is designed and manufactured according to requirements imposed by the highest safety category/class.	PA	To keep preventive, text was modified		

[1] The confinement barriers are different for different plant designs and include the fuel with its cladding (whereby the ceramic material of the fuel itself has an important barrier function, including for the pebble bed modular reactor), the reactor coolant system boundary and the containment.

		footnote 5: The confinement barriers are .... and the containment.					
UK 32	Para 3.9	Meaning of 2nd sentence is unclear.	Safety Function 19 in Annex 1 is equally cryptic. Clarity is needed.	A	Modified text		
ENISS 16	3.9	~~Preventive plant specific safety functions should ensure that the fundamental safety functions are fulfilled in normal operation. Some plant specific safety functions support the three fundamental safety functions only indirectly (e.g. safety function (19) in Annex I). Preventive plant specific safety functions identified during the early stage of the design should be reviewed.~~	Delete as preventive functions are neither safety functions nor supporting safety functions (see our general comment).			R	See response to ENISS 15
FRA 20	3.10/2	Add "relevant" before "acceptance criteria"	Clarification	A			
FRA 21	3.10/2	Delete "for all anticipated operational occurrences and design basis accidents and the consequences of other accidents are reduced."	Superfluous. Ensure consistency with DS414	A			
UK 33	Para 3.10	First sentence is wrong. It needs rewriting.	This relates to the general comment above on terminology. Some of what are called Mitigatory Safety Functions here do not mitigate, but control.	A			
UK 34	Paras 3.9, 3.10, 3.11, 3.12 and 3.15	Change first sentences.	These need to encourage the analysts to identify these safety functions rather than just being a statement of what they are.	PA	Para 3.9, 3.10 were modified		
JPN 1	3.10	Mitigatory plant specific safety functions should mitigate the consequences of initiating events such that the acceptance criteria are met for all anticipated operational occurrences and design basis	Clarification Here other accidents mean all the other accidents than DBAs. Thus other accidents are Design Extension Conditions defined by DS414.	A			

		accidents and the consequences of ~~other accidents~~ design extension conditions are reduced.					
UK 35	Para 3.10	Modify to read: "…of other accidents are appropriately reduced…"	Small reductions may not be enough.	A			
ENISS 17 WNA 16	3.10	~~Mitigatory p~~Plant specific safety functions should ~~mitigate~~ limit the consequences of initiating events such that the acceptance criteria are met for all ~~anticipated operational occurrences and~~ design basis accidents and the consequences of ~~other~~ design extension conditions ~~accidents~~ are reduced.	Example for changes needed following our general comment "Other accidents" is not defined. "Design extension conditions" should be the right wording	PA	To keep AOO to be in line with DS 414	R	
GER 3	3.11	"Safety functions for the mitigation of anticipated operational occurrences should detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to an accident condition."	DS367 should not establish requirements for safety functions or SSCs since it should soley deal with requirements for classification. In paragraph 3.11 however (as well as in some other paragraphs in this chapter and in the whole draft) requirements on safety functions are given. At least, such paragraphs in rev 5.10 of DS367 sould be reformulated as a definition or marked as explanatory statements.	PA	Para 3.11 was modified		
ENISS 18 WNA 17	3.11	~~Safety functions for the mitigation of anticipated operational occurrences should detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences from escalating to an accident condition.~~	Delete as this is not as safety function, also see our general comment			R	See response to ENISS 17
GER 4	3.12	"Safety functions for the mitigation of design basis accidents should control accidents within the acceptance criteria of the plant's	According to para. 3.12 mitigatory safety functions (for design basis accidnets) can be subdivided into two „levels" (A and b) depending on the	PA			

		design basis. Mitigatory safety functions for design basis accidents can be subdivided into levels A and B, depending on the potential consequences of the accident and the timing of achieving a controlled state or safe shutdown state, as described in following paragraphs. This subdivision is based on the definition of plant states in Ref. [1]."	potential consequences of the accident and the timing of achieving a controlled state or safe shutdown state. In the following paragraphs no dependency of this suddividing with regard to potential consequences is addressed. Instead, subdividing solely depends on the achieving a controlled or safe shutdown state.				
UK 36	Para 3.12	Modify to read: "…can be subdivided into two levels (A and B – see following paragraphs)…"	For improved clarity. See also deletion in next comment.	A			
UK 37	Para 3.12	Modify to read: "…and the time needed to achieve a controlled ~~state~~ or safe shutdown state, ~~as described in following paragraphs~~.. The two levels are based on the definition of plant states in Ref. [1]"	Rephrased for improved clarity and so that it is more technically accurate.	A			
ENISS 19 WNA 18	3.12	Safety functions for the ~~mitigation~~ control of design basis accidents should ~~control accidents~~ keep the plant states within the acceptance criteria of the plant's design basis. ~~Mitigatory~~ Ssafety functions for design basis accidents can be subdivided into levels A and B, depending on the potential consequences of the accident and the timing of achieving a controlled state or safe shutdown state, as described in following paragraphs. This subdivision is based on the definition of plant states in Ref. [1].	Example for changes needed following our general comment	PA			Other comments
GER 5	3.13	"Level A mitigatory safety functions	See comment no. 3.	PA	Modified		

		for design basis accidents should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible. A controlled state should be ensured by means of operator actions or by the active or passive safety systems that control reactivity, heat removal and releases to the environment within prescribed limits. However automatic means should be preferred to reach the controlled state."					
Bel 1	3.13	A controlled state ~~should~~ can be ensured by means of operator actions or by the active or passive safety systems that control reactivity, heat removal and releases to the environment within prescribed limits.	This "should" does not help defining the Level A, and should be limited to a descriptive sentence like "A controlled state CAN be ensured...". Indeed, in order to comply with human factors, level A functions do not require operator actions before a "grace period". It is thus not appropriate to give the impression that operators should perform those functions!	A			
FRA 22	3.13/5	Delete "However automatic means should be preferred to reach the controlled state"	Not relevant to classification of SSCs (it is a design option)	A			
UK 38	Paras 3.13 and 3.14		Why does para 3.13 talk about systems and para 3.14 features? We don't believe there should be such a distinction.	A			
ENISS 20 WNA 19	3.13	Level A ~~mitigatory~~ safety functions for design basis accidents should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible. ~~A controlled state should be~~	The guide is dealing with safety classification and so these sentences are out of the scope of this guide.	PA	Modified text		These sentences are explanatory for better understanding.

		~~ensured by means of operator actions or by the active or passive safety systems that control reactivity, heat removal and releases to the environment within prescribed limits. However automatic means should be preferred to reach the controlled state~~					
Bel 2	3.14	A safe shutdown state ~~should~~ can be ensured by means of operator actions or by the active or passive safety features that control reactivity, heat removal and releases to the environment within prescribed limits.	The same comment as for 3.13 apply. A Safety Guide should not expect particular design solutions!	A			
FRA 23	3.14/8	Delete "within prescribed limits"	Superfluous	A			
FRA 24	3.14/10	At the end, add "and radiological release don't exceed those of normal operation"	To ensure consistency with the previous sentence where releases are mentioned.	A			
UK 39	Para 3.14	Modify to read: "These safety functions should be achieved by means of operator actions or by.."	This is a paragraph about safety functions.	PA	Modified but see Belg 2		
UK 40	Para 3.14		Why should there not be a preference for these to be automatic too (as per para 3.13)?	PA	It was removed from 3.13 see FRA 22		
ENISS 21 WNA21	3.14/Line 7	A safe shutdown state should be ensured by means of operator actions or by the active or passive safety features that control reactivity, heat removal and radioactive releases to the environment within prescribed limits.	The term radioactive is needed to clarify the releases that are of concern in this statement	A			
ENISS 22 WNA 20	3.14	b) Minimize the challenge to the remaining barriers (see para. 2.12 of Ref. [1]) from the design basis accident.	Comment: Check that para 2.12 of Ref [1] is still applicable.	A			
Bel 3	3.15	Safety functions for the mitigation of	It is inappropriate to provide a recommendation in a definition: the	A			

		consequences in excess of acceptance criteria for design basis accidents ~~should~~ are intended to limit accident progression (e.g. in-vessel mitigation before significant core degradation occurs) and ~~should~~ are intended to mitigate the consequences of a severe accident[2] (e.g. ex-vessel mitigation to control the remains of a significantly degraded core).	"should" means here ""are intended" or "are expected".				
FRA 25	3.15/1	Replace "consequences in excess of acceptance criteria for design basis accidents" by "design extension conditions"	To be consistent with DS414	A			
FRA 26	3.16		Are preventive safety functions all to be categorized as important to safety ? See comment 4.				Preventive safety functions categorized on the basis of their safety significance (consequence of the failure of the function)
GER 6	3.17	"The severity should be considered 'high' if: • The failure of the safety function could lead to a release of radioactive material that exceeds the specified limits for design basis accidents set by the regulatory body; or • The values of key physical parameters could challenge or exceed specified design limits for design basis accidents."	The severity levels given in para. 3.17 are not adequate because it should be distinguished between failures that (in any case) lead to large/early releases (such as the failure of the pressure vessel) and failures that exceed specified limits but may be prevented to escalate to severe accident conditions (e. g. by severe accident management measures).			R	Not clear

[2] Mitigation of the consequences of severe accidents includes limitation of radiological consequences, control of reactivity excursions, removal of decay heat for as long as necessary, confinement of radioactive material by means of the remaining barriers, and monitoring of the state of the plant and radiation levels.

			Thus, an additional severity level should be added.				
FRA 27	3.17/2	Replace "should" by "is usually"	To allow flexibility	A			
FRA 28	3.17/3	After "and low", add "as assessed assuming that subsequent plant specific safety functions respond as designed. Notwithstanding, particular attention should be paid to ensure that the probability claimed for its failure is achieved with the selected safety category."	This addition in the previous editions and should be kept for a right understanding of the methodology. Second sentence is of importance in order not to forget that, in a sound design, every level of defense must justify a certain reliability and the limitation of consequences cannot rely on the last line of defense only	A			
FRA 29	3.17/1st bullet/1st bullet	Delete "specified" and "set by the regulatory body"	Superfluous	PA			
FRA 30	3.17/2nd bullet/1st bullet	Delete "specified" and "set by the regulatory body"	Superfluous	PA			
FRA 31	3.17/2nd bullet/2nd bullet	Delete "specified"	Superfluous	A			
FRA 32	3.17/3rd bullet/2nd bullet	Delete "specified"	Superfluous	A			
UK 41	Para 3.17 High	Modify to read: "The failure of the safety function could lead directly to a release of radioactive material that exceeds the specified limits for design basis accidents"	This reflects more closely with what is done in reality.	A			
UK 42	Paras 3.17 Medium and Low	Modify to read: "The failure of the safety function could at worst lead to a release of radioactive..."	This reflects more closely with what is done in reality.	A			
FRA 33	3.19/3	Delete "design basis"	DEC should also be considered	A	Modified text DEC included		
FRA 34	3.19/4	Delete "preferably using automatic	Not relevant to classification of SSCs (it	A			

		means."	is a design option)				
FRA 35	3.19/5	Replace "that need to be performed" by "needed"	Alternative wording	A			
UK 43	Para 3.19	Modify to read: "The time factor should be considered for the control/mitigation of design basis accidents and for design extension."		A			
UK 44	Para 3.19	Consider re-phrasing this example.	It doesn't really illuminate what the authors are seeking here.	A			?
GER 7	3.19	"Factor (4) of para. 2.4 reflects the time at which or the period for which a plant specific safety function will be called upon. The time factor should be considered for the mitigation of design basis accidents. For example, a controlled state should be reached as soon as possible, preferably using automatic means. After a controlled state is reached, a safe shutdown state should be achieved and maintained as long as is necessary. The safety functions that need to be performed to reach and maintain the safe shutdown state may be categorized lower than the safety functions needed to reach the controlled state."	It is not convincing that solely due to the fact that a safety function (SF) is needed to reach the safe shutdown state (SSS) this SF may be categorized lower. According to para. 3.12 mitigatory SF can be subdivided into two „levels" (A and b) depending on the potential consequences of the accident and the timing of achieving a controlled state or safe shutdown state Thus, according to 3.12, there should be prerequisites for a SF, with regard to the potential consequences and to the time at which the SF will be needed, so this SF may be categorized in a lower category. However no such prerequisite is addressed in para. 3.19. At least it should be made reference to a time limit that, when reached, allows to categorize the SF into a lower category.	A			
USA 14 (7)	3.19/1	General Comment: Add a statement that indicates that certain safety functions must be complete by within a defined time, e.g., temperature or	The time factor could be influenced by the environment in which sensors and other equipment must operate to mitigate the PIE. The SSC must be	PA	See new footnote		

		pressure sensors that must trigger safety systems before they can be damaged by a PIE-induced hostile environment. Refer to Section 4.10.	complete its safety function before a hostile environment can damage it.				
WNA23	3.20	include footnote 13 into the text of SC 2 and 3	To include footnote 13 into the text – to be consistent it needs to be added at safety categories 2 and 3 as well with medium and low consequences.			R	To keep in Footnote as an example for LWRs
GER 8	3.21	"Safety category 1: • Any preventive plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1. • Any mitigatory plant specific safety function required to reach a controlled state following a design basis accident or anticipated operational occurrence or any other mitigatory plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1."	According to para. 3.12 the subdiving of SF into Level A or B is foreseen for mitigatory SFs for design basis accidents. According to para 3.21 also SF for anticipated operational occurences may be subdivided. If this is really intended this leads to the situations that a SF for an anticipated operational occurences will be categorized in the same category as a SF for a design basis accident. This is not consistent.	A	Modified text		
GER 9	3.21	"Safety category 1: • Any preventive plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1. • Any mitigatory plant specific safety function required to reach a controlled state following a design basis accident or anticipated operational occurrence or any other mitigatory plant specific safety function whose failure would result in consequences with a 'high'	Bullet 2 may be interpreted in two different manners that have different meanings: First interpretation: The allocation of a SF to safety category 1 is valid - for all SFs that are necessary to reach a controlled state (Level A) independently of the severity of a postulated failure of this SF, or - for any other SF whose failure lead to 'high' consequences.	A	Modified text		

		severity should be assigned to safety category 1."	Second interpretation: The allocation of a SF to safety category 1 is valid for any SF whose failure leads to ‚high' consequences (including Level A SF). According to Table 1 of DS367 Level A SF whose failure lead to ‚high' consequences are allocated to safety category 1. The „any other" mitigatory SF addressed in para. 3.21 are missing in Table 1.				
FRA 36	3.21/3	Delete "in one of the following safety categories" and after "according to the risk", add "Four categories may be used"	To allow for flexibility (e.g. for additional categories for DEC equipments…). The number of categories is limited to avoid having too many collections of engineering rules…	A			
FRA 37	3.21/Safety category 1/2nd bullet	After "anticipated operational occurrence", add "and whose failure would result in consequences with a 'high' severity"	Without this addition, it could be understood that all mitigatory functions required to reach a controlled state following AOO should be assigned in safety category 1 which would be too stringent.	A			
FRA 38	3.21/Safety category 3/last bullet	Add "any preventive plant specific function required to prevent significant staff exposure to direct radiation, or the monitoring of radiation level" before "and monitoring of releases of radioactive materials"	These preventive and monitoring functions related to safety were missing.	A			
FRA 39	3.21/Safety category 4/1	Replace "consequences in excess of acceptance criteria for design basis accidents" by "design extension condition"	To be consistent with DS414	A			
GER 10	3.21	"Any mitigatory plant specific safety function designed to limit the consequences of hazards should be assigned at least to safety category	What is meaning of „hazards" in 3.21? External and/or internal hazards?	A			

		3."	Is this categorization independent from the consequences of a failure of the related SF ?		Yes		
USA 15	3.21/last	General Comment: Include a matrix showing how SSCs of the three safety classes are used to perform the four categories of safety functions	Clarity	PA	Figure 2		
ENISS 23 WNA 24	3.21	Safety category 1: • ~~Any preventive plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1.~~ • Any ~~mitigatory~~ plant specific safety function required to reach a controlled state following a design basis accident ~~or anticipated operational occurrence~~ or any other ~~mitigatory~~ plant specific safety function whose failure would result in consequences with a 'high' severity should be assigned to safety category 1. • <u>any other function, e.g. for integrity, where a failure (e.g. reactor pressure vessel break) cannot be covered by any other safety function and which results to high</u>	ENISS: As preventive plant specific functions are not safety functions, high consequences are not possible – see our general comment. WNA: With the definition given in 3.8 and 3.9 for preventive plant specific safety systems, high consequences are not possible – also see our general comment! Delete mitigatory following our general comment ENISS: To include footnote 13 into the text – to be consistent it needs to be added at safety categories 2 and 3 as well with medium and low consequences.	A		R	See earlier responses to comments to 3.8 and 3.9 s

		consequences should be assigned to safety category 1					
WNA25	3.21 p 17	Safety category 3, last bullet • Even if they are not directly needed to ensure the performance of the fundamental safety functions, any preventive plant specific function required to prevent significant staff exposure to direct radiation, or the monitoring of radiation level and monitoring of releases of radioactive materials at the site should be assigned at least to safety category 3.	These preventive and monitoring functions related to safety were missing. Footnote 13 should be included into the text	A			
ENISS 24 WNA 26	3.21	**Safety category 4:** ~~• Any mitigatory plant specific safety function required to control consequences in excess of acceptance criteria for design basis accidents, in order to prevent core melt or to mitigate other consequences in a design extension condition, should be assigned to safety category 4~~	If a function satisfies none of the criteria of the categories 1, 2, 3, it must be considered as not classified. There is no need to have a safety category 4 (see general comment).			R	FRA 36
UK 45	Para 3.21	Major Comment: This para needs to be reviewed in detail and brought into line with the rest of the text, particularly Table 1. Better still, seek a clearer way of explaining Table 1.	There seem to be a number of logical inconsistencies in this paragraph. For instance: Category 2 includes some but not all of Level B; the clause in Category 1 to include any mitagatory safety function that could lead to high severity will include design extension SSCs; I would have expected category 3 to equate to Low severity (the limit of	A	Revised text		

			the AOO range), but the wording has it at the edge of normal operations (which leaves a hole in the coverage!). I found several other anomalies besides these.				
UK 46	Para 3.21	Safety Category 3 bullet 3 needs rephrasing.	This meaning of this bullet is unclear; it needs to relate to Low severity.	PA			
UK 47	Para 3.21	Major Comment: Remove Category 4	The move to 3 classes of SSCs in this draft is welcomed. The continuing use of 4 categories of safety function doesn't seem to add any real value though and introduces a surprising discontinuity in Table 1.			R	FRA 36
UK 48	Table 1	Use either "No safety category" or N/A - but not both	The use of two terms for the same thing is confusing.	A			
FRA 42	Table 1/Line before last line	Delete footnote 16 and have safety category 4 for the 3 columns	For new reactors, it is expected that DEC consequences will limited (no or only minor offsite consequences). Footnote 16 would be untrue for DEC where preventive/mitigatory measures enable not to exceed design basis accidents limits.	PA	Deleted		
FRA 43	Table 1/ Safety functions level B	The last column (low) should be modified to include a safety classification	It it is a safety function, then it should be safety classified (it can't be "no safety category")	A			
FRA 44	Table 1/ Last line (safety function)	Delete last line	If a SSC is implementing or contributes to the implementation of a safety function, it can't be "no safety category"	A			
FRA 45	Footnote 15	Delete footnote 15	As the requirements associated to a category are not defined and the number of category may be higher (see comment)	A	Deleted		
FRA 46	Footnote 17		A picture would be more illustrative			R	It will be in the TECDOC

UK 49	Footnote 15	This is illogical.	How can something put into Safety Category 4 lead to SSCs classed as Not Important to Safety? The fact that the designers have gone to the trouble of specifying the need for SSCs suggests: a) it is relevant to safety; and b) it is important.	PA	Deleted		
UK 50	Footnote 16	Rephrase.	While I agree with the sentiments of this footnote, it fails to provide a logical argument that I could repeat.	PA	Deleted		
USA 16	Para. 3.22 Table 1	Modify Table 1 to specify Safety Category 2 (rather than Safety Category 3 or No Safety Category) for Safety Functions for Mitigation of Anticipated Operational Occurrences, and Safety Functions for Mitigation of Design Basis Accidents (Level A and Level B). Otherwise, modify Table II-III in Annex II to specify that Commercial Grade must be supplemented with sufficient treatment consistent with the categorization to provide confidence in these SSCs to perform their safety functions.	Table 1 indicates that safety functions with medium or low consequences of failure can be categorized as Safety Category 3 or No Safety Category. Figure 2 indicates that Safety Category 3 functions can be performed by Safety Class 3 SSCs. Table II-III in Annex II allows Safety Class 3 SSCs to be designed and qualified as Commercial Grade. The Safety Guide should indicate that SSCs that perform safety functions need to be designed, qualified, manufactured, constructed, procured, installed, commissioned, maintained, tested, inspected, and included within the scope of the quality assurance program to provide confidence in their capability to perform the applicable safety functions. Table 1 also allows safety functions for the mitigation of design-basis accident (Level B) to have No Safety Category. Mitigation of design-basis accidents should be performed by SSCs with a safety classification such that their design, qualification, manufacture, construction, procurement, installation, commissioning, maintenance, testing, inspection, and quality assurance will be sufficient to provide confidence that they are capable of performing their safety functions.	PA	Modified table		In the table there is the categories of safety functions, in the ANNEX II Table III are rules for safety classes

FRA 40	3.23	Locate 3.23 after Table 1		A			Editorial review
FRA 41	3.23/4	Delete "This is further considered in Section 4."	See comment 1			R	Section 4 is important see earlier comments
ENISS 25 WNA 27	3.23.	~~By categorizing the plant specific safety functions in accordance with Table 1, engineering design rules (functional requirements such as single failure criterion, diversity, etc.), linked to the applicable safety categories, can be assigned to the plant specific safety functions or to groups of SSCs performing plant specific safety functions. This is further considered in Section 4.~~	This is addressed in 2.16.			R	Section 4 is important see earlier comments
GER 11	Table 1	"Safety functions for mitigation of	The plant design must be such that			R	In principle it can

	Line ##	anticipated operational occurrences" Severity of the consequences of the failure of plant specific safety functions: High	the failure of a mitigatory SF needed for an anticipated operational occurrence can not lead to a release of radioactive material that exceeds the specified limits for design basis accidents set by the regulatory body. It is confusing that such a situation is introduced into the categorization system.				happen in the practice it should not
GER 12	Table 1 Line ##	"Safety functions for mitigation of anticipated operational occurrences" Severity of the consequences of the failure of plant specific safety functions: Low	If the failure of a mitigatory SF needed for an anticipated operational occurrence does not affect the fulfilment of the related acceptance criteria why should this SF be allocated to this event?			R	High probability of event Category 3
GER 13	Table 1 Line ##	"Safety functions for mitigation of design basis accidents (level A)" Severity of the consequences of the failure of plant specific safety functions: Medium	If the failure of a mitigatory SF needed for an design basis accident does not affect the fulfilment of the related acceptance criteria why should this SF be allocated to this event?			R	Not to have medium releases
GER 14	Table 1 Line ##	"Safety functions for mitigation of design basis accidents (level A)" Severity of the consequences of the failure of plant specific safety functions: Low	A SF needed for a design basis accident whose failure has the effect that the acceptance criteria of anticipated operational occurrences are fulfilled should not be allocated to the design basis accident.			R	Not to have low releases
GER 15	Table 1 Line ##	"Safety functions for mitigation of design basis accidents (level B)" Severity of the consequences of the failure of plant specific safety functions: High	There is no reasoning for the allocation of a Level B SF to a lower safety category if the postulated failure of this SF leads to ‚high' consequences (see comment No. 2 and 5).			R	Lower probability and more time for mitigation
GER 16	Table 1 Line ##		The „any other" mitigatory SF addressed in para. 3.21 are missing in Table 1.	PA	Deleted from the table		?
GER 17	Table 1 Line ##	"Safety functions for mitigation of design basis accidents (level B)"	See comment No. 13.			R	?

		Severity of the consequences of the failure of plant specific safety functions: Medium					
GER 18	Table 1 Line ##	"Safety functions for mitigation of design basis accidents (level B)" Severity of the consequences of the failure of plant specific safety functions: Low	See comment No. 14.			R	?
JPN 2	3.23/Table 1	The rightmost column "Low" of (level B) should be changed from "No safety category" to "Safety category 3".	Clarification This should be Safety category 3 according to the 3rd and 4th bullets under Safety category 3 in para. 3.21: • Any mitigatory plant specific safety function designed to limit the consequences of hazards should be assigned at least to safety category 3. • Even if they are not directly needed to ensure the performance of the fundamental safety functions, monitoring of releases of radioactive material at the site should be assigned at least to safety category 3.	A			
ENISS 26 WNA 28	Table 1	Add footnote: Factor (3) and Factor (4) are taken into account indirectly through the type of plant specific safety function	Factor (3) and Factor (4) are not explicitly taken into account in this table so it is unclear how they have to be considered in the categorization ("p14, section 3.16 "should be categorized on the basis of their safety significance. […] taking into account the factors (2), (3) and (4)…"	A			
ENISS 27 WNA 29	Table 1	Delete the first two rows of table 1 In the table 1 the cell safety category 4 should be replaced by safety category 3 or no safety category	See general comment To be consistent with the general comments and comment on 3.21.			R	See response to comment to 3.21

		See ENISS proposal in the annex to our comments WNA: (see proposal at the end of these list)					
ENISS 28 WNA 30	Page18/ Footnote 17	"...consequences of anticipated operational occurrences....	"operation" must be changed to operational ... " for this sentence to read correctly.	A			
UK 51	Para 3.24	Expand this paragraph to include advice on why this is beneficial.				R	
UK 52	Para 3.25		The first sentence is of course impossible to achieve for SFC Category 4.	PA			
ENISS 29 WNA 31	3.25 fig 2	The text box "plant specific safety function category 4" should be replaced by "function important to safety and not classified"	To be consistent with comment on 3.21			R	Para 3.21
JPN E7	3.25/Fig.2	"Plant Specific Safety Function Category" should be changed to "Safety category".	There is no definition of "plant specific safety function category" in the present draft.	PA			
ENISS 30 WNA 32	3.26/Line 6	The SSC would already be in operation at the moment the postulated initiating event occurs, and would not be affected by it; ".....	The sentence is missing "be".	A			
GER 19	3.26	"If justified by an appropriate safety analysis, a safety class lower than the safety class initially assigned can be proposed for a SSC. For example, an SSC can be assigned to a lower safety class, generally of one level lower, in the following cases:"	Since no further requirements or prerequisites are given here any justification can be used to argue for a lower classification of SSCs. Since the main output of the classification process is the adequate allocation of SSCs into safety classes such an undefined allocation process is not useful.			R	
GER 20	3.26	•"The SSC does not directly support the accomplishment of the plant specific safety function in the corresponding safety category;"	What is the meaning of „does not directly support"? Either the SSC is necessary for the SF or not.			R	Supporting items
GER 21	3.26	•"The SSC would already in	If the SSC is necessary to control the			R	It covres it

		operation at the moment the postulated initiating event occurs, and would not be affected by it;"	event and in addition, failure of the SSC leads to ‚high' consequences, the allocation of this SSC to a lower safety class is not justified. In addition it has to be mentioned that any "structure" and most of the "components" are continuously "in operation. Does this mean that all Ss and Cs may be allocated to a lower class ? Or is this only valid for "systems				
UK 53	Para 3.26 Bullet 1 (and whole section)	Contradicts para 3.28.	I suggest the concept here is to do with the probability that the supporting SSC, in failing to deliver its function, causes the overall system to also fail to deliver its function. This then comes down to matters of redundancy and diversity. This is where the final bullet of para 3.26 comes into play – the principal means should not be downgraded. Para 3.31 on conditional probabilities is also important. This whole section could usefully be re-written to improve the clarity of the intended message.			R	
USA 21	Para. 3.26 Line 6	Insert "be" in the first line of the second bullet following "already"	Editorial	A			
GER 22	3.27	"If there are main SSCs (also known as lead SSCs or frontline SSCs) within certain safety functional groups whose failure cannot be accepted because the conditional probability for unacceptable consequences is 1 or close to 1 (e.g. the reactor pressure vessel for light water reactors), then these SSCs	What is the meaning of „additional requirements"? Design requirements or classification requirements ? DS367 should not handle design requirements.	A	Engineering design rules		

		should be allocated to the highest safety class, and additional requirements should be specified on a case by case basis."					
FRA 47	3.28/2	Replace "then" by "eventually"	It is not systematic	A			
ENISS 31 WNA 33	3.28.	Supporting SSCs should generally be assigned to the same class as that of the frontline SSCs to be supported. The class of a supporting SSC can ~~then~~ be lowered according to the rules set out in para. 3.26.	For clarification	A			
ENISS 32 WNA 34	3.31	The SSC may ~~be~~ later be assigned to a lower safety class depending on the conditional probability of the consequential failure of the safety functional group.	Delete the extra "be" to make the sentence read properly.	A			
UK 54	Para 3.32	Modify to read: "An exception may be made where there is no identified mechanism…"	Technical	A			
FRA 48	3.33/1	Replace "engineering design rules" by "engineering rules for the design, manufacturing, installation, commissioning and operation (including periodic tests and inspection as well as maintenance)"	To be consistent with 1.4 and 2.14			R	DS414
FRA 49	3.33/2	Replace "is achieved" by "are achieved, thus safety"	Safety is the goal	PA			?
FRA 50	3.33/3	Delete "Recommendations on assigning engineering design rules are provided in Section 4."	See comment 1			R	
UK 55	Para 3.34	First sentence is not logically possible.	DBA can verify the importance of the safety functions. However the classes have more to do with reliability.			R	
UK 56	Footnote 19	This describes very valuable employees! – an unreachable standard	The wording suggests each expert needs to have these skills. We need to say that the team of experts has	PA			

			members with these skills.				
USA 22	Para. 3.34 Line 6	Delete "of" following "using"	Editorial	A			
ENISS 33 WNA 35	3.34	The adequacy of the safety classification should be verified using deterministic safety analysis, which should cover all postulated initiating events and all aspects of the prevention of events that are credited in the concept for the safety design ~~safety~~ of the plant. This should be complemented, as appropriate, by insights from probabilistic safety assessment and **/or** should be supported by engineering judgement Consistency between safety classifications verified using ~~of~~ deterministic analyses and probabilistic analyses will provide confidence that the classification is correct.	Rearranging safety and design makes the sentence read correctly. See comment on 2.16 Delete "of" ...so that sentence reads correctly.	PA			
UK 57	Para 3.35	a) b) and c) are relevant to safety functions, not SSC classes as stated.	As per para 3.34, the logic has become confused.			R	
UK 58	Para 3.36	Modify to read: "…assigned to an appropriate safety class and the appropriate.."	There can be more than one.			R	
ENISS 34 WNA 36	3.36	… b) the SSCs in each safety functional group are assigned to the correct safety class and the appropriate engineering ~~design~~ rules are applied; …	See rationale for 1.4			R	DS414
	Section 4						
GER 23	Chapter 4		Statements like "SSCs should be designed, constructed, qualified, operated, tested and maintained to ensure the			R	DS 414 and DPP for better understanding

			proper capability, dependability and robustness." do not belong into a guide on Safety Classification. There are several such statements.				
UK 59	Section 4		This section fails to give helpful and specific examples of what is meant by the term Design Rules. As it stands, this section is too theoretical.	PA			DS 414 and DPP for better understanding
ENISS 35 WNA 37	4	SELECTION OF APPLICABLE ~~DESIGN~~ ENGINEERING RULES FOR STRUCTURES, SYSTEMS AND COMPONENTS	To be consistent with our former remarks and also there is more to select than the design of systems (also i.E. for the operation the water chemistry and much more)	PA	ENGINEERING DESIGN RULES		
UK 60	Para 4.1	Contradicts Figure 1.	Engineering Design Rules come from the SSC Class, not the safety function.	PA			
ENISS 36 WNA 38	4.2	The engineering ~~design~~ rules selected should reflect the required quality and should be assigned in accordance with ~~the category of the safety function and~~ the safety class of the SSC.	There is no category of a safety function – also it is enough to reflect the safety class.	PA			
USA 17	Para. 4.2 Line 3	Insert "with any applicable regulatory limitations and modifications" following "appropriate codes and standards" in the last sentence of this paragraph.	The Safety Guide should indicate that any regulatory limitations or modifications for the use of codes and standards by the applicable regulatory body in the Member State need to be met.	PA			
UK 61	Para 4.3 b)	Change safety function to "plant specific safety function"	For consistency with earlier terminology.	A			
UK 62	Para 4.3 b)	Modify to read: "..the required safety function with a suitably low failure rate consistent	We shouldn't encourage "safety by numbers".	PA			

		with the safety analysis..."					
ENISS 37 WNA 40	4.3	Engineering ~~design~~ rules are related to the three characteristics of capability, dependability and robustness:	See above			R	
USA 18	Para. 4.3 Line 11	Insert "manufactured, procured, installed, inspected, commissioned, and included within the scope of the quality assurance program," following "qualified" in the last sentence of this paragraph.	The engineering design rules addressed in the Safety Guide should ensure that the SSCs are manufactured, procured, installed, inspected, commissioned, and included within the scope of the quality assurance program, to provide confidence in their capability, dependability, and robustness in addition to the activities listed in the Safety Guide, such as design, construction, qualification, operation, testing, and maintenance.	A			
ENISS 38 WNA 41	4.4	The engineering ~~design~~ rules relating to dependability and robustness of an SSC may be adjusted in accordance with the probability of failure of the SSC and the associated consequences.	See above	A			
UK 63	Para 4.5	Annex II doesn't provide a link to classes as stated, but to categories.				R	
PAK 2	Para 4.8 Page 23	Quality assurance or management system requirements for the design, qualification, procurement, construction, inspection, installation, commissioning, Operation, testing, surveillance and modification of SSCs should be	QA during commissioning and operation is an important aspect which is considered in IAEA Safety Series 50-C/SG-Q.	A			

		assigned on the basis of ……					
UK 64	Para 4.9	Modify to read: "The seismic classification of safety related SSCs…"	Category is reserved for safety functions in this SG.			R	Ref [17]
		Appendix I, II					
ENISS 39 WNA 47	Appendix I	Delete	The appendix does not show any relationship between safety functions and the DID levels and should therefore be deleted. Following our general comment only DID Level 3 needs safety functions.			R	
ENISS 40 WNA 46	App II/first cell/Line 2	"…for the safety design ~~safety~~ of the…."	Safety design reads better…			R	
USA 23	References Ref. 7	Insert "NRC Regulatory Guide 1.201" in Reference 7.	Editorial	A			
		Annex					
ENISS 41	Annex 2	Table	Table needs modification according to our general comment, e.g. delete "preventive safety functions", delete AOOs from mitigatory safety functions. Further more in the column "robustness" of the mitigatory safety functions the AOOs needs to be added.			R	
FRA 51	Annex II Table II-III	I&C (IEC 61226) Safety class 1: ~~B or C~~ A or B Safety class 3: ~~B or C~~ C	Mistakes to be corrected if the table is maintained.	A			To be discussed on NUSSC
USA 19	Table II-II Annex II	Insert "Surveillance methodology" in the list of Design Solution Examples for Dependability.	The Safety Guide should alert the user that the adequacy of the surveillance methodology for SSCs is important to ensure their dependability, in addition to	A			

			maintainability and testability listed in the table.				
USA 20	Table II-III Annex II	Insert a footnote regarding the use of Commercial Grade that states: "Commercial Grade practices need to demonstrate that the SSC is capable of performing its safety function consistent with its categorization."	In Section 69 of Part 50 in Title 10 of the *Code of Federal Regulations* (10 CFR 50.69), the NRC allows nuclear power licensees to request a license amendment to apply the treatment of SSCs based on their risk categorization. As discussed in NRC NUREG/CR-6752, "A Comparative Analysis of Special Treatment Requirements for Systems, Structures, and Components (SSCs) of Nuclear Power Plants with Commercial Requirements of Non-Nuclear Power Plants," significant variation exists in the application of industrial practices at nuclear power plants. Therefore, the NRC stated in the *Federal Register* notice issued with 10 CFR 50.69 that a simple reference to industry practices would not satisfy the rule's requirements. The Safety Guide should indicate that Commercial Grade practices will need to demonstrate and maintain the design-basis capability	A			

			of SSCs to perform their safety functions.				
WNA42	Annex II Table II-I	Table needs modification, e.g. delete "preventive safety functions", delete AOO's from mitigatory safety functions at columns "capability" and "dependability". Further more in the column "robustness" of the mitigatory safety functions the AOOs needs to be added.	Table needs modification according to our general comment			R	PIE includes AOO
ENISS 42 WNA 43	Annex II/SC2/Preventive/Line 1	"...from normal operational..."	"Operation" needs to be replaced with "operational" to read correctly.	A			
ENISS 43 WNA 44	Annex II/SC4/ Robustness/Line 1	"...Withstand conditions	Space required between "Withstand" and "condition"	A			
ENISS 44 WNA 45	Annex II Table II	Delete the last row "safety category 4"	To be consistent with the general comments and comment on 3.21.			R	
WNA48	TABLE II-III p 32	I&C (IEC 61226) Safety class 1: ~~B or C~~ **A or B** Safety class 3: ~~B or C~~ **C**	Mistakes to be corrected	A			
JPN E8	Page 30 / ANNEX II Heading	'EXAMPLES OF DESIGN RULES FOR SAFETY FUNCTIONS AND SSCS'	TABLE II-1 specifies the design rules for safety function.	A			
JPN E9	Table II-III	Seismic category I [II-5]	Add reference [17] NS-G-1.6 as for [II-5].	A			
UK 65	Annex II	This needs to be reviewed in detail for consistency with the main text.	There appear to be many inconsistencies here, e.g. Safety Category 2 in the text equates to Medium severity (the limit of DBA), but the Annex has this at the AOO limit.	PA			

DS367 - Draft 5.10, page 17,

TABLE 1. RELATIONSHIP BETWEEN TYPE OF SAFETY FUNCTION AND SAFETY CATEGORIES FOR PLANT SPECIFIC SAFETY FUNCTIONS (Rejected)

Safety Function Type	**Severity of the consequences of the failure of plant specific safety functions**		
	High	**Medium**	**Low**
~~Preventive safety functions~~	~~Safety category 1~~	~~Safety category 2~~	~~Safety category 3~~
~~Safety functions for mitigation of anticipated operational occurrences~~	~~Safety category 1~~	~~Safety category 2~~	~~Safety category 3~~
Safety functions for mitigation of design basis accidents (Level A)	Safety Category 1	Safety Category 2	Safety Category 3
Safety functions for mitigation of design basis accidents (Level B)	Safety Category 2	Safety Category 3	No safety category
Safety functions for mitigation of consequences in design extension conditions	~~Safety Category 4~~ Safety Category 3 or No safety category [15]	N/A [16]	N/A
Functions not included above	No safety category		

footnotes:

[15] SSCs performing safety functions in safety category 4 could be assigned to safety class 3 or classified as not important to safety, with additional specific requirements to be applied.

[16] These categories are not applicable because the consequences in a design extension condition have already exceeded the consequence levels of medium (for design basis accidents) ~~and low (for anticipated operational occurrences)~~.

Safety Function Type	Severity of the consequences of the failure of plant specific safety functions		
	High	Medium	Low
Safety functions for mitigation of design basis accidents (Level A)	Safety Category 1	Safety Category 2	Safety Category 3
Safety functions for mitigation of design basis accidents (Level B)	Safety Category 2	Safety Category 3	No safety category
Safety functions for mitigation of consequences in design extension conditions	Safety Category 3 or No safety category	N/A[3]	N/A
Functions not included above	No safety category		

[3] N/A indicates that not applicable because the consequences of a BDBA have already exceeded the consequence levels of medium (DBA) and low (AOO).