DS 509 Instrumentation and Control Systems and Software Important to Safety for Research Reactors (Revision of SSG-37)

COMMENTS BY REVIEWER Reviewer: Page. Country/Organization: Date: 24 October 2019					RESOLUTION			
Comment No.	Country Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
General								
1.	USA 41		There is little to no inclusion of QUALITY ASSURANCE	After designing (selecting) a system that meets the design criteria and design bases, the most important aspects of installing or upgrading to a digital I&C system are Quality assurance, configuration management, and V&V. QA is missing from this document and should be interspersed throughout especially in section 8.			X	Section 2 discusses the quality and management system aspects on the topic, and paras 8.32 – 8.35 provide specific advice on V&V
2.	Korea 1	Contents	Propose to insert the number of relevant paragraph in contents as follows: Background (1.1-1.2) Objective (1.3)	Propose the unified format of Contents for the uniformity and consistency with other Safety Guides.	X			

Section 1								
3.	Korea 2	1.1	~~1.2. This Safety Guide is a revision of IAEA Safety Standards Series No. SSG-37, Instrumentation and Control Systems and Software Important to Safety for Research Reactors1, which it supersedes.~~ 1.1 This publication supersedes the Safety Guide on Instrumentation and Control Systems and Software Important to Safety for Research Reactors that was issued in 2015 as IAEA Safety Standards Series No. SSG-371. ~~1.1~~ 1.2 This Safety Guides supplements and elaborates upon …	Propose the unified format of Background of each Safety Guide for the uniformity and consistency with other Safety Guides.		X 1.2. This Safety Guide is a revision of IAEA Safety Standards Series No. SSG-37, Instrumentation and Control Systems and Software Important to Safety for Research Reactors[1], which it supersedes.		The original wording in 1.1 is according to the IAEA standard format. All 8 guides in DS509 will be formatted consistently during the editorial review.
4.	Germany 1	1.5. Line No.2	The recommendations and guidance apply to both the design and configuration management of instrumentation and control systems ~~and software~~ for new research reactors <u>including their software (if applicable).</u> ~~Over the lifetime~~	Scope of the guide is focused on I&C systems; therefore it is necessary to clarify the scope between non software based and software based I&C systems. Wording/correction: lifecycle vs. lifetime.		"The recommendations and guidance apply to both the design and configuration management of instrumentation and control systems and		Minor edit for clarity

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

			During lifecycle of a research reactor, one or more refurbishments of instrumentation and control systems would be expected. […..]			software for new research reactors including software (if applicable). **Throughout the lifecycle** of a research reactor...”		
5.	USA 1	1.4	Research reactors with power levels in excess of several tens of megawatts, ~~fast~~ specialized reactors (e.g. homogeneous reactors, fast spectrum reactors or reactors with a liquid fuel loading, and reactors using experimental devices (e.g., ~~such as~~ high pressure and temperature loops and cold or hot neutron sources) and critical and subcritical assemblies.	Fast reactors don’t use moderators and require high enrichment. They are beyond the scope of this SSG.		The text is consistent with SSR-3 para 1.8 and the scope of the DPP. However the text of section 1 will be standardized across the guides.		
6.	USA 2	1.4	Should include sub-critical assemblies in scope?	See line 1		Subcritical assemblies are covered in the scope, in accordance with the definition of research reactor in SSR-3		
7.	USA 3	1.4	may require the application of supplementary measures such as the use of additional defense-in-depth, redundancy, and diversity ~~even the application of guidance for power reactors.~~	Sentence as written is vague. State what is supplementary (except use a more common word like additional or added)? Just saying use power reactor		The text is consistent with SSR-3 para 1.8 and the scope of the DPP. See resolution to USA comment 1		

				guidance is not helpful.		above.		
8.	USA 4	1.4	…, the application of certain guidance may be graded up or down. The level of protection and resources should be allocated to sufficiently mitigate the risk or reduce it to an acceptable level. Each case in which the application of guidance is graded should be identified with account taken of the nature and possible magnitude of the hazards presented by the given facility and the activities conducted	This implies that grading could be up or down, which I think is the right interpretation. In other words, deviations from the recommendations of this guide, if it is used, should be explained, regardless of why.		The text is coherent with SSR-3 para 1.9:...the application of certain requirements may be graded. The definition of graded approach is included in the IAEA safety glossary 2018.		
9.	USA 5	1.5/ 2nd sent.	The recommendations and guidance apply to both the design and configuration management of instrumentation and control systems and software for new research reactors and for refurbishment of I&C systems for existing reactors.	Needs a transition sentence between the first and second sentence. First sentence discusses new designs and then does not elaborate, but instead 2nd sentence talks about refurbishment of existing systems. SUGEST REWORDING (The deleted words provided some of that transition)	X			
10.	USA 6	1.5	~~Over the lifetime of a research reactor, one or more refurbishments of instrumentation and control~~	Delete sentences. If a facility is replacing their system, they know why they are doing it. Stating in guide is		X Throughout the lifecycle of a research reactor, one		Agreed – the reasons have been deleted

			~~systems would be expected. Reasons for modernization projects for instrumentation and control systems of a research reactor might be obsolescence or ageing, improvement of maintainability and reliability, reactor reconstruction and upgrading, new utilization or experiments and enhancement of safety~~	superfluous.		or more refurbishments of instrumentation and control systems would be expected. ~~Reasons for modernization projects for instrumentation and control systems of a research reactor might be obsolescence or ageing, improvement of maintainability and reliability, reactor reconstruction and upgrading, new utilization or experiments and enhancement of safety.~~		
11.	USA 7	1.5	The scope of this safety guide covers new designs and modification and modernization of instrumentation and control systems of existing research reactors	1.5 has a lot of words that are subjective and unnecessary. Eliminate to include just what is needed and the facilities to which it applies		X Revised. See resolution of Germany comment 1 above on para 1.5.		
12.	USA 8	1.6	This Safety Guide ~~also~~ provides recommendations and guidance on human factors engineering	As it was written, sentence is confusing. [Computers have HMI criteria too.]	X			

			and human–machine interfaces for hardware, and for computer based systems and software for use in instrumentation and control systems important to safety					
13.	USA 9	1.7	This safety guide is structured as follows: • Section 2 discusses the identification of instrumentation and control functions and systems, the method and the basis for safety classification into safety functions and systems and safety related functions and systems. • Section 3 gives guidance on how instrumentation and control systems are to be arranged into a hierarchy. • Sections 4 and 5 provide an overview on meeting the general and specific design requirements for instrumentation and control systems. The operational aspects of instrumentation and control systems are presented in • Section 6. Section 7 expands on the guidance given in	This would be much easier to read and follow if it was a bulleted list (or at least each section on its own line).		Original text is consistent with the scope of DPP509, however the text of section 1 will be standardized across the guides during the editorial review.		Standards format for structure as used in IAEA safety standards.

			Section 4 in the area of human–machine interfaces. • Section 8 provides guidance on design aspects and other aspects of computer based systems and software. • Section 9 provides guidance on configuration management for instrumentation and control systems. • Section 10 presents considerations in the modification and modernization of instrumentation and control systems. The Annex identifies instrumentation and control systems that can be used in a research reactor.					
14.	Viet Nam 1	1.4	1.4. This Safety Guide provides recommendations and guidance on the safety classification, design, implementation, qualification and operation of instrumentation and control systems and software important to safety for research reactors to achieve compliance with NS-R-4SSR-3 [1]. Research reactors with power levels ~~in excess of~~	The regulatory requirement of a nuclear power plant shall be applied for all research reactors with the power excess 30 megawatts.			X	A requirement to apply nuclear power plant standards to high power research reactors is the prerogative of regulatory bodies in each member state. The guidance in 1.4 is indicative but does not impose a specific

			~~several tens of megawatts~~ — *less than 30 megawatts*					limit.
Section 2								
15.	Germany 2	2.1. Line No.3	[…..] Functions, systems and components important to safety are those which ~~permit~~ assure the safe operation of the research reactor and perform the following main safety functions […..]	Clarification		X Reverted to original text.		For consistency with resolution of USA comment 11, 12 and 13 on para 2.1
16.	Germany 3	2.1. Line (c)	[…..] (c) Confinement of the radioactive material, shielding against radiation and control of ~~planned~~ radioactive release, specified in design […..]	Clarification		X Reverted to original text.		For consistency with resolution of USA comment 11, 12 and 13 on para 2.1
17.	Korea 3	2.5	2.5. Para. 6.29 in Requirement 16, para. 6.29 of SSR-3 [1] states, … 4.109. Para. 6.65 of SSR-3 [1] para 6.65 states 5.40. … Requirement 55 fromof SSR-3 [1] requires …	Unified format of referring the requirements and/or paragraph of SSR-3 is necessary, for example, Paras 2.6-3.7 in Requirement 1 of SSR-3 and Requirement 3 of SSR-3.		X The text is consistent with the IAEA standard format. The editorial review will ensure consistency.		All 8 guides in DS509 will be formatted consistently.
18.	Korea 4	2.5 (a)	New paragraph number is necessary for example 2.6 instead of 2.5.a.	New numbering system for paragraph using a, b, and etc. is introduced in this safety guide. However, unified		X The para. numbers will be updated during the editorial		The use of “a” for additional paragraphs helps to preserve the original

			New paragraph numbers are required for 8.65~8.68 to avoid duplication.	paragraph numbering system is preferred for the uniformity and consistency with other Safety Guides.		review of the document to ensure consistency		paragraph numbering and indicates where changes are made.
19.	Germany 4	2.5.a.	~~With respect to the consequences of failure to perform a safety function, an I&C system whose failure or spurious operation may directly cause an initiating event, or that its failure on demand may make the consequences of a postulated initiating event worse, can be classified to a high safety class. This includes the I&C associated with reactivity control systems whose failure would result in accident conditions.~~ The I&C system whose spurious failure or its failure on demand may cause an initiating event or make the consequences of a postulated initiating event worse, shall be classified to a higher safety class. Similar approach shall be applied to the I&C associated with reactivity control systems whose failure may lead to accident conditions.	Clarification of the requirement.		X "An I&C system where a spurious failure, or failure on demand, may cause an initiating event or make the consequences of a postulated initiating event worse, should be classified to a higher safety class. A similar approach should be applied to the I&C associated with reactivity control systems whose failure may lead to accident conditions."		Included the suggested text but changed ‘shall’ to ‘should’ in line with the language of a safety guide.

20.	Germany 5	2.5.b.	Instrumentation and control functions for all ~~facility~~ states of the research reactor should be identified.	Clarification concerning the scope of the requirement.			X	"Facility states" is a term defined in the IAEA 2018 glossary
21.	Ukraine 1	2.8	The safety class of an instrumentation and control system should be the **highest among the safety classes of the systems or equipment that it controls or monitors**.	An instrumentation and control system can control or monitor more than one process system or equipment, which can have different safety classes. Therefore, the instrumentation and control system should have the highest safety class.		X "...should be the same as the highest safety class of the systems or equipment that..."		The comment was incorporated, but with a minor edit for readability
22.	USA 10	2.1	Functions, systems and components important to safety are those which permit the safe operation of the research reactor. Examples of equipment classified according to their importance to safety and ~~perform the following~~ main safety functions:	As it is written now is misleading. It implies that that all main safety functions are in that table/graphic and they are not. That table is power reactor guidance. It does not include important categories for experiments, it does not include other important functions such as seismic detection. Need to revise figure AND move it after bullet list or eliminate graphic! It is also inconsistent with section 2.3		X Reverted to original text in SSG-37 (2015).		Figure has been moved. It contains examples of SSCs in each category

23.	USA 11	2.1a	~~Control of reactivity~~Safely shutting down the reactor and maintaining it in a safe shutdown condition in and after operational states and accident conditions;	Edit is not accurate. Reactivity control is a "control" function. Safety is "SAFE SHUTDOWN." Back out edits. Shutdown margin and excess reactivity are safety aspects of reactivity control, they are design criteria NOT I&C system criteria.	X			Reverted to original text in SSG-37 (2015).
24.	USA 12	2.1c.	Rewrite or retain original text.	Shielding is not an I&C system function. Also, "controlling effluent releases is crossed-out, but that is exactly what the stack monitoring systems do.	X			Reverted to original text in SSG-37 (2015).
25.	USA 13	2.1a, b, and c.	REWRITE	The paragraph is safety classification of I&C systems. But, the examples are written for generic safety systems. They need to be written as examples of the I&C safety systems; reactor protection system, emergency safety system actuation, radiation 14monitoring, ventilation control and isolation systems, etc.		X Reverted to original text in SSG-37 (2015).		
26.	USA 14	2.5a	This includes the I&C associated with reactivity control systems whose failure would result in accident conditions.	Unless you are talking about experiments (in which case you should so state), this statement is not accurate.	X			Sentence deleted

				Core reactivity is set by design of Limiting core configuration, shutdown reactivity, and excess reactivity, which are design criteria for the reactor, they are not a function of the I&C system.				
Section 3								
27.	Germany 6	3.15.(e), (iv)	[…..] To support the compliance of safety systems ~~or groups~~ with the single failure criterion and the fail-safe criterion; […..]	Please delete: misleading statement			X	SSR-3 Requirement 25 discusses the single failure criterion applying to both safety systems and safety groups.
28.	Ukraine 2	3.15, f	Should define the interfaces and means of communication between the individual instrumentation and control systems **and human-machine interface**.	The means of human-machine interface should be defined in the instrumentation and control system architecture based on information required for personnel in normal operation and accidents.		"(f) Should define the human-machine interface as well as the interfaces and means of communication..."		The comment was incorporated, but at the beginning of the sentence for clarity
29.	USA 15	3.1	~~emergency core cooling~~, residual heat removal	Both are listed, eliminate one (functionally, they are same)			X	Emergency core cooling refers to a system which replenishes cooling water in the primary cooling system in response to a loss of

								coolant. Residual heat removal refers to a system that transfers heat from the shutdown core to an ultimate heatsink.
30.	USA 16	3.3	~~Modern instrumentation and control systems are more highly integrated than in the past.~~	The information is not relevant.	X			
Section 4								
31.	Germany 7	4.35.a	Obsolescence <u>and ageing</u> management should be considered in the design of ~~computer-based~~ <u>I&C</u> systems to plan and manage for reductions in service life, diminishing manufacturing sources and material shortages. <u>Special attention should be paid to consider the lifecycle by design and operation of computer-based equipment.</u> […..]	Clarification of the requirement.		"Obsolescence management should be considered in the design of I&C systems to plan and manage for reductions in service life, diminishing manufacturing sources and material shortages. Special attention should be given to the obsolescence of computer-based equipment."		Accepted the suggested change except for "ageing management" which is covered in the previous paragraph.
32.	Germany 8	4.110	The I&C systems <u>and equipment</u> provided for additional safety features for design extension conditions should be subjected	Clarification concerning the scope of additional safety features (accident management measures)	X			

			to the requirements for equipment qualification, reliability, testability, maintainability, and inspectability, as well as ageing management. This equipment should be considered as items important to safety.					
33.	Ukraine 3	4.17	Electrical connections and data connections between redundant divisions within a safety system should be designed so that no credible failure in one redundant division would prevent the other redundant division(s) from meeting their requirements for performance and reliability. **Electrical power supply from two redundant and independent sources should be provided for each instrumentation and control system and for each redundant train of instrumentation and control systems.**	The redundant electrical power supply is an important measure for ensuring independence. A failure of a non-redundant power supply source leads to failure of all instrumentation and control systems and all redundant trains of instrumentation and control systems at the same time.			X	This paragraph is dealing with connections between redundant equipment in safety systems. The issue of design features such as redundant power supplies is addressed in 4.12-4.13
34.	Ukraine 4	4.50	Operating organizations and designers should consider nuclear and computer safety and security in all phases of the project, namely: specification of requirements; conceptual, preliminary and detailed design;	Computer security measures should be provided also at the stage of decommissioning of instrumentation and control systems as recommended in IAEA NSS 33-T. Particularly, it is necessary to avoid the	X			

			and the procurement, fabrication, integration, installation, commissioning, operation, maintenance **and decommissioning** of the instrumentation and control systems.	unauthorized access to sensitive information on the system, its components or software. This information may be used for attacks on other nuclear facilities that operate the same type of system, hardware or software.				
35.	USA17	4.2	~~Adequate analysis of the design requirements is an effective means to achieve simplicity of design.~~	This is too vague. Reword or delete (recommend delete because prior sentence is sufficient)		X "Careful analysis of the design requirements is an effective means to achieve simplicity of design.		Reworded to remove vague word "adequate". There is value in guidance that refers the reader back to design requirements.
36.	USA 18	4.3	Add to list (or into list) • Operating modes of facility and equipment required for each mode (OLCs) • System response time, latency, precision, and any instrument error			X "(d) Performance requirements, including the guaranteed response time for safety functions including latency, precision and instrument error."		Facility modes are addressed in bullets a, b, and c. Response time is addressed in bullet d
37.	USA 19	4.3p	~~The whole lifetime of the facility including accident conditions and conditions following an accident~~	Sentence is confusing. Delete or reword. Do you mean the expected lifetime of service for equipment?	X			deleted

38.	USA 20	4.3q.	Operational constraints.	Need examples, what operational constraints are you referring to?	X			Text added "Operational constraints such as interface requirements with other systems."
39.	USA 21	4.11a.	Where compliance with the redundancy and single failure criteria are ~~is~~ not sufficient to meet reliability requirements, additional design features should be provided, or modifications to the design should be made, to ensure that the system meets reliability requirements	Redundancy should also be referenced (part of section title)			X	Text consistent with SSG-39, para 6.19. Redundancy is discussed elsewhere in this section. This paragraph is specifically addressing cases where compliance with the single failure criterion is not sufficient.
40.	USA 22	4.6	Redundancy and the single failure criterion ADD: The minimum number and location of sensors are identified and shown to be adequate for the safety purposes for those variables of the safety system that have a spatial dependency,. [IEEE Std 603-1991, Clause 4.6 ADD: Redundancy is provided to the extent necessary to assure	Additional criteria for the safety system			X	The guidance provided in SSG-37 may be implemented in different member states according to national requirements and national use of codes and standards. The IAEA cannot specify the use of individual standards.

			that loss of a protective action of the safety system is not credible under normal operations or during and following a design basis event [IEEE Std 603-1991, Clauses 7.5 and 8.3 ADD (or integrate): The design should preclude the effects of normal operating, maintenance, testing, and postulated accident conditions on redundant channels from resulting in the loss of the protection function. Design Basis requirements that address this include the application of the single-failure criterion; quality; equipment qualification; system integrity; physical, electrical, and communications independence; manual controls; setpoints; and independent power sources					This paragraph is defining for the reader what is meant by a single failure The need for the design to ensure the success of safety functions in different operational and accident states is covered in 4.3 and 4.9 etc.
41.	USA 23	4.89	4.89. Where temporary connections of equipment are required for periodic testing or calibration, the operator should be alerted by alarms and/or warning lights of the presence of the temporary connection and use of such equipment should be	Need more than administrative controls for potentially disabling or bypassing a safety system.	X			

			subject to appropriate administrative controls.					
Section 5								
42.	Germany 9	5.23	For computer based reactor protection system~~s~~ and equipment, the ~~system~~ design needs to consider and include computer security features (see paras 4.39–4.51) for the whole lifecycle of the reactor protection system.	Consideration of the lifecycle aspects (e.g. manufacturing, configuration management, commissioning, testing, maintenance)	X			
43.	Germany 10	5.26	The safe operation of a research reactor, intended to cover all ~~normal~~ modes of operation, should be considered in the design process. …	Delete unnecessary limitation.	X			
44.	Germany 11	5.26 A New item	Design of computer based I&C systems and equipment shall consider adequate computer security measures.	Please add a new, additional requirement concerning computer security aspects.			X	The IAEA safety guides do not provide security guidance
45.	Ukraine 5	5.10	The reactor protection system should include, as a minimum, a function to initiate shutdown of the reactor. In case of subcritical assemblies, the shutdown may be achieved by withdrawing the neutron source. **The reactor protection system should shut down the reactor in case of complete loss of power supply.**	It is important requirement that the loss of power supply shall not prevent the possibility of reactor shutdown. The reactor shall be shut down immediately if power supply is lost.			X	The range of initiating events and accident sequences for which a shutdown is required, will vary from one design of research reactor to another. Instead of singling out this

			The reactor protection system may also provide other safety functions such as initiation of emergency core cooling, confinement functions and maintaining of the reactor in a safe and stable condition (the features of the reactor protection system acting in this case as extended engineered safety features of the instrumentation and control system).					scenario of a loss of power, SSR-3 requirement 7 requires a systematic approach for identifying all scenarios which require shutdown, cooling and confinement of radioactive material.
46.	USA 24	5.18	~~5.18. Paragraph 4.89 provides a recommendation on temporary connections used for maintenance and testing. This recommendation should be strictly applied to the reactor protection system.~~	Its not practical to point back by number. If it is important to the system specific design guide, then restate.		X "Where temporary connections of equipment are required for periodic testing or calibration, of the reactor protection system, the operator should be alerted by alarms and/or warning lights of the presence of the temporary connection and use of such equipment should be subject to appropriate administrative controls."		

47.	USA 25	5.19.	The design should ensure that safety system settings can be established with a margin between the initiation point and the safety limits where the action initiated by the reactor protection system will be able to ~~control the process~~ correct the abnormal situation before the safety limit is reached	automatic protective action should correct the abnormal situation before a safety limit is exceeded. Not sufficient to say "control process." What is the "process."		X "…the reactor protection system will be able to control the parameter before the safety limit is reached"		
48.	USA 26	5.20	(a) Hardware and software of **high quality** should be used and **best practices** should be employed	Terms are vague and ambiguous in interpretation. Either define or reference standard definition to use. (otherwise delete)	X			Bullet deleted as it contradicts requirement in SSR-3
49.	USA 27	5.20b.	(b) The ~~whole~~ life cycle of the system should be systematically documented and reviewed;	Unneeded word. Life cycle implies from beginning to end.	X			
50.	USA 28	5.27, 5.28, and 5.29	CONTROL ROOMS These requirements should be deleted and instead talk about the area where the control console is located	This is too restrictive. In simple research reactors (most TRIGAs) (or sub-crits) there won't be a "control room" that is to this degree. Should reword to be control console (but leave discussion of 5.30 and 5.31 (as when applicable)			X	Though the configuration may vary between facilities, the concept of a control room is well understood and identifiable at any research reactor including TRIGAs
51.	USA 29	5.36	5.36. The control consoles for irradiation facilities and experimental devices should be devoted exclusively to the	Reword to be, if safety analysis shows. MANY research reactors safely perform irradiation and	X			

			irradiation facilities and experimental devices if the safety analysis identifies events that shows an independent I&C system is required for irradiation facilities to keep a functional separation from the other activities at the research reactor.	experimentation, with main reactor system				
52.	USA 30	5.37	5.37. Parameters important to the operation of the reactor should be covered by the alarm system. Other alarms of experimental devices should be presented with a functional separation from the reactor alarms.	This is very weak application fo human factors, suggest reword.		X “Parameters important to the operation of the reactor should be covered by the alarm system. Alarms of experimental devices, with no reactor safety implications, should be presented with a functional separation from the reactor alarms”		
53.	USA 31	5.38	5.38. Communication systems should be provided for staff to have secure interfaces between the main control room, the supplementary control room if applicable), and	“if applicable should appear after every use of supplemental control rooms. The extra room is NOT required for all designs (recall it is based on safety analysis)	X			
54.	USA 32	5.41 to 5.49	PROVISIONS FOR FIRE DETECTION AND EXTINGUISHING	I disagree that fire detection and extinguishing systems are part of reactor protection			X	Fire detection and extinguishing systems are essential

			(Retain 5.49, delete all else)	system. Rather, I&C systems and components determined in the SAR analyses to be important to the safe operation or shutdown of the reactor should be designed, located, ·and protected so that the effects of fires or explosions would not prevent them from performing their safety functions. FIRE Alarms and suppression systems should be part of the building design and built to local/national building code.				systems for reactor safety and must be integrated in the control room with other alarms and annunciations. Guidance in this section also includes the specifics of fire systems in a nuclear facility
Section 6								
55.	USA 33	6.2	The design of the instrumentation and control systems of the reactor should ensure that, for the operational states of the reactor, the instrumentation and control systems contribute to keeping the reactor's operating parameters within the operational limits and conditions					No change suggested
56.	USA 34	6.4	~~The required instrumentation and control systems that are to~~	Delete. This is an unrealistic requirement. An analog	X			

			~~provide these functions should have the capability of storing and recovering these safety system settings.~~	system may have the ability to have a setpoint set for the trip without the ability of storing and recalling. That sentence is indicative of a digital system and should not be used without proper reference. Plus, it is not needed.				
57.	USA 35	6.5	Acceptable margins should be allowed for instrument accuracy, expected drift, and allowable margin of error in measured signals and for all expected variations in normal operation.	As written, the sentence is necessary, but not sufficient.	X			
58.	USA 36	6.14	ADD: Additional guidance is provided in IAEA Safety Standards Series No. NS-G-4.2, Maintenance, Periodic Testing, and Inspection of Research Reactors	Add the needed reference to ensure consistent guidance	X			
59.	USA 37	6.15	REWORD: The instrumentation and control systems should include~~, where applicable, on-line testing functions and~~ the capability to facilitate periodic testing and, where applicable, on-line testing functions to reduce the time such testing takes, improving the availability of the reactor	Online testing is not a requirement and should only be used when needed for operational commitments or in a system that has multiple channels, diverse means of measuring, etc. A channel in test MUST always generate a trip, so online maintenance, if used, must not interfere with the ability of system to	X			

				perform its intended safety function.				
Section 7								
60.	Korea 5	7.8	7.8. Requirements for design for the human–machine interface should be specified on the basis of all the tasks to be supported by the human–machine interface, including normal operation, ~~and~~ anticipated operational occurrences and accident conditions, for the operators as well as for the maintenance staff, the experimenters and personnel with responsibilities in an emergency.	To provide clear understanding, the "normal operation and anticipated operational occurrences" should be replaced with "normal operation, anticipated operational occurrences and accident condition" as in the expression of 7.24.	X			
61.	Korea 6	7.12	7.12. The reactor operator should be provided with sufficient indicators and recording instrumentation to be able to monitor relevant reactor parameters in, and following, normal operation, anticipated operational occurrences and accident conditions.	To provide clear understanding, the "anticipated operational occurrences and accident conditions" should be replaced with "normal operation, anticipated operational occurrences and accident condition" as in the expression of 7.24.			X	This para is addressing specifically the need for clear information following deviations from normal operation.
Section 8								

62.	Ukraine 6	8.47	In **software of** systems important to safety, unnecessary complexity should be avoided at all levels of design. The simpler the design is, the easier is to achieve and demonstrate all other attributes. It also gives greater confidence that the software is fully understood.	The name of the subchapter is “Software design”. Thus, it is reasonable to consider software (not the systems).	X			
63.	USA 38	8.58e.	8.58.e. Any shortfall in the verification results against the verification plan (e.g. in terms of the test coverage achieved) should be documented and resolved or justified	Need proper documentation	X			
64.	USA 39	8.58f	8.58.f. Any errors detected should be analysed for cause and should be corrected by means of agreed modification procedures, and regression tested, as appropriate, to ensure that previously developed and tested software still performs after a change.	For clarity	X			

65.	USA 40	8.65	8.65. A third party assessment of safety system software ~~should~~ can be conducted concurrently with the software development process.	I don't think this should be a "should" Use "can" instead or language that it is optional, even if a good idea.			X	This is the formal language of IAEA Guides where "should" denotes the recommended approach
Section 10								
66.	Korea 7	10.1	10.1. … are given in IAEA Safety Standards Series No. SSG-10, Ageing Management for Research Reactors [4].	It is not necessary to delete 'in IAEA Safety Standards Series No.' and 'Aging Management for Research Reactor [4]'			X	The IAEA standard format is to use the full title the first time a safety guide is referenced, which is in para 4.35a. Subsequent references just use the document number e.g. "SSG-10"