MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
153	FR	0	Annex 1		This annex is a very good idea.	x			We agree.
154	FR	0	Annex 2		This annex might be deleted and captured in a TecDoc. (It is not a usual IAEA practice to insert such type of annex in a new version of a Safety Standard or a combination of Safety Standard).			**x**	**This was agreed in response to concerns on replacing NS.G.1.1 and NS.G.1.3 with one combined safety guide**
155	FR	0	Annex 3	Delete annex 3	Safety Standard establish what is the international expectation, not a collection of national practices. Information in annex 3 would therefore be more relevant as a TecDoc or a Safety Report….			x	Anex III has already been subject to considerable discussion and negotiation.
12	Spain	0	Annex I, I-8	and '1E' as equivalent instead of and 'IE' as…	Editorial correction.	x			
13	Spain	0	Annex I, Table I-2, 6	Set points: IEC 61888 and ISA-S67.04	ISA-S67.04 is a well known standard used by worldwide nuclear power plants.			x	We should limit references to IEC only.
1	HU	0	Definitions	Common Mode Failure - components fail due to the same design or manufacturing deficiency.	Common Mode Failure should be defined, because there is such like possibility when different pieces of components of the same type fail in different times due to the same design or manufacturing deficiency. Without proper collection of event statistical data the cases may represent single failures at the first sight. However there is the possibility of worse case, when the same design or manufacturing deficiency manifests at the same time at the components of the same type in different locations of the same facility, or on different trains of the safety systems causing Common Cause Failure. DS431 writes about CMF (Eg. on page 25 and 43.)			x	
17	ISO/ WNA	0	Definitions	**non-functional requirements:** p.130 4th line from the bottom: "Characteristics specified in non-functional requirements **may** include …".	"Characteristics specified in non-functional requirements include …" . the sentence should be softened by saying: Since the list of the possible non-functional requirements include also terms that might be listed as functional requirements	x	See comment #109 USA		
109	USA	0	Definitions	**non-functional requirements:** Quality (popularly known as non-functional) requirement~~s~~. Requirement~~s~~ that ~~specify~~ specifies a quality (set of inherent properties or characteristics and their inter-relationships) ~~required characteristics~~ of an item, other than the required functions and behaviours. Examples of ~~Characteristics~~ characteristics: ~~specified in non-functional requirements include, for example,~~ analyzability, assurability, auditability, ~~availability~~, ~~compatibility, documentation,~~ integrity, maintainability, safety, security, and verifiability ~~reliability, and usability~~.	Fundamental definitions should conform to broader international standards, e.g.: ISO SQuaRE series; see linked references below. The SQuaRE series of standards does not define or use the term "non-functional requirement." Its closest counterpart is the term "quality requirement," which encompasses the specification of requirements for all the characteristics implied in the popular usage of the term "non-functional requirement." To satisfy §2.69 of DS431, a requirement should be verifiable. To enable verifiability, the SQuaRE series of standards provides a framework, which allows the specification of a property of interest (e.g., safety) as an evaluate-able composition of characteristics and verifiable sub-characteristics. The list of examples should focus on the most relevant properties or characteristics, e.g., SAFETY and its most important supporting characteristics, e.g.: Assurability Verifiability Analyzability Such composition-decomposition of the safety property is important, because architectural requirements and constraints are derived from the verifiable (sub-) characteristics.	x	Definition should not lose anything but we could to it to help accomodate proposal. I suggest change to: **non-functional requirements** (also known as quality requirements): Requirements that specify inherent properties or characteristics of an item, other than the required functions and behaviours. Example characteristics include analyzability, assurability, auditability, availability, compatibility, documentation, integrity, maintainability, reliability, safety, security, usability and verifiability.		
110	USA	0	Definitions	Add: **Hazard analysis:** Hazard analysis (HA) is the process of examining a system throughout its lifecycle to identify inherent hazards (see) and contributory hazards, and requirements and constraints to eliminate, prevent, or control them.	Add new para.			x	Proposal appears to have missed there is already a definition.
6	FR	0	Fig. 1	FIG.1, Interaction with Cybersecurity program	Typo	x			
3	ISO/ WNA	0	Fig. 1	Update of Figure 1 regarding: (1) incorrectly representation of the interfaces between I&C lifecycle and I&C security lifecycle, (2) Integration of the required input data from plant life cycle. Proposal for Figure 1 – see attachment 1	Item 1: The interactions with the I&C security program should be ongoing and on all levels. In other words, the interactions of the I&C lifecycle with the security activities should exist both on the individual system (I&C subsystem) and overall I&C levels; Item 2: To start the I&C life cycle, input data are required which should be derived from the plant safety design base.	x	Fig. 1 modified in accrdnace with UK and French comments.		Fig. 1 is only example, however modified along with UK and USA comments.
3	UK	0	Fig. 1	Amend Fig 1 to show complete lifecycle through to I&C system decommissioning.	Consistency with paragraph 2.23	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
5	USA	0	Fig. 1	System validation should be represented as a parallel activity to the entire life cycle instead of a single activity to be performed upon completion of system development. Ex. System requirements should be validated as they are developed to ensure correctness.	System validation is shown as a sequential activity to be performed on the final hardware and software product, however, both verification and validation activities described on page 23 should be performed throughout the development lifecycle. It is incorrect to characterize Validation as an activity only to be performed on final products.	x	Fig. 1 modified in accrdnace with UK and French comments.		
6	USA	0	Fig. 1	Incorporate separate Verification activities at various stages of the development process.	This figure does not reflect any Verification activities.		Fig. 1 modified in accrdnace with UK and French comments.	x	No problem in principle but in practice this is likely to make the figure too complicated
7	USA	0	Fig. 1	Add Cyber Incident Response as part of the O&M Interactions with Cybersecurity Program.	Cyber Incident Response is an important part of the Cyber Security Program and should be included as part of the O&M Interactions with Cybersecurity Program.		Fig. 1 modified in accrdnace with UK and French comments.		
85	USA	0	Fig. 3	*FIG. 3. Setpoint terminology and errors to be considered in setpoint determination*	Figure 4 should be Figure 3. Apparently, the previous Figure 3 was deleted from DS431 in the development of Rev L.	x			
1	BEL-V	0	General	The IAEA document DS431 is a revision and combination of the safety guides NS-G-1.1 and 1.3. The Safety Guide NS-G-1.1 was prepared in order to provide guidance on the collection of evidence and preparation of documentation to be used in the safety demonstration. The Safety Guide NS-G-1.3 was prepared to provide guidance on the design of I&C systems. This latter guide NS-G-1.3 is a combination of the previous Safety Guides 50-SG-D3 (Safety Systems) and 50-SG-D8 (Safety Related Systems). As a result, the NS-G-1.3 clearly makes a distinction for the systems important to safety between safety systems and safety related systems. In fact, table 1 of the Safety Guide NS-G-1.3 (p19) gives an overview of the requirements which are applicable for either system. This distinction between safety systems and safety related systems does not clearly appear in the IAEA document DS 431.				x	No recommendation provided
2	BEL-V	0	General	For the classification of instrumentation and control systems it would be advisable to use the existing and applicable norm IEC61226 as a reference.				x	No recommendation provided
3	BEL-V	0	General	For the requirements on software for computer based systems important to safety it would be advisable to use the existing and applicable norms IEC60880 (Type A – Safety Systems) and IEC62138 (Types B and C - Safety Related Systems) as a reference.				x	The IAEA does not reference international standards uch as IEC.
37	CH	0	General	Intermediate headers: INDEPENDENCE *Diversity* Has the different font a meaning?Different ranking / subheader?				x	Intermediate headers are used in line with a writer's guide
1	FR	0	General	DS431 is addressing, for NPP, the topic addressed in DS for Research reactors. DS436 was approved by CSS in November 2013 and wording of recommendations of DS436 should be kept unless it is technically wrong for a NPP. (Additional recommendations relevant to NPP should obviously be kept)	Consistency between IAEA Safety Standards.			x	DS431 superseeds NS-G-1.1. and 1.3. It keeps consistency with wording and terminology used in; There is no indications that this terminology is different than that one used in DS436. This comment could have been seen from the other side, whether the DS436 keeps consistency with terminology used for nuclear power plants. It is the original intention of safety guides to furter ellaborate on requirements SSR 2/1 which are meant to be for nuclear power plants.
2	FR	0	General	The whole draft should be revisited to ensure adequate use of “safety system” vs use of “system important to safety”, to ensure consistency with IAEA Safety Glossary	Consistency with IAEA Safety Glossary definitions.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
3	FR	0	General	The document mixes recommendations (with “should” statement) and explanations, usually related to a recommendation. Explanations should be either merge with the recommendation (not an independent paragraph) or transfer into footnotes	To focus the document on recommendations.		However, I do agree that a different font for recommendations and explanations would be beneficial, if this is still possible.	x	The approach used was not to combine informative and normative pars together. Different fonts will be discussed with IAEA editor.
1	ISO/ WNA	0	General	Usage of wording should be harmonized within the document especially the use of very important items like “Safety System”. In paragraph 1.4 it is mentioned that: “In a few cases, recommendations or explanations apply to both I&C systems important to safety and I&C systems that are not important to safety; in that case the term ‘All I&C systems’ is used.” This is not consequently applied in the document. Use the wording from NS-G-1.3 (see figure)				x	DS 431 follows terminology of the IAEA safety glossary defines plant equipment; items impoftant to safety and safety systems.
2	ISO/ WNA	0	General	The DS-431 specifies requirements for the I&C without the explanation of their origin / source. This leads in some cases to problems of misunderstanding single paragraphs. It is important not only to “know how” but also “know why” which is essential for the effective interpretation and realization of the specified requirements. For example, paragraph 7.45 (Comment No. 26) could be misunderstood.				x	We believe that 7.45 is clear enough. The imoplementation guiedance is not part of the IAEA Safety Guides.
1	RF	0	General	We propose to add new chapter devoted to I&C equipment ageing (or provide a reference to some document which covers ageing aspects).	I&C systems ageing management is important aspect of ensuring quality of I&C.			x	I am afraid it si too late to add a I&C specific section on ageing. The IAEA currently reviews the NS-G-2.12, which has I&C in the scope and related ageing aspects will be covered.
3	SWE	0	General	A list of abbreviations?	All abbreviations that are used in the text are not included in the list of definitions. E.g. it could also be useful to define what is meant by HMI station (are e.g. all control room work stations, local stations and control centers etc. included?)			x	Safety Stadards do not include list of abbreviations.
1	UK	0	General	UK strongly supports this draft standard since it contains es-sential requirements for the design of I&C at NPPs that are necessary in the interests of safety. We note there are a number of potentially conten-tious issues addressed in this Safety Guide where the inter-national technical community has needed to work hard to reach a common position eve-ryone has been able to support. In particular, the consensus achieved in addressing NUSSC comments at the technical meeting held earlier this year (involving experts representing US, France, Finland and Germany) should be preserved. It is important that, when ad-dressing comments from Member States, decisions reached at this meeting are not undone.	This is UK’s key comment The paragraphs seen as po-tentially contentious, but where keeping to the previously negotiated technical line is essential are: 2.85, 2.86, 2.138, 2.139, 3.13, 4.11, 4.17, 4.18, 4.30, 4.32, 4.40, 6.13, 6.52, 6.54, 7.6, 7.7, 7.60, 7.75, 7.96, 7.143, 7.172, 9.99-9.102, Annex III (specifically paras 3-5, 8 and 13-14).	x	Not surprisingly, I think all UK comments should be accepted. We already excluded comments that were of less value before submitting to the IAEA. None however are vital to the UK position except this one.		
17	UK	0	General	Include a list of abbreviations	Clarity			x	Safety Stadards do not include list of abbreviations.
		0	List of contributors	As previously requested by email, please change "Office of Nuclear Regulation" to "Office for Nuclear Regulation". This applies to Bowell M, Tate R and Yates R		x			Changed "of" to "for".
11	Spain	0	List of definitions (related to Annex I, I-7&8)	General comment: the terms safety items, safety related items, items important to safety, etc. should be included, defined in the List of definitions and compared to those used in IEEE. Alternatively, include a reference to IAEA Safety Glossary.	IEEE standards are widely used by several members of the IAEA, which could potentially cause misunderstandings when implementing DS-431.			x	The IAEA Safety Glossary defines term "item important to safety". We cannot use IEEE definitions.
2	UK	1	3	“…system receiving data is of a higher class than the system sending data.”	Align terminology with eg 2.73.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
1	USA	1	4	"In cases where recommendations or explanations are applicable to both I&C systems important to safety and I&C systems that are not important to safety, the term 'All I&C systems' is used."	The existing sentence is ambiguous and is a run-on.	x			
2	RF	1	7	1.7 - 1.4: In object: there are no comments to software for computer based systems	Not correspond to NS.G.1.1			x	SW is mentioned in 1.11 - applicability of the safety guide.
2	USA	1	9	Add sentence: "For such cases, this Safety Guide identifies relevant sections of these other safety guides that are being addressed."	The second sentence doesn't specify how the recommendations of other Safety Guides are designated in this SG.	x			
3	USA	1	11	Suggested change: From "Computer systems" to "Computer systems and associated communication systems"	Communication is an important part of DI&C system that should not be overlooked. As a matter of fact, Pages 79-82 discuss the digital communication systems.	x			
3	RF	1	13	We propose to provide reference to specific IAEA Nuclear Security Series documents	Providing a reference will allow to make the document more specific.	x	**The IAEA proposal to add ref. To NSS17.**		
4	USA	1	16	Revise as follows: "This safety guide provides recommendations for the development of computer software for use in I&C systems important to safety. It also provides guidance for digital data communication, and specifies measures needed for I&C functions that are programmed into integrated circuits using HDL descriptions."	The first sentence of this clause is a run-on and should be broken into two or three separate sentences.	x	**The IAEA Proposal: This safety guide provides recommendations for the development of computer software for use in I&C systems important to safety as well as digital data communication. This safety guide also defines measures needed for I&C functions that are programmed into integrated circuits using HDL descriptions.**		We believe that existing text is sufficient, but I have no problem with breaking down into a number of sentences. But proposal is worse than existing text because it suggests HDL and digital data communication link together.
4	RF	1	28	We propose to mention shortly Annex III and its content	Providing a reference to Annex III seems to be useful	x			
19	FR	2	3	Transform 2.30 into a footnote to 2.29	Explanation only			x	We do not combine informative and normative pars together. We avoid footnotes.
1	SC 45X	2	4	GS-R-3 Paragraph 4.1 states: Information and knowledge of the organization shall be managed as a resource. In order to ensure safety, design bases documents and related information or records related to I&C systems important to safety must be controlled by suitable processes, such that they are complete, clear, concise, correct and consistent over the entire lifecycle. The management system must ensure design bases documents and related or derived information or records are sufficient and adequate, and are maintained over time to reflect design changes or changing conditions in the plant. This includes documents and information that may be derived from the design bases documentation and that may have an impact on safety, such as procedures or manuals related to operation, maintenance, or modification of such systems. GS-R-3 Paragraph 4.4 states: Senior management shall ensure that individuals are competent to perform their assigned work and that they understand the consequence for safety of their activities. Individual shall have received appropriate education and training, and shall have acquired suitable skills, knowledge and experience to ensure their competence. Training shall ensure that individuals are aware of the relevance and importance of their activities and of how their activities contribute to safety in the achievement of the organization's objectives. Management shall ensure the needed specialized or multi-disciplinary knowledge and experience is sufficiently available within the organization to properly interpret and maintain the design bases documents (and related information or records or derived documentation) of I&C systems important to safety.	Add new text.	x	Added 4.1, not 4.4 (not related to recommendations in this saefty guide).		
13	FR	2	5	Merge 2.50 with 2.52	Same topic			x	We do not combine informative and normative pars together.
4	FR	2	12	Merge 2.12 with 2.11	No need for a separate paragraph as both paragraphs address the same topic (modern I&C).			x	We do not combine informative and normative pars together.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
5	FR	2	13	~~As a result~~ In modern I&C systems, demonstration that the final product is fit for its purpose depends greatly, but not exclusively, on the use of a high-quality development process that provides for disciplined specification and implementation of design requirements. ~~In modern I&C systems~~, verification and validation is necessary to ensuring that the final product is suitable for use…	Clarification	x	In digital I&C...		
1	SWE	2	18	Furthermore, human factors and security features are easier and more cost efficient to implement in the design phase. Afterwards changes can be very difficult or even impossible to implement.	The two sentences are also valid for human factors issues in the design, but the original sentence may be understood to only point out security features. It could also be said, that it is important to include these issues as early on as possible in the design process, e.g. some issues need to be resolved already in (or before) the architectural design, as shown in figure 1.	x			
5	RF	2	22	We propose to elaborate the chapter and provide requirements to the documents for life cycle	Current version of draft use term «documented development life cycle» but does not specify their meaning.			x	It means that every step in I&C lifecycle should be documented.The implementation guideline "how" it should be done is outside the scope.
8	USA	2	25	Add “Software Training Plan” to list.	No plan for I&C system training is listed.	x	I suggest simply "Training"		
9	USA	2	25	Add “I&C System Operations Plan” to list.	No plan for System Operations is included.	x	I suggest simply "Operations" If training or operations are outside the scope of the document it would be helpful to point this out and indicate where they are covered instead		
7	FR	2	26	Merge 2.26 with 2.25	Same topic			x	We do not combine informative and normative pars together.
6	RF	2	28	We propose to specify who approve plans mentioned in p/2/28				x	The implementation guideline "how" it should be done is outside the scope.
1	CH	2	31	2.31 g, 2.43, 2.55, 2.62, 2.64, 2.78 and others. Requirements / recommendations should be clearly distinguished from explanations / comments (e.g. different numbering or *different font*)	Better recognition of the requirements / recommendations		By our rule normative and informative paras are not combined. Using different font may be discussed with the IAEA editor.	x	
8	FR	2	31	Merge bullet g) with bullet f)	g) explains f).	x			
9	FR	2	32	e. Validate, using performance based measures, that operating personnel can carry out their functions using the I&C system under all conditions under which the system is expected to function, including when some I&C parts are supposed to be out of service (for example for maintenance or testing purposes).	Clarification	x	Better English might be: including when some parts of the I&C system are out of service for authorised reasons		e. Validate, using performance based measures, that operating personnel can carry out their functions using the I&C system under all conditions under which the system is expected to function, including when some parts of the I&C system are out of service for authorised reasons (for example for maintenance or testing purposes).
10	FR	2	34	2.34. The overall I&C should implement the security measures that are assigned to it by the computer security plan, which may.~~2.35. The computer security plan should~~ be updated, as necessary, during the project to take into account the overall I&C architecture and individual I&C systems.	Merge 2.34 and 2.35 (same topic and simplification)			x	There are two separate recommendations.
7	RF	2	43	Delete second sentence	The sentence does not correspond to p.2.44.	x			
11	FR	2	43	Merge 2.43 and 2.44	Both 2.43 and 2.44 are explanations relevant to the recommendation established in 2.42.			x	We do not combine informative and normative pars together.
12	FR	2	47	2.47. Life cycle process records should be under configuration management~~.~~ even if ~~2.48.~~ The configuration management program ~~for life cycle records~~ may be different from that used for I&C products.	Same topic and simplification			x	We do not combine informative and normative pars together.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
10	USA	2	48	Suggested change: From : “The configuration management program for life cycle records may be different from that used for I&C products.” To: “The final version of I&C products in configuration management program for life cycle records should be the same as that used for I&C products.”	Configuration management should keep the same copy of the program as used in I&C system.			x	This is not the purpose of the existing text. A new para could be added but it is confusing because it is so obvious
2	CH	2	53	If this shall include development and manufacturing of an item or platform on the supplier/vendor side it is not practicable			This is en informative para - an example.	x	
8	RF	2	54	Add words “as a rule” after word “should”.	The para is not applicable to the programmable devices (FMGA)			x	We believe that "should' is sufficient.
14	FR	2	54	2.54. The identity of software installed in I&C equipment and the values of configuration data should be retrievable from the I&C equipment~~. 2.55.~~ as The ability to retrieve the identity of installed items and the values of configuration data support verification that the devices are properly configured. Automatic checking features or tools may assist this verification.	Same topic			x	We do not combine informative and normative pars together.
12	USA	2	56	For the overall I&C architecture, hazard analysis should be performed to identify conditions that might compromise the defence-in-depth or diversity strategy of the plant design.	Need to identify conditions that might compromise diversity. Trend of increasing interconnections is increasing the hazard space of common causes and contributing factors, i.e. threatening to compromise DIVERSITY. Consistency with §: 2.82 third bullet; 4.9; 4.37	x			
15	FR	2	56	2.56. For the overall I&C architecture, hazard analysis should be performed to identify conditions that might compromise the defence-in-depth strategy of the plant design. ~~2.65.~~ The hazard analysis methods should: - be appropriate for the item being analysed~~. ; 2. I&C system hazard analysis should~~ - consider all plant states and operating modes, including transitions between operating modes.	Combine these paragraph as they set general expectations for hazard analysis		I prefer Gary's strategy of having a separate paragraph for each recommendation.	x	We do not combine informative and normative pars together.
11	USA	2	56	2.56-2.65	I&C systems hazard analysis. The section describes the need and scope for hazards analysis but does not provide guidance on specific types of hazard analysis that are acceptable. References to various HA techniques would be helpful.			x	Is this an intention to detail how hazard analysis should be done in this safety guide?
13	USA	2	57	For safety systems, hazards analyses should be performed to identify conditions that might ~~defeat~~ degrade the performance of their safety function.	The proposed change makes it consistent with IEEE Std 603-Clause 4h, which is incorporated by reference in NRC’s regulation. “Degrade” covers a broader malfunctioning range than “defeat.”	x			
14	USA	2	58	Hazards to be considered include internal hazards and external hazards, failures of plant equipment, and I&C failures or spurious operation due to hardware failure or to software errors. Also included are contributory hazards due to unwanted interactions.	Trend of increasing interconnections is increasing the hazard space of unwanted interactions. This hazard space is not well understood and difficult to recognize. Therefore, this guide should identify it explicitly.	x			
16	FR	2	58	2.58. Hazards to be considered include credible internal hazards and external hazards, failures of plant equipment, and I&C failures or spurious operation due to hardware failure or to software errors.	Clarification (especially relevant for external hazards)			x	What is "credible"?
15	USA	2	59	I&C system hazard analysis should consider all plant states and operating modes, including transitions between operating modes. Degraded states should also be included.	Consistency with 3/14/d/2	x			
3	CH	2	60	Is this realistically achievable		x	Yes, we hope so.		
16	USA	2	61	The hazard analysis should be updated at every phase of the development lifecycle, including (but not limited to) ~~during~~ the design of the overall I&C architecture, and ~~during~~ the specification of requirements, design, implementation, installation and modification of safety systems.	Generalization through the phrase “at every phase of the development lifecycle ….” makes the guideline more comprehensive and inclusive. Listing a few phases of the lifecycle activities allows for an interpretation that omits other phases. All the phases cannot be enumerated, because developers may select different lifecycle models.	x			
4	CH	2	61	That means over the whole life cycle			Yes	x	
17	FR	2	61	Merge 2.61 and 2.62	Same topic			x	We do not combine informative and normative pars together.
18	FR	2	63	Measures should be taken to eliminate, avoid, or mitigate the consequences of identified hazards that can defeat safety ~~system~~ functions.	Reference to Safety system is restrictive as the concept also applies to systems important to safety.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
17	USA	2	63	Measures should be taken to eliminate, avoid, or mitigate the consequences of identified hazards that can ~~defeat~~ degrade the performance of safety system functions.	The proposed change makes it consistent with IEEE Std 603-Clause 4h, which is incorporated by reference in NRC's regulation. "Degrade" covers a broader malfunctioning range than defeat."	x			
9	RF	2	68	We propose to specify when Requirements Traceability Matrix shall be prepared	Adding the information will make the requirement be more precise.			x	
18	USA	2	69	Replace term "validated" with "verified" and add a clause to describe "Validation" activities as follows: "The requirements defining the overall I&C, each I&C system, and each I&C component should be validated to confirm they are fulfilled as intended."	This is an incorrect use of the term "Validation" and it is not consistent with the glossary definition provided on page 131. Instead, the term "Verification" should be used to confirm implementation of requirements. Validation confirms that the requirements are satisfied ***as intended***. A distinction should be made between performance of ***verification*** activities and performance of ***validation*** activities. See Glossary definitions for Verification and Validation on page 131.	x			The IAEA accept modification and add new sentence to 2.69 as suggested.
19	USA	2	71	Section 2.71 states, "Verification and validation should be carried out by teams, individuals, or groups that are independent of the designers and developers."	This statement is incomplete. Independent V&V should be performed by independent teams; however, the design and development organization should also perform their own V&V independent of the IV&V team. That is, IV&V does not obviate the need for V&V. See IEEE Std. 1012-2012 for guidance on the difference between IV&V and V&V.	x	Verification and validation should be carried out by individuals, teams, or organizational groups that are independent of the designers and developers.		
20	FR	2	71	Merge 2.73 with 2.71	Same topic and 2.73 should appear before 2.72 (2.72 presents a whole range of degree of independence)			x	We do not combine informative and normative pars together.
5	CH	2	72	What is the difference between teams and groups?	Delete all unnecessary wording for better readability..	x	Establishing independence of verification and validation normally involves ensuring that the V&V teams, individuals or organizational groups: (bullets remain the same)		
20	USA	2	72	Delete the third bullet or combine with the fifth as follows: "Are not subject to pressure from the development group, (i.e. are allowed to submit their findings to program management without adverse pressure from the development group)."	The third and fifth bullets are essentially the same. These should be combined.		(see CH#5 above) Establishing independence of verification and validation normally involves ensuring that the V&V teams, individuals or organizational groups: (bullets remain the same)	x	They are not the same - adverse pressure could affect judgment and hence formulation of findings
6	CH	2	73	Who defines what is suitable?		x	Added new 2.73a (now 2.73): V&V may occur in parallel at different levels of independence (for example V&V carried out by testers independent from developers in the original development organisation, plus independent V&V carried out by a separate organisation).		
7	CH	2	74	What is the difference between documented and recorded?	dito	x	deleted recorded.		
21	USA	2	74	Suggest adding a paragraph as follows: If anomalies are detected in the V&V stage, the resulting design modifications and their implementation should be subject to the same V&V process performed previously.	We should consider iterative applications of V&V, not only record anomalies and stop there (as discussed in 2.74).	x			
8	CH	2	75	If there is a difference, why only recorded in this case?	I hope it does not mean voice recording!!!!	x	Technical communications between the V&V teams, system integration teams, commissioning teams and the system designers and developers should be documented.		
10	RF	2	77	Provide reference to PSA Safety Standards	In order to make the requirement more specific we propose to provide a reference to the necessary Safety Standard.		Already covered in 2.78?	x	The implementation guideline "how" or "when" it should be done is outside the scope.
21	FR	2	79	2.79. Safety assessment of I&C should be conducted according to the requirements of GS-R-4, Ref. [7] and the recommendations of SSG-2, Ref. [16] and SSG-3, Ref. [14].	PSA should also be reference as they are a means to assess safety	x			
22	USA	2	80	Revise clause as follows: "Design analyses and verification and validation, should be performed to confirm that all design basis requirements of the overall I&C architecture and each individual I&C system are met, and that all requirements are as intended."	This clause described the activities associated with "verification" but not "validation" as defined in the glossary.	x	Design analyses and verification and validation should be performed to confirm that all design basis requirements of the overall I&C architecture and each individual I&C system are met.		
22	FR	2	81	Transfer 2.81 before 2.96	Current location is not appropriate. 2.93 to 2.95 deals with design requirements			x	We believe that current position is correct.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
9	CH	2	82	….FMEA is often used…. / ….FMEA should be used….				x	FMEA is not the only method.
23	FR	2	82	Defence-in-Depth and Diversity Analysis. Defence-in-Depth and Diversity Analysis is one of the means of investigating vulnerability of safety systems to common cause failure*. ~~See NP-T-3.12, Ref. [12]. *~~ See NP-T-3.12, Ref. [12], gives additional information on this topic.	NP-T-3.12 is not a safety standard.	x			
23	USA	2	82	6th bullet: Rewrite clause as follows: "Security testing. Security testing usually ~~involves~~ requires input from a vulnerability assessment and ~~respect~~ should confirm the use of security good practice."	Security analysis and security testing are two very different concepts and should not be stated as being equivalent as this clause implies.	x			
24	FR	2	83	Locate 2.83 at the end of 2.84	2.84 is on the definition of the methodology for analysis as well as analysis input. Assumptionds (2.83) are therefore a specific aspect of 2.83			x	We believe that current position is correct.
25	FR	2	85	Locate 2.86, as modified, before 2.85	2.86 is the recommendation about reliability claim justification. 2.85 gives indication on what claims could be reasonable….			**x**	**We believe that current position is correct.**
26	FR	2	86	Delete reference annex 3	Annex 3 is giving information on some MS practices and compiles information for which consensus was not obtained during consultancy meeting. Therefore, it should not be in the safety standard and a TecDoc would be more appropriate.			**x**	**Deleting Annex 3 would challenege a consensus reached among MS participated in the development of DS 431.**
4	UK	2	89	"….plant and I&C system maintenance.."	Clarity	x			
10	CH	2	91	What is meant with operating organization? Utility/plant or MCR-staff?	If MCR-staff it goes too far		What is MCR? Main control room	x	This is IAEA terminology
25	USA	2	91	o. Operating instructions, emergency operating procedures, and severe accident guidelines, to cover all normal operation modes and postulated accident scenarios;		x	Might be better to add a separate bullet		
24	USA	2	91	g. As-built location of systems and their main components, including sensors and actuators;	The location of sensors and actuators are very important for maintenance and accident response.	x			
11	CH	2	94	2.95...Unclear, what comes first (feedback)				x	This is correct statement.
5	UK	2	97	Add a new bullet: k. Robustness to the full range of operating environment associated with normal and accident plant conditions and foreseeable internal and external hazards	Consistency with 2.135 bullet h.	x			
6	UK	2	97	Add a new bullet: "l. Facilities and features required for maintenance."	Omission from draft	x			
27	FR	2	98	Delete 2.98	Superfluous as covered by 2.102 and 2.104			x	We believe that this is not superfluos.
26	USA	2	98	Where design constraints are necessary, they should be specified, justified, ~~and~~ traceable, verified and validated.	The constraints must also be verifiable and validated.			x	Do we have a different understanding of "constraints"? I wouldn't V&V the constraints, I would V&V the system to ensure it managed despite them.
28	FR	2	99	Transfer 2.99 into bullet g. of 2.97	Same topic			x	We do not combine informative and normative pars together.
27	USA	2	100	Specific processes should be used to manage requirements throughout the life cycle and to ensure that all requirements are fulfilled, verified, validated, and implemented.	There should be a validation requirement included in this section.	x			Ties in with US comment on 2.69. If this is achievable I would support it.
12	CH	2	100	What are specific processes? Controlled / documented processes?				x	This is correct statement.
13	CH	2	102	… using a predetermined combination …Explain? Why not just e.g. .. documented unambiguous and traceable…				**x**	**This is correct statement.**
28	USA	2	104	The origin of and rationale for every requirement should be defined, to facilitate verification, validation, traceability to higher level documents and demonstration ~~that all relevant design basis requirements have been accounted for~~ of an accounting of all relevant design basis requirements.	Include validation in this section. Also rephrase the section to remove the dangling preposition.			x	1st part: Accept 2nd part: Reject. Change to end of sentence is for the sake of an archaic rule that in this case reduces comprehension
29	FR	2	104	Locate 2.104 after 2.108	More logical order as other paragraph are addressing the requirements (and not their origins)	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
30	FR	2	109	Restructure as follows, using 2.115 as a footnote : 2.109. ~~2.118.~~ Pre-developed items should have documentation that gives the information necessary for their use in the I&C system. 2.110 Pre-developed items should be appropriately qualified* in accordance with the guidance given in paragraphs 6.79 through 6.135. ~~2.115~~ * Qualification of a COTS device could be more difficult because commercial development processes may be less transparent and controlled than those described in this guide. Often qualification is impossible without cooperation from the vendor. The difficulty with accepting a COTS device may often be with the unavailability of the information to demonstrate quality and reliability.	More logical order : - documents should be available to demonstrate COTS adequacy for use in I&C ; - qualification is a pre-requisite and documents are needed as part of demonstration of qualification		Avoid footnotes	x	We do not combine informative and normative pars together. We avoid footnotes.
14	CH	2	110	Delete “Commercial off the shelf (COTS) devices”,	All other listed items are or can be COTS devices			**x**	**This is correct statement.**
31	FR	2	110	Transform 2.110, 2.111, part of 2.115 as footnote to 2.109 : - 2.109. Pre-developed items* should be appropriately qualified in accordance with the guidance given in paragraphs 6.79 through 6.135. * Pre-developed items might be hardware devices, pre-developed software (PDS), commercial off the shelf (COTS) devices, digital devices composed of both hardware and software, hardware devices configured with hardware definition language or pre-developed functional blocks usable in a HDL description. Often the pre-developed items selected are commercial off the shelf (COTS) devices. Use of COTS devices might reduce costs and design effort. Furthermore, there may be no nuclear specific device available and use of well-proven commercial product could be more effective or more safe than development of a new item. 2.115. COTS devices tend to be more complex, may have unintended functionalities and often become obsolete in a shorter time. They will often have functions that are not needed in the nuclear power plant application.			Avoid footnotes	x	We do not combine informative and normative pars together. We avoid footnotes.
15	CH	2	112	2.113, Delete here	Belongs to design, 2.112 covered by 2.122			x	This is correct place.
11	RF	2	117	We propose to reformulate sentence	It is not clear what “cases” and what “dependencies” are mentioned.			x	First part of the sentence provides explanation.
12	RF	2	122	We propose to delete sentence.	The document deals with I&C systems important to safety.			x	We believe that current wording is correct.
29	USA	2	123	Design rules should be established to ensure that the internal logic of each I&C system is amenable to verification and validation.	Include validation in this section.	x			
30	USA	2	124	The design should account for I&C parameters that need to be configurable, verified, and validated during operation …	Whether I&C parameters are configurable is independent of the need to verify and validate the parameters.	x			
32	FR	2	126	A consistent configuration of verified modules (hardware and software) should be ~~submitted~~ available prior to the beginning of to system integration.	Submission to who ?	x			
16	CH	2	126	What else?				x	Do not undesrtand comment
31	USA	2	130	Last sentence: “These may be included in commissioning tests provided that the results are included into validation test records and appropriate independence, as defined in Clauses 2.71 and 2.72, is maintained between the design team and the validation team.	The reference to “appropriate” independence is ambiguous. Clauses 2.71 and 2.72 provide direct guidance on this matter and should be referred to.	x	I suggest "… appropriate independent (see 2.71 and 2.72) is maintained…"		
17	CH	2	130	2.134. Belongs together?				x	We do not combine informative and normative pars together.
18	CH	2	131	It should be the final system which will be implemented in the plant!!!				x	Existing text is more pragmatic
33	FR	2	131	Combine as follows: - 2.131. The system subjected to validation testing should be representative of the final configuration of the I&C system at the site. - ~~2.132.~~ if software is used, The software subject to system validation should be identical to the software that will be used in operation.	Same idea in both paragraphs. The one on software could be superfluous but is kept for clarity.			**x**	**We prefer keeping the existing text.**

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
19	CH	2	132	Of course				x	What is the recommendations?
20	CH	2	134	Covered by 2.130? if not include in 2.130				x	We do not combine informative and normative pars together.
7	UK	2	135	Robustness and fault tolerance	Consistency with 2.97	x			
34	FR	2	137	Combine 2.136 and 2.137	Same topic.			x	We do not combine informative and normative pars together. We avoid footnotes.
35	FR	2	141	Locate 2.141 before 2.140	More logical order. 2.140 deals with documentation and is applicable whether validation uses statistical techniques (2.139) or simulators (2.141)	x			
13	RF	2	145	We propose to give explanation what «commissioning tests» means	It is not clear – who (also when and where) should do «commissioning tests».			x	The implementation guideline "how" or "when" it should be done is outside the scope.
36	FR	2	148	Combine 2.148 with 2.147	Same topic.			x	We do not combine informative and normative pars together. We avoid footnotes.
37	FR	2	150	During the commissioning period all I&C systems should be operated ~~for an extended time~~ under operating, testing and maintenance conditions that are as representative of the in –service conditions as possible	The notion of extended time is not sufficiently precise			x	We agree it is not precise but communicates an idea that is lost if deleted
21	CH	2	151	Covered by 2.1.40? if not include in 2.140				x	There is a difference between these two paras.
38	FR	2	153	Combine 2.153, 2.154, 2.155 into a single paragraph	The 3 paragraphs are dealing with NS-G-2.6	x	Combined 2.153 and 2.154.		
22	CH	2	158	Adequate quantities of spare parts and components. What is the difference between spare parts and components in this case?		x	Deleted Components.		
8	UK	2	158	Add “throughout the intended service lifetime.”	Clarity	x			
23	CH	2	160	d) Delete possible	There is always a need, even if only a part no. changes	x			
32	USA	2	165	Insert after: Suggest adding an item as follows: 2.159. V&V should be conducted after each I&C modification. Alternatively, 2.165. The life cycle for even the simplest changes should include at least the phases of the individual system life cycle shown in Figure 2, including V&V after each I&C modification.	V&V should be always performed after design/implementation changes.	x	2.165 modified as suggested.		
39	FR	2	165	Combine 2.165 with 2.164	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
24	CH	2	167	**Hardly realistic and manageable/ feasible especially for process level (sensors/actuators) Can be counterproductive due to additional complexity/interfaces**				x	This is a regular practice when replacing I&C systmes imprtant to safety. It does not say thart sensors must be duplicated too.
40	FR	2	167	When an I&C system is replaced, running the new I&C in parallel with the old system for a probationary period…could be considered	There could be constraints that doesn’t allow this practice (no sufficient room for example)			**x**	**This is allowed for by saying it should be considered rather than it should be done.**
1	Spain	2	168	When considering parallel operation of I&C systems, the interim configuration shall not cause inacceptable adverse effects on nuclear safety. The disadvantages of operational problems and added complexity should be weighed against the gain of confidence.	Additional emphasis on nuclear safety is placed in this paragraph.			x	We believe that current wording is sufficient.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
41	FR	2	168	Combine 2.168 with 2.167 : 2.167. When an I&C system is replaced, running the new I&C system in parallel with the old system for a probationary period, i.e., until sufficient confidence has been gained in the adequacy of the new system should be considered. ~~The equivalent of parallel operation might be possible by installing new redundant equipment in one train at a time. 2.168.~~ When considering parallel operation of I&C systems, the disadvantages of operational problems and complexity should be weighed against the gain of confidence, and the risks should be evaluated. The equivalent of parallel operation might be possible by installing new redundant equipment in one train at a time.	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
33	USA	3	5	The required functions (and corresponding requirements for properties such as safety, security, and timing constraints) of the I&C systems should be determined as part of the nuclear power plant design process.	§2.69 scope includes validation of non-functional requirements; however, DS431 does not mention anything about how these are created. Requirements for such properties should flow down from the NPP-level analysis. See reason later for avoiding the term: non-functional."	x	Better to write "The required functions (and corresponding non-functional requirements) of the …		
42	FR	3	6	• Provide information necessary to Mitigate the radiological consequences of significant releases of radiation.	I&C can not mitigate a release…			x	It referes to I&C "functions" that provide "informations" …..
43	FR	3	9	Transform 3.10 as a footnote of 3.9 : 3.9. The overall I&C architecture* and each I&C system should have a documented design basis. ~~3.10.~~ *The overall I&C architecture is the organizational structure of the plant I&C systems. The overall I&C architecture of a nuclear power plant includes multiple I&C systems, each playing specific roles.	3.10 is somehow a definition			x	We do not combine informative and normative pars together. We avoid footnotes.
9	UK	3	11	This information will then be used to categorize the functions and assign them to systems of the appropriate class.	Consistency with 3.13 bullet c and accepted good practice	x	3.11. The design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system. This information will then be used to categorize the functions and assign them to systems of the appropriate class.		
44	FR	3	11	Transform 3.12 as a footnote of 3.11 : - 3.11. The design basis identifies functions, conditions and requirements* for the overall I&C and each individual I&C system. This information will then be used to allocate functions to each I&C system and to identify the safety classification of I&C systems. Also, the design basis will be used to establish design, implementation, construction, testing, and performance requirements. ~~-3.12. Note that~~ *in some instances, I&C system requirements will be identified as the nuclear power plant design and design basis are developed. Thus, the complete content of the I&C design bases might not be available at the beginning of the project.	3.12 is not a recommendation but an acknowledgement of reality…			x	We do not combine informative and normative pars together. We avoid footnotes.
45	FR	3	13	e. ~~Member State~~ National requirements for I&C licensing, ~~, f. Member state requirements~~ for I&C safety classification~~, g. Member State requirements with respect~~ or relating to operational requirements,	Group into one bullet national requirements, whatever their topic			x	The IAEA does not refer to National requirements.
25	CH	3	14	Isn't this covered by 3.14 a 8 (functional requirements)				x	No
26	CH	3	14	The individual I&C system role		x			
27	CH	3	14	Combine in 2 or put 4 after 2	Better readability			x	Do not undesrtand comment
28	CH	3	14	Location and interfaces are different things, should be separated here				x	
46	FR	3	14	d. 4.The range of plant environmental conditions under which the system is required to perform functions important to safety; Plant environmental conditions of concern include the normal conditions, abnormal conditions, and the extreme conditions that I&C equipment might experience during ~~design basis~~ accidents, internal events, or external events.	No reason to exclude DEC from accidents to consider. Actually, Fukushima Daiichi accident clearly showed the need to have some I&C still working….	x	clarify to: "accidents (including all design basis accidents)"		

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
34	USA	3	14	d. 4.…Plant environmental conditions of concern include the normal conditions, abnormal conditions, and the extreme conditions that I&C equipment might experience during design basis accidents, internal events, or external events. Also included are conditions such as interactions across I&C systems and components qualified to different levels (degrees).	The addition alerts the DS431 reader to a new kind of contributory hazards arising from the introduction of interconnections and software.	x	**Kept as originally proposed with UK suggestion "degrees".**		Better to write "… and components qualified to different degrees."
47	FR	3	16	Locate 3.16 after 3.14	3.16 gives additional recommendations to 3.14 and 3.15 is applicable both to 3.14 and 3.16 items.	x			
35	USA	3	16	3.16. a. "…see paragraph 6.209 and figure 3);"	The correct figure number is figure 3.	x			
29	CH	4	1	4.13. Sort of redundancy / repetition?	Combining may provide better readability			x	We do not combine informative and normative pars together.
50	FR	4	1	Delete 4.10	Superfluous			x	We believe that this is not superfluos.
36	USA	4	1	4.1. 1st bullet· The ~~high level definition~~ identification of the comprised I&C systems, including the requirements (and constraints) allocated to them, definition of their boundaries, and relationships (including interactions) with their environments. Constraints include prohibited interactions and behaviors;	The term "high level definition" is ambiguous. The addition provides clarity.			x	Too much detail at this point
37	USA	4	1	2nd bullet The ~~tiered structure~~ organization of these systems, including inter-relationships, required interactions and resulting behaviors, and prohibited interactions;	The term "tiered structure" is too presumptuous. "Organization" is more general. The 'inter-relationships, interactions, etc." elaborate on the information content implied in the term "organization. "Use "allocation" for consistency with usage at other places in			x	See above. Although accept that "organisation" may be better than "tiered structure"
38	USA	4	1	3rd bullet The ~~assignment~~ allocation of I&C functions and behaviors (including behavior-constraints and prohibitions) to these systems, and	DS431."Functions" provide static information only. Information is needed on both, the behaviors required and prohibited.			x	See above. Although accept that "allocation" is better than "assignment"
39	USA	4	1	4th bullet The communication~~s~~ channels between I&C systems and their topology ~~of communication links~~, the interaction communications allocated to them, and the communications prohibited.	The term "communications" might imply content such as messages; that is not necessary at this early stage. In the previous bullet, the addition of "interactions": provides the information that might have been intended here. The term "channel" implies the presence of a connection (link).The "allocation of interaction to channel" is an elaboration of the basic definition of the term "architecture." "Prohibitions" serve as information to evaluate whether unwanted interactions are prevented.			x	See above.
48	FR	4	2	Locate 4.2 after 4.9	Independence is one way of achieving DiD	x			
40	USA	4	2	The overall I&C architectural design also establishes the level of independence between the I&C systems that support the different levels of the plant's defence in depth and diversity concepts.	Need to identify conditions that might compromise diversity. Trend of increasing interconnections is increasing the hazard space of common causes and contributing factors, i.e. threatening to compromise diversity.	x			
41	USA	4	3	3rd bulletThe hierarchical structure of subsystems and the hierarchical structure of individual I&C items within subsystems, the behavioral relationships across items and subsystems, the required interactions, and the interactions prohibited;	Applying the basic definition of architecture to the intra-system level.			x	Too much detail at this point
42	USA	4	3	4th The ~~assignment~~ allocation of I&C functions and behaviors (including behavior-constraints) to individual I&C items;	Applying the basic definition of architecture to the intra-system level.			x	See above. Although replace "assignment" with "allocation"
43	USA	4	3	5th The ~~layout of~~ communication channels between items and subsystems within the individual I&C system, the interaction communications allocated to them, and the communications prohibited; and	Applying the basic definition of architecture to the intra-system level.			x	See above
44	USA	4	3	6th The partitioning to avoid unnecessary system complexity and unnecessary interactions between individual I&C system elements, and to prevent propagation of a fault that might degrade the performance of a safety function.	The added information item is needed for safety evaluation of the architecture			x	See above

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
45	USA	4	4	Modern I&C systems are more ~~integrated~~ interconnected and more ~~complex~~ difficult to analyze (and thus more difficult to assure) than were the earlier generations of I&C systems. A well designed I&C system architecture will ensure ~~proper implementation of a~~ defence-in-depth and diversity ~~concept~~ and ~~locate~~ localize and contain ~~essential complexity in~~ difficult-to-analyze features in systems ~~where it can be better managed or~~ where ~~it~~ these features will ~~pose less risk to~~ not render plant safety unassurable.	Need to identify conditions that might compromise diversity. Trend of increasing interconnections is increasing the hazard space of common causes and contributing factors, i.e. threatening to compromise diversity. Use of the word “integrated” in this manner is improper; proper integration should not introduce adverse effects. This clause is concerned with interconnection ignoring proper integration. The term “complex” does not have a broadly-accepted, well-understood meaning. The expression “difficult to analyze …” serves the intended purpose and aligns with the familiar relationship Analysis assurance. The terms “localize” and ”contain” align with the well-understood fault-containment concept. The term “managed” introduces ambiguity unnecessarily. This clause introduces unnecessarily “pose less risk”; it is difficult to evaluate when the causes are systemic. The intended purpose can be satisfied by building on the relationships: Assurability Verifiability Analyzability	x			
46	USA	4	5	The overall I&C architecture and the individual system architectures should satisfy the plant requirements, including system interfaces, ~~performance~~ requirements for properties such as safety, security, verifiability, analyzability, and timing constraints, ~~(e.g., timing and reliability)~~, and ~~facilitate achievement of computer security goals~~ prevent interactions that could degrade a safety function.	The term “performance” can be misinterpreted to imply “short response time” or “speed” or “throughput”; by themselves, these do not satisfy the safety property. Generalization through the phrase “requirements for properties …” provides the broader coverage intended with the list of examples. For background information on this approach, see the SQuaRE series of ISO standards and the “Software Engineering Institute” web pages for “Quality Attributes.” Requirements for such properties are colloquially called “non-functional requirements”; however, the authorities mentioned above do not support the use of this term. The example list should focus on the most important properties, starting with Safety and Security. Since Security fits well in the list of properties, a separate clause for security is not needed. Addition of “prevent interactions that could degrade a safety function” alerts DS431 users to the potential of such interactions when interconnecting different systems.	x	**The overall I&C architecture and the individual system architectures should satisfy the plant requirements, including system interfaces and requirements for properties such as safety, security, verifiability, analyzability and timing constraints**		But no need for last addition. I suggest: … including system interfaces and requirements for properties such as safety, security, verifiability, analyzability and timing constraints.
49	FR	4	7	Merge 4.7 with 4.6	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
47	USA	4	8	The overall I&C architecture should not compromise the defence-in-depth and diversity ~~strategy~~ strategies of the plant design.	Need to identify conditions that might compromise diversity. Trend of increasing interconnections is increasing the hazard space of common causes and contributing factors, i.e. threatening to compromise diversity.	x			
31	CH	4	11	g/h/I, This is basis I&C know how / business/ matter of course, what of it is “safety guidance”?				x	What should be included in the I&C architecture.
10	UK	4	11	Add “and maintainability” to the 1st sentence.	Clarity – factors associated with maintenance need to be considered here.	x	Strategies for achieving reliability requirements might include, for example, compliance with the single failure criterion, redundancy, independence between redundant functions, fail-safe design, diversity, testability and maintainability.		But it reads strangely now….
51	FR	4	11	c. Identify the individual I&C systems that will be included in the overall I&C architecture in order to: 1. Support the plant defence-in-depth concept; 2. Support overall I&C design basis requirements for independence; and 3. Adequately separate systems and functions of different safety classes; 4. Ensure adequate diversity where required	Diversity issue is missing.	x	c. Identify the individual I&C systems that will be included in the overall I&C architecture in order to: 1. Support the plant defence-in-depth and diversity concepts; 2. Support overall I&C design basis requirements for independence; and 3. Adequately separate systems and functions of different safety classes.		
52	FR	4	11	g. Provide necessary information in the main control room, the supplementary control room, and other areas where information is needed for operation or managing accident ~~management~~;	Accident management is defined in the IAEA Safety Glossary. It use here would be too restrictive	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
53	FR	4	11	h. Provide necessary operator controls in the main control room, the supplementary control room, and other areas where controls are needed for operation or managing accident ~~management~~; and	Accident management is defined in the IAEA Safety Glossary. It use here would be too restrictive	x			
48	USA	4	11	Support the plant defence-in-depth and diversity concepts	Need to identify conditions that might compromise diversity. Trend of increasing interconnections is increasing the hazard space of common causes and contributing factors, i.e. threatening to compromise diversity.	x			
49	USA	4	11	d0 Define the interfaces and ~~means~~ channels of communications between the individual I&C systems	Channel allows for an abstract definition. Means might imply a physical means – that information is not necessary at the early stages of safety evaluation.			x	Means equally allows for abstract definition.
50	USA	4	11	e) Establish the design strategies to be applied to fulfill the ~~reliability~~ requirements of each safety function allocated to the overall I&C architecture, including the corresponding properties and derived constraints to prevent the degradation of the safety function	The appended addition broadens the statement and focuses it on safety. Then “reliability” is not necessary.			x	This removes the central thrust of the requirement, which is about reliability.
51	USA	4	11	e) Strategies for achieving ~~reliability~~ these requirements might include, for example, compliance with the single failure criterion, redundancy, independence between redundant functions, fail-safe design, diversity, and verifiability (including: analyzability; testability). Section 7 discusses considerations in implementing strategies to achieve reliability.	See reason above. The list of examples should focus on the properties or characteristics next-closest to SAFETY, e.g.: Assurability, Verifiability, Analyzability “Testability” is not sufficient. Verifiability is more general and allows for a combination of many approaches, e.g. Analysis.			x	See above
32	CH	4	12	Basics/matter of course				x	There is no recommendation.
4	ISO/ WNA	4	15	4.15. The overall I&C architecture should neither compromise the independence of safety system divisions, nor the independence implemented at the different levels of the plant defence-in-depth concept systems **as far as is practicable.**	Requirements not completely consistent with “4.6. SSR 2/1 Requirement 7 states: The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable »			x	SSR 2/1 has a general validity. The objective of DS 431 is to further develop SSR requreirements. This is wat wewant to accomplish in the I&C architecture.
33	CH	4	17	4.18. Basic requirements, belongs to architectural design				x	Disagree.
54	FR	4	17	Merge both paragraph and limit their application to I&C : 4.17. For I&C, Safety systems should be independent from systems of lower safety classification and~~.~~ ~~4.18.~~ Redundant divisions within safety systems should be independent of each other. Exchanges between divisions of a same system could be used when specifically justified..	Clarification: It could be useful to share information from other division (for example for vote)	**x**	We prefere keeping it separate. 4.18 chaged as follows: Redundant divisions within safety systems should be independent of each other to the extent necessary to ensure all safety functions can be accomplished when required. Where communication between divisions is necessary, for example for voting or partial trip, there should be sufficient measures to ensure electrical, physical and information separation. Communication for voting can limit spurious actuation caused by random failure, which could jeopardize safety		Confuses the main requirement. More explanation would be necessary to introduce this idea without compromising the essential principle.
5	ISO/ WNA	4	18	Redundant divisions within safety systems should be independent of each other unless sufficient measures are implemented to insure appropriated electrical and physical separation.	The commonly used nuclear industry design exchanges analog / binary measurements between the divisions to increase the reliability of the systems. à Not to use the exchange of the values leads to a late detection of a sensor fault (only if threshold is activated). By installing specific measures to ensure sufficient electrical / physical separation between the divisions, exchange of data should be permissible.	x	See above proposal.		It may be possible to add some text to clarify the role of information exchange that cannot compromise the safety function, but the essential principle should remain.
55	FR	4	26	Merge 4.26 with 4.25	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
11	UK	4	27	Add “or errors in maintenance.”	Clarity and consistency with 4.39	x			
52	USA	4	27		This ignores software as a source of common-cause failure.			x	
34	CH	4	28	Repeats (in my opinion) what is already stated in 4.8/4.9/4.15				x	There different subheadings
30	CH	4	30	4.13. Sort of redundancy / repetition?	Combining may provide better readability			x	We do not combine informative and normative pars together.
35	CH	4	31	Why should a CCF not to be considered and how can it than be justified?				x	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
56	FR	4	31	Merge 4.31 with 4.30	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
36	CH	4	39	Diverse systems* can be subject to the same error in specification but rarely to the same errors in design, fabrication. That's why they are diverse!	* Except that there is only "functional" diversity provided and using a common platform (HW/SW)			x	True statement, that is why we keep it here.
57	FR	4	39	Delete 4.39	An error could always occur, whether it is a diverse system or not…			x	This is correct, that is why we would like to avoid this situation to occur.
53	USA	4	40		Use of common software is also a reason for not treating items as fully independent.			x	
54	USA	4	40	Probabilistic studies should not treat I&C items important to safety as fully independent unless they are diverse, and meet the criteria ~~guidance~~ for ~~functional~~ independence (examples of dependence: functional; data or information; services or, resources for computing, communication or storage; environmental conditions; conceptual), electrical isolation, ~~communications independence~~, environmental qualification, seismic qualification, electromagnetic qualification, physical separation, and protection against internal events given in this document.	Even if the DS431 guidance may not specify criteria, the system engineering process should specify and satisfy criteria. Dependencies are not only functional. The proposed list of examples provides a broader coverage.			**x**	**This degrades the critical requirements for functional and communications independence**
58	FR	4	41	Transform 4.41 into a footnote to 4.40	4.41 explains how independence is credited in PSA…			x	We do not combine informative and normative pars together. We avoid footnotes.
1	UK Def	5	0	The previous Safety Std (NS-G-1.3) included clear definitions and examples of the safety classification scheme, complete with a useful illustration (Figure 1 in NS-G-1.3). Please re-instate and update these examples.	This will help provide clarity and consistency in the application of the safety classification.			x	Safety Glossary and DS 367 Classification guide use different classification scheme.
59	FR	5	1	Group 5.1 to 5.5 in a single paragraph	These are all quotation of SSR-2/1.			x	This would be a very cumbersome single paragraph.
14	RF	5	5	Delete sentence	The reference to DRAFT is not aceeptable			x	Update if possible
60	FR	5	6	Delete 5.6	Does not bring any new information.			x	That depends on the knowledge of the reader!
38	CH	5	8	Hen and egg situation?? Can safety I&C cause a PIE?				x	Strongly dissagree.
6	ISO/ WNA	5	8	The possibility that the failure or spurious operation of an item important to safety may directly cause a PIE, or **that the failure on demand of an item important to safety may make the consequences of a PIE worse**, should be considered when the list of PIE is established.	Spurious is unlikely based on use of highly reliable platform that decrease spurious failure occurrence and measures taken at development Life cycle and associated V&V levels place CCF leading to spurious actuation at residual risk. Nevertheless robustness analysis against potential spurious actuation can be performed to check robustness of the plant design against these postulated failures considered as beyond design basis. Consideration of the superposition of Spurious operation with independent PIE is even more unlikely and shall not be considered. Moreover, there is no consensual practice between in all member states on this question.	x	**The possibility that the failure or spurious operation of an item important to safety may directly cause a PIE, or that the failure on demand of an item important to safety may make the consequences of a PIE worse, should be considered when the list of PIE is established.**		We prefer keeping existing simple text; "failure" has a broader meaning, which includes failure on demand.
39	CH	5	9	This must be done / is done already before. See architecture 4.1 / 4.3				x	Compliance with the IAEA classification safety guide DS 367
40	CH	5	10	*All* the I&C system functions ….	Because of comment 39	x			
41	CH	5	10	5.10 .. categorized… (function/SW?) 5.11 ..identified and classified (HW?) Must be performed before architecture is designed				x	Compliance with the IAEA classification safety guide DS 367
61	FR	5	10	The I&C system functions should then be categorized on the basis of their safety significance, ~~using a constant risk approach~~, with account taken of the three following factors…	This wording was deleted from DS367	x			
55	USA	5	10		The frequency of occurrence of events related to spurious actuations or to malfunction of digital systems cannot be determined, since digital system reliability cannot be quantified.			x	
56	USA	5	12		I&C system failures would include the results of software problems, which are not amenable to this sort of analysis that would be required to meet this provision.			x	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
42	CH	5	13	.. However, a larger or smaller number of categories and classes may be used if desired…Isn't categorization and classification defined / given by the standards, i.e. IEC 61226 and 61513?				x	Compliance with the IAEA classification safety guide DS 367
62	FR	5	13	Delete 5.13	Superfluous (not used in this guide)			x	We believe that this is useful information.
63	FR	6	4	Merge 6.4 with 6.2	Same topic (complexity)			x	We do not combine informative and normative pars together. We avoid footnotes.
64	FR	6	6	Group 6.6 to 6.8 in a single paragraph	These are all quotation of SSR-2/1.			x	Would give a cumbersome paragraph
57	USA	6	10	Recommend moving Clause 6.13 to the beginning of the Single Failure Criterion section and revising as follows: Single Failure Criterion: Definition: Each safety group should perform all actions required to respond to a PIE in the presence of the following:a., b., c., d., e.. …	The discussion of single failure applicability should begin with a definition of what SFC actually is. Clause 6.13 seems to define what the SFC is, but it does not state this. This definition should be the first thing in the section and should precede all other clauses that use the SFC term.			x	This claus is taken from the IAEA SSR 2/1 and cannot be modified. SFC is dfefined in the IAEA Safety Glossary.
65	FR	6	10	Merge 6.10 and 6.11	These are all quotation of SSR-2/1			x	Would give a cumbersome paragraph
58	USA	6	11		There can be many possible spurious actuations, including some that may not be anticipated. It is not clear how the phrase "one mode of failure" should apply to these. This provision of the SSR should be explained and clarified in this Safety Guide.			x	
7	ISO/ WNA	6	13	6.13. Each safety group should perform all actions required to respond to a PIE in the presence **of any single failure, detectable within the safety system, in combination either**: ~~a.~~ ~~Any~~ ~~single~~ ~~detectable~~ ~~failure~~ ~~within~~ ~~the~~ ~~safety~~ ~~system~~ ~~in~~ ~~combination~~ ~~with:~~ a. Any undetectable failures, i.e., any failure that cannot be detected by periodic testing, alarm or anomalous indication, b. All failures caused by the single failure, c. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety group, and d. The removal from service or bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions.	The listed failures shall be not combined all together. Only single detectable failures should be combined with items listed in the paragraph. It could be misunderstood, that the items should be combined not only with the single failure even also with the other items.	x	**Each safety group should perform all actions required to respond to a PIE in the presence of any single detectable failure within the safety system in combination with:** **a. Any undetectable failures, i.e., any failure that cannot be detected by periodic testing, alarm or anomalous indication;** **b. All failures caused by the single failure and the undetectable failures;** **c. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety group, and** **d. The removal from service or bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions.**		
59	USA	6	13		This should be clarified to specify that the Safety Group must not rely on any entity in a lower safety classification (especially nonsafety) to perform the required functions or to cope with the listed points "a" through "e."			x	
2	Spain	6	13	b) All undetectable failures, i.e., any failure that cannot be detected by periodic testing, alarm or anomalous indication,	Since this kind of failures are not detected by periodic testing, alarm, etc. all of them should be assumed to be present at the time the system has to perform its function. The proposed wording avoids any misunderstanding.	x			
3	Spain	6	13	c) All failures caused by the single failure <u>and the undetectable failures</u>,	There is no reason to exclude failures caused by undetectable failures unless they are also considered undetected failures. If so, this comment does not apply.	x	**See comment resolution on ISO#7 above.**		
60	USA	6	14		Exclusion of "design errors" can be read as excluding consideration of software-related problems. Section 4 also omits explicit consideration of software-related problems. Because such problems can be difficult to deal with, they should be explicitly addressed.			x	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
61	USA	6	15	"Non-compliance with the single failure criterion should be ~~exceptional,~~ considered as an exception to regulatory guidance. Such cases should be identified in design documents and clearly justified in the safety analysis."	The use of the term "exceptional" in this clause could be read to imply that non-compliance with single failure criteria is a desirable or positive thing.			x	6.16 provides more detail
66	FR	6	16	6.16. For a safety group, non-compliance with the single failure criterion may be justified for…	Clarification	x			
62	USA	6	16		The listed justifications for noncompliance with the single-failure criterion are not quantified, and in some cases (especially software-related issues) are based upon an undefined assessment of unquantifiable criteria. The final bullet allows for noncompliance with no firm criteria at all. Item 6.16 is entirely unacceptable as written.	x	**IAEA propose to delete the entire para.**		
63	USA	6	17	"…systems ~~that~~ that are necessary…"	Editorial	x			
64	USA	6	18		Reliability analyses and probabilistic assessment are not applicable to software. Operating experience is not likely to be of sufficient duration and is not likely to include sufficient occurrences of applicable stimuli to be useful for quantitative assessment of modern digital systems. Engineering judgment can easily become a matter of opinion that multiple practitioners do not agree upon and that can be used to justify questionable practices.			x	
65	USA	6	19	Re-word Clause 6.19 as follows: "Maintenance, repair and testing activities should be consistent with plant operating limits and conditions even in situations in which the single failure criterion is not met."	Maintenance, repair and testing activities should be consistent with plant operating limits and conditions regardless of whether the criteria for single failure are met.	x			
66	USA	6	21	"I&C systems should be redundant to the degree needed to meet the I&C reliability requirements and single failure criterion."	Redundancy is also a means of meeting SFC criteria.	x			
67	USA	6	22	Suggest removing the third sentence which states: "Taken alone, redundancy increases the reliability, but it also increases the probability of spurious operation."	This sentence is not closely related to the main topic of the paragraph. Also it may not be always accurate in all circumstances.	x	**Redundancy is commonly used in I&C systems to achieve system reliability goals including conformity with the single failure criterion. Redundancy is not fully effective unless the redundant elements are also independent. In general, redundancy increases the reliability, but it also increases the probability of spurious operation. Coincidence of redundant signals (voting logic) or a rejection scheme for spurious signals is commonly used to obtain an appropriate balance of reliability and freedom from spurious operation.**		But suggest changing "Taken alone..." to "In general"
67	FR	6	23	Merge 6.23 and 6.24	These are all quotation of SSR-2/1			x	Would give a cumbersome paragraph
68	USA	6	31	• May be used to protect against common cause failure due to normal, abnormal, or accident environments, the effects of design basis accidents, or the effects of internal and external hazards. Examples include: space to attenuate effect of EMI; separation between systems and components qualified to different levels.	The provided examples would help the DS431 understand the breadth of utility of PHYSICAL SEPARATION.	x			
68	FR	6	31	Second bullet: May be used to protect against common cause failure due to normal, abnormal, or accident environments, the effects of ~~design~~ ~~basis~~ accidents, or the effects of internal and external hazards…	No reason to exclude DEC from the bullet	x	but clarify to: "accidents (including all design basis accidents)"		
69	FR	6	36	Transfer 6.36 in 6.31 bullet list	More logical place			x	Current place seems correct.
70	FR	6	38	Locate 6.38 before 6.35	6.35 deals with exceptions and 6.38 presents places where exceptions may occur.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
8	ISO/ WNA	6	49	6.49. Monitoring systems of lower safety classification may be connected to safety systems provided that it is demonstrated that they cannot disturb them. When safety systems may be connected to maintenance systems of lower safety classification, the connection should be made only: when the affected division or channel is offline **depending on the I&C architecture and the impact to the process**, use of data from the maintenance system is restricted to a specific purpose, and connection of the maintenance system complies with computer security programs.	Depending on the effects of the maintenance measure it could be required to set the related lower classified system to off line. But should not be the typical solution. In case a complete functionality of 1 division is out of order due to a specific maintenance activity. It shall be clearly defined which level of maintenance requires a “off line” division of a system (e.g. for software loading if not sufficient evidence could be provided). The request for “off line” depends on the system architecture. For a typical PS system (realized in 4 redundant trains) maintenance activity should have no impact to the plant (except maintenance on the actuation channel – after voting). For a two-redundant system measures should be in place (e.g. for Master – Hot-Standby Configuration, the maintenance is only allowed in the standby redundancy). A analysis should be performed to verify for which system architecture or which actuation path, preventive measures should be installed to set the system / channel “off line”.			x	The proposed new wording would make the requirement meaningless. The rationale is not sufficiently reflected in the proposed change.
69	USA	6	52	Suggest combining 6.52 and 6.55 as one item, which should read as follows: “6.52. In justified cases signals may be sent from systems of lower to systems of higher safety classification via individual analogue or binary signal lines, provided that: - Credible failures, signals, or commands from the lower class system *do not prevent* the receiving higher class safety system from accomplishing its safety functions. -the potential for failures in the system of lower safety classification that cause spurious actuation of safety components is assessed and shown to be acceptable.”		x	**In justified cases signals may be sent from systems of lower to systems of higher safety classification via individual analogue or binary signal lines, provided that:** **• The recommendation in 6.52 is still satisfied, and** **• The potential for failures in the system of lower safety classification that cause spurious actuation of safety components is assessed and shown to be acceptable.**		
70	USA	6	61	6.61. Examples of different types of diversity include:…Add a 6th bullet: Logic diversity achieved by use of different software/HDL languages, different algorithms, different timing of logical functions, and different order of logical functions.	Section 6.61 provides, as examples of different types of diversity, Design diversity, Signal diversity, Equipment diversity, Functional diversity, and Life cycle diversity. Another important diversity attribute is Logic diversity, which includes different languages, algorithms, timing, and order of logic.	x			
71	FR	6	61	Merge 6.61 with 6.60	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
71	USA	6	71		The classification must be comprehensive, not just “most likely.”	x	**The IAEA propose to delete "most likely" and continue sentnece with " Possible failure modes…".**		
72	USA	6	72	The failure modes that are most likely to result from systematic ~~errors~~ causes in the design of hardware or software are essentially unpredictable. Consequently, the concept of fail-safe design is not effective for dealing with failures resulting from such ~~errors~~ causes. Disciplined development processes (see section 2), Hazard analysis (paragraphs 2.56 to 2.65), the concept of defence in depth (see section 4), and the application of diversity (see paragraphs 6.58 to 6.64) are more effective tools for reducing the number of such ~~errors~~ causes, and coping with the effects of such causes ~~errors~~ that remain.	Given that the predominant systemic cause is “incomplete or inconsistent or ambiguous requirements.” terms such as “failure” and “error” do not apply to the work products of subsequent phases in the development lifecycle. JG:	x			
73	USA	6	73		Failure of self-test, self-alarm, etc. features themselves must be detected and revealed.	x	Added to 6.75 "Failure of self-test, self-alarm, etc. features should be detected and revealed."		
12	UK	6	74	Amend to: 6.74 It is preferred that failures be self-revealing. The mechanism for self revealing faults should not put the system in an unsafe state or result in spurious activation of safety systems.	The current wording could be interpreted to mean that we would prefer that failures that lead to unsafe conditions are not revealed	x			
9	ISO/ WNA	6	75	*Remove paragraph*	As identified failures are detectable, it is suggested to delete this requirement or provide some clarification and/or an example of such fault.			x	"Identified" means awareness of potential, not necessarily a means is provided to detect them.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
74	USA	6	77		This provision is known to cause serious safety violations if the digital system is re-initialized to a state incompatible with the present plant state. For example, a plant was in operation when the digital system re-initialized after a local power transient, and the resulting “safe” state (designed for start-up) was actually dangerous for the present state of the plant equipment & process fluids.			x	
72	FR	6	81	Merge 6.81 with 6.79	Same topic (purpose of qualification)			x	These are two separate requirements
75	USA	6	83		Commercial equipment found suitable for safety service is not likely to have sufficiently well documented design and fabrication history to support qualification based upon past experience or upon manufacturing process or inspections. Qualification of such “dedicated” equipment should be addressed explicitly.			x	
73	FR	6	85	Merge 6.85 and 6.84 : - 6.84. The method, or combination of methods used for equipment qualification should be justified. It is generally not necessary to apply all of the methods mentioned. The specific combination of methods will depend upon the system or component under consideration. For example, the qualification of pre-existing items might place more emphasis on past experience and analysis to compensate for a lack of completely documented verification and validation during engineering and manufacturing. ~~6.85. The method, or combination of methods used for equipment qualification should be justified.~~				x	We do not combine informative and normative pars together. If combined, this opara would become too long.
74	FR	6	87	6.87. For safety systems, qualification evidence based upon operating experience is not enough and is therefore normally combined with type testing, and testing of supplied equipment, as well as evaluation of manufacturers’ production processes, or inspection of components during manufacture.	Clarification	x			
76	USA	6	88		The size and other characteristics of the sample set should be shown to be representative of the population of devices placed into service. For example, qualification based upon one or two devices would not be credible, since such a small sample is unlikely to be representative of the population covered by the qualification. This applies to qualification by test as well as by experience.		**The IAEA propose to keep existing text.**	x	
75	FR	6	89	Combine 6.89 with 6.88	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
76	FR	6	91	Combine 6.91 with 6.90	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
77	FR	6	92	Combine 6.92 to 5.95 in a single paragraph with bullet list: 6.92. The equipment qualification program should demonstrate that the design of I&C systems, and components meet all functional, performance, and reliability requirements contained in the I&C design bases and equipment specifications~~.~~ ~~:6.93.~~ - Examples of functional requirements include, functionality required by the application, functionality required to support system or equipment operability, operator interface requirements, and input /output range requirements. ~~6.94.~~ - Examples of performance requirements include accuracy, resolution, range, sample rate, and response time requirements. ~~6.95.~~ - Examples of reliability requirements include, requirements for a minimum mean time between failures, fail-safe behaviour, independence, failure detection, testability, maintainability, and service life.	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
13	UK	6	97	Add electromagnetic phenomena.	Clarity and consistency with 6.114 to 6.135.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
77	USA	6	97	Revise Clause 6.97 as follows: “In this guide environmental qualification is qualification for temperature, pressure, humidity, chemical exposure, radiation, submergence, electromagnetic compatibility, and ageing mechanisms that affect the proper functioning of components under those conditions.	Electromagnetic compatibility aspects should be included as environmental conditions in this clause. There is a category for Electromagnetic Environment Qualification in 6.114, below.	x			
78	USA	6	109	The plant design basis and the plant’s safety analysis will identify internal and external hazards, such as fire, flooding and seismic events, which the plant is required to tolerate for operation or which the plant is required to withstand safely, and for which protection or system qualification is needed. The plant design basis and the plant’s safety analysis will also identify hazards contributed through systemic causes such as an engineering decision or deficiency that could result in the degradation of a safety function; commensurate system constraints should be identified to prevent the degradation of a safety function.	Alerts the DS431 reader to systemic causes rooted in engineering.			x	The section is about internal and external hazards
79	USA	6	130	~~Emission limits placed on individual components should be below the EMI operating envelope by an amount that is sufficient to ensure that no single item makes a significant contribution to the EMI hazard.~~ Emission constraints placed on individual components should be such that the resultant emission in the operating environment is within the safe (hazard-free) envelope of every component, in all modes or states of the system and the components, including transitions across modes/states and including degraded conditions.	(1) The term “significant contribution” is ambiguous. (2) The term “limit” might imply a single static threshold value. The safe envelope might be a multivariable function. Even when no single item makes a contribution that exceeds the safe envelope of some other item, when assembled and placed in operation, under certain conditions, the resultant emission (compositional effect) may exceed the safe envelope. Known as “emergent behavior” the system and its components should be analyzed for a contributory hazard.	x	Added "EMI" before "envelope" to clarify the requirement is about EMI		
78	FR	6	136	Merge 6.136 and 6.138	These are all quotation of SSR-2/1			x	Would give a cumbersome paragraph
79	FR	6	139	Combine 6.139 and 6.140 as follows: 6.139. The qualified life of electrical and electronics systems and components might be considerably less than plant life. ~~6.140.~~ For example, Age degradation that impairs the ability of a component to function under severe environmental conditions might exist well before the functional capabilities under normal conditions are noticeably affected.	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
80	FR	6	142	Merge 6.142 with 6.141	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
14	UK	6	144	“…degradation (ageing), including the detection of precursors, that could cause…”	Reflects an aspect of effective management of C&I ageing and obsolescence.	x			
81	FR	6	145	Merge 6.145 with 6.144	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
82	FR	6	149	Locate 6.149 before 6.148	More logical order.			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
80	USA	6	152	6.152. At the present time it is expected that ageing or obsolescence may cause the service life of some I&C systems to be significantly shorter than ~~that~~ the plant life.	Correct the typographical errors.	x	Also change first "that" so "that that" becomes "than the"		
83	FR	6	161	Merge 6.161 with 6.160	These are all quotation of SSR-2/1			x	Would give a cumbersome paragraph
4	Spain	6	165	[…] however it is sometimes desirable to avoid testing during power operation if it puts at risk the plant safety. The benefits of testing and calibration during power operation must be balanced with the adverse effects they may cause on the plant safety.	Normal operation and safe operation are not antagonistic concepts. Adverse effects on plant safety are not enough to discard testing and calibration if the absence of testing and calibration causes a higher negative impact on plant safety.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
84	FR	6	179	Make bullet f. of 6.179 a separate paragraph and combine with 6.180. 6.180 ~~f.~~ Provisions for testing I&C systems and components should Be located such that neither testing nor access to the testing location expose operating personnel to hazardous environments. Example considerations include: • Location of sensors such that testing and calibration can be performed at their location. • Location of test devices and test equipment in areas convenient to the equipment to be tested. • Plant or administrative features that could make it difficult to bring test equipment to the location of components to be tested, e.g., the necessity to move equipment along narrow paths, or in and out of contaminated areas. • Convenience of component status indication and test connections. ~~6.180.~~ Where equipment to be tested is located in hazardous areas, facilities should be provided to allow testing from outside the hazardous area.	Same topic (equipment location)			x	It would lead to repeating the 6.179 heading.
81	USA	6	180	Suggest modifying the third sentence as follows: "Where equipment to be tested is located in hazardous areas, ~~facilities should be provided to allow testing~~ provisions should be made to allow testing to be controlled from outside the hazardous area."	Clarity	x			
82	USA	6	182	Suggest adding a bullet as follows: "Criteria for passing or failing the test, and a process for handling non-conformance to these criteria;"		x			
15	UK	6	190	Replace 6.190 with 6.189	Editorial	x			
85	FR	6	190		Typo in cross reference	x			
5	Spain	6	190	In addition to the recommendations of paragraph 6.189, the processes […]	Numbering error.	x			
86	FR	6	190	6.190. In addition to the recommendations of paragraph 6.190, the processes defined for periodic tests and calibration of safety systems should: a. Be a single on-line test unless it is not practical; Such an on-line test will be able to identify specific defects directly when initiated, without the need for making test connections or disturbing the on-line equipment or its operation for more than a limited time. ~~When a single on-line test is not practicable, the test program may combine overlapping tests, to achieve the test objectives.~~ b. Independently confirm the functional and performance requirements of each channel of sense, command, execute, and support functions; c. Include as much of the function under test as practical (including sensors and actuators) without jeopardizing continued normal plant operation;	More logical			x	
87	FR	6	191	Combine 6.191 and 6.192 and last paragraph of 6.190 a. 6.191. Where a single on-line test is not provided for a safety system channel,: - the test program should combine overlapping tests, to achieve the test objectives; - documented justification should be provided for the use of overlapping tests. ~~6.192.~~ Typically the justification will demonstrate that the overlapping tests provide complete coverage, that reliability of the equipment is acceptable given the longer test interval, and that any components not tested on-line will be tested during plant shutdown.				x	We do not combine informative and normative pars together. If combined, this opara would become too long.
10	ISO/ WNA	6	198	*Remove paragraph*	A division under maintenance shall not be automatically disabled. Not wrong but there are also possibilities – the document shall not influence the design			x	They are examples

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
83	USA	6	208		Setpoints measured during periodic testing should be evaluated to confirm that deviation from the previous setting is consistent with expectations used in the uncertainty analysis. Excessive deviation that does not result in violation of the allowable value (for instance, deviation in the conservative direction) might still be indication that the channel is not behaving as expected, and that either the equipment needs to be repaired, or the analysis needs to be revised.	x	Although no rec this text could be inserted "as is" as a new para after 6.208		
6	Spain	6	208	ISA S67.04 Setpoints for Nuclear Safety Related Instrumentation gives additional guidance on setpoint determination. (to be added at the end of the paragraph)	ISA S67.04 is a widely used standard which addresses setpoint determination in nuclear industry.			x	No strong opinion, but my understanding is that it is not normal to refer out to non IAEA guides. If it is, there are a lot more references we could put in.
84	USA	6	209	"Figure 3 illustrates the relationship..."	Correct the figure number to Figure 3.	x			
88	FR	6	209	Merge 6.209 with 6.208				x	We do not combine informative and normative pars together. If combined, this opara would become too long.
89	FR	6	219	Merge 6.219 with 6.216	6.219 gives justification for 6.216			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
86	USA	7	5	"The sensor for each monitored variable and its range should be selected on the basis of the accuracy, response time, operational environment, and range needed to monitor the variable in all plant states during which the information from the sensor is needed."	Operational environment should be a factor to be considered.	x			
90	FR	7	6	The consequences of sensor CCF ~~combined with a PIE~~ should be integrated in the analysis described in paragraphs 4.30 to 4.34.	As 7.6 mention 4.30 to 4.34, it should be consistent and not mention consequences criterion.	**x**			
108	FR	7	12	Merge 7.120 with 7.116	Same topic.		Assuming 7.119 is meant	x	We do not combine informative and normative pars together.
91	FR	7	14	The effects of automatic control system failures, ~~including multiple spurious control system actions~~, should not exceed the acceptance criteria established for anticipated operational occurrences	Multiple failures of classified systems are beyond design basis, so their effects are not subject to design basis criteria. Thus the "multiple spurious" part of the clause does not apply to control systems when they are classified, which happens in some designs. It is necessary and sufficient to require that "failures" be considered, as the range of credible failures (fail to actuate, spurious actuation, single or multiple, etc.) depends on properties specific to each design and thus has to be established and justified case by case.	x	The effects of automatic control system failures should not create a condition which exceeds the acceptance criteria or assumptions established for design basis accidents. Failure modes such as multiple spurious control system actions should also be considered when a potential for such failures exists for a specified system design. Appropriate design measures such as segmentation can be used as a means to eliminate the plausibility of multiple spurious control system actions or reduce the likelihood of occurrence to an acceptable level.		Note UK are aware this comment may be contentious and hence are also content for 7.14 to remain unchanged On 20 Jan, UK commented: Apologies for misunderstanding - UK strongly reject this comment. The requirement has already been subject to considerable discussion and negotiation. We need to account for credible combinations of system actions.
11	ISO/ WNA	7	14	The effects of automatic control system failures, ~~including multiple spurious control system actions~~ **as single failure**, should not exceed the acceptance criteria established for anticipated operational occurrences.	Single failure should be accounted for safety analysis of AAO but not the multiple spurious as spurious are considered as residual risk based on use of highly reliable platform and development life cycle.	x	The effects of automatic control system failures should not create a condition which exceeds the acceptance criteria or assumptions established for design basis accidents. Failure modes such as multiple spurious control system actions should also be considered when a potential for such failures exists for a specified system design. Appropriate design measures such as segmentation can be used as a means to eliminate the plausibility of multiple spurious control system actions or reduce the likelihood of occurrence to an acceptable level.		Note UK are aware this comment may be contentious and hence are also content for 7.14 to remain unchanged

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
92	FR	7	21	Combine 7.21 with 7.20	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
93	FR	7	22	e) For new design it is advisable to design such that …	Typo	x			
2	HU	7	22	7.22 e). For new designs and reconstructions it is advisable to design such that during the first 30 minutes of a design basis event, operator actions are not needed to maintain plant parameters within the established limits.	The >> 30 minutes rule << has a very common and long history. The present time I&C reconstructions usually give the opportunity to establish it if it had not been earlier.	x	**For new designs or significant modifications, it is advisable to design such that during the first 30 minutes of a design basis event, operator actions are not needed to maintain plant parameters within the established limits.**		
87	USA	7	22	e) If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable human factors engineering (HFE) analysis should be performed to ensure that plant conditions can be maintained within recommended acceptance criteria for each PIE. As the difference between Time Available and Time Required for operator action is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available.	Change the fixed 30-minute limit to a limit that is determined by specific plant designs and PIEs.			x	The proposal says something very different ("diverse means") to the existing bullet. The 30 minute rule is a basic piece of accepted guidance that provides a helpful endstop. The first part of existing bullet e sets out the requirement
94	FR	7	25	Combine 7.25 with 7.23	Same topic			x	We do not combine informative and normative pars together. If combined, this opara would become too long.
95	FR	7	26	Transform 7.26 as a footnote to 7.23. 7.23. Means should be provided to manually initiate the mechanical safety systems* and the individual components that are necessary to initiate and control performance of their safety functions. ~~7.26.~~ *Mechanical safety systems are, for example, the individual divisions of control rods, emergency feed water, emergency core cooling, or containment isolation.	Explanation			x	We do not combine informative and normative pars together. We avoid footnotes.
96	FR	7	40	7.40. Actions initiated by the protection system should be latched so that once an action is started, it will continue although the initiating state might have ceased to be present. ~~7.42.~~ Once a protection system function is initiated all actions performed by that function should be completed.	Same topic			x	We do not combine informative and normative pars together. We avoid footnotes.
12	ISO/ WNA	7	45	Provisions to reset **the safety functions** ~~safety~~ ~~systems~~ should be part of the safety system.	The safety function not the safety system should be reset	x			
97	FR	7	45	Locate 7.45 before 7.4	More logical order			x	We prefer keeping the existing order.
98	FR	7	47	Merge 7.47 with 7.46	7.47 explains why spurious actions are to be avoided			x	We do not combine informative and normative pars together.
99	FR	7	51	Merge 7.51 with 7.50	These are all quotations of SSR-2/1			x	Would give a cumbersome paragraph
100	FR	7	59	Delete 7.59	No added value (7.58 is enough)			x	It will help some readers.
101	FR	7	61		What about I&C needed for DEC			x	I&C for DEC are covered in Chapter 8.
88	USA	7	68	The use of digital systems for NPP I&C functions provides advantages that include the flexibility to provide complex functions, improved plant monitoring and operator interfaces, capability for self-test and self-diagnostics, better environment to facilitate lessons learned based on tremendous data recording capability, low physical size and low cabling needs...	The huge data recording capability of DI&C has played an important role in lessons learned in many industries, including the nuclear industry.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
102	FR	7	68	7.68. The use of digital systems for NPP I&C functions provides advantages but also introduced challenges in demonstrating adequate safety*/ * Advantages ~~that~~ include the flexibility to provide complex functions, improved plant monitoring and operator interfaces, capability for self test and self diagnostics, low physical size and low cabling needs. They can have test and self-check functions that improve reliability. ~~7.69.~~ However, I&C functions are implemented differently in digital systems than they are in analogue systems. In digital technology functions are combined in one or more processing units. Combining functions in a processing unit could lead to a high degree of complexity and the failure of a processing unit will result in simultaneous failure of several functions. ~~7.71.~~ In digital systems, inputs are sampled at discrete points in time, signals are periodically transmitted between system elements, and outputs are also produced periodically. Consequently changes of processing or communication load of a digital system could affect transmissions speed and response time, if they were not correctly designed. Changes to processing or communications load might result from changes in plant parameters, operation in different system or plant states, or equipment failures. ~~7.72~~. Section 3 of Ref. [12], NP-T-3.12: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants discusses the special nature of digital systems in more detail.	These paragraph do not provide recommendations. Simplification would be beneficial.			x	Would give a cumbersome paragraph
89	USA	7	69	I&C functions are implemented differently in digital systems than they are in analogue systems. In digital technology functions are combined in one or more processing units. Combining functions in a processing unit could lead to ~~a high degree of complexity~~ conditions which are very difficult to analyze and the failure of a processing unit will result in simultaneous failure of several functions. Also, one function may degrade the performance of another (without any identifiable “failure”) through unwanted interactions.	The term “complex” does not have a broadly-accepted, well-understood meaning.The expression “difficult to analyze …” serves the intended purpose and aligns with the familiar relationship Analysis → assurance.Reason for addition of last sentence: The DS431 reader should be alerted to the potential for interference.	x	Except additional "which" should be "that"		
18	ISO/ WNA	7	69	7.69. I&C functions are implemented differently in digital systems than they are in analogue systems. In digital technology functions are combined in one or more processing units. ~~Combining~~ **Combined** functions in a processing unit could lead to a high degree of complexity and the failure of a processing unit will result in simultaneous failure of several functions.		x			
90	USA	7	70	7.70. Full verification and validation of such complex components could be very difficult or even practically impossible if they are not designed correctly ~~designed~~. Unidentified errors might exist ~~and they might exist~~ in all redundant components uses or ~~to~~ spread to other systems…”	Rephrased to improve clarity..	x	1st sentence change ok. 2nd sentence better to read: "Unidentified errors might exist, and these might be replicated in all redundant components or spread to…"		
13	ISO/ WNA	7	70	Full verification and validation of such complex components could be very difficult or even practically impossible ~~if they were not correctly designed~~. Unidentified errors might exist and they might exist in all ~~redundant~~ component uses ~~or to spread to~~ **in redundant systems or** in other systems based on the same platform., ~~because software modules, programmed devices, or libraries could be common to all.~~	The development life cycle and associated V&V effort insure correct design. The level of V&V is not link to the correctness of the design. It is also suggested to simplify the requirement.			x	This is explanation not a requirement. Poor design can make V&V more difficult. It is important to be aware of commonality of software.
91	USA	7	71	7.71 In digital systems, inputs are sampled at discrete points in time, signals are periodically transmitted between system elements, and outputs are also produced periodically. Consequently changes of processing or communication load of a digital system could affect transmissions speed and response time, if they are not designed correctly...”	This section is phrased awkwardly.	x			
103	FR	7	83	Merge with 8.82	Same topic		Assuming 7.82 is meant	x	We do not combine informative and normative pars together.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
104	FR	7	97	Merge 7.97 and 7.98. 7.97. Communications, including communications errors or failures, in a safety divisions should not prevent connected safety divisions from performing their safety function. ~~7.98.~~ The intent ~~of the recommendation in paragraph 7.97~~ is to prevent the propagation of failures between divisions. Typically a combination of data validation (see paragraphs 7.82 to 7.94), and buffering is employed.				x	We do not combine informative and normative pars together. If combined, this opara would become too long.
92	USA	7	104	~~The failure modes~~ Potentially degrading effects of computer security features ~~and the effects of these failure modes~~ on I&C functions should be ~~known~~ identified, documented, and considered in system hazard analyses. Constraints should be identified to prevent degradation of a safety function.	The term “failure mode” is not sufficiently comprehensive and clear. Failure is defined as: “The termination of the ability of an item to perform a required function.” Then, if the security feature is performing its required function, it has not failed. Yet, it could degrade the performance of a safety function, e.g. through interference. Just knowing, documenting and considering is not sufficient. Hazard analysis must also identify the system constraints to prevent degradation of a safety function.			x	Proposal changes the meaning of the 7.104, which is about security breaches compromising the safety function. The new meaning in the proposal is already covered in 7.103.
105	FR	7	107	Merge 7.107 and 7.106	Same topic			x	We do not combine informative and normative pars together.
106	FR	7	113	Merge 7.113 with 7.112	Same topic			x	We do not combine informative and normative pars together.
107	FR	7	115	Merge 7.115 with 7.114	Same topic			x	We do not combine informative and normative pars together.
109	FR	7	124	Male 7.214 a footnote to 7.122	7.124 describe example of data to be communicated			x	We do not combine informative and normative pars together. We avoid footnotes.
110	FR	7	125	Active computer security features should be considered	Typo	x			
7	Spain	7	125	Active computer security features should be considered for detecting and mitigating computer security threats.	Editorial correction (missed space)	x			
93	USA	7	130	See Attachment 1 for recommended additional guidance in this area.	The cyber security guidance does not include criteria for maintaining computer security once a system has been put into operation.			x	This is guidance is included in a security publications NSS 17 which is under the revision.
111	USA	7	130	An understanding the security life cycle aspects of the overall architecture, different safety systems and any potential changes that have occurred should be maintained during normal modernization of the site	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.
112	USA	7	130	The computer system should be periodically evaluated for security performance with consideration for design changes and protecting against possible new security threats. This effort should include a review of the recent global security incidents and events.	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.
113	USA	7	130	Security audits and vulnerability scans should be conducted on a periodic basis. These should include reviewing the computer equipment and architecture assessment for effective protection and should consider discovered incidents.	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.
114	USA	7	130	All assessment documentation, including notes and supporting information should be retained.	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.
115	USA	7	130	Training of personnel should be conducted with an approved security education program. This program should maintain routine communication with security awareness and support organizations.	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.
116	USA	7	130	A review of the interfaces between physical and computer security and safety functions should be performed when any changes or emergent activities in either domain are performed. The object of these reviews is to identify and correct any adverse interaction effects that may be introduced as a result of modifications.	Add new para.		See response above to US comment on 7.130.	x	This is guidance is included in a security publications NSS 17 which is under the revision.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
94	USA	7	131	Add sentence that clearly states: “Based on this definition, this safety guide does not address HDL configured devices that embed a processing unit that executes instructions (e.g., microprocessor or microcontroller with executable software, etc.), such as through an IP Core.” Or: Enhance the safety guidance to clarify how embedding a processing unit that executes instructions within a HDL configured device affects the application of the safety guidance.	It is unclear whether the safety guide intends to allow embedding a processing IP Core within a HDL configured device. As written, the scope of HDL configured devices in 7.131 appears to exclude embedding a processing unit that executes instructions. However, it is not clear whether this is the actual intent of the safety guide. Furthermore, if this is the intent of the safety guide, then the relationship between the HDL configured device section and the software section and the appropriate applicability of each, becomes less clear.			x	A valid technical question, but it is too late in the guide's development to address this issue.
111	FR	7	132	Merge 7.132 with 7.131	Same topic			x	We do not combine informative and normative pars together.
96	USA	7	139	a) Either: Delete the use of the phrase “qualified vendors” from this section, and revise it accordingly to address the use of an IP Core within a “system, equipment, component, device or instrumentation.” Or: Provide clear unambiguous guidance associated criteria for qualifying a vendor that also explains how a vendor’s “IP Core” is to be treated in terms of its use as a programmable device within a component. Or: Change the paragraph to address the development of the IP Core consistent with the safety guide (e.g., 7.143, 7.144, etc.) and verification and validation of the IP Core (rather than “qualification of an IP Core vendor”) in a manner consistent with Section 9, and the use of pre-developed components.	As currently written, no guidance is provided that identifies whether an IP Core vendor is adequately qualified. The safety guidance discussions of qualification relate to “system, equipment, component, device or instrumentation” rather than vendors or their processes and procedures. Also consider that the discussions of software in Section 9 deal with verification and validation rather than “qualification” of software components. Likewise, Clauses 7.158 and 7.160 deal with “verification and assessment” of tools rather than “qualification.” If “IP Core vendor” qualification is required, then the revised text should provide adequate supporting guidance for “vendor qualification.”			x	It is probably too late in the guide's development to make these changes.
95	USA	7	139	Change “If use of IP Cores cannot be avoided” to: Either “Under the following conditions, IP Cores may be used:” Or“Use of IP Cores in equipment of the highest quality criteria is prohibited.” Also add: “For equipment of lesser quality criteria, IP Cores may be used under the following conditions:”	As currently written, no guidance identifies suitable criteria to determine whether using an IP core is acceptably unavoidable. The safety guide should provide a positive and unambiguous statement in lieu of a negative ambiguous one. Additionally, the revised text should provide adequate supporting guidance to apply the clause. If compliance with 7.139 a & b provides an acceptable level of assurance when using an unavoidable IP core, then reason for including an IP core avoidance statement is unclear.	x	IAEA propose: "IP cores should only be used if the following conditions are satisfied:"		
97	USA	7	142	Either: Delete the use of the phrase “qualified tools” from this section, and revise it accordingly to address “verified and assessed tools as applied to create a system, equipment, component, device or instrumentation.” Or: Provide clear unambiguous guidance associated criteria for qualifying a HDL configured device tool that also explains how the tool is to be treated in terms of its use when creating a programmable device within a component. Or: Change the paragraph to address the verification and validation of the tools themselves (rather than a tool’s “qualification” in a manner consistent with Section 9.	As currently written, no guidance is provided that identifies whether a tool is adequately qualified. The safety guidance discussions of qualification relate to “system, equipment, component, device or instrumentation” rather than tools and their use. Additionally, clause 7.154 deals with the selection of tools for life-cycle compatibility, clauses 7.155 and 7.156 deal with a tool’s application, and clauses 7.158 and 7.160 deal with a tool’s “verification and assessment.” None of these constitute “qualification” of a tool, as the term “qualification” is used elsewhere in the safety guide. Also consider that the discussions of software in Section 9 deal with verification and validation of tools rather than their “qualification.” If tool qualification is required, then the revised text should provide adequate supporting guidance for “tool qualification.”			x	As for 7.139a above
98	USA	7	143	Same indent should be used for items a-f.	Editorial	x			
99	USA	7	146	7.146. Verification and validation should:	Change the title of section 7.146 to include validation since some of the bullets are validation activities (e.g., testing).	x			
112	FR	7	147	7.147. Environmental qualifications and analyses should demonstrate that the inclusion of predeveloped items or auxiliary features does not degrade the ability of ~~safety~~ systems important to safety to perform their safety functions.	Safety related system have to be included so the scope has to be broaden	x			
113	FR	7	148	7.148. Software Tools should be used to support all aspects of the I&C development life cycle where benefits result through their use and where tools are available.	Clarification	x			
114	FR	7	151	7.151. A key element of integrated project support environments is to ensure proper control and consistency. If software tools are not available, the development of new tools might need to be considered.	Clarification	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
115	FR	7	152	7.152. The benefits and risk of using a software tool should be balanced against the benefits and risk of not using a tool.	Clarification	x			
116	FR	7	157	Merge 7.157 with 7.152	Same topic			x	There is a link to 7.156 (as well as 7.152)
117	FR	7	159	~~• Less rigour in tool verification may be accepted if there is mitigation of any potential tool faults (e.g. by process diversity or system design).~~	The previous section stresses the need to have a high quality development of software. High quality tools are therefore needed.			x	This bullet adds useful explanation for 7.158.
118	FR	7	164	Merge 7.164 with 7.163	Same topic			x	We do not combine informative and normative pars together.
119	FR	7	167	Merge 7.167 with 7.166	Both paragraphs explain what is a device of limited functionality.			x	We do not combine informative and normative pars together.
14	ISO/ WNA	7	169	7.169. Information developed during safety certification for other industries may be used as evidence to support device qualification. A certificate alone **may** not **be** sufficient **for all safety related components**, it is the information developed by the certification process that may provide value.	The level of documentation required for the certification should be based on the safety relevance of its functionality and context.			x	A certificate alone is never sufficient without knowledge or confidence in the underlying information which led to its issue.
120	FR	7	171	Merge 7.171 with 7.170	Same topic			x	It is helpful to take this step by step
121	FR	7	175	Merge 7.175 with 7.174	Same topic			x	We do not combine informative and normative pars together.
122	FR	8	2	Merge 8.2 and 8.3 with 8.1	These are all quotations of SSR-2/1			x	Would give a cumbersome paragraph
123	FR	8	6	8.6. Safety classified indications and controls should be provided to implement emergency operating procedures (EOP) and, as far as practicable, for SAMG. ~~8.7.~~ * Thеis ~~guidance of paragraph 8.6~~ is not intended to preclude the option to use other means appropriate to satisfy the goals of the EOP.	SAMG should also rely, as far as possible, on safety classified indications. 8.7 is not a recommendation and a footnote would be enough.			x	We do not combine informative and normative pars together. We avoid footnotes.
124	FR	8	14	Transform 8.14 as a footnote to 8.15	Not a recommendation.			x	We do not combine informative and normative pars together. We avoid footnotes.
125	FR	8	21	Merge 8.21 with 8.20	Same topic			x	We do not combine informative and normative pars together.
126	FR	8	25	Merge 8.25 with 8.24	Same topic			x	We do not combine informative and normative pars together.
8	Spain	8	26	b) Either not depend upon external power, or have a designed capability to be powered from sources other than the plant electrical offsite power system.	The plant power systems does include Diesel Generators, batteries, etc. which are deemed to be a valid power source. The proposed text uses terminology equivalent to that in 8.45.b.			x	The point is the functions should not depend on the main onsite power system (including emergency diesel generators etc). The full wording in 8.45b is clearer and could be used instead.
127	FR	8	28	8.28. Where failure of a single display channel of instrumentation performing the functions given in paragraph 8.22 items a, b, c, d and f could result in ambiguous indication, means should be provided that allows operators to resolve the ambiguity.	DBA should be considered.			x	This seems too onerous
128	FR	8	33	Transform 8.33 into a footnote to 8.32	Not a recommendation			x	We do not combine informative and normative pars together. We avoid footnotes.
129	FR	8	34	Transform 8.34 into a footnote to 8.32	Not a recommendation			x	We do not combine informative and normative pars together. We avoid footnotes.
130	FR	8	35	8.35. Operator aids that are not dependent upon a power source should also be available for instrumentation performing the indication functions given in paragraph 8.22 items a, b, c, d and f.	DBA should be considered.			x	This seems too onerous

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
2	SWE	8	35	Operator aids that are not dependent upon a power source, such as …., should also be available …..	It is not explicitly clear what is meant by “operator aids that are not dependent upon a power source”. For clarification and better understanding it would be helpful to set some examples of such operator support, otherwise readers can misunderstand what is meant. For non I&C experts the paragraph could also be understood to refer to administrative tools, e.g. operating procedures etc. even though the reviewers understanding is that this is not the intention.			x	For example calibration curves to read instrumentation under different RCS parameters, etc.
131	FR	8	37	Merge 8.37 and 8.38 with 8.36	These are all quotations of SSR-2/1			x	Would give a cumbersome paragraph
132	FR	8	42	Merge 8.42 with 8.41	Same topic			x	We do not combine informative and normative pars together.
9	Spain	8	43	a) Areas where communications are needed during Anticipated Operational Occurrence (AOO) or Accident Conditions,	This acronym AOO has not been defined so far.	x			
133	FR	8	44	Merge 8.44 with 8.43	Same topic			x	We do not combine informative and normative pars together.
16	UK	8	44	Replace “standard telephone, battery operated telephones, self-powered telephones” with “landline, satellite and cell telephones”	More effective diversity	x			
134	FR	8	48	Merge 8.48 and 8.49 with 8.47	These are all quotations of SSR-2/1			x	Would give a cumbersome paragraph
135	FR	8	50		Very unclear recommendation… Deletion should be considered			x	
136	FR	8	55	Locate 8.55 before 8.53	More logical locatin	x			
137	FR	8	56	Merge 8.56 with 8.55				x	We do not combine informative and normative pars together.
138	FR	8	59	No single operator error should result in loss of reactor control, ~~equipment damage, injury, or inadvertent operation of a safety system~~.	This recommendation goes far beyond I&C topic. It is unlikely to be realistic…. Deletion should be considered. “single” is ambiguous: for example, if an operator trigger the safety injection button, is it one or two errors ? Thus, the last part of the sentence is too precise and mention item that would not systematically challenge safety.	x			
139	FR	8	60	Bullet b should be located before d	d is a means of achieving b	x			
140	FR	8	60	h)	Why limiting to video display ? what about analog display ?	x			
141	FR	8	64	Merge 8.64 with 8.63	Same topic			x	We do not combine informative and normative pars together.
142	FR	8	66	Transform 8.66 as a footnote to 8.65	8.66 is explanation			x	We do not combine informative and normative pars together. We avoid footnotes.
143	FR	8	67	Transform 8.67 as a footnote to 8.65	8.67 is explanation			x	We do not combine informative and normative pars together. We avoid footnotes.
15	ISO/ WNA	8	78	A ~~complete~~ task analysis will consider all plant states, all plant operating modes and all groups of operating personnel, e.g., ~~licensed operators, unlicensed operators,~~ reactor operator, turbine operator, shift supervisor, field operator, safety engineer, operation and maintenance staff ~~maintainers~~. Task analysis will provide design input ~~into~~ for the characteristics of I&C such as the accuracy~~,~~ and precision of displayed information, ~~time~~ system response time, physical layout, type of controls, ~~and~~ displays, and alarms and the integration of soft controls ~~association~~ within information displays.	Wording like “complete” should be avoided as long as the scope of being “complete” is not specified. Proposal: Recall that part of the task analysis methodology is a screening methodology used to select the tasks for analysis, based on criteria specifically established to determine whether analyzing a particular task is necessary. Task Analysis will normally begin with narratives of what plant personnel have to do to accomplish the functions allocated to personnel. Subsequent analysis should be sufficiently detailed to define the alarms, information, controls, and task support needed to accomplish those duties. The results of task analysis serve as inputs for the analysis of staffing and qualifications; the design of HMIs, procedures, and training program; and criteria for Task Support Verification	x			
146	FR	9	1	Merge 9.10 with 9.9	Same topic			x	We do not combine informative and normative pars together.

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
144	FR	9	2	9.2. Digital systems require different approaches to the assessment of reliability than analogue systems. Reliability is inferred from the assessment of the quality of production activities, and the results of verification and validation. Software implementation tends to be complex and prone to design errors which may be more difficult to detect than in analog or mechanical system. Complexity in software implementation can generate additional faults in design, increase the difficulty in detecting and correcting faults, introduce failure modes and effects that are not present in simpler design, and reduce the confidence in any demonstration of conformance to safety system design criteria such as independence, testability and reliability.	The paragraph may be understood as implying than analog systems have never encountered design errors. There are plenty of example of equipement (without software) which were subject to undetected design error up to an event which question their design…	x			
10	USA	9	2	Section 9.2 states, in part, "…Software implementation tends to be complex and prone to design errors…"	Software implementation may introduce errors into the developed system, but not into the system design. Further, software implementation is not prone to errors, as most implementations are done with certified tool sets, such as function block libraries.	x	**The IAEA propose to modify this setence as follows: Software tends to be complex and prone to design errors which may be more difficult to detect than in an analogue or mechanical system.**		
145	FR	9	3	Merge 9.3 with 9.2	Same topic			x	Not the same topic
4	BEL-V	9	9	**(a)** Some of the greatest difficulties now encountered with the validation of the new reactor I&C designs come from the ways the software is conceived and implemented. As recent history shows, these difficulties continue to be sources of design and licensing delays. These difficulties are exacerbated by the increased complexity of the functionality; an increase made possible by computer and software technology. The consequences would be better controlled if the guidance of SG1.1 was followed by designers and operators and thus better taken into account in the IAEA document DS 431. **(b)** At the outset, safety is indeed a plant and system issue. But the implementation of a safety system by means of a computer architecture and software raises specific issues. The architecture and the software must be dependable; that is, convincing evidence must show that, despite their potential failures, they implement correctly, safely and reliably the functionality and the safety system requirements. It is the provision of this evidence which raises major difficulties when the architecture and the software are not properly derived and designed from the system and safety requirements. The provision of evidence of sufficient dependability for computer-based systems was the essence of the SG1.1 guidance and should therefore also appear in the IAEA document DS 431. **(c)** The issues of computer architecture and software design are of course not independent from the safety requirements expected from nuclear safety systems. These interrelations, in particular with respect to their implications on independency, redundancy and diversity, documentation, testing, calibration, in-service maintenance, etc… were taken into account in SG 1.1 and carefully discussed in the context of nuclear power plants. **(d)** Despite the large impact and the importance gained by these issues today, among the great number of IAEA documents, SG1.1 remains with the technical report TRS 367 of 1994, the only IAEA documents dealing with the subject. The IAEA document DS 431 does not go deep enough in these issues. The technical report TRS 367 of 1994 should therefore appear in the references of the IAEA document DS 431.				x	Reference might be useful but is probably too out of date.
101	USA	9	11	a) Define what each individual software item is required to do and how it will interact with other components of the system, as well as interactions that are prohibited.	Whereas the developer's primary focus has been on realizing functionality through functional decomposition and allocation to software components, requirements to prevent unwanted interactions and side effects are often not cascaded down explicitly.	x	Added a new bullet: j. Define any functions, behaviour or interactions that it is particularly important the software does not do		

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
102	USA	9	11	b) Originate from the relevant processes of the I&C life cycle (including consideration of system hazards identified in previous analyses and including results of hazard analysis of the software for contributory hazards) and from processes that interface with the I&C life cycle, e.g., human factors engineering and computer security activities. See Fig. 2.	More interconnections and more software are a new source of internal hazards, not previously recognized as such.			x	This is already included in previous analyses if relevant at this stage
103	USA	9	13	The origin of every software requirement should be documented sufficiently to facilitate verification, validation, traceability to higher-level documents and a demonstration that all relevant requirements have been addressed.	Requirements must also be testable. Include validation in this section.	x			
104	USA	9	16	The completed software design should be… verifiable, able to be validated, traceable, maintainable and documented."	Requirements must also be able to be validated. Include validation in this section.	x			
147	FR	9	20		"Design elements" should be defined	x	**The IAEA propose: Parts of the software design should be distinguished sufficiently to enable useful traceability of requirements through the design.**		
148	FR	9	22	Merge 9.22 with 9.21	Same topic			x	We do not combine informative and normative pars together.
149	FR	9	38	Merge 9.38 with 9.37	Same topic			x	We do not combine informative and normative pars together.
105	USA	9	42	In section of SOFTWARE DESIGN, suggest adding an item as follows:"9.43 Where appropriate, software design should be peer reviewed."	Peer review for software design is part of the independent V&V. This review may find design faults in the early stage and improve software quality.	x			
150	FR	9	50	Restructure 9.50, 9.52 and 9.53 as follows: 9.50. ~~The programming language used for safety systems should support simple implementation. 9.52.~~ For safety systems, the choice of programming language should be justified and documented. Their programming language should support simple implementation and ~~.~~ ~~9.53. For safety systems,~~ the language syntax and semantics should be complete, available, and rigorously defined.	Simplification			x	These are different requirements.
106	USA	9	60	Section 9.60 states, "Software diversity (i.e., the use of different languages, different timing, different order of functions, and different algorithms) may be considered as a means of reducing the likelihood and effect of software common cause failures. However, this can introduce design constraints that could themselves lead to new failures."	Independent development teams and methods are forms of Life Cycle diversity, not software diversity. Software diversity consists of using different languages, different timing, different order of functions, and different algorithms.	x	Change to: "Software diversity (ie the use of independent development teams, and/or different methods, languages, timing, order of functions, algorithms) may be considered…		
151	FR	9	69	Merge 9.69 with 9.68	Same topic			x	We do not combine informative and normative pars together.
152	FR	9	72	Merge 9.72 with 9.71	Same topic			x	We do not combine informative and normative pars together.
107	USA	9	74	A test strategy (e.g., bottom-up or top-down) should be determined for ~~verification~~ validation of the software implementation.	Testing is a validation activity.	x	Change to: "… should be determined for verification and validation of the software implementation."		
108	USA	9	80	Verification and validation should be carried out by teams, individuals, or groups that are independent of the designers and developers.	Since some of the referenced activities are validation activities; add validation to this section.	x	Verification should be carried out by teams, individuals or organisational groups that are independent of the designers and developers.		
10	Spain	9	93	(such as penetration test)	The term 'penetration test' is better understood than 'pen testing' by a wider audience.	x			

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection
16	ISO/ WNA	9	99	9.99. **If required by national practice**, a third party assessment of safety system software should be conducted concurrently with the software development process. 9.100. The objective of the third party assessment is to provide a view on the adequacy of the system and its software that is independent of both the supplier and the operating organization. Such an assessment may be undertaken by the regulator or by a body acceptable to the regulator. 9.101. It is important that proper arrangements are made with the software originator to permit third party assessment. 9.102. The assessment should involve an examination of: a. The development process (e.g., through quality assurance audits and technical inspections, including examination of lifecycle documents, such as, plans, software specifications, and the full scope of test activities) and b. The final software (e.g., through static analysis, inspection, audit and testing), including any subsequent modifications.	The development life cycle, independent V&V and quality audit effort performed for the safety systems provide high quality systems. This practice is not applied in all member states so proposal to emphasize that the recommendations 9.99 to 9.102 should be implemented if required by the national practice.			x	**This requirement has already been subject to considerable discussion and negotiation.**

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection