RESOLUTION OF MEMBERS COMMENTS

ON

DS436 Version 2

CONTENTS:

DS436 Instrumentation and Control and Software Important to Safety for Research Reactors

COMMENTS BY REVIEWER Reviewer: Canadian Nuclear Safety Commission industry Page.... of.... Country/Organization: CANADA Date: October 24, 2012				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	General (ZCZ)		**Comment**: Both phrases “experimental devices” and “experimental facilities” have been used in DS-463. In comparison, only “experimental devices” has been used in NS-R-4. Consistency between these two document is required	Accepted			
2.	Para. 2.1 (ZCZ)	Suggested change 1: Delete Bullet 4 or Suggested change 2: I&C systems important to safety are those I&C systems used to accomplish functions important to safety.	Bullet 4 states that “*I&C systems important to safety are those systems used to accomplish functions important to safety*.” **Comment**: Emergency power supply is ITS but not necessarily be I&C system	Accepted			
3.	Fig. 1 (ZCZ)		I&C for Command and Monitoring, such as post accident monitoring system and safety parameter command and display console and panels is listed under “Protection Systems” **Comment**:		“*Safety Parameter Command and Display Consoles and panels*” will remain in FIG. 1. meanwhile “*Post Accident*		“*Safety Parameter Command and Display Consoles and panels*” belong to the Protection System (PS) itself.

			Classification of I&C system for RRs might be different than NPPs, but should not be too far apart. Clarification is required why I&C for command and monitoring be part of the protection systems		*Monitoring System*" will be removed from it.		
4.	Para. 2.3 (ZCZ)	Re-organize Para. 2.2 and Para. 2.3	It states that "*Safety related systems are systems important to safety and performing other safety functions not mentioned in par. 2.2.*" Command: The first statement of para. 2.2 defines what the safety systems consisted of (protection system, the safety actuation systems and the safety system support features). The second statement simply says that do not add functions or components that are not strictly required by the highest safety classification. It should be noted that there is no mention of what the safety functions of safety systems suppose to perform in para. 2.2.		Yes		It will be re-phrased as: *"Safety related systems are systems important to safety performing other safety functions not mentioned in par 2.2 as monitoring the availability of safety systems or diminishing the needs of a safety system to actuate performing other smooth actions in advance."*
5.	Para. 2.5 (ZCZ)		It states that "*For I&C systems having safety importance, graded approach to the requirements of NS-R-4 can be applied but the*	Accepted			

			extent of grading should be clearly justified in the Safety Analysis Report (see paragraph 1.14 of Ref. [1]).” **Comment**: New terminology “having safety importance” is used in this paragraph. If it is refer to “important to safety”, then, “important to safety” should be preferred. Otherwise, it should be defined.				
6.	Para 2.7 (ZCZ)		It states that “*Functions of safety systems are to ensure timely detection of violations of limits and conditions for safe operation of research reactor and automatically initiate reactor shutdown, emergency core cooling and residual heat removal, and containment of radioactive materials and/or limitation of accidental releases.*” **Comment**: It looks like that “containment” should be replaced with “confinement.” According to IAEA safety glossary, terminology	Accepted			

			“confinement” is defined as “*Prevention or control of releases of radioactive material to the environment in operation or in accidents,*” while “containment” is defined as “*Methods or physical structures designed to prevent or control the release and the dispersion of radioactive substances.*”				
7.	Para. 2.10 (GR)	o I&C for Command and Monitoring: - Safety Parameter Command and Display Consoles and Panels; and - Accident Monitoring Instrumentation	o I&C for Command and Monitoring: - Safety Parameter Command and Display Consoles and Panels; and - Post-Accident Monitoring System. **Comment**: Accident monitoring might be the correct terminology then post—accident monitoring system	Accepted			
8.	Para. 2.17 / 2.18 (ZCZ)		**Comment 1**: Bullet 2 of para. 2.18 is same as Bullet 3 of para. 2.17 and should be deleted. **Comment 2**: Bullets 4 and 5 of para. 2.18 are	**Comment 1** accepted. Part 2 of **Comment 2** accepted,	**Comment 3** Bullet 3 of 2.18 will be re-phrased as: - *“the potential of the I&C system itself to*		Regarding to part 1 of **Comment 2**, Bullets 4 an 5 of 2.18 consider timeliness for alternative actions and detection of

			the expansion of Bullet 4 of 2.17. In addition, what are the rationales to put timeliness (30 minutes and 12 hours) in Bullet 4 and 5 of para. 2.18. Clarification is required. **Comment 3**: Bullet 3 sates that “*the potential of the I&C system itself to cause a Postulated Initiating Event (PIE) (i.e. the I&C system’s fail-safe modes), ...*” It is not clear from the above quoted statement that whether causes PIE is the intention or one of consequences of fail-safe design. Clarification is required.	there will be deleted the references to specific numbers.	*cause a Postulated Initiating Event (PIE) (i.e. the I&C system’s fail-safe modes), ~~the provisions made in the safety systems or in other I&C systems covered by this Safety Guide for such a PIE (i.e. provisions for detection of I&C system failure),~~ and the combination of the probability and consequences of such a PIE (i.e. frequency of failure and radiological consequences)* ”		failures meanwhile Bullet 4 of 2.17 is focused in the time at which it is expected the response of the dedicated I&C system following a PIE.
9.	Para. 2.21 (ZCZ)		It states that “*All I&C systems and equipment should be designed,*	Accepted			

			constructed and maintained in such a way …” **Comment**: It looks like that “operated” is missing from and should be added after “constructed.”				
10.	Para. 3.2 (ZCZ)		**Comment**: “para. 2” and “para. 6” is used. Should “para.2” be “Section 2” and “para. 6” be “Section 6”. Please refer to para. 1.5. It states that NS-R-4 consists of 8 sections.	Accepted			
11.	Para. 3.4 (ZCZ)		**Comment**: It states that “*A well designed architecture can reduce the complexity of I&C systems and can locate essential complexity in systems where it can be better managed or where it will pose less risk to the facility safety.*” It looks like “locate” should be “allocate.”	Accepted			
12.	Para. 3.4 (ZCZ)		It states that “*For example, in existing designs the separation of I&C functions between safety and safety related systems allocates complex functions to safety related systems and limits the safety systems to the performance of*	Accepted			The example will be deleted and 3.4 will be re-phrased as: “*Modern I&C systems are more highly integrated*

			simpler functions.” The statement is unclear and confusion. **Comment**: The statement is not in alignment with those for Method of Classification (paras. 2.17 to 2.20). Separation of I&C functions between safety and safety related system IS NOT for allocating complex functions to safety related systems.				*than were the last generations of I&C systems. The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A well designed architecture can reduce the complexity of I&C systems by a rational allocation of functions only in the systems where they are needed.* ~~*and can locate essential complexity in systems where it can be better managed or where it will pose less risk to the facility safety. For example, in existing designs the separation of I&C functions between safety and safety related systems*~~

							~~*allocates complex functions to safety related systems and limits the safety systems to the performance of simpler functions.*~~
13.	Para. 3.7 / 3.8 (ZCZ)		**Comment**: Paras. 3.7 and 3.8 should be merged.	Accepted			
14.	Para. 3.18 (ZCZ)		It states that "*A common cause failure (CCF) is defined as the concurrent failure of two or more structures, systems or components due to a single event or cause.*" **Comment**: The definition of CCF by DS431 removed "concurrent failure." There should be consistence between these two DSs related to I&C systems.		Yes		Definition as in IAEA Safety Glossary will be used.
15.	Para. 3.27 – 3.29 (ZCZ)		It states that *"… provide a hierarchical system design where I&C safety system keep the highest hierarchy and priority to perform the safety functions for which they have been designed.*" **Comment**: Hierarchical system design might	Accepted	Yes		It will be re-phrased as: *"… provide preferably a hierarchical system design where I&C safety system keep the highest ~~hierarchy~~ and*

			not be the only solution considered the variety of types of RR and possible graded approach could be used in the design. In addition, according to FIG. 3.1, the safety systems might not necessary be on the highest hierarchy (supervision level is on the top). Therefore, keeping the highest priority for safety system is fine but not for highest hierarchy. According to para. 3.29, safety and process functions should be allocated to the control level, which is not the highest hierarchy according to FIG 3-1. Clarification is required.				*priority to perform the safety functions for which they have been designed.*”
16.	Para. 3.27 (ZCZ)		**Comment**: The 4th Bullet requires the definition of interfaces between the individual I&C system. The 5th Bullet requires dividing overall I&C system into individual systems. Logically, it is better that the 4th and 5th Bullet be swapped.	Accepted			
17.	Para. 3.28 (ZCZ)	Member State requirements for I&C licensing~~, e.g., security, software qualification~~;	It states in para. 3.28 h) that “*Member State requirements for I&C licensing, e.g., security, software qualification;*”	Accepted			The objection is right so *“Software qualification”* will be deleted as the

			Comment: It is understandable security requirements for I&C licensing influences the overall I&C architecture design. However, it is not clear why software qualification requirements play a role in the design of I&C architecture. Does it refers to the decision on the selection of computer based systems or hardwired systems? Clarification is required.				example does not play any role in the design of I&C architecture.
18.	Para. 3.31 (ZCZ)		**Comment**: In power reactor, the decision on implementing redundancy might not be strictly based on safety classification of each I&C system. Sometimes, the decisions are made based on providing reliable power production. Clarification is required for research reactor.	Accepted			It will be added a last sentence in the paragraph to clarify this issue as follows: *“In case of redundancy, other factors as availability of I&C systems should be considered*
19.	Para. 4.4 (ZCZ)		It states that “*The intent of avoiding complexity is to keep the I&C system as simple as possible but still fully implement its safety requirements.*” **Comment**:	Accepted			It will be deleted Paragraph 4.4 will be deleted. The first sentence of the paragraph will be deleted and the remainder of it will

			The design should first meet its functional requirements. It looks like implementing functional requirements is missing from here. Clarification is required.				be merged with 4.3 as examples, so 4.3 will be re-phrased as: *4.3 Unnecessary complexity should be avoided in the design of I&C systems.* *Examples of complexity to be avoided are the inclusion of functions not important to safety, architectures involving overly complex communication or system interactions, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration. Careful*

							documentation and review of the rational for each requirement is one effective means for avoiding inessential complexity.”
20.	Para. 4.5 (ZCZ)		**Comment**: Delete Item j because items listed (except Item j) are part of acceptance of criteria.	Accepted			
21.	Para. 4.9 (ZCZ)		**Comment**: It states that “*I&C systems important to safety have a critical role in achieving the three basic safety functions* — ....” It is recommended to replace “three basic safety functions” with “main safety functions” to be consistent with IAEA safety glossary.			Rejected	NS-R-4 uses the concept of “*basic safety functions*”,
22.	Para. 4.11 (GR)	Non-compliance with the single failure criterion may be justified for: • Very rare PIEs, that are found to be less frequent by alternate methods (e.g., site specific	Non-compliance with the single failure criterion may be justified for: a) Very rare PIEs Comment: Very rare PIEs are not well defined. Instead, justification method could be defined or ‘very		4.11 will be rephrased as: “*No single failure could result in a loss of a system to perform its intended safety function.*”		To be consistent to what is stated in Safety Requirements for Research Reactors, NS-R-4, para. 6-36

		data);	rare’ should be defined for clarity				
23.	Para. 4.18 – 4.26 (ZCZ)	It is suggested to use “four elements” principle of independence, which is more appropriate to the digital I&C systems. It is suggested to use “functional independence” to replace “functional isolation” to avoid potential confusion.	It states that “*The principle of independence (e.g. functional isolation, electrical isolation and physical separation by means of distance, barriers or a special layout for reactor components) should be considered and applied, as appropriate, to enhance the reliability of systems.*” **Comment**: According to the document, independent is achieved by three elements: functional isolation, electrical isolation and physical separation. In DS431, independent is achieved by four elements: functional independent, electrical isolation, physical separation and independent of communication. Should DS436 considered to “mitigate” to the four elements principle of independence? Phrase “functional isolation” is used in DS-436, which is in alignment with NS-R-4. However,	Accepted			

			in the some IAEA document, “functional isolation” was referred to as “electrical isolation” as noted by IEC 61513-2011 a special note for section 3.31 as quote below: “*NOTE Means to achieve independence in the design are electrical isolation (also called functional isolation in IAEA documents), physical separation and communications independence.*”				
24.	Para. 4.32 (ZCZ)		Para. 4.32 lists variable diversity as one of the diversity applied to I&C systems. **Comment**: Variable diversity might not be directly related to I&C systems. For example, the selection of trip parameters is not based on diversification of requirement from I&C systems. It is based on trip parameter coverage (PIE, primary and secondary trip parameter)	Accepted			The bullet “*variable diversity…”* will be deleted
25.	Para. 4.33 (GR)	The diversity should extend to the equipment’s components to ensure that actual diversity exists. For example, different manufacturers might use	The diversity should extend to the equipment’s components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system,	Accepted			The paragraph will be re-phrased as: *The diversity should extend to the equipment’s components to*

		the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers’ names are insufficient without consideration of this possibility. To minimize common failure modes, the design should consider the options of same processor with different operating system or different processors with same operating system or different processors with different operating system. However, this should be described in paragraph 8.10.	thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers’ names are insufficient without consideration of this possibility. Comments: Guidance on achieving this may require clarification.				*ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers’ names are insufficient without consideration of this possibility. To minimize common failure modes, the design should preferably consider the option of different processors with different operating system.”*
26.	Para. 4.38 (ZCZ)		It states that “*Any identified failures that are not detectable by periodic testing, alarm, or anomalous indication should be assumed to exist in conjunction with*		Yes		Paragraph 4.38 will be deleted

			single failures when evaluating conformance with the single failure criterion.” **Comment**: Common cause failure due to latent software design error(s) is an example of such failure. However, MDEP common position on software common cause failure stated that software common cause failure should not be considered when evaluating conformance with SFC				
27.	Para. 4.40 (ZCZ)		It states that “*Age degradation that impairs the ability of a safety component to function under severe accident conditions should exit well before the functional capabilities under normal conditions are notably affected.*” **Comment**: Combine with “under severe environment conditions” and “age degradation” might not be appropriate. Equipment qualified for mild or even harsh environment might not be functional under severe environment condition they are not qualified to even when the	Accepted			It will be re-phrased as: “*Ageing degradation that impairs the ability of a qualified safety component to withstand and function under severe accident conditions should exit well before the functional capabilities under normal conditions are notably affected.*

			equipment is newly manufactured and installed				
28.	Para. 4.99 / 4.100 (ZCZ)		**Comment**: It is suggested to merge paras. 4.99 and 4.100 or even delete para. 4.100 completely. Redundant information provided by these two paras.	Accepted			Paragraph 4.100 will be deleted
29.	Para. 5.14 (ZCZ)		**Comment**: Compare with NS-R-4 para. 6.96, "*action is clear defined*" is probably missing from para. 5.14 and should be added into it	Accepted	It will be added an additional bullet: • *The diagnosis is simple and the action is clearly defined*		
30.	Para. 5.16 (ZCZ)		It states that "*In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as safety interlocks.*" **Comment**: Please clarify phrase "are classified as safety interlocks" not "are classified as safety system"	Accepted			It will be re-phrased as: "*In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as components/functions of safety systems ~~interlocks.~~*"
31.	Para. 5.21 (ZCZ)	To use programmable devices instead of computer based systems	Comment: IEEE 7-4.3.2 is currently under revision. It is proposed to replace			Rejected	It needs to keep consistency with IAEA terminology.

			“computer-based systems” with “programmable devices.” The para. is limited itself to computer-based system only. It should clarify whether the requirement is applicable to HDL configured device (such as FPGA) as well.				
32.	Para. 5.25 (ZCZ)		**Comment**: The requirements presented in para. 5.25 should not only be limited to computer based system. As mentioned in Comment to para. 5.21, it is applicable to HDL configured device as well. Additional Comment: Please clarify why the concept of I&C life cycle is not used.	Additional comment accepted		**Comment** Rejected	It needs to keep consistency with IAEA terminology. For the Additional Comment the 2nd bullet will be re-phrased as: “*the whole life cycle of the system ~~development process, including control, testing and commissioning of the system~~ should be systematically documented and reviewed; and*”
33.	Para. 5.48 (ZCZ)		It states that “*Some actions in the facilities could affect the safety of the facility and they should be included in the safety system functions.*”	Accepted			This paragraph will be re-phrased as: *“~~Some~~ If there are identified actions in the facilities that*

			Comment: It is not clear with the intent of the statement. For example, is it because some actions could affect the safety of the facility, therefore, there should be corresponding safety functions to protect / mitigate consequences of such actions? Clarification is required.				*could affect the safety of the facility ~~and they should be included in the~~; safety functions to protect / mitigate the consequences of such action should be considered and implemented.”*
34.	Para. 6.15 (ZCZ)		It states that “*Where a safety system, or part of a safety system, has to be taken out of service for testing, adequate provisions should be made for the clear indication in the control room.*” **Comment**: Clarification is required for “*the control room*” as quoted above. Is it referred to the main control room only. Should such indication be displayed in the supplementary control room and to some extent, to rooms where irradiation and experiment facility control systems are located? Clarification is required.	Accepted			This paragraph will be re-phrased as: “*Where a safety system, or part of a safety system, has to be taken out of service for testing, adequate provisions should be made for the clear indication in the control room as well as the supplementary control room if any.*”
35.	Para. 8.1 (ZCZ)		It states that “*They are used both in safety related applications, such as some functions of the process*	Accepted			This paragraph will be re-phrased as: “*They are used both*

			control and monitoring systems, as well as in applications important to safety, such as reactor protection systems.” **Comment**: Please clarify whether “important to safety” and “safety related” used in the above quoted statement are the same as those used in Fig. 1. If they do, which we belief they should, then, please make appropriate modifications to the above statement because according to FIG. 1, safety related applications are also part of the applications import to safety.				*in safety related applications, such as some functions of the process control and monitoring systems, as well as in safety applications ~~important to safety~~, such as reactor protection systems.*”
36.	Para. 8.5 (ZCZ)		**Comment:** Please clarify “…*functionally split the development of Computer Based System in reactor and experimental facilities system*.” Will this requirement impose separation of CB reactor system and experimental facilities system or only the development should be split?	Accepted			This paragraph will be re-phrased as: “…*functionally split the ~~development of~~ Computer Based System in reactor and experimental facilities system*.”
37.	Para. 8.7 (ZCZ)		It states that “*For safety systems, the functional requirements that have to be fulfilled by a computer*	Accepted			This paragraph will be re-phrased as: “*For safety*

			system should all be essential to the achievement of safety functions. Functions not essential to safety should be separated to avoid any impact to safety functions.” **Comment:** It is not clear what the phrase “be separated” means. Does it mean be separated from the functions essential to the safety but be implemented as part of the computer based safety system, or separated and implemented outside of the computer based safety system? It is not clear what the “essential to the achievement of safety functions.” Does self-diagnostic function be considered as essential to the achievement of safety functions?				*systems, the functional requirements that have to be fulfilled by a computer system should all be essential to the achievement of safety functions. Functions not essential to safety should be isolated ~~separated~~ to avoid any impact to safety functions.*”
38.	Para. 8.10 (ZCZ)		**Comment**: Phrases such as “software common cause failures” and “common mode software errors” are used in this paragraph. There should be consistence for using terminology.	Accepted			“*common mode software errors*” will be by replace by “*common mode software failures”*
39.	Para. 8.12	It should be demonstrated	It should be demonstrated that			Rejected	Current

	(GR)	that measures have been taken to protect the computer based system throughout its entire lifetime against physical attack, intentional and non-intentional intrusion, fraud, viruses and so on. Safety systems should not be connected to external networks. If the safety systems are connected to the external network, it should follow the paragraph 8.21 and 8.22.	measures have been taken to protect the computer based system throughout its entire lifetime against physical attack, intentional and non-intentional intrusion, fraud, viruses and so on. Safety systems should not be connected to external networks. Comment: This strategy is not followed in many member state countries. Invariably, for the purpose of information to the corporate HQ or for other requirements, the data is communicated to the external networks. In that case, this should follow certain requirements.				recommendation is an effective countermeasure against external attacks.
40.	Para. 8.12/8.13 (ZCZ)		**Comment**: Phrase "The computer based system" is used in these two paras. It is better to use "Computer based systems" or "A computer based system."	Accepted			
41.	Para. 8.13 (ZCZ)		**Comment**: Benefits of software modular design are described. However, these benefits might not be true, especially "easier to modify without introducing new errors."		Yes		Modular software design facilitates maintenance in comparison with non-modular software design. The phrase: "…

							and easier to modify without introducing new errors" will be deleted.
42.	Para. 8.26/8.11 (ZCZ)		**Comment**: Paras. 8.11 and 8.26 should be moved close to each other because these two paras. are highly related.	Accepted			

Reviewers:	PC	Peter CORCORAN	Canadian Nuclear Safety Commission (CNSC)
	ZCZ	Zhao Chang (Charles) ZENG	Canadian Nuclear Safety Commission (CNSC)
	RG	Guna Renganathan	Canadian Nuclear Safety Commission (CNSC)

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.			During NUSSC28, DS436DPP was discussed. The issue of a guide specific to research reactor (RR) vs a guide addressing both NPP and RR was discussed, eventually with sections with common aspects and then sections with aspects relevant to one type of installation or the other. The TO emphasized that DS436 would address the specificities of RR. Except for very few paragraphs (5.44 to 5.49, ;6.16 and 6.17, fugure 1, 8.5, 10.1, 10.10), the guidance developed in this guide is not specific to RR. This guidance would also be relevant to NPP and, with a few modification, to other nuclear installations. Of course, additional guidance would be useful for NPP (see DS431). The value of this guide for RR and the potential to expand the scope to other nuclear installations should therefore be discussed at NUSSC.				It will be discussed during NUSSC meeting.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
2.			The draft contains specific recommendations on security issues (6.1 to 6.8, 8.77 to 8.81). This draft should be reviewed by NSGC	Accepted			The document will be reviewed by NSGC
3.	1.8	Delete 1.8	Superfluous. 1.10 is enough	Accepted			
4.	1.9	Delete 1.9	Superfluous. 1.10 is enough	Accepted			
5.	1.11	Besides such technically based decisions also other aspects (such as new regulatory requirements…) may influence the final decision for modernization of the I&C system ~~of a given facility as technical specification and/or regulatory requirements might have been changed in the past. As an additional benefit an I&C modernization process might also be accompanied with the decision of a facility power increase, and it is important to take into consideration in these assessments that the facility will be forced to continue to enhance safety, to increase reliability, to shorten outage time and to reduce staff.~~	No need for a lengthy paragraph	Accepted			
6.	1.11	Merge 1.11 as modified according previous comment with 1.10	No need to keep 2 lines as a separate paragraph.	Accepted			
7.	2.1	• functions, systems, and components important to safety are those which ~~significantly~~ contribute to:	Superfluous	Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 10 October 2012				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
8.	2.1	reduce the potential for the release of radioactive material and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after ~~design basis~~ accidents.	BDBA should not be set aside.	Accepted			
9.	Fig 1	In Fig 1 title, add “see also Annex 1”	Clarification	Accepted			
10.	2.7 to 2.16	Delete 2.7 to 2.16	Figure 1 and annex 1 are enough. These paragraphs are quite general and are not specific to I&C. They address the general design of a research reactor.			Rejected	Most of the paragraphs are specific to I&C. Other members of NUSSC valued the paragraphs and provided useful comments to improve them.
11.	2.18	~~• the probability that the I&C system will be called upon to perform a safety function;~~	Redundant with 3rd bullet of 2.17	Accepted			
12.	2.18	• the timeliness ~~(e.g.: up to 12 hours, beyond 12 hours)~~ and reliability with which any failure in the I&C system can be detected and remedied.	Including a 12 hours criteria may be questionable and not relevant for all RR depending on their power.	Accepted			
13.	2.20	Once each of the factors has been considered and analysed for each I&C system a decision should be made by the operating organization on system’s classification (after considering relevant inputs, for example from designer or regulatory body).	Clarification	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
14.	2.21	All I&C systems and equipment should be designed, constructed, operated and maintained	Consistency with usual wording	Accepted			
15.	2.21	that their specification, verification and validation process, quality ~~assurance, quality control~~ and reliability	Superfluous	Accepted			
16.	2.22	in order to ensure that any failure in a system classified in a lower class (less stringent requirements) will not propagate to a system classified in a higher class	Clarification	Accepted			
17.	2.23	~~It should be ensured that the classification of necessary service systems (electrical, pneumatic or hydraulic power supply, lubrication systems) is commensurate with the classification of the safety functions that they support.~~ I&C system or equipment safety class should have the same safety class as the system or equipment they control/monitor. If an I&C system or equipment controls or monitors several systems or equipments, its safety class should be the one of the highest safety class of these systems or equipments.	This recommendations seems less stringent than the one developed in DS367 for NPPs (para 3.2, 3.20 and 3.21), and not focused on I&C	Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 10 October 2012				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
18.	3.1	the containment of radioactive materials and/or limitation of ~~accidental~~ radioactive releases during Anticipated Operational Occurrences (AOO) or during and after accident conditions.	Clarification		It will be re-phrased as: *“the ~~containment~~ confinement of radioactive materials and/or limitation of ~~accidental~~ radioactive releases during Anticipated Operational Occurrences (AOO) or during and after accident conditions”*		*“Confinement”* used instead of “*containment*”
19.	3.2	I&C system architecture should support all I&C functions needed to ensure the safety of the facility ~~fulfil the design basis~~.	The goal should be safety, even if the design basis may be wrong.	Accepted			
20.	3.2	~~The set of Research Reactor I&C systems may vary depending on the type of reactor and their operation modes and usually include those systems stated in section 2 as examples of I&C systems.~~	Superfluous	Accepted			
21.	3.4	Modern I&C systems are more highly integrated than were the ~~last~~ previous generations of I&C systems.	The notion of “generation” is unclear. “Last generation” is even more unclear.	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
22.	3.4	~~A well designed architecture can reduce the complexity of I&C systems and can locate essential complexity in systems where it can be better managed or where it will pose less risk to the facility safety. For example, in existing designs the separation of I&C functions between safety and safety related systems allocates complex functions to safety related systems and limits the safety systems to the performance of simpler functions.~~	Superfluous. .		Yes		The example will be deleted and 3.4 will be re-phrased as: "*Modern I&C systems are more highly integrated than were the last generations of I&C systems. The architecture of highly integrated systems should be carefully considered to ensure proper implementation of the defence in depth concept. A well designed architecture can reduce the complexity of I&C systems by a rational allocation of functions only in the systems where they are needed.*
23.	3.5	Delete 3.5	Superfluous. No recommendation		It will be merged with 3.4		To cite Annex I

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
24.	3.7	The facility design should incorporate the defence in depth.	Clarification	Accepted			
25.	3.8	Merge 3.8 with 3.7 and modify 3.8 as follows : "(see also INSAG-10 [6] and INSAG-12 [7]) ~~further amplify the previous paragraphs~~.	Clarification	Accepted			
26.	3.10 to 3.12	3.10 The overall I&C architecture should: • implement a defence in depth concept. For I&C, Defence in depth ~~should consist of~~ includes implementing successive I&C functions designed to limit the consequences of a PIE ~~design basis event to an acceptable level~~ despite the failure of I&C functions designed to respond first. • not compromise the Defence in Depth strategy of the facility design.	Combine paragraphs with some modifications (changed text is strike out or underlined)	Accepted			
27.	3.15	Safety systems should be independent from systems of lower safety classification as ~~necessary~~ far as practicable to ensure that the safety systems can perform their safety functions during and following any PIE ~~design basis event~~ that requires these functions without any interference or degradation from those systems of lower safety classification.	Nota : independence is somehow defined in the IAEA safety glossary ("independent equipment")	Accepted			
28.	3.19	Merge 3.19 with 3.18	3.19 clarifies 3.18 but is not a recommendation	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
29.	3.20	justification should be provided for any which the operating organization does not ~~that need not be considered~~ as credible sources of CCF between systems or individual components.	Clarification. The regulator may have a different view.		It will be re-phrased as: ¨…*justification should be provided for any which the operating organization does not* ~~*that need not be*~~ *consider as credible sources of CCF between systems or individual components.*		Clarification, “consider” was stroked-thorough
30.	3.21	Transform 3.21 in a footnote to 3.20: Latent failures and common failure modes which potentially might result in a common failure of the redundancies should be identified, and justification* should… *footnote: 3.21 text	It is not a recommendation and other arguments may be used…		3.21 will be combined with 3.20		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Country/Organization:	F. Féron France/ASN		Page Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
31.	3.22	should be no greater than those ~~accepted~~ ~~tolerated~~ for design basis accidents ~~based conditions~~.	Design bases conditions is unclear. “Accepted” may be too strong…		It will be re-phrased as: *¨...should be no greater than those ~~accepted~~ tolerated for design basis accidents ~~based conditions~~.*		Clarification, “tolerated” was stroked-thorough.
32.	3.23	Combine 3.23 with 3.22 or transfer 3.23 as a footnote to 3.22.		Accepted			3.23 will be combined to 3.22.
33.	3.24	Transfer 3.24 after 3.26	More logical location			Rejected	Paragraph 3.26 is appropriate as the final paragraph for the section.
34.	3.26	~~A complete elimination of all vulnerabilities of I&C systems and architecture to CCF is not required, but~~ justification should be provided for accepting identified vulnerabilities, if any, of I&C systems and architecture to CCF that ~~have~~ are not addressed.	Clarification	Accepted			
35.	3.27	• Provide all I&C functions needed to ~~fulfil the design basis~~ ensure the safe operation of the facility and manage AOO and accident conditions;	Clarification	Accepted			
36.	3.27	a) Support ~~design basis~~ requirements for independence between functions in different levels of the defense in depth concept;	Superfluous			Rejected	More specific

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
37.	3.27	c) Establish the redundancy needed to fulfill ~~design basis~~ reliability requirements;	Superfluous			Rejected	More specific
38.	3.28	The inputs to the overall I&C architecture design process should refer to the facility ~~safety~~ design ~~basis~~ documents,	Superfluous			Rejected	More specific
39.	3.28	h) ~~Member State~~ National requirements, including those for I&C licensing, e.g. security, software qualification; and	Some general requirements may also be applicable to I&C	Accepted			
40.	3.28	~~i) Member State requirements with respect to operational requirements (i.e., the I&C design as it affects the interface with facility operators) for systems important to safety.~~	Superfluous considering the proposed modification to 3.28 h).		Yes		It will be re-phrased as: *i) Research reactor operating organization requirements with respect to operational features (i.e., the I&C design as it affects the interface with facility operators) for systems important to safety.*
41.	3.30	to ~~be possible to~~ establish a communication interface	Superfluous	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
42.	3.31	The use of diversity, redundancy, physical separation, electrical and functional isolation, in the overall architectural design of the I&C system, should be ~~based on~~ consistent with the safety classification of each I&C system and the defense in depth concept, both for the overall facility and for the I&C.		Accepted			
43.	3.31	~~the impact in the safe state of the reactor upon the presence of an I&C system's failure (failure or faulty performance of the function(s)) and the probability that a specific I&C system will be called upon to perform a safety function.~~	Superfluous	Accepted			
44.	3.32	Delete 3.32	This anticipates on the result of the safety assessment and on the regulator opinion…		Yes		It will be re-phrased as: *¨The use of the same features (those mentioned in 3.31) in the design of different architectural levels should be applied to reducing the probability of dependant failures of the levels.*
45.	4.2	a demonstration that all relevant design ~~basis~~ requirements have been accounted for.	Superfluous	Accepted			
46.	4.2	Merge 4.2 with 4.1	Same topic				

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
47.	4.4	Merge 4.4 with 4.3	Same topic	Accepted			
48.	4.4	The intent of avoiding complexity is to keep the I&C system as simple as possible ~~but still fully implement its safety requirements~~. to ease safety assessment and future operation and maintenance of I&C systems	Need to clarify why avoiding complexity is to be sought..	Accepted			
49.	4.4	Transfer "Examples of complexity to be avoided are the inclusion of functions not important to safety, architectures involving overly complex communication or system interactions, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration." as a footnote	Explanation and example…			Rejected	To ensure continuity of the text.
50.	4.4	~~Careful documentation and review of the rational for each requirement is one effective means for avoiding inessential complexity~~.	The review of requirement is not enough to avoid complexity… Partially redundant with 4.2		It will be re-phrased as: *Careful ~~documentation~~ ~~an~~d review of the rational for each requirement is one of effective means for avoiding inessential complexity.*		In paragraph 4.2 "*review of the rational for each requirement*" is used with another purpose other than avoiding complexity.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
51.	4.5	c) Functionality requirements for each facility state (including ~~and~~ during extended shutdown~~)~~.	Shutdown is a plant state, as well as extended shutdown			Rejected	Extended Shutdown is not a plant state
52.	4.5	~~j) The acceptance criteria of the system.~~	All items in the bullet list give rise to acceptance criteria	Accepted			
53.	4.5	m) The range of environmental conditions, including those arising from natural phenomena hazards, under which the system is required to perform functions important to safety.	Initial wording is too restrictive	Accepted			
54.	4.7	The level of system reliability should be commensurate with the safety importance of the system. ~~and could be achieved by means of~~ A comprehensive strategy that uses various complementary means (including an effective regime of analysis and testing) at each phase of development of the system and a validation strategy to confirm that the design requirements for the system have been fulfilled should be established and implemented to substantiate the claimed reliability.	Clarification	Accepted			
55.	4.7	Make the following text a separate paragraph: “All I&C systems important to safety regardless of technology should be developed using a defined development process that includes verification and validation. In case of safety systems the verification and validation process should be independent (see 8.34).”		Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Country/Organization: France/ASN		Page Date: 10 October 2012		RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
56.	4.9	I&C systems important to safety have a critical role in achieving the ~~three basic~~ main safety functions	Consistency with IAEA safety glossary (see also DS367)	Accepted			
57.	4.11	Non-compliance with the single failure criterion may be ~~justified~~ envisaged for:	To give flexibility for the regulator…	Accepted			
58.	4.11	At the end of 4.11, add "Adequate justification should be provided before concluding that the SFC does not need to be complied with"	It is up to the licensee to justify why the SFC should not be implemented (unless the national regulation is clear on cases…)	Accepted			
59.	4.12	Delete 4.12	Superfluous. 4.13 is enough		Yes		4.12 and 4.13 will be merged
60.	4.14	Locate 4.14 after 4.16					
61.	4.16	~~When feasible~~ As far as practicable, redundant safety systems should be physically separated from each other and from systems of lower safety classification.	"Feasible" is weak	Accepted			
62.	4.17	The design of I&C system important to safety should ~~provide additional features to~~ minimize the possibility of common cause failures	Superfluous	Accepted			
63.	4.18	The principle of independence (e.g. functional isolation, electrical isolation and physical separation by means of distance, barriers or a special layout for reactor components) should be ~~considered and~~ applied, as appropriate and as far as reasonably practicable, to enhance the reliability of systems.		Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Country/Organization:	F. Féron France/ASN		Page Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
64.	4.19	Delete 4.19	Example only. Furthermore, TEPCO Fukushima accident showed physical separation may not be enough to avoid CCF…			Rejected	Physical separation is used to avoid common cause failures produced by fire, flooding, and abnormal, or accident environments. This does not mean that certain events or the magnitude of those events cannot affect simultaneously systems or redundancies physically separated if these events did not be considered during the design.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
65.	4.21	Delete 4.21	Unclear and difficult to implement at the component or module level.		Yes		It will be re-phrased as: *“Different safety functions should be performed by different modules, components or systems to avoid the ~~influences from~~ effect of the mode of failure of~~-~~these items on each other~~ one module, component or system on another.”~~*
66.	4.27	Diversity is the presence of two or more ~~redundant~~ systems or components to perform an identified function, where the ~~different~~ systems or components have different attributes so as to reduce the possibility of common cause failure,	Avoid mixing diversity principle and redundancy principle.			Rejected	According to the definition of diversity at the IAEA Safety Glossary
67.	4.28	to provide more than one way to detect and respond to a ~~significant~~ specific event.	To avoid potential misunderstanding	Accepted			
68.	4.29	Diversity ~~should~~ provides defence against common cause failures, ~~it is complementary to the principle of defence in dept~~h and ~~significantly~~ increases the probability that safety actions will be performed when necessary.	Diversity is part of DiD. Whether diversity increases significantly or marginaly the reliability needs a specific assessment…	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
69.	4.30	Delete 4.30	Already covered by 4.34			Rejected	The risk to loose diversity throughout the life cycle of the facility is not covered at 4.34
70.	4.31	Where independence is claimed between two systems (for example a RR's main reactor protection system and its second diverse reactor protection system) through multiplying their failure probabilities within the PSA, then ~~the system platforms should be diverse and that~~ their diversity should ~~also extend to~~ be substantiated, considering the full I&C chain from the facility sensors, calculators to actuators.	To offer flexibility, while stating the objective (claims need to be substantiated)	Accepted			
71.	4.33	In assessing claimed ~~The~~ diversity, attention should be paid ~~should extend~~ to the equipment's components to ensure that actual diversity exists.	Clarification	Accepted			
72.	4.34	Locate 4.34 after 4.28	4.34 is recommending diversity and 4.28 to 4.33 highlight points to consider in assessing whether diversity is enough achieved	Accepted			
73.	4.35	~~As far as possible~~ the more probably failure modes should neither place the system in an unsafe state	Failure mode which are probable should be addressed…	Accepted			
74.	4.38		This is a very demanding recommendation.	Accepted			Paragraph will be deleted.

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
75.	4.40	The ~~qualified~~ service life of electrical and electronics systems and components	IAEA glossary does not define “qualified service life” but does define “service life”	Accepted			
76.	4.40	Age degradation that impairs the ability of a safety component to function under severe environmental conditions ~~should~~ are likely to exist well before the functional capabilities under normal conditions are noticeably affected.	Clarification	Accepted			
77.	4.42	Component replacement ~~before the end of its qualified service life.~~	Superfluous			Rejected	It needs to be specific
78.	4.48	Examples of functional requirements should include, ~~for example~~:	Superfluous	Accepted			
79.	4.49	Examples of performance requirements should include, ~~for example~~:	Superfluous	Accepted			
80.	4.50	Examples of reliability requirements should include, ~~for example~~:	Superfluous	Accepted			
81.	4.51	Locate 4.51 before 4.46	More logical order	Accepted			
82.	4.52	I&C systems and components should be protected against or designed and qualified to withstand internal and external hazards, including seismic hazards, they may be subject to.	Clarification	Accepted			
83.	4.55	~~It is common practice to apply the most rigorous environmental qualification methods to safety systems and safety components.~~	Superfluous. The first sentence gives a clear expectation.	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
84.	4.56	~~It should be addressed~~ significant ageing effects (e.g., thermal and radiation ageing) should be addressed to show the required functionality is maintained up to the end of service life.	Clarification	Accepted			
85.	4.56	Locate 4.56 after 4.41	It is a provision which deals with design for ageing	Accepted			
86.	4.63	Any electrical or electronic equipment in the ~~research reactor~~ facility	Superfluous	Accepted			
87.	4.64	electromagnetic interference among ~~reactor~~ facility equipment.	Reactor could be understood as only a part of the facility	Accepted			
88.	4.65	The design of all I&C systems important to safety should include provisions that allow performance of the required testing during reactor operation, or, if justified, during shutdown* only	Testing should be made possible during operation, unless it is sown it is acceptable to do it during shutdown only.	Accepted			
89.	4.65	Transfer “*Most of the research reactors are operated on relatively short operating cycles therefore provisions for testing during operation generally are not necessary.” as a footnote	See previous comment		It will be re-phrased as: *“*~~Most~~ Many of the research reactors are operated on relatively short operating cycles therefore provisions for testing during operation may be ~~generally are~~ not necessary.*		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: F. Féron Country/Organization: France/ASN		Page Date: 10 October 2012					
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
90.	4.72	• location of sensors such that testing and calibration can be performed preferably at their location;	To offer some flexibility (for sensors located in hazardous area). To be more consistent with 4.73	Accepted			
91.	4.77	test can be immediately assessed without, as far as practicable, further testing of other components or systems	To offer some flexibility	Accepted			
92.	4.80	Make the following text a separate paragraph to be located after 4.77: "4.## The test programme should define processes for periodic tests and calibration of systems that: • specify overall checks of all functions from the sensors to the actuators, capable of being performed in situ and with a minimum of effort; • confirm that design basis functional and performance requirements are met; • test all inputs and output functions, such as alarms, indicators, control actions, and operation of actuation devices; • ensure the safety of the facility during the actual testing; and • minimize the possibility of spurious initiation of any safety action and any other adverse effect of the tests on the availability of the research reactor."	Beginning of 4.80 deals with corrective actions (need after a failed test), not the test programme	Accepted			
93.	4.82	For testing purposes, Temporary modification of computer code in systems and components is not allowed.	Clarification	Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Country/Organization: France/ASN		Page Date: 10 October 2012		RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
94.	4.84	Test of a safety system channels should preferably be single online.	To be more consistent with the 2nd sentence f 4.84	Accepted			
95.	4.93	Transfer "Failure Mode and Effects Analysis is often used to confirm compliance with the single failure criterion, and to confirm that all known failure modes are either self-revealing or detectable by planned testing." as a footnote a)	Explanation only		It will be re-phrased and kept as c): *"Failure Mode and Effects Analysis ~~is often used~~ to confirm compliance with the single failure criterion, and to confirm that all known failure modes are either self-revealing or detectable by planned testing."*		Revised to indicate a specific activity
96.	4.93	Transfer "Defence-in-Depth and Diversity Analysis is one means of investigating vulnerability of safety systems to common cause failure." as a footnote to e)	Explanation only. I understand what can be a diversity analysis. It is not so clear what is a DiD analysis		It will be re-phrased and kept as f): *"Diversity Analysis to investigate vulnerabilities of safety systems to common cause failure."*		Revised to indicate a specific activity.
97.	4.93	Combine g) and e)	Same topic	Accepted			
98.	4.93	Combine h), i) and j)	Same topic	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
99.	4.93	Transfer “Typically traceability analysis is used to confirm implementation and validation of requirements.” as a footnote to j)	Explanation only.	Accepted	It will be re-phrased and kept as f): “~~Typically~~ Traceability analysis ~~is used~~ to confirm implementation and validation of requirements.		Revised to indicate a specific activity.
100.	4.94	Transfer 4.94 at the end of 4.95	4.94 is a precision of items listed in 4.95	Accepted			
101.	4.96	in the design for the ~~research reactor~~ facility	Superfluous	Accepted			
102.	4.98	Combine 4.98 with 4.97		Accepted			
103.	4.101	Delete 4.101	Redundant with 4.99 and 4.100	Accepted			
104.	5.7	the minimum number and locations of sensors should be identified by the design and justified.	Clarification	Accepted			
105.	5.9	even if the reactor protection system is subjected to a ~~feasible~~ credible common cause failure	Alternate wording	Accepted			
106.	5.10	The protection system should~~, as a minimum,~~ include a function to initiate automatic shutdown of the reactor.	Superfluous (“include” is not limitative) To be consistent with 5.12	Accepted			
107.	5.11	Locate 5.11 after 5.12	More logical order	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Country/Organization:		F. Féron France/ASN	Page Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
108.	5.11	As part of the DiD, the need for a second protection system, with all or part of the functions of the primary protection system should be considered. Where two independent reactor protection systems are provided, these two systems should be independent and diverse from each other.	Before giving attributes of the 2nd protection system, its need should be established.	Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Country/Organization: France/ASN			Page Date: 10 October 2012	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
109.	5.16	Transfer “Sometimes it is necessary to inhibit the action of protection system functions to allow changes in reactor conditions. For example, the trips that limit reactor power during start-up must be inhibited at some point to allow power increase past the low power trip safety system setting. In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as safety interlocks.” as a footnote	Explanation only.			Rejected	To ensure continuity of the text. It will be re-phrased as: “*Sometimes it is necessary to inhibit the action of protection system functions to allow changes in reactor conditions. For example, the trips that limit reactor power during start-up must be inhibited at some point to allow power increase past the low power trip safety system setting. In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as components/functions of safety systems ~~interlocks~~.*”

COMMENTS BY REVIEWER Reviewer: F. Féron Country/Organization: France/ASN			Page Date: 10 October 2012	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
110.	5.19	Delete 5.19	Redundant with 4.80 and guidance is guidance (if it is to be strictly applied, then it should be a requirement…)		It will be re-phrased as: *“Paragraph 4.80 gives recommendations on temporary connections used for maintenance and testing. This recommendation should be strictly applied to reactor protection systems.”*		

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
111.	5.21 5.25	Combine 5.21 and 5.25 as follows: If a computer based system is intended to be used in reactor protection system~~, it should prove to offer advantages of improved reliability, accuracy, functionality and maintainability in comparison with analogue systems.~~ ~~Where a computer based system is intended to be used in a reactor protection system~~, the following requirements should be applied: • hardware and software of high quality and best practices should be used; • the whole development process, including control, testing and commissioning of the system should be systematically documented and reviewed; and • independent verification and validation process should be applied.”	A guide is not a place to promote the use of computer based system.	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
112.	5.22 5.23 5.24	Combine 5.22, 5.23 and 5.24: “Where the necessary integrity of a computer based system that is intended for use in a reactor protection system cannot be demonstrated with a high level of confidence, diverse means of ensuring fullfilment of the protection functions (e.g. hard wired backup system) should be provided. Diversity may be provided: - internal to the reactor protection system or by a separate and independent system, ~~as long as the design bases are met~~. - by a Diverse systems which may be hardwired or computer-based as long as ~~the existence of~~ adequate diversity can be justified. ~~Normally, it is easier to justify diversity between computer-based and hardware-based systems than between two computer-based systems.~~”	These paragraphs address diversity. “integrity” should be defined. Hardware based system may include some programmable devices…			Rejected	Separation between paragraphs will be kept to consider the comments of other NUSSC members. 5.22 will be re-phrased as: “*Where the necessary ~~integrity~~ reliability of a computer based system that is intended for use in a reactor protection system cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfillment of the protection…*” “*Hardware based system*” will be replaced by “*hardwired based system*”
113.	5.28	instrumentation to monitor ~~important~~ relevant reactor parameters	Clarification	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
114.	5.32	supplementary control room (if exists – see 5.38),	Clarification	Accepted			
115.	5.32	the necessary provisions should be ~~made~~ implemented to ensure	Clarification	Accepted			
116.	5.33	normal and ~~abnormal~~ accident conditions.	Clarification	Accepted			
117.	5.34	after the onset of anticipated operational occurrences and ~~design basis~~ accident conditions. ~~In addition, measures can be taken from the control room to mitigate the consequences of BDBAs~~.	Accident conditions include BDBA	Accepted			
118.	5.35	providing to operating personnel with both: - an adequate overall picture of the status and performance of the facility, and; - .detailed information, where necessary on specific systems or equipment status or performance	Overall picture is needed but is usually not enough…	Accepted			
119.	5.36	for all operational states and ~~design basis~~ accident conditions,	BDBA should not be excluded	Accepted			
120.	5.37	• take specific manually-controlled actions for which no automatic control is provided and that are needed ~~to respond to AOOs or accident conditions~~;	It is also true in normal operation		It will be re-phrased as: • *take specific manually-controlled actions for which no automatic control is provided.*		Clarification

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
121.	5.37	• confirm facility critical safety functions availability and performance of automatic safety action;	To be consistent with 5.12	Accepted			
122.	5.37	• determine the magnitude of ~~the~~ any release of radioactive materials	Clarification	Accepted			
123.	5.42	putting the facility in a safe condition during and after accident conditions and mitigate the consequences of ~~a beyond design basis~~ accident ~~(BDBA).~~	DBA consequence should also be mitigated.	Accepted			
124.	5.43	The design of supplementary control rooms should take into account ergonomic factors and include suitable provisions for preventing unauthorized access and use.	For consistency with 5.35	Accepted			
125.	5.45	The operator of experimental facilities should have communication links with reactor operator to share information on experience and reactor status and make each other aware of the expected actions (e.g. in special situations to require shut-down of the reactor).	To enable two way communication… Clarification	Accepted			
126.	5.45	~~The reactor may be shut-down on the decision of reactor operator despite of running an experiment in order to mitigate any dangerous situation caused by running an experiment~~	No link with I&C (it is a management rule)	Accepted			
127.	5.48		Very vague and unclear… Either make it clerarer or delete it	Accepted			5.48 will be deleted.

COMMENTS BY REVIEWER Reviewer: F. Féron Country/Organization: France/ASN		Page Date: 10 October 2012		RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
128.	5.49	associated facilities, the on-site emergency centre ~~control system~~, and to external emergency organizations without having to leave the control room.	Clarification	Accepted			
129.	5.51	The diverse communications links should be routed such that they will not both be affected by loss of the primary communications links, whatever its origin (including external events) ~~common mode failures, fires, or PIE~~,	Gives a more general objective	Accepted			
130.	5.57	such as the sampling of the gaseous atmosphere ~~from the protected area for analysis~~ by remote detectors with automatic operation.	Superfluous	Accepted			
131.	5.58	The design should allow the operation of the system to be stopped if the actuation is ~~found~~ confirmed to be spurious.	Clarification	Accepted			
132.	5.58	~~There should be annunciation prior to the actuation of any automatic extinguishing system.~~		Accepted			
133.	5.61	in operational states or ~~design basis~~ accident conditions	To include BDBA	Accepted			
134.	5.62	Transfer 5.62 as a footnote	Explanatory note	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
135.	6.3	prevent the exceeding of safety limits during the operational states of the reactor and ~~AOO, during design basis~~ accident and as far as reasonably practicable during beyond design basis accidents ~~conditions~~.	Safety limits may be exceeded during some BDBA		It will be re-phrased as: “…prevent the exceeding of safety limits during the operational states of the reactor, ~~and~~ ~~AOO,~~ during design basis accident and, as far as reasonably practicable, during beyond design basis accidents ~~conditions~~.”		
136.	6.4	~~there should be~~ an I&C system ~~that~~ should monitor~~s~~ the parameter	Clarification				
137.	6.5	Acceptable margins between normal operating values and the safety system settings should be considered in the functions of the I&C systems to assure a safe operation of the reactor and avoid too frequent actuation of safety systems.	The objective of margin is also to avoid using safety system…	Accepted			
138.	6.1 to 6.17		Numbering issue as 6.1 to 6.5 are already used…	Accepted			

COMMENTS BY REVIEWER Reviewer: F. Féron Page Country/Organization: France/ASN Date: 10 October 2012				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
139.	6.1	prevent persons from deliberately carrying out unauthorized actions that could jeopardize safety when accessing I&C systems or performing tasks on I&C systems.	The initial recommendation was too general and going far beyond I&C…	Accepted			
140.	6.13	Delete 6.13	Duplicates 4.67, 4.74, 4.81	Accepted			
141.	6.15	Delete 6.15	Duplicates 4.67, 4.74	Accepted			
142.	7.1	Human factors and Human-Machine Interfaces (HMI) considerations should be ~~given systematic consideration~~ embedded throughout the entire design process.	Initial recommendation is too weak	Accepted			
143.	7.2	Effective HMI should be ~~considered and~~ applied for systems	Initial recommendation is too weak	Accepted			
144.	7.6	to confirm that the design adequately accommodates all necessary operating actions and operating organization organizational arrangements.	Operating actions is not enough.	Accepted			
145.	7.8	Delete 7.8	Superfluous.	Accepted			
146.	7.13	The I&C system design should ensure ~~that operator tasks can be performed within the time required~~ take due account of the time needed by operators to perform their expected tasks.	Clarification	Accepted			
147.	7.15	Delete 7.15	Too much stringent for all displays…	Accepted			
148.	7.26	during and following anticipated operational occurrences and accident conditions ~~DBAs. This instrumentation should be adequate for the purposes of emergency response (BDBAs)~~.	Simplification	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:		F. Féron	Page				
Country/Organization:		France/ASN	Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
149.	7.29	ensure safety in all operational states and ~~following design basis~~ accident conditions.	To include BDBA	Accepted			
150.	8.2	~~The current technology allows developing computer based instrumentation and control systems for systems important to safety that has the potential for improving the level of safety and reliability with sufficient reliability.~~	Superfluous…	Accepted			
151.	8.3	Since software faults are systematic and not random in nature, potential common mode failure of computer based safety systems employing redundant subsystems using identical copies of the software should be systematically considered ~~as a critical issue~~.	Common mode of failure of identical redundant equipment is always an issue…	Accepted			
152.	8.4	Delete 8.4	Not specific to computer based system	Accepted			
153.	8.6	In safety systems implementation ~~it should be considered that~~ all unnecessary complexity ~~has been~~ should be avoided both in the functionality of the system and in its implementation, ~~and showing evidence of compliance to~~ by complying with a structured design, following a programming discipline.	Gives a clearer objective and means to achieve it	Accepted			
154.	8.8	important concepts for coping with ~~the problems of~~ complexity.	Superfluous	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
155.	8.9	A top-down design and development process for the system and its associated software should be used to facilitate the assessment of whether design objectives are achieved.	Clarification	Accepted			
156.	8.13	facilitate the detection, location and diagnosis of potential or actual failures	Clarification	Accepted			
157.	8.13	Software that has a modular structure ~~will~~ can be easier to repair, ~~and will also be easier~~ to review and analyse	Clarification and simplification	Accepted			
158.	8.13	The design of a computer based system should ~~ensure~~ allow, as far as practicable, that changes are confined to a small part of the software	"ensure" is too strong	Accepted			
159.	8.14	Locate 8.14 after 8.9	More logical location as it relates to topic addressed in 8.9	Accepted			
160.	8.27	to facilitate the ~~licensing~~ independent assessment of systems important to safety.	Licensing is too restrictive and is one independent assessment	Accepted			
161.	8.31	A quality assurance programme should be prepared and implemented ~~and should be available for regulatory review~~ before the project begins.	Although true, this remark also applies to other documents related to I&C…	Accepted			
162.	8.34	~~It is recommended that~~ the teams performing verification and validation ~~will~~ should be independent of the development team.	Alternate wording (the whole guide is giving recommendations)	Accepted			
163.	8.42	This description should be understandable ~~to regulatory body and experts~~ independent reviewers involved.	Licensing is too restrictive and is one independent assessment	Accepted			

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer:	F. Féron		Page				
Country/Organization:	France/ASN		Date: 10 October 2012				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
164.	8.74	• Hardware components replacement due to ~~random~~ failures.	Superfluous	Accepted			
165.	8.76	After failure of a hardware component, corrective actions should first be limited to one-for-one replacements of hardware and to the reloading of the existing software modules. These actions should not include any modification unless analysis of the failed component reveals such a need.	Hardware change may be necessary…	Accepted			
166.	8.79	Locate 8.79 before 8.78	More logical location	Accepted			
167.	9.1	A full set of documentation reflecting the configuration and status of I&C systems in the facility should be available prior to the commissioning of the facility and maintained up to date throughout the lifetime of the facility.	This should not stop at commissioning.	Accepted			
168.	10.16	Safety Systems are required to be independent as far as reasonably practicable of other reactor systems.	Absolute independence may not be achieved	Accepted			
169.	10.22	the new I&C system may ~~should,~~ when appropriate, be run in parallel with the old system for a probationary period,		Accepted			

Draft Safety Guide DS436 „Instrumentation and Control and Software Important to Safety for Research Reactors“
Status: SPESS Step 7 - First review of the draft safety standard by the Safety Standards Committees

	COMMENTS BY REVIEWER Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of GRS) Country/Organization: **Germany**			Page 1 of 10 Date: 23.10.2012	RESOLUTION			
Rele-vanz	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
3	1	General	defence in depth	Use unique wording within this guide.	Accepted			
2	2	General	Research reactor	To avoid confusing one should use the phrase “research reactor” instead of “reactor”	Accepted			
2	3	General	Avoid abbreviations	Abbreviations should be explained each time in order to avoid confusion	Accepted			
3	4	General		Replace *irradiation facilities* with *irradiation installations* to use same terminology as in IAEA NS-R-4 “Safety of research reactors”	Accepted			
3	5	General		Replace *experimental facilities* with *experimental devices* to use same terminology as in IAEA NS-R-4 “Safety of research	Accepted			

				reactors”				
2	6	1.12 Instead of 1.11	As an additional benefit an I&C modernization process might also be accompanied with the decision of a facility power increase, and it is important to take into consideration in these assessments that the facility will be forced to continue to enhance nuclear safety~~, to increase reliability, to shorten outage time and to reduce staff~~.	To emphasize safety and to give priority to nuclear safety over more non safety relates aims.	Accepted			
2	7	2.1/4	All I&C functions, systems, and components fit into one of two safety categories: items important to safety or items not important to safety (see Fig.1);	Clarification	Accepted			
2	8	2.1/6	(…) are further categorized as either safety systems or safety related items	Terminology: see Glossary “plant equipment”	Accepted			
2	9	2.2	Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some facility operational states and safety related functions and/or non-safety functions in other operational states with the premise that the design should consider to do not add any component or function that are not strictly required by the highest safety classification.					The proposed text is identical to the existing one.
1	10	2.7	Functions of safety systems are to	Here, the safety	Accepted			

			ensure timely detection of violations of limits and conditions for safe operation of research reactor and automatically initiate reactor shutdown, emergency core cooling and residual heat removal, and ~~containment~~ confinement of radioactive materials and/or limitation of accidental releases.	function “confinement” of radioactive materials is meant. A containment is a technical solution for preventing releases of radioactive material to the environment. See also definition in the IAEA Safety Glossary for “confinement”				
1	11	2.8	• Confine radioactive materials and ~~control of operational discharges, as well as~~ limit accidental releases	The control of operational discharges is not a function of the safety systems. This function shall be part of systems related to level of defence 1 and 2, and not the level of defence 3.	Accepted			
1	12	2.8	• Mitigate the consequences of design extension conditions (DEC)~~beyond design basis accidents (BDBAs)~~.	Replace BDBA by DEC in accordance with new terminology introduced by IAEA SSR 2/1. This guide shall be based on the requirements for new built research reactors (see also IAEA SSR 2/1 para.1.2 and 1.3).		Accepted with modifications		BDBA has consistency with NS-R-4, however the principle of design extension conditions will be included as a foot note.
2	13	2.9/2	(...) Postulated Initiating Events	Abbreviation should be	Accepted			

			(PIEs) (…) ~~PIEs~~	explained				
3	14	2.10	• Sensors and instruments which monitor neutron flux, flow rates, temperatures, pressures, and other safety variables and by demand, safety variables from experimental facilities and devices ~~safety variables~~.	To make statement clearer.	Accepted			
3	15	2.10	• ~~Decay~~ residual heat removal	Usually, *residual heat removal* is used in IAEA documents instead of *decay heat re1moval*.	Accepted			
1	16	2.10	• ~~Confinement~~ Containment isolation	As confinement is a safety function which cannot be isolated.	Accepted			
2	17	2.10	~~○ and I&C for:~~ ~~• Emergency Power Supply.~~	Delete last bullet and add *Emergency power supply* to the list actuation I&C and initiation I&C in the same manner as e.g. emergency core cooling			Rejected	Emergency Power Supply has its own classification as it is not actuation I&C nor initiation I&C.
2	18	2.11	~~• Maintain the integrity of the cladding for the fuel in the reactor core;~~ • ~~Maintain the integrity of the reactor coolant boundary;~~	In contrast to a NPP, where the reactor coolant boundary is one of the barriers, this is no longer true for research reactors, especially for		Bullet "*Maintain the integrity of reactor coolant boundary*" will be deleted. The other two		*"Maintain integrity of the cladding for the fuel in the reactor core"* and

			• To maintain integrity of the barriers;	the usually used swimming pool reactors. Here, integrity of the barriers are important.		bullets will remain.		“*Maintain integrity of the barriers*” are applicable for research reactors.
2	19	2.14/6	I&C for Humidity Ventilation and Air Conditioning for Controlled and Supervised areas (HVAC) ~~HVAC~~ for Controlled and Supervised areas	Abbreviation should be explained	Accepted			
2	20	2.14/7	I&C for Close Circuit Television (CCTV) ~~CCTV~~ for Operation	Abbreviation should be explained	Accepted			
1	21	2.16	• I&C of irradiation devices and experimental devices not affecting reactor safety	Add I&C of experimental devices and irradiation devices. These shall be mentioned here as well.	Accepted			
1	22	3.1	The research reactor should be provided with sufficient Instrumentation and Control systems in the form of an architectural design for a safe operation of the research reactor during normal operation, shut down, refuelling, maintenance and, to automatically initiate reactor shutdown, emergency core cooling, residual heat removal, and the ~~containment~~ confinement of radioactive materials and/or limitation of accidental releases ~~during Anticipated~~	Replace *containment* by the intended safety function *confinement*. According to the defence in depth concept no accidental release during AOO (level of defence 2) shall be allowed.	Accepted			

			~~Operational Occurrences (AOO)~~ or during and after accident conditions.					
2	23	3.4	For example, in existing designs the separation of I&C functions between safety systems and safety related systems allocates complex functions to safety related systems and limits the safety systems to the performance of simpler functions.	Clearification, seems that a word was missing in this sentence.	Accepted			
3	24	3.8	Add as footnote to para 3.7	No further guidance, but referencing to further documents related to para 3.7.	Accepted			
2	25	3.16	~~Safety items~~ Items important so safety should be independent of the effects of the design basis accidents to which they must respond.	Replace *safety items* by *items important to safety* in accordance with terminology used in IAEA safety standards.	Accepted			
1	26	3.26	A complete elimination of all vulnerabilities of I&C systems and architecture to CCF is not required for I&C systems performing functions on level of defence 1 or 2, but justification should be provided for accepting identified vulnerabilities that have are not addressed. I&C systems performing functions on level of defence 3 (e.g. safety systems, reactor protection systems) should completely	To strengthen the defence in depth concept and to control CCF on level of defence 3.	Accepted			

			eliminate all vulnerabilities of I&C systems and architecture to CCF.					
2	27	4.7	Verification and validation of safety systems should be performed by a independent group different from the design team.	To emphasize indepency between design team and V&V team.	Accepted			
1	28	4.11	Non-compliance with the single failure criterion may be justified for: ~~a) Very rare PIEs~~ ~~b) Very improbably consequences of PIEs~~ c) Withdrawal of certain components from service for limited period of time for the purposes of maintenance, repair, or periodic testing. d) Components whose likelihood of failure can be shown to be sufficiently remote as to be discounted.	In order to strengthen the defence in depth concept the single failure should be applied to *very rare events* and *very improbably consequences* too, but could be restricted to active parts only, at least for new research reactors. Exceptions could be made by applying a graded approach.		4.11 will be rephrased as: "*No single failure could result in a loss of a system to perform its intended safety function.*"		To be consistent to what is stated in Safety requirements for Research Reactors, NS-R-4, para. 6-36
3	29	4.8 – 4.11 and 4.12 – 4.16	Maybe change order: First: redundancy Second: single failure	The single failure approach is a deterministic method to determine the necessary degree of redundancy for items important to safety. A statement shall be included in section redundancy and should refer to the section single failure	Accepted			

2	30	4.17	The design of I&C system important to safety should provide additional features to minimize the possibility of common cause failures by means of independence, physical separation and diversity of equipment. <u>Especially safety systems should be designed in such a way that occurrence of CCF are safely prevented.</u>	In order to strengthen level of defence 3.	Accepted			
3	31	4.75	~~●~~A test programme should include:	Delete circle. Its not an item of the list	Accepted			
	32	4.80	~~●~~The test programme should define processes for periodic tests and calibration of systems that:	Delete circle. Its not an item of the list	Accepted			
3	33	4.91/3	(…) and risk of high radiation levels <u>exist</u>;	Verb is missing for better understanding	Accepted			
2	34	4.93 e)/1	Verification that common cause failure <u>(CCF) </u>(…)	Abbreviation should be explained	Accepted			
3	35	4.93	Combine f) an g)		Accepted			
3	36	5.8/1	The <u>reactor</u> protection system (…)	Word missing	Accepted			
3	37	5.10/1	The <u>reactor</u> protection system (…)	Word missing	Accepted			
1	38	5.11		Can be deleted, there is no requirement for a redundant reactor protection system in this guide. In case of digital I&C (see e.g. para 5.22) diversity is provided by		Yes		5.11 will be rephrased as: *“Where two reactor protection systems are provided, these two*

				the hard wired backup / non computer based system for the reactor protection system.				*systems should be independent and diverse.”*
3	39	5.13/1	The reactor protection system (…)	Word missing	Accepted			
2	40	5.14	• the operator is allowed sufficient time (at least 30 minutes) to evaluate the status of the reactor facility and to complete the required actions; and	To make “sufficient time” more concrete. Within the first 30 minutes the shift shall be able to determine the plant condition and could start the relevant procedures.			Rejected	It is preferred to avoid specific numbers.
1	41	5.16	For example, the trips that limit reactor power during start-up must be inhibited at some point to allow power increase past the low power trip safety system setting. In this guide such reactor protection system inhibit functions are called operational interlocks and are classified as safety interlocks. Another example would be the necessity for inhibition of certain functions in case of pulsed operation of the research reactor.	Some research reactors, like the widespread TRIGA reactors, allow for steady state as well as for pulsed operation (making the research reactor core supercritical). This has implications for the I&C system too.	Accepted			
3	42	5.22	Where the necessary integrity of a computer based system that is intended for use in a reactor protection system cannot be demonstrated with a high level of confidence, diverse means of	There is a tendency to use the term *non computer based systems* instead of *hard wired backup*, taking the technological		It will be re-phrased as: “*Where the necessary ~~integrity~~ reliability of a computer based*		*Non computer based systems* include, among

			ensuring fulfilment of the protection functions (e.g. ~~hard wired backup system~~ non-computer based system) should be provided.	development of I&C devices into account.		*system that is intended for use in a reactor protection system cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the protection functions (e.g. ~~hard wired backup system~~ non-computer based system, as hardwired or other technology backups) should be provided.*		others, devices subjected to complex process to prove their reliability.
3	43	5.24	Diverse systems may be non-computer based ~~hardwired~~ or computer-based as long as the existence of diversity can be justified. Normally, it is easier to justify diversity between computer-based and non-computer~~hardware-~~based systems than between two computer-based systems.	There is a tendency to use the term *non computer based systems* instead of *hard wired backup*, taking the technological development of I&C devices into account.		It will be re-phrased as: "*Diverse systems may be non-computer based systems, including hardwired or other technology backups or computer-based systems as long as the existence of diversity can be justified. Normally,*		Clarification

						it is easier to justify diversity between computer-based and non-computer based systems than between two computer-based systems.”		
2	44	5.33	Normal working environments to be considered include: lighting, temperature and humidity for normal, abnormal and accidental conditions. ~~Hazards to be considered include radiation, fire smoke or toxic substances in the atmosphere.~~ The design of the main control room and supplementary control room should take into account conditions resulting from internal hazards (e.g. fire smoke or toxic substances in the atmosphere) and external hazards (e.g. earthquakes, flooding, extreme meteorological conditions, man-made hazards) ~~environmental and/or seismic conditions expected during both normal and abnormal conditions.~~	To emphasize, that the control rooms shall be protected against internal as well as external hazards. Stronger distinction between conditions resulting from AOO, DBA and DEC and from internal / external hazards.	Accepted			
1	45	5.34	In addition, measures can be taken from the control room to mitigate the consequences of ~~BDBA~~DECs.	Use design extension conditions (DEC) instead of BDBA according to IAEA SSR 2/1.		Yes		See response to comment 12.

				This strategy shall also apply for research reactors.				
3	46	5.38/5	(…) any actions beyond reactor trip in case when ~~after~~ operations (…)	Clarification		It will be re-phrased as: *“A supplementary control room (or emergency control console) should be provided if operators are required to perform any actions in case of the main control room is unavailable or operations from the main control room are inhibited.”*		
2	47	7.29/1	In control room design Human Factors Engineering (HFE) ~~HFE~~ (…)	Abbreviation should be explained at least by the first appearance in the text.	Accepted			
3	48	8.1 /1	(…) importance to safety in ~~nuclear~~ research reactors (…)	That guide is devoted to research reactors	Accepted			
1	49	8.3	Since software faults are systematic and not random in nature, common mode failure of computer based safety systems employing redundant subsystems using identical copies of	In order to strengthen the defence in depth concept and control CCF on level of defence 3.				It will be re-phrased as: *“Since software faults are*

			the software should be considered as a critical issue. CCF should be safely prevented by a proper design of safety systems / reactor protection systems.					*systematic and not random in nature, potential common mode failure of computer based safety systems employing redundant subsystems using identical copies of the software should be systematically considered ~~as a critical issue~~.”*
3	50	8.4/2	(…) at a very early stage of the project ~~in order to ensure its success~~.	Not relevant	Accepted			
3	51	8.13/2	(…) to facilitate the detection, localisation, ~~location~~ (…)	The location should be found therefore localisation.	Accepted			
3	52	10.11/1	The effect ~~affect~~ the modification (…)	Incorrect wording	Accepted			

TITLE

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: KINS Page 36 of DS 436 Country/Organization: Korea Institute of Nuclear Safety Date: 2012. 10. 15							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	5.33	Normal working environments to be considered include: lighting, temperature, humidity, noise, and vibration.	Control room environments should provide adequate condition to communicate and stability. So it is desirable to add noise and vibration components.	Accepted			

Comments on IAEA Draft Safety Guide
“Instrumentation and Control and Software Important to Safety for Research Reactors” (DS436)

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	1.2/line 1	The rate of ageing and obsolescence of research reactor I&C systems has increased due to the technological advancements in the field of electronics.	Proposed sentence provides additional clarity	Accepted			
2	1.2/line 3 1.2/line 4	“…refurbishments…” “…I&C modernization projects…”	Editorial	Accepted			
3	1.4	This safety guide ~~deals mainly with~~ provides additional guidance for implementing requirements for those I&C systems that are important to safety.	As worded, implies that document contains requirements.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
4	1.8 through 1.11	Delete	Paragraphs add no value to the overall text. The decision whether to upgrade I&C systems is facility specific, and an attempt to capture all possible reasons in 4 paragraphs is unnecessary.				
5	2.1/line 3 (first bullet)	…and components fit into one of two ~~safety~~ categories: important to…	There are two categories, “important to safety” and “not important to safety.” As one category is called “not important to safety” it is incorrect to state that there are two **safety** categories.	Accepted			
6	2.1/line 15, bullet 5, *iii*	prevent or reduce the potential for the release of *radioactive…*		Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
7	2.2/line 2, second sentence	Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some facility operational states and safety related functions and/or non-safety functions in other operational states. ~~With~~ The design premise ~~that the design~~ should ~~consider to do not add~~ be to prevent the addition of any component or function not strictly required by the highest safety classification.	2nd sentence is a run on sentence. The second half of the sentence is not easy to understand and should be made clearer.	Accepted			
8	2.8/first bullet	….leading to design basis accident (DBA) conditions;	Define acronyms for frequently used series' of words or phrases				It will be resolved during technical edition activity according to Safety Standard Series style
9	2.8/ third bullet	…..operational states and ~~design basis accident~~ DBA conditions	Use acronyms, once defined				See response to comment 8
10	2.9	…full range of postulated initiating events (PIEs) to terminate the event safely	PIE is not previously defined				See response to comment 8

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
11	2.10	Reactor trip, initiated by the Reactor Protection System (RPS), which ~~which consists in the Reactor Protection System that~~ includes:	clarification	Accepted			
12	2.10	Add “safety interlocks” to list.	In addition to protective instrument systems and safe shutdown systems, *safety interlocks* also exist to limit the magnitude of design basis events.	Accepted			
13	2.14/10th bullet	I&C for fire detection and suppression systems ~~extinguish I&C~~	Clarity	Accepted			
14	2.17	…based primarily on deterministic methods and documented engineering judgment…	Add the word “documented.” The use of engineering judgment should always be supported by a documented basis when associated with systems important to safety.	Accepted			
15	2.17	…complemented where appropriate by available Probabilistic Safety Assessment…	PSAs are not available for all research reactors especially those less than 10 MW.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
16	2.18/1st bullet	the estimated frequency or probability (if available) of PIEs and the potential severity of their consequences…	The use of the term “probability,” would imply that a PSA is available	Accepted			
17	2.18/ 2nd bullet	the estimated frequency or probability that the I&C system will be called upon to perform…	The use of the term “probability,” would imply that a PSA is available		the estimated frequency or probability (if available) that the I&C system will be called upon to perform…		Consistency
19	3.1	The research reactor should be provided with sufficient I&C ~~Instrumentation and Control~~ systems ….	Suggest acronyms be defined at the beginning of the document and used throughout.	Accepted			
20	3.3	….communications (Interfaces) between I&C systems ~~(Interfaces) between them~~ and with the facility operators.	Clarity	Accepted			
21	3.15	Safety systems should be independent from systems of lower safety classification ~~as necessary~~	Removing this term clarifies ambiguity in the meaning of this statement.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
22	3.16	Safety ~~items~~ systems and components should be ~~independent of~~ environmentally qualified for the effects of the design basis accidents to which they must respond.	The term safety item is not defined ~~clear as to its meaning. Revise section 3.16.~~	Accepted			
23	3.19	….against internal (e.g. fire or flooding) or external hazards (e.g. earthquake or tornado),…	Provide examples of internal and external hazards for clarity	Accepted			
24	3.20 / 3.21	Latent failures and common failure modes which potentially might result in a common failure of the redundancies should be identified, and justification should be provided for any that need not be considered as credible sources of CCF between systems or individual components. For example, justification could be based on the component dependability, technology, or feedback gained over its wide usage.	Combine 3.21 with 3.20 since 3.21 provides an example related to 3.20	Accepted			
25	3.24	…For CCFs ~~common cause failures~~ of items…	Acronym previously defined				See response to comment 8

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
26	3.26	…vulnerabilities that ~~have~~ are not addressed.	Editorial				
27	3.27 e)	…and supplementary control rooms, if applicable;	Supplementary control rooms do not apply to all research reactor facilities	Accepted			
28	3.27 f)	…and supplementary control rooms, if applicable; and	Supplementary control rooms do not apply to all research reactor facilities	Accepted			
29	3.28 b)	The groups of functions to be provided to address ~~Postulated Initiating Event (~~PIE~~)~~ sequences	PIE is previously used and defined (no need to spell out here)				See response to comment 8
30	3.32	The use of the same design features ~~those~~ mentioned in 3.31, where these features ~~be~~ are reasonably and justifiably applicable ~~to~~, should be enough to avoid ~~that~~ a failure in one level caus~~es~~ing failures in another subsequent level(s).	clarification	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
31	New 3.33	The I&C system should have a fail-safe design such that no malfunction within the system caused solely by variations of external conditions within the ranges detailed in the design basis, will result in an unsafe condition or failure.	Consider adding a bullet for fail-safe design.	Accepted			
32	4.5/sub-section c)	Functionality requirements for each facility state ~~and during~~ including extended shutdown	Extended shutdown is a unique research reactor state. ~~The original statement would imply it is not.~~	Accepted			
33	4.5	Add bullet “For each manual protective action the points in time and the plant conditions during which manual control is allowed.”	This should be part of the Design Basis.	Accepted			
34	4.9	…Systems, the single failure criteri~~a~~on should be applied so that the system is capable of performing its ~~task~~ safety function in the presence…	Use of the term “safety function” is more specific and clear than the use of the term “task.”	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
35	4.11	Delete this step (4.11), which states: “Non-compliance with the single failure criterion may be justified for:…”	The safety requirements for research reactors, NS-R-4, para. 6-36 states “no single failure could result in a loss of a system to perform its intended safety function.” Therefore there cannot be any justification for non-compliance with single failure criterion.		Yes		4.11 will be rephrased as: “*No single failure could result in a loss of a system to perform its intended safety function.”*
36	4.12	considered a~~s~~ provision of alternative…SSCs, ~~so~~ such that ….	Editorial	Accepted			
37	4.17	…~~common cause failures~~ CCFs by…	Acronym previously defined				See response to comment 8
38	4.29	…cause failures~~,~~. ~~i~~It is complementary…	Two sentences read better.	Accepted			
39	4.31	Acronyms (RR and PSA) should be written out when first used.	Need consistent use of acronyms throughout document. Suggest a list up at the beginning and only use acronyms from then on.				See response to comment 8

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
40	4.34	~~It should be considered~~ Both the scope and the type of the diversity provided should be considered.	Clarity	Accepted			
41	4.35/4.36	Put 4.36 before 4.35	Reads better.	Accepted			
42	4.39	…systems to fail ~~pass~~ into…	Clarification of meaning	Accepted			
43	4.40	…conditions ~~should~~ may exist well...	Age degradation is not a certainty. Thus, the suggested term change from should to may.	Accepted			
44	4.47	…should ~~demonstrate to~~ meet all.…	Not needed	Accepted			
45	4.48	~~Examples of~~ Functional requirements should include, for example: functionality required ….	The word “examples” was repetitive.	Accepted			
46	4.56	~~It~~ Environmental qualifications should ~~be~~ address~~ed~~ significant ageing effects (e.g., thermal and radiation ageing) to show the required functionality is maintained ~~up~~ to the end of service life. Further conservatism ~~ought to~~ should be provided,…	Clarification	Accepted			
47	4.59	…electrical components~~,~~. ~~t~~Testing should be done to demonstrate …	Make two sentences for clarity.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
48	4.59	I&C systems and components ~~could be~~ already qualified ~~in which case, I&C systems and components~~ should be …..	clarification	Accepted			
49	4.62	…should ~~also~~ be taken ….	Editorial	Accepted			
50	4.63	Any electrical or electronic equipment in the research reactor facility will contribute to the electromagnetic environment. ~~That must be withstood by~~ I&C systems important to safety must be capable to perform safety functions in such an environment. ~~Therefore, the need to apply limits to electromagnetic emissions should apply to all equipment, not just equipment important to safety~~. The contribution of electromagnetic emissions from all equipment, not only equipment important to safety, must be evaluated as to its impact on the performance of I&C systems important to safety.	Clarify the original statement.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
52	4.70	Testing should neither compromise the ~~independence of~~ the safety ~~systems~~ function nor introduce the potential for common cause failures.	Independence is just one characteristic of the safety function which cannot be compromised.	Accepted			
53	4.74	Design of I&C systems important to safety should include provisions, such as an alarm, to automatically alert operators that channels or components are in test mode.	Eliminates an unnecessary sentence, providing a clearer statement.	Accepted			
54	4.80/1st bullet	Make 1st bullet Section 4.81	This appears to be the original intent of the author.	Accepted			
55	4.88	Revise section 4.88. The intent of the section is not clear.	All trains of equipment must be tested which would include redundant equipment.	Accepted			
56	Header before 4.89	MAINTAINABILITY	Editorial	Accepted			
57	4.91 – first bullet	…in areas ~~where conditions~~ of extreme	Clarification	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
58	4.93	The first paragraph under “Design Analysis” starts with “Safety analysis.” Consider titling this entire section “Safety analysis.”	There is no entity titled “Safety Analysis” in the guide. The requirements std. (NS-R-4) does state that a safety analysis is necessary.				
59	4.93	Improve organization of 4.93 and its bullets. Suggest combining bullets a and c; d and f; e and g; and h and j.		Accepted			
60	4.93 c)	~~Failure Mode and Effects Analysis~~ FMEA ….	Acronym could be defined in 4.35.				See response to comment 8
61	4.93 g)	~~Common cause failure (~~CCF~~)~~ …	Acronym previously defined				See response to comment 8
62	4.99/4.100		Sections seem highly redundant. Consider combining these sections into one section.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
63	5.5	No identified common cause failure vulnerability of sensing devices should have the potential of denying operators the information and parameters that they need to control and mitigate accident conditions. An example is the saturation of radiation monitors.	Include an example for clarity.	Accepted			
64	5.6	If more than one sensor is necessary to cover the entire range of the monitored reactor parameter, a reasonable amount of overlap from one sensor to another should be provided. Examples include source range, intermediate range, and power range nuclear instrumentation.	Include an example for clarity.	Accepted			
65	5.7	If the monitored variables have a spatial dependence (i.e., the measured value of a parameter depends upon sensor location), the minimum number and locations of sensors, such as flow measuring elements, should be identified by the design.	Include an example for clarity.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
66	5.9	…a ~~feasible~~ common cause failure…	The extra term does not seem needed	Accepted			
67	5.10	...maintaining the reactor in a safe and stable condition (acting in this case as extended ESF I&C system.)	Editorial	Accepted			
68	5.12	…. ~~Postulated initiating events~~ PIE ….	Acronym previously defined				See response to comment 8
69	5.13	…initiating state ~~may have ceased~~ ceases to be ….	Clarification	Accepted			
70	5.20	…these margins should ~~need to~~ take…	Editorial	Accepted			
71	5.21	….it should ~~prove to~~ offer ….	Editorial	Accepted			
72	After 5.26	For computer based RPS systems, the system design should include ~~protection against cyber attack~~ computer security.	A new section should be provided following existing section 5.26.	Accepted			
73	5.27 & 5.28	The reactor operator ….	Clarification	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
74	5.27	The reactor operator should be provided with sufficient instrumentation for monitoring the operation ~~and~~ of the reactor process systems ~~of the reactor~~ during normal operation, shut-down, refueling and maintenance, ~~and for~~ including the recording all variables important for safety	Provide clarification of intent.	Accepted			
75	5.32	….control room (if ~~exists~~ required)….	Clarification	Accepted			
76	5.34	The principal location for safety systems and safety related actions is the main control room.	Per Fig. 1, Items important to safety include Safety systems and Safety related items.	Accepted			
77	5.34	…~~main control room~~ MCR…	Acronym previously defined.				
78	5.35	…information ~~providing~~ to operating…	Editorial	Accepted			
79	5.63	…and avoided ~~in~~ to the extent…	Editorial				See response to comment 8

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
80	6.1 – 6.5	Correct the numbering.	Numbering for sections 6.1-6.5 is used twice: once under the OLC section and again under the Control of Access section.	Accepted			
81	6.1	All reasonable precautions ~~shall~~ should be taken to prevent	By IAEA guidelines, Safety Guide recommendations are expressed as “should” statements. Safety Requirements are expressed as “shall” statements.			Rejected	Direct quotes to statements of the Safety of Research Reactors, Safety Requirements, No. NS-R-4.
82	6.2	…keep the settings and values….	Editorial	Accepted			
83	6.4	...to provide ~~those~~ these functions should include the capability of storing ~~of~~ these….	Editorial	Accepted			
84	6.5	…assure ~~a~~ safe…	Editorial	Accepted			
85	6.6	….connections should ~~also~~ be ~~strictly avoided~~ prohibited.	Clarification	Accepted			
86	6.7	…to restrict authorised users to only access ~~to~~ data and commands for which they are enabled.	Editorial	Accepted			
87	6.9	…all their components ~~are able~~	Editorial	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~to~~….					
88	6.16	….extended shutdown ~~pending decisions on its future~~.	Not needed			Rejected	It reflects actual status of several research reactors where a final decision was not adopted yet.
89	6.17	….the minimal I&C systems required for safety to be kept operational ~~that shall keep in operation mode~~ during that extended shutdown.	Clarification	Accepted			
90	7.9 (new)	In the case where only a portion of the I&C system is modernized, careful consideration should be given to the design, compatibility and human interaction of the modernized portion of the I&C system to the existing systems to ensure proper and continued operation with the considerations given in 7.1 through 7.8.	Provide recommendations for partial modernization for compatibility	Accepted			
91	7.28	Compare 5.35 and 7.28.	Coordination is needed with information in 5.35 (possibly unneeded duplication)	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
92	8.2	…developing sufficiently reliable computer based instrumentation and control systems for systems important to safety that ~~has~~ have the potential for improving the level of safety and reliability.	Clarification	Accepted			
93	8.12	It should be demonstrated that measures have been taken to protect the computer based system throughout its entire lifetime against physical attack, ~~intentional and non-intentional intrusion~~ unauthorized access, fraud, viruses and so on. Safety systems should not be connected to external networks.		Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
94	After 8.12	The use of external memory devices such as USB drives should be restricted or strongly controlled in both the operational and development environments. If allowed, any such device should be actively scanned for viruses or other malware prior to use on the system and its use logged.	New bullet to add.		It will be re-phrase as: *“The use of external memory devices such as USB drives should be prevented. If the design contemplates its use, it should be restricted or strongly controlled in both, the operational and development environments. If allowed, any such device should be actively scanned for viruses or other malware prior to use on the system and its use logged.”*		

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
95	8.27	…clear evidence~~s~~…	Editorial				
96	After 8.27	Part of the project planning and management stages should be the identification, assessment and management of project risks. Also, the V&V plan should provide procedures for evaluating risks in each development activity.	Add discussion of project risk management	Accepted			
97	8.29	…and implementation. ~~And~~ T~~t~~he…	Editorial	Accepted			
98	8.30	…be identified ~~as well~~.	Editorial	Accepted			
99	8.34	~~It is recommended that the~~ ~~t~~Teams…~~will~~ should be independent…	Strengthen the statement	Accepted			
100	8.35	…by means of ~~the~~ an approved change control…	Should be an approved process	Accepted			
101	8.44 add bullet	Add: That requirements not directly associated with safety (such as availability) will not adversely affect the ability of a safety function to be performed when required.	It should be clear that any such requirements (using term from 8.41) will not have an adverse effect on safety.	Accepted			
102	After 8.45	Add: The software requirements should include description and consideration of software hazards and associated software safety analyses.	Hazards that affect software operability or when software has a role in controlling a hazard should be identified.	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A.			Date: 10/30/2012	RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
103	8.53	~~If verification is made by human inspection, t~~T	All such code should be readable, etc. The intent of this paragraph does not seem to be machine code (compiled).	Accepted			
104	Before 8.67	Add: A Software Test Plan should be developed, covering all testing to be done, including unit, integration, factory and installation.	Only one characteristic of test plan related to software is identified – facilitate regression testing. There are many more.	Accepted			
105	9.5 (new)	Operational and maintenance staff should collaborate on the update of existing documentation to ensure all modernization activities are completely captured in the I&C configuration control documentation.	Specify need to update CM docs post modernization	Accepted			
106	10.1	Upgrade and modification of I&C systems should be performed in accordance with the guidance ~~of~~ provided in Safety Standard SSG-24, ~~[4],~~ Ref. [4], ~~provides guidance~~ on planning, organizational aspects, safety assessment,…	Editorial	Accepted			

COMMENTS BY REVIEWER Reviewer: **U.S. Nuclear Regulatory Commission** Country/Organization: U.S.A. Date: 10/30/2012				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
107	Reference Section	Add to References: For Quality Assurance Requirements – IAEA 50-C/SG-Q "Quality Assurance for Safety in NPP and other NI."	Section 8.31 discusses that a quality assurance programme should be prepared, but includes no references to standards.	Accepted			