NUSSC and NSGC comments on:
Design of Instrumentation and Control Systems for Nuclear Power Plants (DS 431, Rev. “M”)

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
1	USA	0	Definitions	The hazard analysis definition and associated note should be revised to read “is the process of examining a system throughout its lifecycle to identify inherent hazards and contributory hazards, and requirements and constraints to eliminate, prevent, or control them.” Also, delete the last sentence from the “Note:”	Hazard analysis covers more than failure mechanisms (for example, interactions between and across system boundaries).	x				
2	USA	0	Definitions	Add new definitions for “hazard” and “contributory hazard” to read as follows: a. Hazard – Potential for Harm. b.Contributory hazard - Factor contributing to potential for harm.		x				
2	USA Suppl.	0	Definitions	Add the following definitions: **Requirement** Expression of a perceived need that something be accomplished or realized. (Adapted from §4.47 in ISO/IEC 25000: 2005(E) Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE) Notes: 1. Functional requirement: Requirement that specifies a function that a system or its element must be able to perform, (Adapted from §4.22 in ISO/IEC 25000: 2005(E) Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE) 2. Quality requirement: Requirement that specifies a quality of a system or its element, where quality may be one of the following: 2.1. Quality in use (e.g., safety). Quality in use requirements specify the required level of quality from the end user’s point of view. Also see note 5 in definition of quality. 2.2. External quality. Also see note 6 in definition of quality. 2.3. Internal quality. Also see note 7 in definition of quality. **Quality** Capability of product to satisfy stated and implied needs when used under specified conditions. (Adapted from §4.51 in ISO/IEC 25000: 2005(E) Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE) Notes 1. This definition differs from the ISO 9000:2000 quality definition; it refers to the satisfaction of stated and implied needs, while the ISO 9000 quality definition refers to the satisfaction of requirements. 2. The term “implied needs” means “needs that may not have been stated explicitly (e.g., a need that is considered to be evident or obvious; a need implied by another stated need).” 3. Quality model: Defined set of characteristics, and of relationships between them, which provides a framework for specifying quality requirements and evaluating quality. (Adapted from §4.44 in ISO/IEC 25000: 2005(E) Software engineering – Software product Quality	These definitions are needed because the concepts underlying “quality requirements” are not well understood and some older standards define “quality” inadequately. For example, the ISO 9000 quality definition refers to the satisfaction of requirements, excluding the effect of deficiencies in the requirements (even though these deficiencies are known to be the largest contributor to mishaps). The {“quality in use”; external quality; internal quality} concepts bring this gap to light. Because these {quality model; quality measure} concepts are not well understood, the flow down {derivation; decomposition} from the top-level “quality requirements” is not well executed in practice. Flow-down Example: A top-level system property such as SAFETY may depend upon a supporting property SECURITY. To assure these properties, supporting properties {ASSURABILITY→ ANALYZABILITY→ VERIFIABILITY} are needed. A commensurate hazard analysis (HA) identifies conditions that could prevent the satisfaction of these properties; the HA leads to identification of commensurate constraints. These constraints lead to architectural constraints to prevent hazardous interactions between a safety system and its environment and across items in the safety system. Such a “quality model” driven analysis ensures that the derived architectural constraints (1) satisfy (fulfill) the top-level properties; (2) are verifiable. This flow-down process is followed at every level of integration down to the indivisible items.			x	Requirement and quality already included in the IAEA Safety Glossary. Quality magement is contained in GSR-Part 3, which is refernced in DS431. Besides that the term is used in the text with its normal, everyday meaning. - Another reason for not including it is because it is used in a very special way in the standards in general (and in DS431 in particular) that is precisely NOT the way it’s being defined, e.g. requirement (OK, ‘requirements’ is used in many ways in DS431, and this is only one of them) - Another reason is because the term is not actually used in the text, e.g. quality measure, quality in use, scale, etc. - Another reason is because we try to standardize terminology among all standards and it wouldn’t be particularly helpful to have a special meaning in DS431 that doesn’t work in the other standards (they form a complete body, and are not just individual books; and great efforts are made to ensure this), e.g. process	

NUSSC and NSGC comments on:
Design of Instrumentation and Control Systems for Nuclear Power Plants (DS 431, Rev. “M”)

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
1	USA Suppl.	0	Definitions	**Hazard analysis** (HA) is the process of examining a system throughout its lifecycle to identify inherent hazards (see) and contributory hazards, and constraints to eliminate, prevent, or control them. Notes: 1. Terms used above are defined below. 2. “Hazard identification” part of HA includes the identification of losses (harm) of concern. Add the following definitions: Hazard Potential for harm Examples: 1. A condition; 2. A circumstance; 3. A scenario. Notes: 1. Definition §3.1283-1 in ISO/IEC/IEEE 24765 Systems and software engineering – vocabulary, 2010) elaborates on the “potential for harm” as follows, “An intrinsic property or condition that has the potential to cause harm or damage.” 2. To be meaningful, the scope is bound to an item in the context of its (defined) environment. 3. At the initial stage of hazard logging (before any analysis of the initial finding), the log may include an item, which, after some analysis, is re-characterized (differently from the originally characterized hazard; possibly, an event). **Contributory hazard** Factor contributing to potential for harm. Notes: 1. (Excerpt from <http://aviationglossary.com/aviation-safety-terms/contributory-hazard/>) …. An unsafe act and / or unsafe condition which contributes to the accident (in I&C safety systems, degradation of a safety function), ... 2. Figures 7-1 - 7-4 in FAA System Safety Handbook, Chapter 7: Integrated System Hazard Analysis, December 30, 2000 illustrate	“examines” characterizes the definition more precisely than “explores” (the verb used In the DS431 definition). The space of this activity, “conditions that are not identified by the normal design review and testing process” is identified incorrectly In the DS431 definition. It seems to imply that HA activities would occur mainly after a “normal design review” and after a “normal testing process.” On the contrary, as proposed, HA should commence at the beginning of the lifecycle (and iterate at every phase); then, the result of HA includes constraints on the system, to be satisfied through the subsequent engineering phases. The DS431 assertion, “Hazard analysis focuses on system failure mechanisms” is flawed. Given that DS431 defines failure as loss of ability to function within acceptance criteria. The DS431 would exclude from the HA scope mishaps resulting from inadequate acceptance criteria. HA should produce the criteria and constraints to prevent harm, including harm from degradation of the safety function. Engineering deficiencies (e.g., inadequate constraints) and such systemic causes are increasingly contributing to degradation of a safety function (leading to mishaps) in all mission-critical application domains of digital systems. The DS431 definition limits the scope of HA (~ identifies conditions ~) to “hazard identification”; it should also include identification of the constraints, which, then drive the requirements/specifications for subsequent engineering phases. Also include the supporting definitions, because these concepts are not well understood, confounded by many different definitions in technical literature, further confounded through ambiguities and inconsistencies entailed in those definitions.	x	Accepted partly; added definitions of hazard and contributory hazard.		Notes as well as refernce to industry standards have not been included; we usually only define terms where we use them in a special way or where there’s likely to be confusion. This seems to be the case for the definitions proposed for hazard, hazard identification, analysis, process, product.	
1	FI	0	General	Design and implementation of the modern I&C is a challenging task. Development of the revision of up-to-date guidance given recommendations on the design of I&C systems to meet the requirements in SSR-2/1 is an important step towards harmonization of the approaches in the field.		x			We appreciate that comment!	
2	FR NSGC	0	General	The document should also whenever practicable take into account the reciprocity: security should not adversely affect functions important for safety and vice-versa.				x	It I already covered in section ***Interaction between safety and security*** , and in particular para 7.103	
1	IEC	0	General	**IEC/SC45A fully supports this draft M dated 24th of March 2014 as submitted for the 37th NUSSC meeting** considering the effort done in particular by the experts to take into account the comments formulated by Member States before the 36th NUSSC meeting and the consensual result obtained.	**IEC/SC45A experts acknowledged the work done by the IAEA Technical Officers and the expert teams which produced this draft and recognized the high technical quality of this document and the high level of consensus it reached.** IEC/SC45A noted that the vast majority of the numerous comments formulated on the previously circulated versions of DS431 were taken consensually into account according to the NUSSC members recommendations in particular the ones formulated during the 34th, 35th and 36th NUSSC meeting. IEC/SC45A will use and reference this IAEA Safety Guide as a basic document to develop IEC/SC45A standards, as soon as it will be published.	x			We appreciate that comment!	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
1	FR NSGC	1	3	This document presents a lot of interfaces between nuclear safety and nuclear security. The document shall limit the security consideration to the area of safety/security interfaces. It shall not provide guidance for nuclear security. (eg : p7 – 1.3 is to be modified “Provisions for ensuring the security of digital safety systems . note: 1.13 gives appropriate scope 2.34, 2.35, 6.154 to 6.158...)		x				
1	RoK	1	13	More detailed information on computer security is available in the IAEA Nuclear Security Series ~~documents Ref NSS17~~ No.17, Ref.[13].	To Correct the wrong reference Number	x	Corrected			
4	PK	1	18	Para1.18 (Addition of new para): Cost effective and qualified engineering solution should justify the assessment and deployment of software based I&C system.	Cost effectiveness may also be given some importance with safety.			x	Cost effectiveness, although important, is not subject for this SG, but it is generraly addressed in GSR Part 3.. See 2.4, the fourth bullet.	
1	FR	1	20	Combine 1.20 to 1.26 into a single paragraph	Usual format of IAEA Safety Standards			x	Followed IAEA editor's recommendation	
2	FR	2	5	Management systems include the organizational structure, organizational culture, policies, processes, including those to identify and allocate resources (e.g., personnel, equipment, infrastructure, working environment), ~~and processes~~ for developing I&C system that meets safety requirements.	Resources is not really in the management system but are identified and allocated through such system	x	Currently 2.6 after renumbering			
2	RoK	2	13	Consequently, confidence in the correctness of modern systems derives more from the discipline of the development process~~,~~ than ~~was~~ the case for systems implemented purely with hardware.	Delete unnecessary word.	x				
1	AR	2	16	Add the following item to the list of aspects to be considered in the design of an upgrade or a modification:- The electromagnetic environment of the place where the upgrade or modification will be installed should be considered, mainly when there will be coexistence between old and new technologies.	Usually the I&C technologies have different noise immunity, then it is possible that an upgrade can interfere with the existing I&C			x	EMI is covered in the Section 6, equipment qualification.	
3	FR	2	18	Other activities, sometimes outside of the I&C development, will have an important influence on the I&C system requirements and design. xHuman factors engineering and computer security are examples of such activities.	The initial sentence implies that HF and security are not within the scope of I&C development. They are.	x				
4	FR	2	20	This model illustrates the relationship between requirement specification, design, integration, and system validation activities and how verification and validation (V&V) activities relate to development activities.	Clarification	x				
5	FR	2	26	Combine 2.26 with 2.25	Both sections are about the topics			x	Topics are slightly different, we prefer keeping it separate.	
7	FR NSGC	2	36	Need for dialog or mixed (safety/security) team to develop ICS should be suggested.		x	added to para 2.36 as follows: Development of I&C should be conducted through dialogue between personnel responsible for safety and for nuclear security or by a mixed team of safety and nuclear security personnel in a development environment that meets the technical, procedural and administrative requirements of the computer security plan.			
6	FR	2	48	Combine 2.48 with 2.47	Same topic.			x	Topics are slightly different, we prefer keeping it separate.	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
7	FR	2	70	Transform 2.70 as a footnote to 2.69: 2.69. The overall I&C, each I&C system, and each I&C component* should be verified to confirm it implements all of their requirements (both functional and non-functional), and to investigate for the existence of behaviour that is not required (see paragraphs 2.129 to 2.143). 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. ~~2.70.~~ *Note that the term component includes hardware, software such as application software and firmware, and HDL descriptions.	2.70 and 2.69 have to be together.	x	We put this as a footnote in para 2.22, where similar bracket was.			
8	FR	2	73	Combine 2.73 with 2.71. 2.71. Verification and validation should be carried out by individuals, teams, or organizational groups that are independent of the designers and developers. ~~2.73.~~ The amount and type of independence of the V&V should be suitable for the safety class of the system or component involved.	2.73 is a key aspect in applying 2.71 and should not appear separately	x				
2	DE	2	83	Bullet 4: Reliability analysis. Reliability analysis uses statistical methods to predict the reliability of systems or components. Commonly used reliability analysis techniques include parts count analysis, parts stress analysis, field and life data analysis, reliability block diagrams, and fault tree analysis.	The modern standards (e.g. Telcordia SR332, IEC 61709, IEC 62380) for reliability prediction of the electronic components require also lab test data and field failure tracking	x				
4	FR NSGC	2	83	2.83 bullet point n°6, Delete	Not correct		Security testing. Security testing usually requires input from a vulnerability assessment and is used to confirm the use of good practice in security.	x	We believe that it belongs to para 2.83 Typical design analysis, ***verification and validation*** techniques include, ***for example*** , the following:	
3	DE	2	86	~~Given current state of the art, for an individual system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10–4 to 10-5 failure/demand may be an appropriate overall limit to place on the reliability that may be claimed in the probabilistic safety analysis, when all of the potential sources of failure (excluding cyber security related ones) due to the specification, design, manufacture, installation, operating environment, and maintenance practices, are taken into account. This figure may need to include the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors through processing to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification, taking into account all of the factors mentioned.~~ Delete or clarify the statement clearly and comprehensively	In the PSA will be claimed usually probability value of the failure of the system functions. Further in the text are used such unclear terms as individual system, whole system. Is it applicable commonly for all architecture of safety I&C: e.g. for ESFAS function actuated by Primar or Secondary/Diverse I&C systems.			x	This current wording is already a fragile consensus among MS.	
2	FI	2	92	…o. Operating procedures; to cover all normal operational states and modes p. Emergency operation procedures, and severe accident procedures or guidelines, to cover all postulated accident scenarios;	the o. and p should be clarified and harmonized. There could be severe accident procedures or guidelines.	x				
9	FR	2	102	Delete 2.102	2.102 is neither a recommendation nor an explanation of the previous recommendation.			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	
3	RoK	2	110	~ in paragraphs ~~6.79~~ 6.78 through ~~6.135~~ 6.134.	Reflect changed paragraphs numbers.	x				
10	FR	2	112	Combine 2.112 with 2.111	Both or informative sentences. No need to make them separate sections.			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
11	FR	2	115	Combine 2.116 with 2.115. 2.115. 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. ~~2.116.~~ However, 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. 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.	Both or informative sentences. No need to make them separate sections.			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	
4	DE	2	140	~~Validation testing using statistical techniques should be considered.~~ Statistical testing may provide additional confidence for validation of I&C systems.	As long as the quantitative (statistical) methods have no general acceptance (state of the art) for validating software-based I&C systems, this technique should only be treated as an option in the V & V process.			x	This wording is already a fragile consensus.	
12	FR	2	162	Combine 2.162 with 2.161	Same topic (defining the level of rigour)			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	
2	AR	2	167	Add the following phrase: If an upgrade or modification in a probationary period does not generate any action (only it is energized for evaluation), it should be demonstrated as a minimum, (through qualification certificates) that it does not affect other installed I&C (due to electromagnetic interference, etc.).	The scenario proposed can take place in the process of evaluating an I&C modification. This situation requires an authorization from the regulatory body to the NPP´s operator; the final approval of the modification will require fulfillment of points 2.159 to 2.166.			x	The implementation guidance is outside of the scope of this safety guide.	
13	FR	3	6	• Mitigate the radiological consequences of accidents ~~significant releases of radiation~~.	More general expectation.	x				
14	FR	3	12	Make 3.12 a footnote of 3.11				x	This is not a reference to be put in a footnote; we prefer keeping it as is.	
5	FR NSGC	3	13h	Delete	Not correct. There are other ICS on a facility.			x	This is something that the I&C engineers must do. Para 3.13 deals with the overall I&C system. By definition there are no other ICS in a facility.	
6	FR NSGC	3	13i	Delete	Not correct; safety design basis do not give information on vulnerability.	x	Vulnerability assessments and impact analyses for computer security.		We believe it should be part of the I&C design basis part. However, the concern is that the vulnerability analysis may be widely available. We can discuss it.	
3	USA	4	1	1st bullet: Revise the first bullet to read “The I&C systems that comprise the overall architecture”	The term “the high level definition of the I&C systems” is not clear	x				
4	USA	4	1	4th bullet: The ~~communications between~~ interconnections across I&C systems and the ~~topology of communication links~~ respective interactions allocated and prohibited.	“communications” (connoting content such as messages) and “topology of communication links” are not the level of detail needed at the initial stage. “Interconnections” is less detail than “topology of communication links.” “interactions allocated and prohibited” are more informative for analysis than the nebulous “communications.”	x				
5	USA	4	1	New bullet: - The design constraints (including prohibited interactions and behaviors) allocated to the overall architecture	Completeness	x				
6	USA	4	1	New bullet: - The definition of the boundaries among the various I&C systems	Completeness	x				

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
6	USA Suppl.	4	1	3rd bullet: The ~~assignment~~ allocation of I&C functions and behaviors (including prohibited behaviors) to these systems, and	“Allocation” is the term used in authoritative literature – not assignment. Allocation of “functions” is not enough. Allocation of quality requirements (relegated to non-functional in DS431) is also necessary. Example flow-down: Constraint identified in HA → Requirement spec for the item → “Prohibited behaviors” allocated to the item.	x				
5	USA Suppl.	4	1	2nd bullet: The tiered structure organization of these systems, including inter-relationships and prohibited interactions;	“Tiered structure” is nebulous and overly prescriptive. Provide meaningful guidance on the architectural information needed for analysis: {inter-relationships; prohibited interactions}.	x				
4	USA Suppl.	4	1	1st bullet: Identification of the I&C systems, their boundaries, relationships with assumptions about their environments;	High level” in the DS431 definition is a nebulous expression. Often assumptions are made because the environment-definition is also co-evolving, but these should be explicit. The proposed definition identifies the minimum information needed at the top-level I&C architecture.	**x**	**See comment resolution on USA 4.1 #3,4,5,6.**			
3	USA Suppl.	4	1	Multiple comments to follow, revised and re-submitted from previous proposals.	IAEA rejected the previously submitted proposals on section 4, alleging “too much detail.” It ignored the need. Current practice does not produce/provide architectural information sufficient for analysis at the early stages of the system development lifecycle, because “Architecture” is a poorly understood subject. Yet, DS431 does not even define the term. On the other hand, in other places, DS431 includes details of secondary value, claiming that the information is needed by nations entering the age of nuclear power generation. For example, the IAEA comment-reviewers deem “topology of communication links” to be more important than identifying the system boundary, its interactions with its environment, and prohibited interactions. Next to inadequacies in hazard analysis, architectural weaknesses are one of the largest contributors to mishaps in digital systems for various critical application domains. “High level” in the DS431 definition is a nebulous expression. Often assumptions are made because the environment-definition is also co-evolving, but these should be explicit. The proposed definition identifies the minimum information needed at the top-level I&C architecture.	**x**	**See comment resolution on USA 4.1 #3,4,5,6.**			
8	USA	4	2	4.2 4th bullet The ~~assignment~~ allocation of I&C functions ~~to individual I&C items~~ , behaviors, constraints, and (derived) quality requirements to each item at each level of integration.	“Allocation” is the term used in authoritative literature – not assignment. The DS431 4th bullet does not provide adequate information to analyze the architecture. Allocation of “functions” is not enough information. Associated behaviors (resulting from interaction of functions) must also be identified. Allocation of quality requirements and constraints is also necessary. Allocation to (leaf-node) items is not enough. Allocations to each item at each level of integration must be identified.	x				
9	USA	4	2	Add a bullet as follows: Rules of composability and composition to assure that the composition of behaviors at one level of integration satisfies the behaviors required at the next higher level of integration and does not introduce other behaviors.	If the composition-decomposition is not constrained through such rules, it cannot be assured that system properties will be satisfied; the number of possible behaviors will be so large that the system would not be verifiable.	x				
10	USA	4	2	4.2.(existing) 5th bullet: Replace existing 5th bullet “The layout of communications between items and subsystems within the individual I&C system; ”with the following: The interconnections across items at each level of integration and across levels of integration and the respective interactions allocated and prohibited.	“Layout of communication” is more detail than necessary at the initial stage; yet it does not provide the information needed for analysis, which is the proposed new text. “communication between items and subsystems ~” is nebulous. For example, communication of the value of some status bit is not very useful in system safety analysis. Complementing the information about the behavior of each item, for safety analysis, it is also necessary to know the associated interactions across items at the same level of integration and across levels of integration.	x				

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
11	USA	4	2	4.2. existing 6th bullet: Delete	"Unnecessary complexity" is nebulous. Flow down the properties {Assurability →Analyzability →Verifiability} and the corresponding constraints, e.g. rules of composibility and compositionality. These flowed-down constraints should naturally lead to solution options such as partitioning. "…unnecessary interactions" is nebulous. "… not introduce other behaviors" is a more precise constraint.	x				
12	USA	4	2	New bullet: - The design constraints (including prohibited interactions and behaviors) allocated to each individual I&C system	Completeness	x				
7	USA	4	2	4.2 bullets # 1-3, Replace bullets #1-3 with the following: "The composition-decomposition relationships through all levels of integration down to the indivisible, individual item."	The proposed change is less level of detail – yet more informative – than the original text. It avoids presumptions about the existence of "subsystems" and "hierarchies." The expression "composition-decomposition relationship" enables association of properties with relationships.	x				
7	USA Suppl.	4	2	existing 6th bullet. Delete.	"Unnecessary complexity" is nebulous. Flow down the properties {Assurability →Analyzability →Verifiability} and the corresponding constraints, e.g., rules of composibility and compositionality (see previous comment on 4.2, new bullet). These flowed-down constraints should naturally lead to solution options such as partitioning. " ~ unnecessary interactions" Is nebulous. See 4.2, proposed new bullet, "… not introduce other behaviors" - a more precise constraint. Further upstream, see the concepts of prohibited interactions (comments on 4.1) and prohibited behaviors (comments on 4.2).	x				
15	FR	4	10	4.10 should appear before 4.9. 4.10 might be combined with 4.8	Same topic.			x	First is a concept, second how to achieve it.	
16	FR	4	41	Make 4.41 a footnote of 4.40. 4.40. Probabilistic studies* should not treat I&C items important to safety as fully independent** unless they are diverse, and meet the guidance for functional independence, electrical isolation, communications independence, environmental qualification, seismic qualification, electromagnetic qualification, physical separation, and protection against internal events given in this document. ~~4.41.~~ *Probabilistic studies include, for example, reliability analysis and probabilistic safety assessment. ** In probabilistic studies systems are treated as fully independent by simply taking the product of their individual failure probabilities.	4.41 brings clarity to 4.40	x				
13	USA	4	11e	After the word "diversity," add the words "verifiability (including analyzability and testability)"	Completeness	x				
17	FR	6	34	Combine 6.34 with 6.33	6.34, as 6.33, gives example of limitations to physical separation.			x	These are all informative paras. Combining all of them, the new para will be too long.	
18	FR	6	60	Combine 6.60 with 6.59	Without 6.60, 6.59 is not understandable…			x	6.58-6.63 are all informative paras. Combining all of them, e.g. 6.58-6.60, the new para will be too long.	
5	DE	6	62	~~Diversity need not always be implemented in separate systems~~ Diversity may be implemented in the I&C architecture of different way. For example, functional diversity and signal diversity might be implemented within a single system.	rephrase	x	6.62. It is not always necessary to apply diversity in separate systems. For example, functional diversity and signal diversity might be applied within a single system.			

NUSSC and NSGC comments on:
Design of Instrumentation and Control Systems for Nuclear Power Plants (DS 431, Rev. “M”)

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
14	USA	6	108	Revise the section to read: “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.” An alternative is to create a new separate section 6.11x to incorporate the underlined sentence above.	For completeness, the concept of hazards contributed through systemic causes should be included.	x				
5	RoK	6	157	Areas of particular concern for ~~are~~ access to ~~set point~~ setpoints adjustments, calibration adjustments, and configuration data, because of their importance to preventing degraded system performance due to potential errors in operation or maintenance.	The term “are” is unnecessary. Also the term “setpoints” rather than “set point” seems to be more appropriate.	x	6.157. Areas of particular concern are access to set point adjustments, calibration adjustments and configuration data, because of their importance to preventing degraded performance of systems due to errors in operation or maintenance.			
3	AR	6	201	Add the following phrase: In case of loss of redundancy in a safety system is not acceptable, then an automatic interlocking should be implemented to prevent such situation.	The objective of such recommendation is to avoid that an operator inadvertently can induce a loss of minimum redundancy.			x	This is a citation from SSR 2/1, we cannot change it.	
19	FR	6	216	6.216 I&C components in the plant should generally be marked with their identifying information. ~~6.217.~~ Components or modules mounted in equipment or assemblies could however ~~do~~ not ~~need~~ have their own identification~~.~~ as Configuration management is generally sufficient for maintaining the identification of such components, modules and computer software.	Combine 6.216 and 6.217 as they seem to oppose if kept separately.	x	6.216. I&C components in the plant should generally be marked with their identifying information. Components or modules mounted in equipment or assemblies do not need their own identification. Configuration management is generally sufficient for maintaining the identification of such components, modules and computer software.			
1	PK	6	221	Para. 6.221(Addition of new para) HUMAN–MACHINE INTERFACE: Effective human–machine interfaces for systems important to safety are necessary to provide the operator with accurate, complete and timely information on plant status and to enable proper operation of the systems controlled by the I&C systems.	The Requirements for Design require that systematic consideration of human factors and the human–machine interface be included in the design process			x	HMI considerations are addressed in greater details in section 8.	
2	PK	6	222	Para. 6.222(Addition of new para). QUALITY: Components and modules of systems important to safety should be of a quality that is consistent with the aim of minimizing maintenance needs and failure rates.	High quality of design and manufacturing is necessary to ensure that systems important to safety can be demonstrated to meet their safety requirements. Design and manufacturing in accordance with appropriate quality levels are important elements.			x	We belive that quality of I&C has been adreesed in a comprehensive way through out the document (sections 2,4,6,7, and 9).	
3	PK	6	223	Para. 6.223 (addition of new para under quality heading): In the selection of equipment, consideration should be given to both spurious operation and unsafe failure modes, e.g. failure to trip when required	In the selection of equipment, consideration should be given to both spurious operation and unsafe failure modes, e.g. failure to trip when required			x	Spurious operation and usafe modes are discussed in a comprehensive way in sections 2, 4, 6, and 7.	
15	USA	7	11	Suggest adding an item after 7.11 but before 7.12 as follows: “7.12. Control system design, including sensors and actuators, should consider design margins.”	The design margin is VERY important. An example of the importance is that NRC is considering requiring NPPs to have the full range level measurement in spent fuel pool (the previous design does not have this margin). In industry practice, all control systems must demonstrate sufficient gain margin and phase margin.	x	Added to 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 necessary to monitor the variable in all plant states during which the information from the sensor is needed. The design of sensors and actuators, should consider design margins.			
16	USA	7	22	Add a new bullet to state that “A suitable human factors engineering (HFE) analysis should be performed to ensure that plant conditions can be maintained within recommended acceptance criteria for each plant initiating event.”	Completeness	x				

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
17	USA	7	22	7.22 e) Add a new sentence that reads – "The associated timing analysis should consider the difference between Time Available and Time Required for operator action since it 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."	Completeness	x	The associated timing analysis should consider the difference between time available and time required for operator action since it 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.		Second part of uncertainty not included, this is an explanation.	
4	AR	7	61	Add the following phrase: The non-interruptible electrical supply for safety I&C should decouple from the electrical supply for the operational I&C and should be fed from two independent lines.	Although these safety measures are possible engineering resources to fulfill the point 7.60, it is considered that they have to be highlighted in the safety guide.			x	This is applicable to "I&C systems that are required to be available for use at all times in operational states or design basis accident conditions"…	
4	RoK	7	165	~ of paragraphs ~~6.79~~ 6.78 to ~~6.135~~ 6.134~	Reflect changed paragraphs numbers.	x				
6	DE	7	172	Examples of techniques to provide compensatory evidence include: • Device specific complementary tests appropriate to the intended application and other elements of evidence of correctness, • Evaluation of applicable and credible operational experience, • Verification of design outputs, and • Complementary the statistical testing.	Statistical testing is not commonly accepted as compensatory evidence for software-based I&C in the nuclear safety domain. This technique should only be treated as an option (complementary measures) in the V&V process.			x	We agree, but para 7.172 reads…Examples….	
20	FR	8	6	Safety classified indications and controls should be provided to implement emergency operating procedures (EOP) and, to extent practicable, SAMG.	Why are SAMG not mentioned (EOP or SAMG) ? This implies than only DBA (and not DEC) are considered…	x	8.6. Safety classified indications and controls should be provided to implement emergency operating procedures and severe accident management guidelines.			
21	FR	8	7	Transform 8.7 as a footnote to 8.6	To avoid			x	Para 8.7 should stay (i.e., not to be a footnote).	
6	RoK	8	17	Where it is impractical (to provide all controls in the supplementary control room) to fulfil the recommendation of paragraph 8.16, controls at local control points may be used.	The modification of the paragraph to provide clear understanding.			x	Current 8.17 is correct; ….all controls needed to fulfil… i.e. not all as in the main control room.	
7	RoK	8	21	The set of displays for monitoring accident conditions is usually called an 'Accident Monitoring System' or a 'Post Accident Monitoring System.'	Simple editorial correction			x	we have both split with "or" .	
22	FR	8	22	d) Determine the status and performance of plant systems necessary to mitigate a design basis accident and design extension conditions and bring the plant to a safe state;	DEC should be addressed. To be consistent with 8.23	x				
23	FR	8	23	Instrumentation performing the indication functions given in paragraph 8.22 items a~~, b, and c~~ to d should be classified as safety and should be provided by I&C equipment capable of performing under design basis accident conditions and design extension conditions.	DEC should be addressed.	x				
24	FR	8	25	Combine 8.25 with 8.24	Same topic			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	
25	FR	8	44	Combine 8.44 with 8.43	Same topic			x	This is a format of a writing style applied for this safety guide; short paras, informative and normative separate.	
8	RoK	8	61	The HMI, procedures, ~~training systems, and~~ training systems should be consistent with each other.	The terms "training system" and "training" are repetitive expression			x	training system and training are different.	
9	RoK	8	65	All aspects of the I&C system (including controls ~~arrangements~~ and displays) should be consistent with the operators' mental models and established conventions.	The term "control arrangements" is not match with the term "display". In this regard, this paragraph can be modified as "All aspects of the I&C system (including controls and displays arrangements) should be consistent with the operators' mental models and established conventions.	x				
26	FR	8	65		It is a quite challenging recommendation as operators' mental models is also depending on training and training is to be consistent with the available I&C…s	x			We agree, but this SG will be in force for the next 10 years.	
27	FR	8	72		8.73 is encompassing 8.72			x	These topics are slightly different.	

NUSSC and NSGC comments on:
Design of Instrumentation and Control Systems for Nuclear Power Plants (DS 431, Rev. “M”)

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
28	FR	8	93	Transform 8.93 as a footnote of 8.92	Enable understanding of 8.92	x				
8	USA Suppl.	9	2	Reword as follows: Software by its very nature and intent tends towards allows for a much larger design space than (electrical or mechanical) hardware. If not systematically constrained, it can become defect-prone and unverifiable.	The reliability related content of this paragraph does not have a sound technical basis; such content should be eliminated. For example, there is no technical basis for the claim, “Reliability is inferred from the assessment of the quality of production activities …”. Current software development standards and guidelines are not specific enough to estimate the quality of the product without verification. While adequate verification of a small simple unit of software may be possible, it becomes increasingly difficult with increasing interactions and feedback paths across units of software and hardware. In currently fielded systems, complete testing is not even feasible. In current practice, the use of analytical verification techniques is very limited. Verification can only be as good as the quality of the requirements specifications. Current practice (narrative in natural language) does not provide unambiguous, complete, consistent, and verifiable requirements specifications. Current practice does not allow the estimation of the incompleteness. Unintended interactions and hidden dependencies contribute unknown uncertainties. There is not broadly agreed upon definition of “Complexity”; some standards define it in terms of verifiability. The proposed change includes an explanation of the underlying phenomenon (much larger design space, by intent). “Failure” and “failure modes” should not be used for software, because it does not fail (“break down”) in operation; if it is faulty, the fault existed from its inception (due to an engineering deficiency). For the same reason “Reliability” and “reliability measure” (R(t1, t2) The probability that an item can perform a required function under given conditions for a given time interval (t1, t2)) should not be applied to software. “Testability” is subsumed in “Verifiability.” “If not properly constrained” provides the introduction for the following guidance paragraphs.	x				
29	FR	9	9	Combine 9.9 and 9.10, 9.9. The developers of software requirements should have an appropriate understanding of the underlying system design basis, as described in section 3, ~~. 9.10. Understanding of the system design basis is needed~~ to ensure that software requirements properly implement essential system properties. Relevant issues include:…	Make obvious the purpose of the recommendation			x	9.9 normative para, 9.10 informative para. We keep them separate.	
18	USA	9	10	Replace “implement” with “satisfy”	Editorial. Requirements don’t implement.	x				
19	USA	9	11	a) Replace component with item.	Consistently use the defined term “item”.	x				
20	USA	9	11	e) “Satisfy the system requirements allocated to the software items, including the quality requirements.”	“Address as appropriate” is nebulous. “Software” is an amorphous term. The system architecture identifies its constituent items.	x				
21	USA	9	11	g) Delete	This paragraph does not have a sound technical basis. “Reliability” and “reliability measure” (R (t_1, t_2) The probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2)) should not be applied to software.			x	It is not acceptable to delete this clause. This has been the subject of considerable discussion and consensus has been reached by the nominated experts by including the explanation (now a footnote) following point g. The explanation already answers this comment.	

NUSSC and NSGC comments on:
Design of Instrumentation and Control Systems for Nuclear Power Plants (DS 431, Rev. "M")

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
1	CA	9	11	g) … The level of reliability and availability might be defined quantitatively and/or qualitatively, for example in terms of the supporting software requirements …	Some member country requires the level of reliability and availability quantitatively and qualitatively. The expression, "and/or" allows the option in the paragraph.			x	This has been the subject of considerable discussion and consensus has been reached by the nominated experts by including the explanation (now a footnote) following point g. The explanation already answers this comment.	Sent on 23 June 2014
2	CA	9	22	… For example of systems of lower safety classification, the balance between safety and complexity should not reduce the safety.	For systems of lower safety classification the balance between safety and complexity is different and higher levels of complexity may be accepted. This paragraph was revised from 2012 November version. However, it is still not clear what is different and what higher levels of complexity are. That's why rephrase is proposed in safety point of view.			x	9.22 is an informative para and provides clarification on a simplicity in systems of a lower safety class to 9.21 (safety systems). There is no "should statement" on it.	Sent on 23 June 2014
3	CA	9	23	Software design architecture" should be defined by the contributors to drafting and review team. It is not a proposed text.	With the definition, it is easy for reader to understand the term. The term is not available in IAEA glossary.	x	Architecture: Organisational structure of the I&C systems of the plant which are important to safety is contained in IEC 61513.			Sent on 23 June 2014
4	CA	9	24	Software design architecture" should be defined by the contributors to drafting and review team. It is not a proposed text.	With the definition, it is easy for reader to understand the term. The term is not available in IAEA glossary.	x	Architecture: Organisational structure of the I&C systems of the plant which are important to safety is contained in IEC 61513.			Sent on 23 June 2014
5	CA	9	25	"Information hiding" should be defined by the contributors to drafting and review team. It is not a proposed text.	With the definition, it is easy for reader to understand the term. The term is not available in IAEA glossary.			x	We believe that 9.25 is self explanatory; there is no need to have a definition of "information hiding"..	Sent on 23 June 2014
1	RoK	9	56	*9. 56, §9.57, §9.61 (comments) Operating experience of operating system should be available.*	According to NS-G-1.1, 9.25, Requirements of operating system (OS) should be added in appropriate section. Especially, operating experience of OS should be included in DS 431.			x	Para 7.68 refer to OEF in digital systems in general. OEF related to HW and SW are explicitely mentioned in 7.68, 7.106, 7.172, 7.173, 9.71, and 9.72.	
6	CA	9	63	Software requirements, design and implementation should be verified against the previous outcome in the I&C life cycle as shown in FIG 2	"Software requirements, design and implementation should be verified against the I&C system requirements specification." It could be interpreted as three outcomes should be verified against the same system requirements, which is not agree with the dotted line (V&V activities) in FIG 2. In addition, FIG 2 should be considered as a general consensus in spite of typical model		Software requirements, design and implementation should be verified against the specification of the I&C system requirements.	x	We belive that curret wording complies with FIG. 2..	Sent on 23 June 2014
7	CA	9	65	The results of each software life cycle phase should be verified against the requirement/design set by the previous phases.	All the outcomes on the life cycle phases are not verified against the requirements. Requirements to be used are plant requirements, system requirements, software requirements, and hardware requirements. The others are system design and software design which are used in the verification too.		The results of each phase in the software life cycle should be verified against the requirements set by the previous phases.	x	We belive that curret wording complies with FIG. 2..	Sent on 23 June 2014
11	RoK	Annex I	Table I-1	*(comments) IEEE Std. 1074, IEEE Standard for Developing Software Life Cycle Processes should be included.*	IEEE Std. 1074 is used for Developing Software Life Cycle Process. This standard corresponds to ISO/IEC 12207.	x				
12	RoK	Annex I	Table I-2	*(comments) IEEE Std. 1074, IEEE Standard for Developing Software Life Cycle Processes should be included.* 9. Software Internationally Used I&C Standards IEC 60880, IEC 62138, IEEE 7-4.3.2, IEEE 1012, ISO/IEC 12207, IEEE 1074	IEEE Std. 1074 is used for Developing Software Life Cycle Process. This standard corresponds to ISO/IEC 12207.	x				
30	FR	Annex III	Annex III	Delete Annex III …	This annex does not reflect international consensus (it actually shows competing/conflicting practices…). **Comment to be discussed at NUSSC**				Technical officer cannot make a decision here. Including ANNEX III was an agreed fragile consensus among several MS. It should be discussed among NUSSC members whether to delete or keep it.	
1	DE	Fig. 1		~~cybersecurity~~ computer security	The term 'cybersecurity' should replace by the term 'computer security' (see current IAEA wording)			x	This figure has bee agreed with NSNS	

MS No.	Member State	Sec.	Para	Proposed new text	Reason	Accept	Accepted, but modified as follows	Reject	Reason for modification/rejection	Remark
3	FR NSGC	Fig. 1		Interfaces between nuclear safety and nuclear security exist also during the operating phase due to maintenance activities and periodical testing. This should be reflected into the figure.				x	We believe that Fig. 1 shows this interface during the operation and maintenance; the security during operations phase would follow directly from cyber security planning and the development of cyber security controls which are already in the figure.	