Resolutions of Member states comments on DS 367 version 5.1

Used abbreviations:
A - Accepted,
PA - Partially accepted,
R – Rejected,
N/A – comment was given to improve the text but the paragraph was deleted or significantly modified because of other technical comments

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
Belg. 1	General	At the last NUSSC meeting it was agreed that a TECDOC would be produced to demonstrate the practicability and the implications of the application of this novel approach to safety classification. As far as we know this TECDOC is not yet available. Without this TECDOC we are unable to support the publication. REASON: .DiD was not developed to be used as a tool for safety classification, and has not been used for that purpose until now (as far as we know). It is important to know where we go when using this new SG	A PA	DiD levels as input for SSC classification have been changed in the process and have been replaced by the bounding PIEs (see paragraphs 2.9, 3.2, 3.35) The term 'DiD level safety functions' has been changed and has been simplified using terms 'preventive and mitigatory plant specific safety functions' of the bounding PIEs (AOO, DBA and Design Extension Conditions)(see Paragraphs 2.9, 3.2,.3.5, 3.6, etc.), Term of 'DiD level safety functional groups' has also been changed to term 'safety functional groups' (see para. 3.24 and footnote 17) More explanations were introduced. An example on application of DS 367 ver. 5.10 for a LWR is available	R	DS 367 ver. 5.10 could be used without a TECDOC. The TECDOC is under development/revision as the DiD terms were changed. Old examples on DS 367 ver 5.1 were available on NUSSC webpage in 2009. These examples are being revised by the designers.
Belg. 2	General	The Safety Guide does not address well the critical step of the section of possible events that are considered outside the Design Basis. This choice affects the corresponding requirements, which are to be – of course- at the highest level.. REASON: The current practice in nearly all PWRs excludes the following	PA	(See Paras 3.8, 3.27) Rupture of RPV is included (Class 1)		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		events: • Sudden rupture of reactor • Steam line break between containment & isolation valves • Steam generator outer shell rupture • Severe criticality accidents Such cases must be identified and excluded for probabilistic reasons by adequate prevention and surveillance measures.				
Belg. 3	General	The Safety Guide should provide an illustration on the practicability of the approach using modern European concepts as given in the European Utility Requirements document (rev C 2001). For example, we believe that there is a need to introduce the concept of time available to perform the safety functions (cfr 2.1.6.8 Classification of Safety Functions and categorization of equipment). REASON: The proposed draft does not describe well known practices, but suggests a novel approach, mainly in the link with the DiDs levels. It was not the intent of the DiD concept to serve this purpose. Consequently, we have found it difficult to understand the implications, particularly for the use of DiD level 1	A	The SG is not a new approach. It is aimed at reflecting the best practices worldwide. However, the SG has been deeply reviewed to take into account the MS comments,, in order to launch the classification process from the bounding initiating events rather than from DID levels. See also resolution of Belg 1 comment	R	The concept of time available to perform the safety functions is included in the approach (see the introduction of level A and B of DBA mitigatory function)
1 CAN	General	There is a basic approach on deterministic methods, with little and vague mention of PSA use. It is in significant contradiction with developments in the North American nuclear power industry in last 15 years.	PA	The classification process in Ds 367 includes both deterministic and probabilistic approaches (more explanation, see para3.26, 3.31)	R	DS 367 provides recommendations to fulfill Requirement23 and Paragraph 5.35 of DS 414 Ref. [1] (Revision of NS-R-1) which states that “The method for classifying the safety significance of items important to safety shall primarily be based on deterministic methods complemented where appropriate by probabilistic methods, with account taken of factors……
2 CAN	General	There is no attempt in classifying SSC based on risk				See CAN 1

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		importance determined through importance measure factors (such as RAW and FV).				
3 CAN	General	The document neglects developments in risk-informed decision-making and its use in this topic (works by NEI, EPRI for example)			R	See CAN
4 CAN	General	It seems that the SSC classification is based primarily on consequences, and takes very little into consideration probability (risk) aspect.			R	See CAN
5 CAN	General	The link to overall safety goals (in term of CDF and/or LERF) is not clearly demonstrated. The document employs allowed regulatory limits for each postulated initiating event (e.g. – see point 3.45)?	PA	the reference made to regulatory limits associated to plant conditions has been introduced		
6 CAN	General	The document mentions a use of PSA but it is very vague and it is not clear how this tool is to be used in this approach (e.g. see the point 2.19, &Appendix 2).	PA	More paragraphs were introduced on grouping of PIEs, references to SSG 3 and SSG 4 and see paragraphs 3.26, 3.31	R	See CAN
7 CAN	General	It is not clear how the engineering (professional) judgment is to be used in this topic. Statements are too general and too vague despite the fact that there are major developments in this area worldwide	A	See 3.34 and footnote 19		
1 CORDEL	General	It is recognized and recommendable to provide guidance on how to identify and classify SSCs according to their safety function and safety significance. On the basis of well described and documented best practice concepts approved in licensing and supervision processes a comprehensive and consistent approach on SSC classification should be ruled in a IAEA Safety Guide. **But DS367 is not really mature enough for a Safety Guide in order to cover that task and should firstly be revised and than be published as a TECDOC.** Following CORDEL's general comments are given to depict the major questions and to justify it.	PA	Draft Safety Guide has been modified according to the Member States' comments. See resolution of Belg. 1 comment	R	(not only TECDOC) Both SG and TecDoc will be issued but it is reminded that TECDOC does not call for any consensus among the Member States and only reflects the position of the contributors.
2 CORDEL	General	This draft proposes an innovative approach in the classification of SSCs by using an allocation process on the levels of the Defense in Depth (DiD) concept and on the more indirect relevant radiological consequences that is not well known and has not been used in licensing and supervision processes. The Assignment of safety functional groups to safety categories only based on the radiological consequences is not feasible. A simplified method having a combination of conservative deterministic assignment of level 2 and 3 mitigation functions	PA	The proposed approach based on the DID levels was not totally innovative, only the use of the terms were new, but the logig has been already applied by some Member States (e.g. Germany). However, the allocation process on the levels of the DID concept has been modified in order to respond to the remarks from several		.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		and probabilistic assignment of level 1 prevention and level 4 mitigation functions would be more applicable. Furthermore, the term "operational limits" is used in Paragraphs 3.24 and 3.25, dealing with the radiological consequences in case of failures. It seems that the term is misplaced in 3.24 dealing with high consequences, which implies not meeting limits for DBAs. Exceeding of operational limits and Exceeding of limits for DBAs should be differentiated regarding consequences. The application of this approach and the effectiveness of this methodology of classification to increase safety benefits should be demonstrated by technical best practice documents of Member States.		Member States. See resolution of Belg. 1 comment DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs See paragraphs 3.16-3.22 Examples from technology dependent Practices in the Member States included in the document.		
3 CORDEL	General	According to NS-R-1 the complete set of characteristics, impacts and aspects should be considered for evaluation of the safety significance of SSCs instead of a more or less reduced consideration on the defense in depth as leading criterion (besides DiD e.g. barriers integrity protection, event frequency, succession of activation should be taken into account).	A	More explanations were provided in Section 2 and 3 Also see resolution of Belg.1 comment		
4 CORDEL	General	Application and interpretation of the DiD concept as well as known terms or subjects should be used in a consistent manner according to existing Safety Standards like e.g.: - the differentiation of classification with respect of graded safety relevant tasks of SSCs during DBA or BDBA is best practice but the splitting of the DiD-concept for the level 3 and 4 into a level 3a/3b and 4a/4b is not recognised in the IAEA classification process (see INSAG-10, NS-R-1) and is also not described here; - the described relationship between severity level of radiological consequences (high, medium) in case of failure of safety functional groups and the DiD level 1 and 2 (see Table 1) is incomprehensible and should be revised according the existing general understanding described in INSAG 10 or other SS; - The use of the term "mitigation" in this guide (DiD 2. 3 and 4) seems misleading and doesn't comply with the IAEA Glossary (DiD level 4: measures to mitigate consequences of an BDBA) - "Safety categories/safety classes": the difference between the two terms, used as example in Paragraph 2.18 is not clear - the need for both is not clear.	A	DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs - Splitting in categories (e.g. 3A and B); is introduced to take into account the duration of the transient and the possibility to recover some SSCs during the long term phase of the transient. For short term actions (e.g. 3A) a higher classification may be required than for SSCs c that could be recovered during the long term phase by the operators (e.g. 3B). See reference [8] The descriptions of the different phase has been improved in the new draft SG. Also see resolution of Belg.1 comment See comment Cordel 6 also		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
5 CORDEL	General	The DiD concept is well described e.g. in Paragraphs 2.9 through 2.11. But some Paragraphs e.g. 3.19: *"Each plant specific safety function allocated to a defence in depth level, whether preventive or mitigatory should be achieved by a single safety functional group..."* could be read or misunderstood as requiring different SSCs for each separate safety level. (This misunderstanding is actually already present in a regulatory body in one country) However, this would obviously be a misunderstanding as demonstrated by the reactor pressure vessel (there is only one for all safety levels) or the reactor trip system which is typically credited for safety levels 2, 3, and 4 (partly). Actually, the aim in reactor safety is *"preventing accidents and ensuring appropriate protection in the event that prevention fails"* (Paragraph 2.10) i.e. to prevent "bad consequences" for the public with very high confidence. There are two ways to contribute to achieving this aim: • Sufficient DiD by providing several different measures "working" independently of each other • Increasing the quality and reliability of the measures provided. In general, it is a prudent way to have a balanced mixture of both. But depending on the safety function to be fulfilled and the technical conditions given, the mixture can go in the direction of more DiD in separate and independent system functions or more DiD with respect to quality and reliability. This means if there is little system functions DiD, one will need very high quality for components (as for the RPV), and if there is a lot of system functions DiD (e.g. typically for steam generator feed in PWRs), the requirements on quality and reliability DiD for each single measure do not need to be quite as high. This logic can be found in the draft if read with in depth knowledge, but it should be more clearly stated to avoid misinterpretation.	PA	Each plant safety function was associated to one or several defence in Depth Levels, but the DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs Also see resolution of Belg.1 comment Text of the SG has been improved for the better understanding. See para 3.22		
6 CORDEL	General	Defence in depth level 3B safety functions: Paragraph 3.11 says: "*Defence in depth level 3B safety functions should:* a) *after a controlled state is reached, achieve a safe*	A	Text was improved with more explanation in para 3.14.		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		shutdown state and maintain it as long as necessary following a design basis accident, …..” The first part (*3B safety functions should, after a controlled state is reached, achieve a safe shutdown state*) is o.k. It is correct to make a difference between • Achieving a controlled state (typically very short grace times; higher requirements) and • Going from a controlled state to a safe shut down state (typically longer grace times, possibility for “second chances”; lower requirements). Up to now, this is not yet common thinking and is not stated in the relevant IAEA documents (see comment 3), but it has technical logic in it. But the second part (…. *and maintain it as long as necessary following a design basis accident*) poses a problem: The period <u>after</u> reaching a safe shut down state can be very long (weeks or months). This means the perspective of the plant personnel and of the actions performed can no longer be restricted to stabilizing plant parameters. It has to be set on building up DiD again i.e. returning to using operational systems as much as possible and shutting safety systems down to have them in standby again. So this phase should <u>not</u> be considered as part of accident mitigation (level 3 B) but as the (slow) return to normal shut down states (“post-accident recovery”?).				
7 CORDEL	General	The necessity of introduction of “safety functional groups” seems not be evident as well as clear definitions and examples are missed. The concept of assignment of a safety functional group in the process of classifying SSCs doesn’t give any added value and is dispensable.	A	See para 3.24 & Glossary		
8 CORDEL	General	Without reasonable justification the number of safety categories was expanded to 4 categories but existing industrial design codes encompasses typically 2 or sometimes 3 categories in order to consider graded design requirements sufficiently. This approach induces more effort on the classification process without added value of benefit.			R	It does depend on the practices in different MS. The four categories are given as example but later it can be reduced to 3 classes of SSCs – most commonly used by MSs and the most reasonable because of the use of design rules and codes (Category 4 used for the DECs – applying specific design rules)

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
9 CORDEL	General	The process as described in the draft is new and has no approval in licensing and supervision processes which can affect the effectiveness such processes. The steps of concept involved (fundamental safety functions, plant specific safety functions, DiD, safety functional groups, severity /consequence level, safety categories, and finally safety classes) lead to a very complex evaluation process to define the safety classification of a component and implies the risk of misunderstandings and conflicts in supervision licensing and supervision processes. Some preconditions for this approach like the typically used methods of PSA required to adjust the deterministic classification results are actually not available. For new NPPs, the issue of implementing passive safety systems into the safety functions / functional groups will add to the complexity of the proposed process and can increase the level of discussion with the regulator.	PA	See Response to comment CORDEL 2		
10 CORDEL	General	Assignment of SSCs to Safety Classes Figure 1 shows only the possibility that final classification can be graded down compared to preliminary classification. This is not correct; see e.g. Paragraph 3.44 which considers upgrading. Paragraph 3.44 allows upgrading only; however, in some cases (significant PSA results) it should also be justifiable to grade down the classification. Fig. 1 could also be misleading due to the fact that no mention is made that besides the consequences of a failure also the probability of being called upon to perform a safety function as well as the probability of failing should be taken into account. (E.g. it seems that in several member countries the reactor building is not classified in SC1 although failure of the reactor building would indeed have high consequences.) Similar arguments would apply looking at Paragraphs 3.37 and 3.38. E.g. the Improved Technical Specifications (NUREG 1431) allow reduced classification for snubbers compared to the associated piping or components because failure of a pipe would have a higher probability of "bad consequences" than failure (inoperability) of a snubber. Paragraph 3.38 does not seem to allow this.	PA	3.44 of ver 5.1 was deleted and Text was improved, see para 3.34		
ENISS – General 4	General	**Number of safety categories**: None of the by EUR analysed designs uses a 4-level safety categorization, which is something quite new. We question the need for so many levels in that it makes sense only if sufficiently graded design requirements are			R	See response to CORDEL 8 The Safety Guide allows flexibility to reduce the number of categories

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		defined in the industrial design codes in order to be able to assign different requirements to the corresponding safety categories. To our knowledge none of the existing industrial design codes encompasses more than 3 levels of design requirements, many of them only two. The designer would have to assign the safety categorized SSCs according to the Safety Guide approach to much less code classes, thus limiting the benefits of a sophisticated classification process.				
1 FIN	General	This draft safety guide proposes an innovative approach in the classification of SSCs. Although the Defence in Depth concept is a solid basis for nuclear safety of nuclear installation, this concept has never been explicitly used in the classification of LWRs SSCs. The introduction of this concept in the methodology of classification introduces complexity without evident safety benefits. We consider it unavoidable to support it with more practical implementation guides.	PA	See response to Belg.1 comment		
2 FIN	General	Connection of the DiD concept with the classification of SSC also leads to interpretation problems. The process as described in the draft SG seems complex and is far from straightforward. The layers of concepts involved: (fundamental safety functions, plant specific safety functions, DiD, safety functional groups, severity /consequence level, safety categories, and finally safety classes) lead to a very complex process to define the safety classification of a component. Such a final feedback from the PSA studies to the safety classification process keeps the whole process unconcluded for a long part of the design process.	PA	See response to Belg.1 comment Description on Use of PSA vas improved		
3 FIN	General	One of the most difficult issues in this kind of safety classification is to connect the passive leak-tight barriers: reactor circuit, primary and secondary confinement, to the active operative safety functions. The guide is not presenting the solution to this problem. Another problem in creating the plant specific safety functions and safety classification is the different functional demands in mechanical and automation areas. The guide should give more guidance to this issue.	PA	It is covered by the Guide, See also 3.8		
5 FIN	General	Because of the technology neutrality the guide is not presenting a clear classification for the containment function based on preventive safety functions. Some real system level classification examples according to some specific plant type	PA	Draft 5.10 gives more examples in paragraphs One example of applications is available		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		should be presented as an annex of the guide.				
6 FIN	General	Giving different requirements for the same safety class depending on the DiD level can be difficult to implement in practice. Also this item needs to be clarified in the guide.	PA	See response to Belg.1 comment It was improved.		
1 FRA	General	At the last NUSSC meeting, it was agreed that, in parallel with the Member State consultation, IAEA would provide MS with examples of application of the proposed classification method to existing NPP and NPP in construction, (EPR…). This has not been done. As a consequence, questions are still pending on whether this guidance will be applicable. REASON: Unable to observe actual implications of the proposed guide	PA	See response to Belg.1 comment		
2 FRA	General	The classification of SSC of most (if not all) operating NPP was done decade are years ago. The question is whether this guide represents at least the very last practices (EPR, AP1000,….). REASON: For example, concept of “controlled state” and “safe shutdown state” are quite new. In France, they have emerged as part of the EPR design process	A	Last practices: German, French, Japan, Russian, UK, USA (ANS/ANSI 58.14) Safety Classification standards, IEC 61226, IEEE (2004) PBMR design, AP 1000 design, EPR design uses the concept of “controlled state” and “safe shutdown state”, from EUR See paragraph 2.19		
1 JPN	General	It is recognized that TECDOC, which shows examples of actual application of the Guide to some type of NPPs, shall be published together with the revised version of DS367 for member state’s comments when the draft for MS comments was reviewed and approved for submission to MS at 26th NUSSC meeting. However, the relevant TECDOC does not yet published at the time of comment limits. It is demanded to have another opportunity to make comments to DS367 after the TECDOC would be published. REASON: Clarification	PA	See response to Belg.1 comment		
1 UK	General	We have some concerns that some of the English is open to unintended misinterpretations in places and are overly repetitive. We feel that a suitably knowledgeable technical copywriter is used to tidy the document. Up.	A	5.10 version was reviewed by IAEA NS technical editor		
2 UK	General	Although the idea of producing a “technology neutral” guide is			R	The SG has been drastically simplified

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		commendable, the current document should probably be regarded as a first attempt, which needs further discussion and development. As such it is not really suitable for publication as a guide, at this stage, but should be published as a TECDOC incorporating the application exercise (See Comment 4). At present, it is obvious that the guide cannot be applied consistently to a full range of existing and future technologies.				and improved and needs to be published as a safety guide See response to Belg.1 and FRA 2 comments
3 UK	General	The terminology used is confusing. We previously suggested a glossary (this comment was submitted October 2008) and still consider this to be a good idea. Failing that, the key terms defined within the guide could be *italicised* or Capitalised, so that it is clear that this is a term with an intended meaning.	A	The draft was improved Definitions have been improved and the IAEA glossary will be updated accordingly if needed (DS 414 contains some new term)		
ENNIS General 1 4 UK	General	IAEA policy in establishing safety standards, recalled on each foreword, is to reflect best practices in Member States. This draft safety guide does not follow this policy, because it proposes an innovative approach in the classification of SSCs. Although the Defence in Depth (DiD) concept is a solid basis for nuclear safety of nuclear installations, this concept has never been explicitly used in the classification of LWRs' SSCs and seems not to have been approved by any regulator. The introduction of this concept in the methodology of classification introduces complexity without evident safety benefits. During the 26th NUSSC meeting the technical officer in charge explained that several ***exercises of application*** of the guide to PWR and BWR have been done. NUSSC members asked that the corresponding documents be sent with the proposed guide, in order to be able to look at the impact of the guide on the existing classification both for operating plant and the one under construction and licensing in various countries. We have not seen documentation of these exercises. ENISS has been working with the "European Utility Requirements" (EUR) organisation to compare the classification proposed in the guide with the EUR classification, which is applicable to GEN 3 reactors, as well as with the safety classification used by all the GEN 3 designs that their vendors had submitted to EUR for their review (ABWR, AP1000, EPR, ESBWR, AES 92, etc). The conclusion is that none of these designs fully complies with the recommendations	PA	See response to Belg.1 comment The SG is not a new approach. It is aimed at reflecting the best practices worldwide. However, the SG has been deeply reviewed to take into account the MS comments,, in order to launch the classification process from the bounding initiating events DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs One example on applications is available more are under revision See paragraph 2.19		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		of DS 367.				
ENNIS General 2 5 UK	General	**Use of DiD as leading criteria** The attempt to link everything to DiD looks plausible. However DiD as defined by INSAG 10 does not lend itself to such a simple interpretation. The problem is that when looking at the safety significance of SSCs we normally consider a range of different aspects; DiD is one, protection of barriers is another (but there is not a one-to-one relationship between DiD levels and barriers), frequency of challenges are important, as is the significance of the system failures. The problem is multi-dimensional, which is already captured in NS-R-1 (2000). The link between defence in depth and "defence in depth safety functions" is also a questionable one. For instance, our interpretation of DiD Level 1 is that safety classification is itself part of Level 1. Under this level (i.e. Level 1) NS-R-1 states that: *"This leads to the requirement that the plant be soundly and conservatively designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices, such as the application of redundancy, independence and diversity. To meet this objective, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction."*	PA	See response to Belg.1 comment The SG is not a new approach. It is aimed at reflecting the best practices worldwide. However, the SG has been deeply reviewed to take into account the MS comments,, in order to launch the classification process from the bounding initiating events DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs.		
ENISS General 3 6 UK	General	**Safety Functional Groups** The proposed procedure with the intermediate step "definition of safety functional groups" makes the classification process more complicated than necessary. It is also unclear how the described workflow can be done, particularly as a clear definition and examples for "safety functional groups" are missing (the term is not found in the IAEA Safety Glossary). An assignment of a safety functional group in the process of classifying SSCs from our view doesn't give any added value and is therefore redundant. We therefore suggest deleting the concept of "safety functional groups".	PA	See para 3.24 Terminology has been changed and clarified (definitions): Plant level safety functions are used		
ENISS General 5 7 UK	General	**Uncertainty of the classification process** The process as described in the draft safety guide seems complex and is far from straightforward. The layers of concepts involved (fundamental safety functions, plant specific safety		See response to Belg. 1 and FRA 2 comments The SG is aimed at reflecting the best	R	Probabilistic criteria used as DS414 requires; For example See paragraphs 3.26, 3.34

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		functions, DiD, safety functional groups, severity /consequence level, safety categories, and finally safety classes) lead to a very complex process to define the safety classification of a component. Many NPPs will not have a list of specific safety functions readily available. To define these, based on the fundamental safety functions, and link them to DiD levels is likely to lead to lengthy discussions with the regulator. The standard list from NS-R-1 cannot of course just be copied. Introducing the safety classification as proposed in the draft safety guide seems to entail a lot of work and extensive discussions with the regulator until the new classification is approved. Moreover, the distinction between safety categories and safety classes seems to be the information from risk analyses, i.e. the original safety classification (categories, based on deterministic analyses) gets adjusted with PSA results, with the safety classes as final result. Such a final feedback from the PSA studies to the safety classification process keeps the whole process unconcluded for a long part of the design process. We see a big risk that the same NPP design project gets different requirements about classification by different national regulators, thus precluding standardization of the SSCs, and eventually of the design. It is not clear that the classification scheme will work in practice, and some examples of how this would align both with the schemes currently used for a range of different reactors and how they would be applied to future reactors are needed. This raises a whole series of questions including: ▪ The definitions of controlled state and safe shutdown state could be different, and in some cases may be the same, depending on the technology and in certain cases on the fault sequence. ▪ The normal approach to barriers/ DiD is to provide protection for all levels, but the technology may make different strengths of claim for different barriers (e.g. clad integrity and containment integrity). How is this to be handled? ▪ Assessment of the frequency and significance of system failures would seem to lend itself to a probabilistic approach based on importance functions, but this would necessitate an iterative approach (to some extent we do		practices worldwide. It has been deeply reviewed to take into account the MS comments,, in order to launch the classification process from the bounding initiating events. . DiD levels as input for SSC classification have been removed from the process and have been replaced by the bounding PIEs Definition of Control State and safe shutdown have been improved (see also Comment 2 FRA) Hopefully the examples will make the process clearer and more certain. B Address application scope of the safety guide.		It was changed to more than radiological criteria. See 3.17

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		this already where PSA is used to "inform" the design basis approach). ▪ Assignment of safety functional groups to safety categories only based on the radiological consequences is not feasible. A simplified method combining conservative deterministic assignment of Level 2 and 3 mitigation functions and probabilistic assignment of Level 1 prevention and Level 4 mitigation functions would be more applicable.				
ENISS 6 8 UK	General	**Extended scope of the safety classification** The guide could be interpreted as requiring most of the systems and components of a plant used for normal operation, which belong to the first level of DID, to be safety categorized. This goes well beyond the current practices.			R	See response to Belg. 1 comment
ENISS 7 9 UK	General	**Passive components** For new NPPs, the issue of implementing passive safety systems into the safety functions/ functional groups will add to the complexity of the proposed process and increase the level of discussion with the regulator.			R	See 3.30 Passive component are part of the plant system functions
ENISS 8 10 UK	General	**Interface with other IAEA standards** DS 367 includes requirements and recommendations that are handled in other IAEA Safety Standards (NS-R-1 and the guides belonging to that; these guides are nearly all listed in the references of DS 367; e.g. NS-G-1.1, NS-G-1-3, NS-G-1.5, NS-G-1.6, NS-G-1.7). It is necessary for the classification to show the interfaces to the design requirements, but referencing the appropriate safety standards could do this. In DS 367 the description of the requirements to the design is often mixed with the definition of safety functional groups.	A	Cross References to the related Safety Standards have been made DS414 NS-R 1 and GSR Part 4 are the main references. More references to other SS. See para 3.24 and section 4		
ENISS 9 11 UK	General	***Clarity of the guide*** The use of "mitigation" in this guide seems misleading. According to the IAEA Glossary, mitigation only means the mitigation of accident consequences in terms of lowering radiation doses for workers, the public and the environment. It is therefore only applicable in DiD-Level 4 and 5. In this guide, the term is used for all functions above DiD-Level 1. Its use in this context should be reviewed.	A	DS 367 gives clear definition and after approval the Glossary will be changed accordingly, more common definitions in DS414 See response to Belg. 1 comment		
12 UK	General	The document appears to assume that SSCs can only have one safety function. The language used needs to be reviewed to avoid this implication.			N/A	3.29 allows more than one safety function.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
13 UK	General	The IAEA have used the word *classification* in their title instead of *categorisation*. These two words are often used with specific meanings to represent different activities; ▪ Identification that a function, independent of its implementation, is a safety function. ▪ Giving a value of safety significance to particular physical item or instruction. Taking account of national guidance (i.e. the UK's Safety Assessment Principles (SAPs)) and common usage, we normally call the former "Classification" and the latter "Categorisation". On this basis the title of the draft IAEA standard would be wrong, unless there is a good reason for making it that way. If IAEA stick with the use of Classification in the title of DS 367, it might have implications for UK's SAPs.			R	DS 367 uses: Categorization is associated to safety functions and safety classification is applicable to SSCs
MOR	General	Relevance & usefuness – The guide's objective is appropriate. A supplementary publication was indeed awaited to show how to meet the requirements for the identification of safety functions and the classification of SSCs as these requirements were stated in NS-R-1 Safety of Nuclear Power Plants: Design". This recommended approach fully answers the guide's goal. Scope & Completeness – The scope set for the guide is appropriate and the guide's content totally covers its objective Quality & Clarity – The guide uses standard, technology-neutral terminology which renders its reading an easy task. The guide would have gained in clarity if is used a simple and "light" ensemblist formalism to designate parts and subparts of NPPs and their safety categories or classes. This would have posed no problem to the potential users of the guide as most of them are familiar with mathematical formalism. Thought one has no past experience in classifying SSCs of NPPs with respect to their significance to safety, the following set of remarks were formulated by the project team members:	A	A TECDOC is under development in parallel		
2 MOR	General	Consider setting a limit for the downgrading of the safety class of SSCs depending on the safety category of the safety functional groups they belong to. For example, lowering of the safety class of SSCs belonging to safety functional groups of the first safety category could be limited to no more than one level.	A	– it is one level in general see para 3.26		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
3 MOR	General	At the end of the classification process, a recommendation could be made towards mapping the entire nuclear power plant using a color code based on the significance to safety of its SSCs. Such a visual representation could help on this further steps of the design process and especially in facilitating the assignment of design requirements to the plant SSCs.			R	It is not practical everywhere
Sweden	General	The approach in DS367 on classification of SSC is new, which is against the IAEA policy saying that safety standard should reflect best practices in Member States. This is especially true taking in account the fact that there is a well established approach for classification of SSC in LWR's. The approach is DS367 is complicated to apply mainly depending on the use of DiD. The principle of DiD was never meant to be applied in this way. In our view there are some aspects that need to be considered before going further with this guide. Some examples of consequences of applying the approach on existing NPP are mentioned below. The approach of the safety standard is intended to be suitable for both new designs and during periodic safety review or upgrades of existing plants. The consequences mentioned below are not just valid for existing NPP'S but can also, depending on the type of reactor is valid for the new designs which are based on an accepted methodology. Examples of consequences of the guide mentioned by the utilities in Sweden: 1) All documentation for existing plants must be reorganized in order to develop and maintain a structure that supports the assignment of SSC into safety functional groups. 2) A new level of safety class must be introduced (SC4). As a minimum non-pressure retaining equipment will be assigned to new safety classes. 3) The requirements are not uniform for SSC assigned to a safety class. The basic idea that the safety class should govern the requirements for SSC is lost. Based on examples in Table 4, many SSC must be assigned a higher safety class in order to maintain the more stringent requirement they are designed to according to today. This must be taken into consideration before approving the guide. 4) In the guide it is said that DS367 was written for NPP's but	PA	DS 367 provides recommendation for fulfilment of NS-R-1 (DS 414) requirements for Safety classification of SSCs in NPPs No technology neutral guide available in the industry DiD terms were changed See response to Belg.1 All steps are used for reactor type specific classifications. See para 1.8 Table-4 was prepared using MSs' experiences/practices The ver 5.10 is more simple, contains resolutions of comments and results of		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		could be applicable to any type of nuclear facility, if the appropriate amendments are made. The guide is quite theoretical and the amendments necessary for applying the guide to other facilities than NPP's are extensive. A more simple approach to classify would be greater value for other facilities.		consultants meetings. DS 367 does not hurt the existing safety classes.		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		Section 1				
1 SAF	1.1	Million of hours REASON: One reactor year is nearly nine thousand hours	PA	Comment is correct but updated version has been written in a more general way (*taking into account the lessons learnt during the operation of existing plants, mainly with light water reactors*.)		
1 MOR	1.1	The introductory para 1.1. might be reserved to elaborate on the usefulness of classification tasks in understanding, designing, constructing, operating and maintaining large and complex systems (industrial plants, major civil buildings, mega-cities, etc.)The introduction of the reference [Risk-informed classification of systems, structures and components, Jan Erik], which could be used as an example, develops on the need for a classification system for the SSCs of nuclear power plant.			R	DS 367 follows the DS 414 (NS-R-1) requirements
1 ROM	P.1.1/L.8	BACKGROUND 1.1 …..safety philosophy has not been described in earlier IAEA publications. The classification…….. REASON: - The safety functions concept represents the objective itself which is coming from the nuclear safety philosophy. In turn, the safety philosophy derives from the existence of an accepted human being activity risk (industrial or radiological risk, in this case).	PA	It is included in para 1.4		
1 USA	1.1 through 1.4	The draft guide should include the caution that the regulatory requirements of the regulatory body in the applicable Member State take precedence over the guidance in Safety Guide DS367 where specific regulatory requirements differ from the guidance in DS367.	PA	See 1.4 and 2.19 May be in the TECDOC a more detailed analysis could be done		
3 FRA	1.3	Delete “Information from a significant number of other international and national publications has been considered in developing this Safety Guide.” or actually insert references of these publications REASON: A bit ambitious…	A	Completed , and 8 international standards were included in the List of References		
2 USA	1.5 & 1.6	The draft guide should include a requirement that the			R	SG can not include requirements only

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		classification approach in Safety Guide DS367 be piloted and tested for comparison to specific regulatory classification methods in Member States to confirm that the DS367 approach is appropriate for various nuclear power plant designs.				recommendation. This exercise will done and will it be included in the TECDOC
3 USA	1.5 / 5	"discussed in general terms. Users of this Safety Guide must comply with the specific requirements issued by the regulatory body in the applicable Member State." REASON: The regulatory requirements of the regulatory bodies in individual Member States might differ from the guidance in Safety Guide DS367. The applicable Member State requirements should take precedence over the guidance in DS367.	PA	New para 1.5		Same as 2 USA
2 SPA	Add new para in SCOPE	Although this Safety Guide can apply to all power plants, this does not imply to re-evaluate the whole operating plants where SSCs are already classified by this or other rules. In this case only the SSC affected by important inputs from operative experience, by a new initiating events etc. should be classified. REASON: Idem comment 1	PA	The scope of applicability of the safety guide has been revised. See para 1.8.		
ENISS 1	1.6 4 2nd sentence	The approach to safety classification presented here is intended to be suitable both for new designs of nuclear power plant and, as necessary, during the periodic safety review of, or upgrades to, existing plants. Reason: It is not necessary to reevaluate and classify all SSC in every periodic safety review (PSR), if they have been examined before. In the PSR only the SSC affected by design changes, operative experience or new development which involve some new PIE or changes in their performance, are revised	PA	The paragraph was modified and extended, see new 1.8		
1 SPA	1.6 4th line	Add: … and "as necessary" during the periodic… REASON: It is not necessary to re-evaluate and classify all SSC in every periodic safety review (PSR), if they have been examined before. In the PSR only the SSC affected by design changes, operative experience or new development which involve some new PIE or changes in their performance, are revised	PA	The paragraph was modified and extended, see new 1.8		
4 FRA	1.6/5	After "existing plants", add a footnote : "It is recognized that, for existing NPP which design have been established decades	A	Scope of application modified in the updated version See new 1.8		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		ago for most of them, as well as NPP being currently under construction, the approach described in this guide is unlikely to have been fully implemented. REASON: See general comment 2				
5 FRA	1.7	Delete "This Safety Guide was written for nuclear power plants but could be extended to any type of nuclear facility, if the appropriate amendments are made." REASON: Out of the scope of the guide. (title specifies NPP). Furthermore, see also the general comment on its effective application to NPP (comment 1)			R	It is fully within the scope to recommend the applications.
4 FIN	1.7 Scope	The guide does not specify actual scope of the plant systems to be classified. It seems that the scope is limited and it does not cover systems outside the actual reactor like re-fuelling machines, cranes, waste system etc. This should be clarified in the guide.	PA	It covers all SSCs which included in Safety Analysis Report See paragraphs 1.8 and 1.9		
ENISS 2	1.7	The guide does not specify actual scope of the plant systems to be classified. It seems that the scope is limited and it does not cover systems outside the actual reactor like refueling machines, cranes, waste system etc.	PA	Same as 4FIN the previous one		
4 USA	1.7	This section should emphasize that the scope of SSCs to which this safety guide applies are all SSCs that perform both safety-related and nonsafety-related functions including those functions that support defense in depth and those SSCs that may adversely affect safety-related functions.	PA	Revised and clarified. See 1.9		
5 USA	1.8	This section should convey that a risk-based approach is unacceptable, but a risk-informed approach combined with a deterministic approach can establish a classification method that promotes safety through enhanced reliability supported by risk insights.			R	Section 1.8 deals with the structure of the document. PSA is used in a risk-informed manner as identified in sections 3.
6 USA	1.8 / 3	"Section 2 also introduces the concept of safety functional groups to perform safety functions to prevent and/or mitigate postulated initiating events (PIE)." *Define PIE* REASON: Do PIEs include AOOs and DBAs; but not BDBAs?	PA	Footnote 2 was added DS 414 (NS-R-1) and the Glossary define PIEs The answer is to the questions is "no." It includes all events: AOOs and DBAs; but not Design Extension Conditions (DEC) –New name for BDBA in DS 413.		
3 SPA	1.8 3rd line	Add: … of safety functional groups "(SFG)" to…			N/A	Text was changed

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		REASON: It is necessary to define all the used acronyms in order to prevents misunderstanding				
ENISS 3	Add new para. in scope	Although this Safety Guide can apply to all power plants, this doesn't imply to reevaluate the whole operating plants where SSCs are already classified by this or other rules. In this case only the SSC affected by important inputs from operative experience, by a new initiating events, etc. should be classified *Reason:* *Idem comment 1*	A	New sentence was added, See para 1.8		
		Section 2				
7 USA	2	Recommend identifying that use of an expert panel with a documented basis is a method of applying engineering judgment.	A	See para 3.34		
2 SAF	2.1	…in Ref. [1 and 3] REASON: The requirements for a safety classification are also established in [3]. These requirements are essential because they are more detailed and include additional requirements not used in this draft: *3.26 The importance to safety of all SSCs should be established and a safety classification system as defined in Ref [1] should be set up in order to identify for reach safety class:* *- The appropriate codes and standards, and hence the appropriate provisions to be applied in design manufacturing, construction and inspection of a component;* *- System related characteristics like degree of redundancy, need for emergency power supply and for qualification to environmental conditions;* *- The availability or unavailability status of systems for PIEs to be considered in deterministic safety analysis;* *- QA provisions.* *3.27. In general the following classifications should be verified for adequacy and consistency:* *- Classification of systems on the bases of the importance of the affected safety function;* *- Classification for pressure components, on the basis of the severity of the consequences of their failure, mechanical complexity and pressure rating;* *- Classification for resistance to earthquake, on the basis of the*			R	R because NS-R-1 and GSR Part 4 provide all needed requirements. The details from NS-G-1.2 is not needed here.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		need for the structure or component considered to retain its integrity and to perform its function during and after an earthquake, taking into account aftershocks and consequent incremental damage; *- Classification of electrical, instrumentation and control systems on the basis of their safety or safety support functions, which may be different from the classification of other plant system owing to the existence of field specific, widely used classification schemes;* *- Classification for QA provision.* *3.28. The assignment of SSCs to safety classes should be based on national approaches and should appropriately credit deterministic and probabilistic considerations as well as engineering judgment* *3.29 Fore the purposes of the deterministic safety analysis, those safety functions that are used to determine compliance with acceptance* ***criteria (I cannot read more)***				
6 FRA	2.1 to 3.5	Delete 2.1 to 2.5 and replace them by : "2.1 The requirements for a safety classification system are established in Ref. [1], mostly at paragraphs 4.7, 5.1 to 5.3." REASON: It is worth recopying the text of other IAEA documents. Just refer to it.			R	Only one page but it is convinient to have them together with the recommendations
14 UK	2.2 and elsewhere	Modify to read: "Paragraph 4.7 in Ref [1] states…." REASON: Reword to improve English	A			
ENISS 4	2.2 to 2.7 and 2.9 to 2.10	Delete these para. They are pure repetition of NS-R-1			R	See response to 6FRA comment
8 USA	2.4 / 5-6	*Insert the following item after item (1):* <u>(2) the probability of failure of the item;</u> REASON: The method for classifying the safety significance of SSC, especially the probabilistic method should include the probability of failure of the item.			R	The text is a quote from NS-R-1, and the concept of the probability of failure is item (3).
4 SPA	2.5 Title after	Add: FUNDAMENTAL SAFETY FUNCTIONS "(FSF)"			N/A	Editorial rule : No abbreviations
3 JPN	2.7	Regarding Spent Fuel Storage System (SFSS), relevant annotation is described in para.2.7. But the function of SFSS should be defined on safety classification including protection	PA	Footnote Quotation from DS414 can not been		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		of criticality and confinement of radiological material other than fuel decay heat cooling. In Annex I, TableII-1,(16),(17), (18), above functions are defined. And it is not necessary to refer to "core". How about revise as follows ? "Above three safety functions are also applied for spent fuels in the storage systems" REASON: This guide aims at technology neutral. So, it might be better generally to define firstly categorization of safety function and then to classify SSCs based on the safety functions.		changed.		
9 USA	2.7 / 1-9	" Ref. [1] in paragraph 4.6 states "To ensure safety, the following fundamental safety functions shall be performed in operational states, in and following a design basis accident or event and, to the extent practicable, on the occurrence of those selected accident conditions or events that are beyond the design basis accidents: (1) control of reactivity; achieve and maintain a subcritical condition (2) removal of heat from the core; prevent buildup of heat in the fuel elements and (3) confinement of radioactive material and control of operational discharges, as well as limitation of accidental releases." ~~[The intent on the core in (2) is for fuel in the core and spent fuel in the storage.]~~" REASON: Events such as "external events" should be included in addition to the "accidents" in the classification process. Control of reactivity implies the adjusting of reactivity level to attain a preset or programmed level. It is possible to remove too much heat from the core. If the moderator temperature coefficient is negative, then this could cause reactivity to increase. Referring to fuel elements instead of "core" includes the spent fuel storage, and makes the [note unnecessary.			R	Quotation from DS414 can not been changed. In the IAEA Glossary, provides the meaning of the terms requested.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
2 JPN	2.7 / L5-8	Three fundamental safety functions of (1) Control reactivity, (2) removal of heat from the core and (3) confinement ----- are listed. The three fundamental functions are referred to as basis for SSCs classification in this safety guide as started in Paragraph 2.7. The three fundamental safety functions are however principally the basic safety functions in and following a design basis accident and B-DBE, as generally understood and explained in the proceeding sentences in Para. 2.7. Nevertheless, preventive safety function is also mentioned, as in the paragraph 2.5, 2.9, 2.11, etc. A fundamental safety function for Defense-In-depth Level 1, which requires high reliability, robustness, quality assurance, etc. to preclude occurrence of abnormal events due to loss of the function or failures, should be included independently from the three fundamentals as the basis of safety classification. REASON: Clarification			R	The IAEA Glossary states that the fundamental safety functions are applicable to all operational states including normal operation so DiD Level 1 (prevention) is included.
5 SPA	2.7 Title after	Add: PLANT SPECIFIC SAFETY FUNCTIONS "(PSF)"			N/A	Title was deleted here. No Acronyms in the Safety guide.
2 SLK	2.7/ (3)	Split into two SF Confinement or radioactive material and control of operational charges REASON: a) it is not logical to have one fundamental SF for operational and accidental situations b) after doing that there is better conformance with para 3.6 to 3.17 which are talking about preventive and mitigation SFs			R	Quotation from DS414 can not been changed. The IAEA Glossary states that fundamental safety functions apply to normal operation as well.
3 SLK	2.7/ (4)	Confinement and limitation of radioactive material and control of accidental releases REASON: a) it is not logical to have one fundamental SF for operational and accidental situations b) after doing that there is better conformance with para 3.6 to 3.17 which are talking about preventive and mitigation SFs			R	Quotation from DS414 can not been changed. The IAEA Glossary states that fundamental safety functions apply to normal operation as well.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
1 SLK	2.7/(2)	Remove “and” removal of heat from core; REASON: ‘and’ seems to be redundant			R	Quotation from DS414 can not been changed.
2 ROM	P.2.7/L.5	REQUIREMENTS FOR A SAFETY CLASSIFICATION PROCESS (1) control of reactivity; (2)nuclear fuel cooling; (3) retention of radioactive material and control the releases to environment; (4) plant status monitoring; (5) mitigation of radiological consequences. REASON: - First essential safety function remains ‘as is’ - The second, will be rephrased in order to cover all fuel locations; - The third, will be rephrased in order to cope with any operational regime and accident condition; - The fourth safety function will be added covering all the operational regimes and accident conditions; - The firth safety function will be added in case an accident still occurs.			R	Quotation from DS414 can not been changed. The IAEA Glossary states that fundamental safety functions apply to normal operation as well.
3 ROM	P.2.8	PLANT SPECIFIC SAFETY FUNCTIONS REASON: - This paragraph has to be deleted because there is no need to reassess the plant safety functions, even if the safety related SSC can be of preventive or protective nature. It has to be detail this characteristic instead.	A	Explanation in Section 3		
7 FRA	2.8	“In line with Refs. [2] and [4], preventive safety functions prevent abnormal operation or system failures” (the failure of a structure or component must also be considered REASON: Quality/clarity	A	In Figure 1 box 2 and Section 3		
3 SAF	2.8	No proposal SSC may be used to detect or control system disturbances to arrest accident sequences, prevent releases or radioactivity, and/or mitigate dose consequences from any releases that do occur	PA	Included in Section 3		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		Annex I provides an example of the safety functions derived from an experience of LWRs, a legacy approach				
10 USA	2.8 / 1-3	"For each type of nuclear power plant, based on the fundamental safety functions, the plant specific safety functions should be defined to prevent or mitigate postulated initiating events." REASON: It is not clear how a safety function (examples in Annex I) can prevent a PIE. Are the reactor control system, and the operator, to be considered as a safety function that prevents a PIE by keeping reactor operation within the acceptable operating range, or is there to be a separate PSF added for this purpose?			R	1) NS-R-1 uses safety function to mean both preventive and mitigatory functions, and 2) human actions such as maintenance procedures and emergency operating procedures are part of a safety function, e.g., switchover from injection to recirculation in older PWRs
6 SPA	2.8 4th line	Add: Plant specific safety functions can be preventive or mitigatory REASON: It makes the text easier to understand			N/A	Editorial check was performed
12 USA	2.9 / 4-5	"facilitate the management of the plant in and following any design basis accident or event, and in those selected accident conditions beyond the design basis accidents or event" REASON: Events such as "external events" should be included in addition to the "accidents" in the classification process.			N/A	Para was deleted
8 FRA	2.11/2	Replace "it should be applied in" by "should be made clearer through" REASON: The proposed classification process shows how defence in depth concept is taken into account			N/A	
1 INS	2.12	**Add to this Para** : "The SSCs is divided into process SSCs and safety systems. The process SSCs fuction during normal operating conditions, and the safety systems do not fuction during normal operating condition. During normal operating condition the safety systems are in the standby operation mode. The safety systems function only during abnormal or accidents condition." REASON: To give a more clear explanation concerning the SSCs of nuclear power plant.			N/A	Text was shortened
ENISS 5	2.12	Safety functional groups, defined a group of SSCs ~~as all the SSCs, including supporting items, that~~ , ~~these~~ that work	A	See 2.12 and 3.24		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		together to perform a plant specific safety function, ~~derived from fundamental safety functions~~, to prevent or mitigate a postulated initiating event and allocated to one defence in depth level, should be identified. Reason: for clarification				
15 UK	2.12	This paragraph should be split into smaller sentences to ensure it's meaning is clear. It needs to say <u>all</u> such Safety Functional Groups need to be identified.	A	See 2.12 and 3.24		
4 SAF	2.12 & 2.13	No proposal Is it not clear what differentiation is made between "Safety Functional Groups" in the document & "Safety Groups" described in NS-R-1 Given that Annex I indicates Plant specific safety functions as assigned to several DID levels, and given the definition of ""Safety Functional Groups" in 2.12, it is difficult to understand how a Safety Functional Group may be "allocated to one DID level", as requir3ed by 2.12. This then makes requirement of 2.13 to categorize a Safety Functional Group according to its safety significance equally confusing. It is assumed that the highest safety significance assigned would be adopted. At this stage it is also difficult to understand the difference between safety 'classification'. It seems later (3.32) that this is merely an intermediate potential downgrading	PA	See 2.12 and 3.24 and footnote 17.		
4 JPN	2.13 2.14	2.13: The safety functional groups should be categorized according to their safety significance. Safety categorization should be based on the consequences of the failure <u>of the SSCs</u> to perform their assigned safety functions. Above may better be written following: 2.13: The safety functional groups should be categorized according to their safety significance. Safety <u>significance</u> should be based on the consequences of the failure to perform ~~their~~ assigned safety functions. REASON: Para.2.13 states that safety categorization should be based on the consequences of the failure of the SSCs to perform their assigned safety functions, while in para.3.18, the likelihood of the safety functional group being called upon to	PA	Safety functions should be categorized See paragraphs 2.11 - 2.13		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		operate is also considered as the criteria for safety classification. Following sentence is proposed for clarification.				
5 JPN	2.13	"Safety categorization should be based on the consequences of the failure of the SSCs to perform their assigned safety functions, and the likelihood of the safety functional group being called upon to operate. And safety categorization should be divided into four equivalent groups." REASON: Clarification	PA	See para 2.11		
6 JPN	2.13	As described in para.2.4, NS-R-1 states that classification shall be done 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 its function; (3) the probability that the item will be called upon to perform a safety function; (4) the time following a postulated initiating event at which, or the period throughout which, it will be called upon to operate." In para.2.13, only (2) is used as judgement factor, however, other factors should be mentioned how are they evaluated in safety classification process. REASON: Regarding reactor coolant pressure boundary, double ended guillotine break is postulated as the PIE of DBA in LWR. But, If only double ended guillotine break is postulated as the PIE of reactor coolant boundary system, the reactor coolant pressure boundary system is categorized into Safety Category 2, and containment system is categorized into Safety Category 1. In order to avoid such incoherence, it is necessary to add annotation	A	See Section 3		
7 JPN	2.13	2.13 states that categorization should be based on the consequences of the failure of the SSCs to perform their assigned safety functions, however, it's necessary to add the definition on the extent of failure. REASON: Clarification	A	See para 2.11		
9 FRA	2.14	Delete 2.14 REASON: Superfluous as 2.15 exists (see also comment 10)	PA	See now 2.13 (modified text) 2,15 was moved to Section 3		
16 UK	2.14 and	None of the analysed designs uses a 4-level safety			R	Russia has 4 categories and there is a

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
	elsewhere	categorisation, which is something quite new. We question the need for so many levels in that it makes sense only if sufficiently graded design requirements are defined in the industrial design codes in order to be able to assign different requirements to the corresponding safety categories. To our knowledge none of the existing industrial design codes encompasses more than three levels of design requirements, many of them only two. The designer would have to assign the safety categorised SSCs according to the safety guide approach to much less code classes, thus limiting the benefits of a sophisticated classification process.				footnote on category 4 that states, SSCs in safety functional groups assigned to safety category 4 could have a safety class non nuclear-safety or specific requirements. If sufficient analysis and understanding exists regarding an event phenomena and consequences, the safety category 3 can be assigned." (three or four classes can be acceptable)
17 UK	2.14 and elsewhere	**N.B. UK's NII feel this is an important issue to be addressed.** As per previous UK comments (submitted for the 26th NUSSC meeting in October 2008), we cannot see the benefit of having four safety categories (the UK has three, and this is only a "for example" in our national guidance). We recommend that this aspect of the guide be made an example of one way of achieving the principles herein, rather than the single recommended approach. UK (NII) recognises that Safety Guide advice is not mandatory. However, NII's policy is to follow IAEA Safety Guides and so it would prefer not to have to opt out of such a key portion of IAEA's safety advice. Is adopting four categories the accepted international approach, i.e. is the UK out of step here?			R	See response to previous comment (16UK).
10 FRA	2.15/3	At the end of 2.15 add "(see Fug. 1 in section 3).			N/A	Moved down
5 SAF	2.16	General remark, not only to 2.16 REASON: This draft describes not only the classification process. The main part is a description of the design for safety process and of the philosophy to develop a safety concept. The crucial parts of the classification process are not described sufficiently, e.g. in appendix III table 4. In 2.16 the safety classification process is restricted to design requirements. This is not acceptable. At a minimum safety classification is also the basis for the requirements in appendix III table 4 as it is stated in [3] too			R	DS 367 draft describes classification process giving recommendation to fulfill DS 414 requirements. Recommendations on design rules are in Section 4 referring to practical examples on application of design rules (listed in DS414) or available industrial standards.
7 SPA	2.16 At the end	Add: These design requirements would turn into operating, qualifying, inspecting and testing requirements, when new classifications are made in operating plants. REASON: Usually it is neither possible nor practical to change	PA	Text was deleted and used for 3.33. design rules are in DS 414 Comment was taken into account with the change in paragraphs 1.6, 3.33, 4.3	N/A	

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		the affected SSCs. It is only possible to take care and supervise more this SSC.				
11 FRA	2.16/2	Replace "that will achieve the" by "to ensure" REASON: Safety functional group expected performance governs SSC design requirement (not the reverse).			N/A	Text was deleted and used for 3.33.
ENISS 6	At the end of para. 2.16	Add: <u>These design requirements would turn into operating, qualifying, inspecting and testing requirements, when new classifications are made in operating plants.:</u> <u>Reason:</u> Usually it is neither possible nor practical to change the affected SSCs. It is only possible to take care and supervise more this SSC.			N/A	Comment was taken into account with the change in paragraph 4.3
12 FRA	2.17/2	Atter "design phases", add a footnote : "This sentence can't obviously apply for existing NPP with regard to the methodology described in this guide as their design was completed before publication of this guide". REASON: See comment 2	PA	This is taken into account with the change in the scope of application of the safety guide (paragraph 1.8) and see new 2.17		
13 JPN	2.18	2.18 The safety classification process should take the following steps: (1) identification of postulated initiating events (2) identification of plant specific safety functions to prevent or mitigate postulated initiating events based on the three fundamental safety functions; REASON: Actually, the process for preparing safety importance classification table begins with identification of postulated initiating events as a first step.	A	See Fig. 1		
6 SAF	2.18	General remark not only to 2.18 See remark to 2.16. Under (6) the classification process stops with the assignment of design requirements! There are a lot of other necessary connections to the classification process: QA, qualification…			R	Design requirements imply all requirements to manufacture test and operate the equipment). See para 4.3.
13 FRA	2.18 (3)/2	Replace "different defence in depth levels" by "each defence in depth level" REASON: To be more consistent with 2.11			N/A	Steps were modified – no Did levels Role of DID in the SG has been drastically modified

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
11 USA	2.18 / 6, 10, & 13	The classification systems accordingly identified the SSCs, mainly from experience and analysis of specific designs, that were deemed to be of the highest importance in maintaining safe operation, such as the continuing integrity of the primary pressure boundary (i.e., in pressurized light water reactors)**,** and classified this at the highest level REASON: DS 367 proposes a technology-neutral approach. Not all reactor designs rely on pressure boundaries to contain fuel and fission products.	A	See para 3.20		
18 UK	2.18 and elsewhere	There may be important safety requirements that do not derive from any of the three fundamental safety functions. This is especially true away from the reactor island, e.g. within the fuel route. However, even for the reactor, the need to provide adequate neutron shielding during normal operations lies beyond the three requirements. Analysts need to focus on these three, but not be limited in their considerations.	A	All safety functions are linked back to the three fundamental safety functions directly or indirectly See 3.9 (see also FIN 4)		
19 UK	2.18, 4th bullet	Replace “consequence” with “consequences” REASON: Correct grammar			N/A	
8 SPA	2.18.6	Add: ... of design, „operating, qualifying, testing, inspecting and maintenance“ requirements REASON: This change applies to the SSCs of operating plants. For those item it is valid the same reason as for the last comment.	A	See para 4.3		
ENISS 7	2.18.	(6) assignment of design <u>operating, qualifying, testing, inspecting and maintenance</u> requirements to the SSCs based upon their classification. *Reason* *This change applies to the SSCs of operating plants. For those item it is valid the same reason as for the last comment*	A	See para 4.3		
ENISS 8	2.17 – 2.20	Move behind 3.1 *Reason:* *Given the subtitle of these para they are falling under the section 3*	PA	Para 2.20 of ver 5.1 was moved behind 3.1		
ENISS 9	2.19	Safety classification may be an iterative process during the design process. Any preliminary safety class assignments should be finalized using deterministic safety analysis and, where ~~available~~ <u>possible</u>, probabilistic safety analysis.	A	See para 2.16		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		Reason: *Use of PSA is state of the art and could be helpful, but they are generally not used and qualified for classification and most of them are not suitable for this purpose.*				
20 UK	2.19	Although there is agreement with the sentiment, the advice here appears to run counter to that in Para 2.4, which places deterministic analysis first, rather than engineering judgement.			R	2.4 is in an agreement with 2.19 of ver 5.1. (new 2.16) Deterministic analysis is primary and PSA is secondary. Engineering judgment is used for verification f it is necessary see 3.34.
9 SPA	2.19 last line	Change: ...“and, where available“... to: ... „and, where possible“ REASON: PSAs at this phase of project are generally not so defined and refined to allow classify SSC’s.	A	See para 2.16		
10 SPA	2.20	See comment 2			N/A	The scope of applicability of the safety guide has been changed
14 FRA	2.20/2	Delete “to the safety functions” REASON: Changes may be on the function categorization or SSC classification…			N/A	
ENISS 10	2.20	~~During the plant periodic safety reviews and before modifications, this safety classification method should be applied to determine if there are any changes to the safety functions to be performed.~~ *Reason:* *See comment 1 & 2*	A			
		Section 3				
13 USA	3	This section should emphasize that, for each SSC, the classification basis and not just the results should be well documented and in an auditable record.	A	See para 2.15		
18 SPA	3 - Add a new point in section	Some SSCs which failure can cause unacceptable consequences (such as economical, environmental or working impact), can be considered as a highest security class with the correspondent requirements REASON: This possibility should be opened			R	This is a safety guide, not a guide to worker protection, security, or economics.
20 USA	3 / Table 1,	Table 1 lists high, medium and low severity levels of		.	R	See Fig 1 and para 3.2

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		consequence of failure of the safety functional group to perform its plant specific safety functions REASON: How can severity levels be determined without knowing the PIEs during which the safety functions must be performed?				
15 FRA	3.1	Delete "The safety classification process should ultimately establish design requirements for all SSCs to achieve appropriate performance of safety functional groups." REASON: Duplicate 2.16	A			
7 SAF	3.1	Safety classification is only a part of the design for safety process, the functional analysis and the safety assessment See remarks to 2.16 and 2.18. There are other Safety Standards responsible for the design [1] and the assessment (3)			N/A	
11 SPA	3.1 last sentence	Idem comment 9			N/A	
12 SPA	3.2 2nd sentence	Change: ..."specific nuclear power plant" ... to „specific design" and ... a „list of plant".. to ..."a preliminary list" REASON: All power plants with the same design have the same systems. Consequently the list of plant specific safety functions will be very similar for all of them.			N/A	
24 UK	3.2	What are "associated supporting functions"? This bit could be clearer.	PA	Example is in Annex I		
23 UK	3.2 and elsewhere	The fundamental safety functions are not so much "broken down" as synthesised into more specific design requirements, e.g. removal of heat becomes provide a feed flowrate of at least X. The use of the phrase "broken down" sends out the wrong messages. Consider rewording.	A	OK, included in the updated version		
21 UK	3.2, 1st sentence	Delete "also" to read: "….based on the fundamental safety functions should be defined during ……." REASON: The use of "also" is inappropriate in the first sentence of a new paragraph.			N/A	

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
22 UK	3.2, 2nd sentence	Modify to read: "For an existing nuclear power plant, a list of plant specific safety functions may already be in place." REASON: For clarity			N/A	The paragraph has been rephrased and there is a desire to avoid reference to existing plants because of the change in the scope of application of the safety guide. To be discussed (since now the SG may be better applicable to existing NPPs)
ENISS 11	Heading for 3.2-3.5	IDENTIFICATION OF SAFETY FUNCTIONS ~~TO PREVENT OR MITIGATE POSTULATED INITIATING EVENTS~~ ~~Reason:~~ For Clarification Focus of these paragraphs lie on the derivation of Plant and SSC Safety Function. The paragraphs 3.2-3.5 should be rewritten considering that the allocation of DiD level is described in 3.6 following.	PA	IDENTIFICATION OF PLANT SPECIFIC SAFETY FUNCTIONS		
ENISS 12 ENISS 13	3.2	A complete set of plant specific safety functions based on the fundamental safety functions should ~~also~~ be defined during the initial design phase for a new nuclear power plant. For ~~a specific~~ an existing nuclear power plant, a list of plant specific safety functions may already exist. … *Reason:* *For clarification*	PA	Text was modified		
ENISS 14	3.2	… If such a list does not exist, the fundamental safety functions should be broken down into plant specific safety functions and associated supporting functions ~~for each defence in depth level.~~ *Reason* *Allocation of DiD level is misplaced here and will described in 3.6 following.*			N/A	Text was modified
ENISS 15	3.3	The plant specific safety functions ~~applied to safety functional groups~~ will prevent or mitigate the postulated initiating events that have been identified and should be broken down as required into SSC level safety functions ~~associated with each defence in depth level.~~ *Reason:* *For clarification.*			N/A	Text was rapidly changed. No DiD level! See response to Belg. 1 comment

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		Allocation to DiD level and assigning of Safety Functional group will be described later. ~~For each defence in depth level, the~~ The fundamental safety functions should be broken down into a consistent group of plant specific safety functions considering the allocation to the defence in depth level (see 3.6 following). ~~(e.g. reactivity control may be broken down into a) preventing unacceptable reactivity transients, as defence in depth level 1 function and b) shutting down the reactor, c) maintaining the reactor in safe shutdown condition, both as defence in depth levels 2 and 3 functions).~~ Acceptance criteria for the performance of plant level safety functions should be defined at each defence in depth level. *Reason:* *Belongs to Allocation of PSF to DID level → transfer sentence to 3.6 following* These are refined during the design process to establish a complete set of safety functions and postulated initiating events. *Reason:* *Relation of PSF and PIE should be stated.*				
16 FRA	3.3	Replace "The plant specific safety functions applied to safety functional groups will prevent or mitigate the postulated initiating events that have been identified and should be broken down as required into SSC level safety functions associated with each defence in depth level." By "Each plant specific safety functions should be allocated a defence in depth level (see paragraph 3.6 and following), depending on its role to prevent or mitigate the PIE that have been identified. Each plant specific safety functions should also be broken down as required into SSC level safety functions associated with each defence in depth level." REASON: The first sentence of 3.3 is confusing and doesn't seem consistent with appendix II flowchart. An alternate wording is proposed but may not capture the whole proposed process….			N/A	Text was changed. No DiD level! See response to Belg. 1 comment
2 INS	3.3	3.3 fuction and b) ***controlling and*** shutting down the reactor,			N/A	Text was changed.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		REASON: Control action should be conducted firstly to guide variables to reach the setting point value. But if the abnormality can not be controlled again, then the plant should be shutted down in a safe manner.				No DiD level! See response to Belg. 1 comment
25 UK	3.3	New terms have been introduced here! Are "SSC level safety functions" (1st sentence) and "plant level safety functions" (3rd sentence) the same as "plant specific safety functions" as defined in Para 2.8.	A	"plant level safety functions" are used		
ENISS 16	3.4	For an existing plant the design should be reviewed periodically <u>as necessary and</u> <u>in case of an event</u> to ensure that the postulated initiating events and <u>the related</u> ~~a sufficient list of~~ plant specific safety functions to deal with them are appropriately defined. *Reason:* *For clarification*	PA	See para 3.3		
13 SPA	3.4 1st line	Add: ... periodically", as necessary," to ensure... REASON; See reasons fpr comment 1 and 2			N/A	
ENISS 17	3.5	For plant modifications, ~~the sub-set of newly identified or modified~~ <u>the affected</u> plant specific safety functions should be assessed <u>and if required modified</u>, taking into consideration the affected interfaces with existing safety functional groups. *Reason:* *For clarification … present wording implements, that a modifications leeds automatically to a "sub-set of newly identified or modified PSF.*	A	See para 3.3		
17 FRA	3.6/3	Delete ",so that the relevant success criteria can be achieved" REASON: Superfluous. Achievement of the success criteria may happen without classification….	A	See para 3.6		
Belg. 4	3.7&3.21	Revise the statements: § 3.7 "DiD level 1 safety functions should be provided to keep the plant within the normal operational envelope, by preventing failures" and § 3.21 "Safety functional groups that only prevent the occurrence of an abnormal event should be assigned to DiD level 1".			N/A	See para 3.8

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		REASON: Those phrases mix elements of DiD Level 1 and Level 2, as defined in INSAG-10. Level 1 objective is "Prevention of abnormal operation and failures", while Level 2 objective is "Control of abnormal operation and detection of failures" Essential means are respectively: o Level1: Conservative design and high quality in construction and operation o Level 2: Control, limitation and protection systems and other surveillance features. The function of "keeping the plant….", which refers to the main regulation systems (control of temperature, pressure etc) belongs thus to Level 2!. Also, the concepts of "Conservative design" and "High quality" are not, for us safety functions but attributes.				
18 FRA	3.7/2	Delete "by preventing failures" REASON: Failures are not the only challenges to normal operation scope	A	See para 3.8		
3 INS	3.7	3.7 the normal operational envelope, by preventing ***abnormal operation and*** failures. REASON: Defence in depth level 1 coveres abnormal operation and failures.	A	See para 3.8		
26 UK	3.7 and subsequent paras	"Defence in depth level N safety functions" should presumably be "Defence in depth level N plant specific safety functions"? Clarification needed.			N/A	Reference made to DID levels has been changed in the document.
14 USA	3.7 through 3.16	Indicate, in the definitions of the defense in depth levels, whether the safety functions must be automatically actuated and controlled or may be manually actuated and controlled. REASON: Design requirements for systems that must respond automatically would differ from design requirements for systems that are intended to be used manually. Requiring all safety functions, through DiD Level 3A, to be automatically actuated would be consistent with current practice in the US. One possible approach would be to specify that consequences of Safety Category 1 require automatically actuated safety	A	See para 3.13	N/A	Reference made to DID levels has been changed in the document.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		functions (see Table 1).				
4 INS	3.8	3.8 return the plant to normal operational conditions as promptly as possible ***without any unconvenient overshoot occured,*** following an anticipated REASON: Performance of the automatric control should be considered in the time variable (setting time) and overshoot constraint			N/A	
15 USA	3.8 / 1-3	"Defense in depth level 2 safety functions are mitigatory safety functions and should detect, control and recover from ~~failures that occur during~~ anticipated operational occurrences." REASON: Anticipated operational occurrences are relatively frequent (or anticipated) equipment failures or operator errors that require operation of a safety function, like a reactor scram. If defense in depth level 2 safety functions are not designed to deal with failures that occur in addition to the AOOs, then "**failures that occur during"** should be deleted. Consider that a common cause failure, occurring during an AOO, would likely produce an ATWS, which could not be mitigated by defense in depth level 2 safety functions.	PA	See para 3.11		
16 USA	3.8 / 3-6	"The assignment of these defense in depth level 2 safety functions should be to **return the plant to normal operational conditions as promptly as possible, following an anticipated operational occurrence, before the occurrence** can progress to a design basis accident (DBA) or a beyond design basis accident (BDBA)." *Clarify whether the defense in depth level 2 safety functions should be designed to demand or to avoid a reactor trip, in response to an anticipated operational occurrence.* REASON: An anticipated operation occurrence often requires a reactor trip. If the reactor is tripped, it would be necessary for the operator to restart the reactor; but only after diagnosing and correcting the fault. Would DiD Level 2 functions include actions like partial reactor trips or turbine runbacks?			N/A	Sentence was deleted
17 USA	3.8 / 3-6	"The assignment of these defense in depth level 2 safety functions should be to return the plant to normal operational	A	See 3.11		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		conditions as promptly as possible, following an anticipated operational occurrence, **before the occurrence can progress to a design basis accident (DBA) or a beyond design basis accident (BDBA).”** REASON: In the US, this is considered a plant design requirement, not a safety function requirement. The plant is designed such that an anticipated operational occurrence would not be capable of progressing to a more serious accident, unless another fault occurs independently. If an anticipated operational occurrence is capable of progressing to a more serious accident, then the defense in depth level 2 function is expected to recognize the situation and perform specific operations to prevent the progression. It is a formidable design requirement for a PSF.				
19 FRA	3.8/2	Delete “from failures that occur during” REASON: Superfluous. See comment 18	A	See para 3.11		
17 SPA	3.9	Add at the end: „Special attention should be paid to the fall of non Security Class or non Seismic Category 1 items, on Classified ones, when a postulated seism occur REASON: In power plants there are a lot of heavy non significant for safety SSCs whose fall, can damage important ones			R	The issue identified here is addressed in paragraph 3.31
ENISS 18	3.9	Add at the end: “ Special attention should be paid to the fall of non safety class or non Seismic Category 1 items, on Classified ones, when a postulated seism occur *Reason:* *In power plants there are a lot of heavy non significant for safety SSCs whose fall, can damage important ones*	A	In other para		
ENISS 19	3.10	Defence in depth level 3A safety functions should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible, ~~preferably using automatic means~~ principally not manually, and is reached once the fundamental safety functions are restored. *Reason:* *The wording would demand automatic systems and discriminate passive safety equipment – so wording should be changed as suggested.*	A	See 3.13 and DS 414		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
20 FRA	3.10	Transform 3.10 in a bullet within 3.9			R	Although using bullets to make all items under DiD level 3 makes some sense, it makes it harder for the user to reference a paragraph.
18 USA	3.10 / 1-4	"Defense in depth level 3A safety functions should establish a controlled state following a design basis accident. A controlled state should be reached as soon as possible, preferably using automatic means, and is reached once the fundamental safety functions are restored." *Give examples of "controlled" states, and "as soon as possible". Provide guidelines to determine when automatic means must be used.* REASON: Design basis accidents are used to set the requirements for safety functions, especially mitigatory safety functions, such as means of actuation, setpoints, time response, duration, and objective (i.e., end) state. Design requirements for automatic systems are harder to meet than those for manual systems.	PA	See para 3.13 Definations in DS 414		
27 UK	3.10, 3.11, 3.13, 3.14, 3.15	Suggest these paragraphs are deleted, and the DiD-concept as described in INSAG 10 and NS-R-1 is used instead. REASON: The splitting of the DiD-concept for the Level 3 and 4 into a Level 3A/3B and 4A/4B is not recognised in the IAEA classification process (see INSAG-10, NS-R-1). A reason for this splitting cannot be seen from a safety or classification point of view; nor is a reason given in the draft.	PA	Paras (3.13-3.16 of ver 5.1) were deleted 3A/3B was kept		
21 FRA	3.11	- A clear definition of Controlled sate and safe shutdown state is needed REASON: Quality/clarity	PA	DS 414 OK		
22 FRA	3.11	Transform 3.11 in a bullet within 3.9			R	Although using bullets to make all items under DiD level 3 makes some sense, it makes it harder for the user to reference a paragraph.
28 UK	3.11, 1st bullet (a)	Replace "or" with "and/or"	PA	No or, or/and		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		REASON: Reword as suggested since designers are likely to want to achieve both (a) and (b)				
8 SAF	3.12	No proposal Defence ion depth level 4 safety functions are preventive and mitigatory safety functions and should…. "…control of…" – typo – delete of This is an example for the consequences of the remarks to 2.11!			R	mitigatory safety functions
29 UK	3.12, 1st sentence	Delete "of" to read: "… and should control severe plant conditions, …" REASON: Correct typo			N/A	Editorial changes in para 3.15
23 FRA	3.13	Transform 3.13 in a bullet within 3.12			N/A	deleted
24 FRA	3.14	Compile 3.14 with 3.13		.	N/A	deleted
25 FRA	3.15	Transform 3.15 in a bullet within 3.12			N/A	deleted
30 UK	3.15	Replace "excursion" with "excursions" and insert "for" to read: "… controlling further reactivity excursions, removing decay heat for as long as required and …" REASON: Correct typos			N/A	deleted
26 FRA	3.16/last sentence	Does this sentence concern on-site equipment ?			N/A	deleted
27 FRA	3.17	Delete 3.17 REASON: Superfluous. Furthermore, issues not related to radioactive release (i.e. chemical discharges, worker radiation safety….) may also warrant a classification that, by ease, may be included in the safety classification			N/A	deleted
31 UK	3.17	Replace "classified" with "categorised" to read: "…should be categorised as non-safety." REASON: For consistency			N/A	deleted
9 SAF	3.18	No proposal It may be helpful to 'categorize' "Safety function l groups", rather than to safety Classify them as an step towards SSC classification, but the attempt to integrate the likehood of the function being required as a 'composite' categorization is not clear and leads to confusion later in the document (3.27, tables 1 & 2). PBMR experience has shown that it is unwise and unnecessary the system for deriving relative importance to			N/A	Traditional means of safety classification inherently take into account likelihood by classifying based on pressure retaining components and protection of the three barriers. DS 367 provides a systematic approach to categorization of safety functions and thus to classification

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		safety. It is better to use a clear and concise system of classification that can then be interpreted (in a necessarily more complex set of arguments related to that safety class) as appropriate safety requirements (Q&SM), capability, reliability, robustness etc.) based on the nature of the function (preventive mitigation), the nature of the design solution (hardware, software) and the design loads of related PIE				
32 UK	3.18	This paragraph does not make logical sense. The third sentence does not derive from the second. This all needs re-phrasing.			N/A	
19 USA	3.18 / 1-6	"Safety functional groups should be categorized primarily according to their safety significance based on the consequences of their failure. The relation of the safety function to defense in depth level reflects the likelihood of the safety functional group being called upon to operate. This should result in "highest" categorization on the safety functional groups where there are potentially the most severe consequences if they fail and which are most likely to be called upon to operate." REASON: The likelihood that a safety functional group will be called upon to operate is conditional to the likelihood of the occurrence of a PIE. This requires assumptions or PSA results. It does not address likely PIEs with minor consequences vs rare PIEs with major consequences.			N/A	Table 1 reflects both consequence and likelihood, but to avoid confusion, the order of the sentences in 3.18 has been changed. The reference made to DID levels has been drastically modified
33 UK	3.18, 3rd sentence	Modify to read: "This should result in the "highest" categorisation being applied to the safety functional groups giving rise potentially to the most severe consequences if they fail, taking into account the likelihood of their being called upon to operate." REASON: For clarity		.	N/A	Paragraph 3.18 has reversed the order of the second and third sentences for clarity. Combining these two sentences may make communication less clear
28 FRA	3.18/2	Delete "The relation of the safety function to defence in depth level reflects the likelihood of the safety functional group being called upon to operate." REASON: Superfluous as the concept is already stated in the last sentence of 3.18			N/A	the paragraph has been changed
34 UK	3.19	Consider adding the following: "Elements of one safety functional group might also be members of other safety functional groups, so that a single SSC			N/A	Last sentence of 3.22

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		might have more than one safety function." REASON: For completeness				
29 FRA	3.19/1	Why limiting to a single safety functional group the achievement of a plant specific safety function ?			N/A	Last sentence of 3.22
ENISS 20	3.19	This para should be clarified because it seems in contradiction with the definition for Safety Functional Groups into 2.12 especially the emphasis of "single" safety functional group.			N/A	Last sentence of 3.22
ENISS 21	3.20	Each safety functional group should contain all the necessary design features to achieve the <u>needed</u> ~~desired~~ capability, dependability and robustness. *It should not be demanded what is desired, but what is needed.*			N/A	See para 3.23
ENISS 22	3.18 – 3.22 and 3.27 - 3.29	These paragraphs (this subchapter as the core of this guide) are diffuse and need more clarification, e.g. - on the relation between Plant, Safety Functional Group and SSC to Plant/SSC safety function, DiD level, Level of consequences of failure and their influence on the allocation of the Safety Categories, definition on Safety Categories 2-4,	PA	Paragraphs were modified N/A		
15 SPA	3.20 last line	Change: ..."the desired"... to: ... „the needed" REASON: Those characteristics are necessary, not a desire			N/A	See para 3.23
14 SPA	3.20, 3.29, 3.30	Idem comment 9			N/A	Paras were changed
8 CAN	3.21	In point 3.21 is not clear what an acceptable risk means (safety goal?)?	PA	para was deleted see para 3.8		
10 SAF	3.21	No proposal See comments on 2.11 (prevention Vs mitigation) & 2.12 (DID levels of Safety Functional Groups). This para appears to be restricted to DID level 1 as a design activity			N/A	
35 UK	3.21, 2nd sentence	The purpose of this final sentence is unclear.	PA	para was deleted see para 3.8OK see also 8 CAN		
30 FRA	3.21/2	Replace "to where the radiological consequences associated with this failure provide an acceptable risk" by "and occurrence of AOO".			N/A	para was deleted see para 3.8
11 SAF	3.22	No proposal See comment on 2.11 (prevention VS mitigation) & 2.12 (DID			N/A	para was deleted see para 3.10

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		level of Safety Functional Groups). This para seems in any case to be contradictory to para 2.12				
36 UK	3.22, 4th sentence	Please look for a better phrase than "enveloping safety functional group"			N/A	para was deleted see para 3.10
31 FRA	3.23	Add "This categorization of consequences in three levels is made assuming that subsequent DiD levels respond as designed" REASON: Quality/clarity		C Sentence added but not the "three levels" OK, DID approach drastically modified in updated version		
16 JPN	3.23	"The severity level of consequence of failure of the safety functional group to perform its plant specific safety functions should be divided into consequence levels such as the high, medium and low." → It is difficult to determine how large degree of failure of the safety functional group is postulated for evaluation. There could be some contradiction between 3.8 and 3.24 as described in right column "Reason". REASON: 3.8 describes that events of DiD level 2 safety functions should recover from failures that occur during (AOO) anticipated operational occurrences. However, according to Table 1, the safety category 1 of DiD level 2 corresponds to high severity level which permits larger radiological releases than AOO (see 3.24).	PA	See para 3.17		
32 FRA	3.24	"operational limits " a clear definition is missing REASON: Quality/clarity	A	See para 3.17		
33 FRA	3.24	Transfer 3.24 in a bullet within 3.23	A	See para 3.17		
12 SAF	3.24	No proposal The para, consisting of a single sentence, is too long to be clear. It appears to be inconsistent with earlier restrictions placed on 'prevention' functions. It is assumed to refer to DBA	A	See para 3.17		
34 FRA	3.25	Definition of normal operation limit is missing: doest it include releases in case of AOOs? REASON: Quality/clarity	A	See para 3.17		Clarified
35 FRA	3.25	Transfer 3.25 in a bullet within 3.23	A	See para 3.17		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
36 FRA	3.26	Transfer 3.26 in a bullet within 3.23	A	See para 3.17		
39 FRA	3.26	What about other adverse consequences on the environment (for example large chemical release) or for workers (over-exposure to radiations)?	A	See para 3.17 last bullet		Operational limits
6 INS	3.26	**Add new Para 3.26.a.**: "The level of consequence should be considered "very low" if the consequence are radiological releases far below the normal operational limits." REASON: This new Para is a proposed acceptance criteria applies to Safety Category 4 of Safety Functional Groups.			R	See para 3.17 The paragraph has been clarified for "low." This will be clarified in the redraft with a figure that details a negligible zone where consequences are below Technical Specification
37 FRA	3.26/2	Delete "close to"	A	See para 3.17		
38 FRA	3.26/2	Delete "This reflects the uncertainty that may exist in the safety analysis or other parameters associated with plant operation."	A	See para 3.17		
8 JPN	3.27 Table 1	It's necessary to add the reason how Safety Categorization is evaluated in Table 1. It's might be defined followings; (1) SSCs categorized in same Safety Categorization level should have the equivalent indication values. Such indication should be defined. (2) Indication which shows the boundary between each Categorization should be defined. (3) Above mentioned indications, values should be equivalent among different type of reactors. REASON: Safety Category 4 is expected to function under BDBA and Severe Accident condition to be mitigated.			N/A	Table 1 has been Changed. See the new Table 1.
13 SAF	3.27 Tables 1&2	No proposal There appear to be several errors Failure of DID level 1 functional groups cannot by definition (3.7) lead to "high" or "medium" safety consequences. Equally, failure of DID level 21 functional groups cannot by definition (3.8) lead to "high" safety consequences			N/A	Table 1 has been Changed. See the new Table 1.
Belg. 5	§3.28 Table 1	The Safety Guide proposal in Table 1 "Relationship between Safety Function Type and Safety Categories of Safety Functional Groups" is not practical for DiD Level 1, and difficult to apply in practice. REASON:			N/A	Table 1 has been Changed. See the new Table 1. and para 3.21.

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		How are the severity levels of consequences of failure of the functional group supposed to be determined? Those consequences depend on the behaviour of all the remaining limes of defence, with thus a wide range of « potential consequences ». We can take the PWR protection system as a test case. Classically, it receives the highest safety class within the I&C. For INSAG-10, it belongs to Level 3, level 3A in this guide. Table 1 gives a choice from Safety Category 1 to 3. Assuming a failure, we are in the ATWs situation, whose consequences depend on the existence or not of mitigation functions. If those exist (and work well!) the potential consequences are clearly «Low». Does it mean that the protection system might be Safety Category 3?				
37 UK	3.28	Consider re-ordering the paragraphs so that Para 3.28 precedes Para 3.27. REASON: Logically, Para 3.28 should precede 3.27.			N/A	3.28 was deleted
43 FRA	3.29	Replace “Design measures should be applied consistently within a safety category or using a graded approach for the different safety categories or safety classes. This is considered further in Section 4.” by “Design measures should : - be applied consistently within a safety category ; - rely on a graded approach for the different safety categories or safety classes. This is considered further in Section 4.” REASON: Alternate wording	PA	See para 3.23		
5 INS	3.29	3.29 requirements can be identified that the appropriate quality, availability, and reliability is achieved. REASON: Besides quality and reliability, availability of SSC is important to be required.	PA	See Section 4		
14 SAF	3.29	No proposal It is not clear how the “safety categorization” proposed can assist in assigning a “set of common design requirements” This	PA	Paragraph has been rewritten to clarify that categorization assigns safety classes which in turn assigns design requirements		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		process is in fact quite complex and dependant on Safety Classification (see comment on 3.18)		Description of Safety Categorization and Safety Classification have been improved in the updated version		
44 FRA	3.30	Delete "This analysis should also provide a preliminary estimation of the plant behaviour and of the required systems performances." REASON: Out of the scope of the guide.	PA	Deleted, see Appendix II		
21 USA	3.30 / 1	"A deterministic or probabilistic safety analysis should be performed that will cover all postulated" REASON: A probabilistic safety analysis should be performed in addition to the deterministic analysis as part of the classification process. The standard recognizes this requirement in certain other portions of the standard.	PA	See 3.2 and 3.26		
16 SPA	3.31 2nd sentence	Add: The „main" purpose... REASON: The PSA provides much more information, even in this preliminary stage like design of enough redundancies, discover of hidden dependencies...			N/A	Deleted, see Appendix II
ENISS 23	3.31 2nd sentence	The main purpose of this preliminary PSA is to identify potential additional initiating events (multiple failures, losses of support functions, etc.) and the required safety functions. *Reason:* *The PSA provides much more information, even in this preliminary stage like design of enough redundancies, discover of hidden dependencies…*			N/A	Deleted, see Appendix II See 3.2 and 3.26
ENISS 24	3.32 following	The connection of this step in the process to its predecessor is not described (especially Safety Functional Group to SSC and Transition Safety Category to Safety Class)			N/A	See para 3.25
7 INS	3.32	**Change text of this Para to (for example) :** "Safety Class 1 should be assigned to the SSCs whose failure could cause a loss of reactor coolant in excess of the reactor coolant normal make up capability." **Add new Para 3.32.a:** "Safety Class 2 should be assigned to reactor containment, to those components in the reactor coolant pressure boundary not in Safety Class 1, and to those components of safety system that are necessary to: 1) remove heat directly from the reactor or reactor containment, 2)			N/A	See para 3.25 This safety guide proposes a technology neutral approach based on a combination of consequences and likelihood of the SSC failure for each bounding PIE. See updated version

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		circulate reactor coolant for any safety system purpose, 3) control radioactivity released within the reactor containment, 4) control hydrogen in the reactor containment, 5) introduce emergency negative reactivity to make the reactor subcritical or restrict the addition of positive reactivity, or 6) provide or maintain sufficient reactor coolant inventory for emergency core cooling. **Add new Para 3.32.b** : "Safety Class 3 should be assigned to those components not in Safety Class 1 or 2 and 1) the failure of which would result in release to the environment or radioactive gases normally required to be held for decay, or 2) that are necessary to provide or support a safety system function, control airbone radioactivity released outside the reactor containment in an accident, provide or maintain sufficient reactor coolant inventory for core cooling." REASON: This new Para is a proposed acceptance criteria applies to Safety Category 4 of Safety Functional Groups.				
46 FRA	3.34	Definition of important items is missing: Definitions of auxiliary, supporting and services functions are needed REASON Quality/clarity	A	See 3.28 and footnote 15 Definition is in DS 414		
14 JPN	3.34	(1) (An omission) This may be, for example, a small instrumentation line or (An omission). “A small instrumentation line” ? or “small instrumentation lines” ? REASON: The condition of down grade could be changed if the sentence concerned is a singular or plural form.	PA	See para 3.26 The ability is needed to downgrade SSC classification based on criteria that allow the plant specific safety functions to be met by the SFG.		
15 SAF	3.34	No proposal Downgrading a safety classification seems fundamentally incorrect unless the design itself and the safety function/DID changes). Associated Quality and Reliability (I cannot read more)			N/A	See para 3.26
44 UK	3.34	These would seem to be examples rather than a complete list of all possibilities. Consider rewording for clarity.	PA	See para 3.26		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
45 UK	3.34, 2nd bullet (2)	For clarity, mention dependent failures.			N/A	See new para 3.26
43 UK	3.34, 3.47 and Annex II	The figure in Annex II is intractable and needs further explanation.	PA	Annex II of ver 5.1 was deleted		
46 UK	3.34, 3rd bullet (3)	Further guidance is needed here to prevent all SSCs providing diversity being downgraded. At least one SSC needs to be retained at the higher class.			N/A	See para 3.26 bullet 3 was deleted
47 FRA	3.35	Fig 1. might be updated to also include potential for upgrading with specific additional requirements	A	See Fig 2		
15 JPN	3.35	If there are SSCs within certain safety functional groups that cannot be accepted to fail (e.g. reactor pressure vessel for pressurized light water reactors), then these SSCs should be allocated to the highest safety class (Class 1), and additional requirements specified on a case by case basis. → (Class 1) should be deleted. REASON: This word could mislead that only the reactor pressure vessel is assigned to Class 1.	A	See para 3.27.		
16 SAF	3.35	… reactors), then to the requirements of the highest safety class (class 1) additional requirements should be specified on a case by case basis		Not clear the comment See para 3.27		
22 USA	3.35 and General Comment	Distinction between safety category and safety class is not clearly defined in the document and the two terms seem to be used inter-changeably.	PA	See 3.27 There is no confusion in because SSCs are classified.		
Belg. 6	§3.35	Delete “within certain functional groups” REASON: The SSCs that can’t be accepted to fail do not belong to a safety functional group but to exclude PIEs (cfr general comment above).			R	See para 3.27
23 USA	3.37 / 1-3	“No account should be taken of whether a safety functional group contains active or passive SSCs, or a mixture of them, as this has neither effect on the safety category of the group nor on the safety class of the SSCs.” *Explain why this has no effect.* REASON: DS 367 does not take into account the frequency of			R	See para 3.30 I would reject the comment, Active and passive systems should be treated at the same level. In addition passive systems are not always able to be tested., so how is it possible to ensure that they would operate at any time and to make any differences

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		failures, except in the PSA. Active SSCs are more likely to fail than passive SSCs; but they are not given more attention in the classification.				between active and passive
47 UK	3.38	Re-phrase this to ensure the meaning of the paragraph is clear.		C Edited Do we have any example? If there is any impact on the safety Functional Group, it should be part of it except if we have example.. See also 3.39		
ENISS 25	3.39	…An exception is where the failure of the SSC with the lower safety class ~~(including a potential common cause failure of identical or redundant items)~~ cannot prevent accomplishment of the safety functions of the SSC with the higher safety class. Reason: Naming of CCF does not make sense, as this para deals with interconnection of SSCs with different classification.	PA	See para 3.31		
ENISS 26	3.40	Move to the front of Chapter 3 (Process overview).	PA	deleted		
48 UK	3.39	The logic here needs to be that no mechanism has been identified that can propagate the failure.	A	Edited See 3.32		
12 JPN	3.42 3.44	3.42 should be deleted. 3.44 If there are deviations between the PSA results and the deterministic based safety classification of an item then the most conservative safety classification (higher safety class) should be used before sufficient experience on use of PSA is accumulated. REASON: Utilization of PSA in these sentences is too limited.	A	after it is suggested that PSA may lead to lowr classification		
24 USA	3.42 / 1-2	We recommend removing this paragraph in its entirety. REASON: Probabilistic methods should be used in all cases.	A	Deleted		
49 UK	3.44	PSA is not covered particularly well in this guide, so it is difficult to know how to implement this paragraph.	PA	deleted		
48 FRA	3.45	Delete 3.45 REASON: Out of the scope of the guide. The balance of a design is not related to SSC classification.			R	See para 3.36 (was modified)
50 UK	3.45	Delete “the” to read:			N/A	Para was edited

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		"… and the SSCs allocated to the group have adequate design requirements and ……" REASON: Correct typo				
49 FRA	3.46	Delete 3.46 REASON: Out of the scope of the guide. Furthermore, the design of a NPP and making a conclusion on its acceptability is not limited to accident prevention and management (environmental impact, radiation safety during normal operation….)	A	Deleted		
50 FRA	3.47	Delete 3.47 REASON: Balance is not expected as the most stringent class has to be kept (see 3.44)	A	Deleted		
25 USA	3.47 / 3-4	Add a paragraph of explanation to describe the approach to combine the deterministic and probabilistic approaches. REASON: Annex II, Figure II-1 does not explain the process very well.			R	See 3.24 Annex II, Figure II-1 was deleted
26 USA	3.47 / 4	*Add paragraph.* "probabilistic methods could be obtained. <u>3.48 Potential common cause interactions should be considered in verifying the safety classification of plant SSCs.</u>" REASON: The safety classification of plant SSCs might be impacted by potential common cause interactions between multiple SSCs.	A	Footnote to 3.34		
51 UK	3.47, 1st sentence	Insert "a" to read: "Ideally, the final goal should be to obtain a balance between….." REASON: Correct typo			N/A	deleted
		Section 4				
27 USA	4	This section should clarify that where existing standards and codes are not adequate, they are to be supplemented as necessary to achieve a quality product in keeping with the required safety function.				R The determination of insufficient codes or standards and the replacement if necessary of the codes

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
						or standards is a national regulatory prerogative
24 SPA	4. Add a new point	Add: These requirements in some cases, can be higher than the requirements of other SSCs of the same security class REASON: Some of them were not previously defined. That can cause confusion.				R The determination of insufficient codes or standards and the replacement if necessary of the codes or standards is a national regulatory prerogative
19 SPA	4.1 2nd sentence	Add: nationally „OR INTERNATIONALLY“ adopted... REASON: International standards should be applied when not national standards are available	PA	See in para 4.2 editorial changes as well		
51 FRA	4.1/3	Replace “applied” by “taken into account” REASON: Such codes may not be nuclear specific. They may not be sufficient…	PA	The requested change implies the use of the codes and standards are voluntary. See in para 4.2 editorial changes as well		
ENISS 27	4.1	4.1 Selection of applicable design requirements is intended to reflect the required quality commensurate with safety function of the SSC. Nationally or internationally adopted codes and standards should be applied for design requirements. *Reason:* *Where National standards are not available also international standards should be applied*	PA	See in para 4.2 editorial changes as well		
52 FRA	4.2	The sentence mixing likelihood of operation and magnitude of consequence is ambiguous.	PA	Deleted but see in para 4.2 editorial changes as well		
20 SPA	4.2	Idem comment 9	PA	Deleted but see in para 4.2 editorial changes as well		
52 UK	4.3	Replace “may be” with “should be” to read: “The requirements for individual SSCs should be consistent with the entire safety functional group(s) to which it belongs.” REASON: This is not an optional design requirement.	PA	Paragraph deleted as confusing.		
21 SPA	4.3	Change: „May be“ for „shold be“ REASON: It is not a possibility. All the individualSSCs of a safety functional group have to have coherent requirements.	PA	Paragraph deleted as confusing.		
53 FRA	4.3/1	Replace “may” by “should”	PA	Paragraph deleted as confusing.		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
ENISS 28	4.3	The requirements for individual SSCs ~~may be~~ should be consistent with the entire safety functional group(s) to which it belongs. *Reason:* *It is not a possibility. All the individual SSCs of a safety functional group have to have coherent requirements.*	PA	Paragraph deleted as confusing.		
ENISS 29	4.4(2)	(2) Ensure that failures within the safety functional group cannot degrade the ability of the group to perform its designated safety function (dependability), *Reason:* *Because of the lack of definition of safety functional group the exact meaning of this sentence is difficult to understand.*			R	Editorial changes, See also Annex II
17 SAF	4.4	**Adequate reliability:** 'On-demand capability', or the probability that a Safety Group or component within a system will meet its minimum performance requirements when called upon to do so and 'Continuous Capability, or the amount of time during which a Safety Group or component will continue to be capable of performing its intended purpose (i.e. resistance to random failure) **Adequate Robustness:** 'Environmental capability' or capability under specified harsh environmental and seismic conditions (i.e. in order to prevent consequential failures resulting from an initiating event The use of "Capability" and "dependability" as proposed is no grammatically appropriate. Capability is an overall quantitative term related to capacity and requires context, as proposed in adjacent column. Dependability is an overall qualitative term, which may be thought of as the "trustworthiness" of a system, and is derived from the implementation of adequate technical requirements (specified to achieve "capability) within a suitable Quality & Safety Management programme.			R	Editorial changes, See also Annex II
28 USA	4.4 / 7-8	"(2) Ensure that failures within the safety functional group cannot degrade the ability of the group to perform its designated safety function" *This is analogous to the American single failure criterion, which is applied to automatic protection systems. DS 367 does not specify which requirements are to be applied to which*			R	Editorial changes, See Annex II

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		safety category. REASON: Safety categories 1 through 4 are designated for preventive and mitigatory functions; but there are no guidelines for application of capability, dependability and robustness for each category.				
53 UK	4.4, 2nd bullet (2)	Following on from previous comments on PSA (Comment 49) – there is an opportunity here to expand this aspect of the guidance.				Editorial changes, See Annex II
22 SPA	4.4.2	Change this sentence REASON: The definition of requirements for dependability is not clear. The failure of one element pertaining to a safety functional group always degrades the ability of the group to perform its designate function.	PA	Editorial changes,		
Belg. 7	§4.5	§4.5: "The dependability and robustness of an SCC should be achieved within an acceptable range of probability of failure and its related consequences" should be clarified or deleted. REASON: The sentence of obscure. What is the link between "robustness" and "probability of failure"? Considering Table 3, only "dependability" can be linked with a probability of failure. Capability and Robustness are deterministic design requirements.	PA	See para 4.4		
Belg. 8	§4.7 & 4.11	Exclude I&C and IT from this safety classification methodology. REASON: As illustrated in comment Belg. 5 , it is not clear how this general guidance applies to I&C; § 4.11 states that NS-G-1.1 AND 1.3 "requirements" should be applied, but those documents do not use this DiD approach.			R	Para 4.7 of ver 5.1 was deleted New 4.7 includes link to I & C it is important to have here.
Belg. 9	§4.7	Can be deleted. REASON: The need to include/use "codes and standards" is stated in §4.1 and again in §4.9. Moreover, §4.7 refers to "safety functional	A	Deleted, See para 4.1		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		groups": requirements apply to SSCs.				
23 SPA	4.7	Idem comment 9	A	Deleted, See para 4.1		
54 UK	4.7 and 4.9	These paragraphs seem to say virtually the same thing. Consider combining to avoid unnecessary duplication.		Deleted both paragraphs		
54 FRA	4.9	Merge 4.9 and 4.1 REASON: 4.9 is partly redundant with 4.1	A	See para 4.1		
29 USA	4.9 / 1	"Applicable Member State regulatory requirements, including ~~The~~ appropriate codes and standards with any limitations and modifications specified in the regulations, should be used for defining design requirements for all types of SSCs." REASON: The guidance in the Safety Guide referred to codes and standards without referencing the Member State regulatory requirements. The users of the Safety Guide should satisfy the applicable requirements issued by the regulatory body in the specific Member State for the design of plant SSCs, including codes and standards specified in those requirements with any applicable limitations and modifications.	PA	deleted, See para 4.1		
55 FRA	4.10, 4.11, 4.13, 4.14	Delete this paragraphs REASON: Also being true, these sentences start a long list of area of requirements which is not exhaustive.			R	These are cases where existing codes and standards are available. It is important to reference these codes and standards.
55 UK	4.12	Replace "Refs. [11]" with "Ref. [11]" REASON: Correct typo	A	Ref. [16]		
30 USA	4.12 / 1-3	"Quality assurance or management requirements for design, qualification, procurement, construction, inspection, installation, testing, surveillance, and modification of SSCs should be assigned based on their safety class as outlined in Refs. [11]." REASON: In addition to the activities listed in the original wording of the Safety Guide, the quality assurance and management requirements for design, qualification, and surveillance are included in the proposed new text for consideration as part of the design requirements for plant SSCs.	A	See para 4.8		
56 UK	4.14	The meaning of "synergistic effects" is unclear.	A	"synergistic effects" was deleted		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
31 USA	4.14 / 2	"associated with normal operation and for postulated initiating events up to DBA conditions where the SSCs may be" REASON: The design requirements for plant SSCs should include consideration of design basis accident (DBA) conditions as part of the environmental qualification.			R	Edited, see para 4.10
9 JPN	Appendix III Table 2	ROBUSTNESS for Safety Category-4 should be "Survive conditions due to normal operation, PIEs to be mitigated, and selected BDBA and Severe Accident to be mitigated" instead of "Survive conditions due to normal operation and PIEs to be mitigated" REASON: There is no Safety Class 4 for DiD Level 1			N/A	Reference to DID levels has been been changed
10 JPN	Appendix III Table 4	Delete the column for Safety Class-4 in the Preventive Safety Function REASON: Safety Class 4 should be operable for applicable BDBA and Severe Accident environmental condition, but qualification level would be different from Class 1, 2 and 3.	A	Deleted the column		
11 JPN	Appendix III Table 4	Environmental qualification for Safety class 4 in the Mitigation Safety Functions had better change to "Specific SSC to be qualified for all normal operation states and applicable PIEs, and to be operable for applicable BDBA and Severe Accident.			N/A	Edited the table
32 USA	Appendix III / Table 2	In Table 2, under "Capability", the requirement for Safety Category 4 is to "Achieve requirements for BDBA and Severe Accidents". *Reconsider this requirement.* REASON: If BDBA and Severe accidents are used to impose requirements for safety functions, then they become a class of design basis accidents that is more severe than the defined DBAs. How does one demonstrate that requirements like "prevention of accident progression" are satisfied? How quickly and to what extent? What frequency of occurrence of BDBAs is needed to justify requiring PSFs for accident mitigation?	A			
57 UK	Appendix	This table does not appear to add any value			R	Just an example moved to Annex

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
	III Table 2					
58 UK	Appendix III Table 4	▪ This table needs to be reviewed for consistency with the remainder of the document. For example: ▪ There are no Safety Class 4 SSCs in DiD Level 1; and, The environmental qualification requirements in DiD 2-4 are less for SFC-3 than for SFC-4.	PA	Deleted the DiD level 4 column from preventive and edited the table		
11 CORDEL	APPENDIX III: TABLE 2	EXAMPLE OF REQUIREMENTS FOR SAFETY CATEGORIES From our view the table is not really consistent with the principles described in the main section of the draft and should be rewritten. E.g. Characteristica like capability, dependability and robustness for DiD level 1 and safety categorie I is over-determined and misleading.			R	Just an example moved to Annex
45 FRA	Fig 1.	The last downgrading possibility (Class 4 to non-safety classified) should be justified as the SCC contribute to a nuclear accident mitigation.	A	Modified, now Fig 2		1,2,3 classes
25 SPA	Fig 3 App 2	Revise the acronyms used in this figure REASON: There is a mistake	A	edited		
59 UK	References	Although details of Refs [5] and [6] are included in the Reference section, they do not appear to be referenced in this draft safety guide. The order of the references as they appear in the current draft needs updating, to ensure for example that Ref [7] appears before Ref [8].	A	Edited		
40 FRA	Table 1	Delete last line of the table REASON: See comment 27	PA	Modified		
42 FRA	Table 1	Why isn't it a class for DiD level 5 ?		R		
38 UK	Table 1	In addition to previous comments in which the need for four separate categories was raised (Comment 17 here and comments made by the UK in October 2008 for the 26th NUSSC meeting), the specific advice provided in this table looks wrong on four counts: **1) DiD 4A/B + High:** These should be 3 not 4. Continued monitoring of the plant during a beyond design basis accident with such high consequences and measures to mitigate the accident's effects are at least as important as preventing a low consequence event.	PA	modified		

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
39 UK	Table 1	**2) DiD 4A/B + Medium:** These should also be 3 rather than 4. This far down the defence in depth scale, we would not design the measures to any lower scale for a medium consequence event than for a high consequence one. Under 1) we suggest the high consequence variant should be a 3.			R	See footnote
40 UK	Table 1	**3) DiD 4A/B + Low:** This should be "not safety categorised" rather than 4. We would not expect accident mitigation measures for an event that could not even reach legal dose limits.	PA	"N/A" for " low" and "medium"		
41 UK	Table 1	**4) DiD 5 + High/Medium:** It is hard to argue that such equipment has no safety function. This should also be 3.	PA	The row was deleted		
42 UK	Table 1 (and throughout the document, e.g. Table 2 and Table 4)	Connection of the DiD concept with the classification of SSCs also leads to interpretation problems. For example, according to Table 1 the failure of a preventive safety function (classified DiD Level 1) could have medium or high radiological consequences (exceeds normal operational limits). From the concept of DiD-Levels as described in INSAG 10, operational deviations on DiD Level 1 should be handled on DiD Level 2, which is still considered as operation, and therefore have a maximum radiological impact as described here as "low" (close to but below normal operational limits). This misinterpretation is included in the whole document and should be avoided.			N/A	No DiD level functions
41 FRA	Table 1 / footnote 1	What does this mean ? This is the first time in the guide that the non-nuclear safety class is mentioned….	A	Modified accordingly		
18 SAF	Table 2	Table 2 is not correct – see comment on 3.27	A	Modified table		
26 SPA	Table 2 Appendix III	Change the number of note (1 to 3) for SC-2 Mitigatory, for dependability Review the note's numbering. It does not seems logical to use the same numbering for the corps of documetn and the appendix. REASON: It make the text more clear.	PA	edited		
ENISS 30	Table2 Appendix III	Review the note's numbering. It seems not logical to use the same numbering for the corps of document and the appendix. It makes the text more clear	PA	edited		
56 FRA	Table 3	Mitigative Safety Functions/ Environmental qualification/Safety class 3: Add "and applicable PIEs" as for			N/A	

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		safety class 4 REASON: Quality/clarity				
57 FRA	Table 3	Definition of important items is missing: -Table 4 Pressure categories high and low REASON: Quality/clarity	A	modified	R	Glossary
58 FRA	Table 3	Preventive safety functions/Requirements/ I&C (IEC 61226 Category)* shall be checked again. Requiring B or C for safety category 1 is unexpected *Category A denotes the functions that play a principle role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences. Category B denoted functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the controlled state has been achieved, to prevent DBEs from leading to unacceptable consequences, or mitigate the consequences of a DBE. Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety.			R	In normal operation B anc C (IEC 61226 Category)
8 INS	Table 4 10	Add to this Table: "Mechanical Systems" in column • Safety Class 1: M1 • Safely Class 2: M2 • Safety Class 3: M2 • Safety Class 4: M3 Note: M1: internal pressure and fluid M2: joints of internal pressure containing elements M3: not pressure containing REASON: Mechanical systems have not been included in the scope of Table- 4 requirements for Safety Classification of Structures, Systems and Components in Nuclear Power Plants			R	Explained bellow
27 SPA General comment	Table 4	Idem to second part of comments 26 REASON: This safety guide proposes a new methodology for the classification of SSCs. It would be necessary, in order to be			N/A	No new methodology

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		able to look at the impact of the guide, to compare the results of classification of SSCs using this guide and the usual methodology, for old plants as wellas for new ones.				
4 ROM	From P.29 up to final	3 SAFETY CLASSIFICATION PROCESS 4 SELECTION OF APPLICABLE REQUIREMENTS FOR SSC have to be rephrased and/or totally reviewed and replaced in order to comply with other types of NPP, except for PWR or BWR. REASON: 1 - The terms of conceptual and nuclear safety meanings are not at all well defined (radiological risk, safety analysis, essential and derived safety functions, nuclear safety principles, safety objectives safety criteria, also); 2 – The defense in-depth principle is not correct assumed and detailed against the nuclear safety concept (the succeeding physical barriers provided against the radioactive material releases to environment); 3 – The plants SSC classification is not well defined (SR, NSR preventive/protective functions) because of wrong defense in-depth assumptions; 4 – The SSC safety classification process is not clear enough, is confusing and full of ambiguities; 5 – There is a lack of systematic approach in documentation for licensing (i.e. no preliminary System Classification List); 6 – The regimes/plant conditions do not represent defense in-depth criteria for assessing the safety functions; 7 – The final judgement on the balance between safety classes and the results of deterministic and probabilistic safety assessment, is not clearly defined in liaison with the plant SSC associated functions; 8 – The nuclear safety philosophy and hence, the safety classification of SSC approach in this draft does not match the CANDU-6 nuclear safety concept.	PA		N/A	The document was improved
60 UK	Annex 1	Replace “FSF1)” with “FSF1”; “FSF3confinement” with “FSF3 confinement” REASON: Correct typos	A			
Belg. 10	Annex I	Change Title in SPECIFIC SAFETY FUNCTIONS for LWRs REASON:			N/A	New title

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		Corresponds to the intent as described in main text §2.8.				
Belg. 11	Annex I	The difficulty of use of Level 1 is further illustrated in Annex I. It correlates the safety function "to prevent unacceptable reactivity transients" to DiD 1! REASON: What does "unacceptable" mean? Prompt criticality? To what function belongs "to prevent reactivity transients"? In fact, there is a spectrum of means to avoid appearance of prompt criticality, starting with an inherent safe design, followed by efficient closed loop control systems, then an automatic shutdown….We do not believe that all this belongs to Level 1, nor to Safety Category 1 as per Table 2	A	modified		
Belg. 12	Annex I	Annex I states that this annex gives an example of safety functions allocated to the 3 FSFs. We recommend to wait for a better list which shows a clear hierarchy, and links with the FSFs. REASON: This list lacks hierarchy and structure, and does not help much to understand what are the safety functions allocated to a particular DiD level. It repeats the list of safety functions from 50-SG-D1 §2.2, while this SG was withdrawn in 2000 (cfr Introduction).			N/A	Teactor type safety functions This is the most commonly used list in the past for LWRs
33 USA	Annex II / Figure 11-1	In Figure II-1, the box denoted "Probabilistic Safety Requirements" has no connections to any of the other boxes in the figure. *Add connections or delete it.* REASON: The role of "Probabilistic Safety Requirements" is not indicated.			N/A	Deleted
34 USA	Annex II / Figure 11-1	"Acceptable ~~failure frequencies~~ <u>deterministic safety analysis results, based upon assumed failure frequencies</u>" REASON: PIE classification should be based, in part, on the PIE's frequency of occurrence. If the analysis result is acceptable, then the frequency may be compared to PSA-based			N/A	Deleted

Comment No.	Para/ Line No.	Proposed new text / Reason	A	Accepted, but modified as follows	R	Reason for modification/rejection
		frequencies that yield acceptable results.				
35 USA	Annex II / Figure II-1	Provide guidance for acceptable failure frequencies. REASON: This Figure mentions acceptable failure frequencies but does not provide any guidance for what are acceptable failure frequencies.			N/A	Deleted