Form for Comments
Instrumentation and Control and Software Important to Safety for Research Reactors (DS436)

Comments by reviewer Reviewer: Page of Country/Organisation: Australia Date:				Resolution			
Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
1.	**General**	Electrical grounding to be considered when designing for independence and separation.					
2.	**General**	Often it is not clear whether the point is related only to protection systems or safety related systems as these are all under the banner of systems important to safety. The requirements can be very different for these systems so care must be taken to use the correct terminology.					
3.	**General**	Additional guidance/references should be given when a specific task is suggested e.g. Verification and Validation or Reliability Analysis.					
4.	**General**	Much of the document is also applicable to hardwired systems; however, there is an emphasis on computerised systems. If the purpose of this document is for guidance on both types then information that is common to both should be specified.					
5.	2.2	Include "...monitoring the availability of a safety system..."	Suggest that monitoring the availability of a safety system is also part of the safety system. This is mentioned in 2.3.			rejected	The availability of the safety systems can be monitored by systems of lower safety class as it is mentioned in paragraph 2.3
6.	2.14	Include "indication of the state and operation of the safety systems as a back-up or for operational convenience;"	Instrumentation associated with the operation and the state of the safety systems are usually of the same safety category as the safety system itself.		Paragraph deleted by other MS comment	rejected	It is mentioned in 2nd bullet of 2.10 and in 4th bullet of 2.14.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
7.	2.14	Consider deleting "Instrumentation and control for close circuit television for operation" or transferring it to 2.16.	In Australia, the CCTV system is classed as not of safety significance. It is a convenient operational tool but does not contribute to the safety of the plant. The OPAL reactor PAM system has CCTV dedicated for monitoring of specific plant areas for accident management.	accepted	Paragraph deleted by other MS comment		
8.	2.14	Consider deleting "Vibration monitoring system" or transferring it to 2.16.	It is the experience at OPAL that specifying the Vibration Monitoring System as a separate system does not add any value. The vibration sensors are part of the process system to which they are connected. Seismic sensors are not included in the VMS at OPAL.	accepted	Paragraph deleted by other MS comment		
9.	2.16	Include an example of "Some facility auxiliary systems"	Clarity	accepted	Paragraph deleted by other MS comment		
10.	2.21	Provide a reference.	To give guidance on a graded approach for the aspects described in this section.	accepted			
11.	2.22	Include reference to isolation devices.	This is referring to isolation devices. While these are referred to later, they could be pointed out here to give some guidance to read ahead.	accepted	Old 2.24 New 2.8		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
12.	2.23	Suggest changing the first sentence to "The safety class of the instrumentation and control system should be based on the safety class of the function of the parameter being controlled/monitored."	Instrumentation important to safety is usually installed in process systems that are of a lesser safety class. These process systems are required for operation and this require to be monitored for any shutdown conditions however they are not necessarily required for shutdown conditions or accident mitigation. In this case the instrumentation is of a higher classification than that of the process system.	accepted	Old 2.25 New 2.9		
13.	3.1	Include "The architectural design of the instrumentation and control systems should provide sufficient capabilities to cover all expected and unexpected operation modes and post-event conditions."	Clarity.		accepted *The architectural design of the instrumentation and control systems should provide sufficient capabilities to cover all anticipated operational occurrences and post-event conditions.*		It is impossible to cover all unexpected (or unanticipated) operation(al) modes.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
14.	3.17	**Comment:** Is this point requiring no common failures/components across RPS's? Or is justification of negligible failures still acceptable?	This paragraph is in contradiction with 3.14.		accepted The paragraph will be deleted to eliminate contradiction with 3.14.		It is a justification for negligible vulnerabilities or failures that can be acceptable and does not need to be addressed. The exception is for functions of level 3 of defence in depth.
15.	3.22	Include required reliability (eg probability of failure on demand) as per the design bases.	Other factors affecting redundancy.	accepted	New 3.18		
16.	3.24	... fail-safe design implemented where possible ...	It is impossible to design a system that will always fail in the safe condition. For example, on a system which de-energised to trip, a welded contact will prevent the trip occurring. This is low probability but still possible.	accepted	New 3.21		
17.	4.2	Add "... and implemented for functions useful for safety" at the end of the first sentence.	For safety systems – accepted. For systems related to safety – not necessarily, e.g. RPS vs. RCMS.	accepted	Paragraph deleted by other MS comment		The modification gives more clarity to the paragraph

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
18.	4.3		The design bases/inputs should all flow from the I&C architecture and overall facility design.			rejected	The comment is not clear
19.	4.3(h)	Constraints on process variables **in all postulated conditions**.	Clarity.	accepted	New (i)		
20.	4.4(a)	Include: The methodology for developing and consistently applying a standard setpoint.	The limiting values for actuating safety systems are typically the least conservative trip setpoints. These should be derived, and documented, directly from the assumptions of the safety analysis report.		accepted New 4.5 (a It will be rephrased as: *The safety system settings of actuation for safety systems;*		The safety system settings include all the uncertainties. Refer to paragraph 4.104 and Fig. 4.1
21.	4.5	Consider removing or rewording.	This statement and 4.6 are not related to reliability, but rather to correctness and suitability of the implemented design to meet functional requirements.	Accepted and removed			
22.	4.6	Consider removing or rewording.	This statement and 4.5 are not related to reliability, but rather to correctness and suitability of the implemented design to meet functional	Accepted and removed			
23.	4.12	Delete	This is the same statement as the last part of 4.10.	Accepted and removed			

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
24.	4.14	Change to " …extent necessary to meet reliability and availability requirements ..."	Clarity	accepted	New 4.12		
25.	4.15		This point is referring to common cause failure, not single failure.		accepted New 4.14 The paragraph will be moved from this section to the section of common cause failure.		
26.	4.15	... redundant systems should be physically **and electrically** separated ...		accepted	New 4.14		
27.	4.15	... Moreover, the principle of independence should be used across the entire safety system e.g. between redundant trains within the same system and across diverse systems such as first and second shutdown systems.	The last sentence is unclear.	accepted	New 4.14		
28.	4.17	"..e.g. functional independen**ce** … independen**ce** of communication)…"	Grammar	accepted	New 4.15		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
29.	Section 4 **Diversity**	**General comment**	Diversity of equipment type opposes the requirement for standardisation. Diversity creates additional challenges for maintenance whereas standardisation minimises maintenance issues.				Diversity is a strong countermeasure for Common Cause Failures even considering the additional challenge
30.	4.37	Add "Instrumentation and control systems that fail safe should do so without any operator initiated actions."	Clarity.	accepted	New 4.34		
31.	4.41	Include: Monitoring of equipment condition for ageing characteristics e.g. condition monitoring/predictive maintenance.	Extra example.	accepted	New 4.38		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
32.	Section 4 **Design for security**	**General comment**	Security is applied with a graded approach depending on the level of security required. Systems should be assessed with regards to their availability, integrity and the sensitivity of data they hold. These items should be assessed to determine the consequences if the system failed in any of these areas from a security incident. System security and physical security measures combine together to protect the systems from malicious acts. As the instrumentation and control system industry merges more to IT type solutions for networking, human machine interface, the use of commercial operating systems, IT type security provisions are becoming more applicable to control systems. Many of the standards applied to high security information systems can be implemented in control systems. However provisions must still allow sufficient access to the system at all times so that control of the plant is never compromised.				
33.	4.49	National IT security requirements should also be considered.	Clarity		accepted it will be included as an additional paragraph new 4.48.		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
34.	Section 4 **Design for security**	**General comment**	Ongoing updates to the IT security system could be assessed against the possibility of introducing unforeseen functional changes.				
35.	Section 4 **Design for security**	**General comment**	Consideration of IT security when IT I&C systems are being maintained e.g. allowing access to contracted staff, use of external media.				
36.	Section 4 **Equipment Qualification**	**General comment**	Not only should the protection system be qualified but all the development tools must be qualified to the same standards. Different methods of development should be designed if the tools are not qualified.				
37.	4.59	... seismic hazards, **that the design bases/safety analysis requires them to withstand and operate through.**	This is the maximum necessary for them to have to withstand,	accepted	New 4.58		
38.	4.64	"Significant sources of electromagnetic interference **could** include…"	Grammar	accepted	New 4.62		
39.	4.64	... **electromagnetic** fields caused by radio ...	Electromagnetic not electric fields from radio transmitters	accepted	New 4.62		
40.	4.66	... should be designed, installed and **tested** to withstand ...	Additional requirement to ensure efficacy of the systems and equipment.	accepted	New 4.64		
41.	4.68	... Wireless systems and devices **could** include, …"	Editorial. Grammar for clarity.	accepted	New 4.67		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
42.	4.70	Add: National and international standards/requirements for electromagnetic emissions should also be considered, as required.	Clarity.		accepted new 4.69 National and international standards for electromagnetic emissions should be considered.		
43.	Section 4 **Testing and testability**	**General comment**	Human tasks need to be considered so that access provisions for testing are provided. The workplace safety regulations should be consulted so that the installation design meets all national requirements. Provisions should be provided so that all regulatory testing can be completed in an efficient and safe manner.				
44.	4.77	Add: Installed test facilities need to be tested independently against another calibrated source on a regular basis.	Tightening the requirements on the test facilities.	accepted	New 4.76		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
45.	4.78	Location **and installation** of sensors such that testing and calibration can be performed preferably at their location, **including facilities for draining, drying, decontaminating, isolating, ventilating.**	Clarity		Accepted New 4.77 The proposed text will be rephrased as: *location including facilities for draining, drying, decontamination, isolation and ventilation where applicable;*		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
46.	4.80	Add extra clauses, as follows: 4.xx Where safety instrumentation is out of service while in test mode, the system should automatically be placed in the trip or failed state, where applicable. Alarms should alert operator. 4.yy Where testing is performed with a channel in service, administrative controls are required such as when performing trip tests during reactor operation. 4.zz Consideration needs to be given on the impact of the channel under test on safety assumptions. (E.g. 2oo3 dropping to 2oo2)	Tightening the requirements on the testing.		accepted Extra clauses will be added to reflect Comment 46. Not implemented due to other MS comments Accepted New 4.79		The proposed extra clauses will be rephrased for clarity

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
47.	4.81	Add: The test frequency should take into account the requirements for accuracy and the stability of the instruments chosen. Stable instruments with low drift can be tested less frequently.	Clarifying frequency of testing	accepted	New 4.81		
48.	4.83	Add: clear procedures for determining return to service are defined.	Tightening the requirements on return to service following testing.		Accepted new 4.83 *The first sentence will be rephrased as: The tests defined in the test programme, through clear procedures should ensure that, during and after completion of the tests:*		The modification gives more clarity to the paragraph

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
49.	4.85 Dot point 2	Consider revising the dot point or clause 4.57 as per the reason comment (right).	Response time was included as a performance requirement (see 4.57). Does testing for performance requirements mean that Response Time Testing is being suggested for research reactors? This is typically done for Nuclear Power Plants but not for Research Reactors. Requirements for Response Time Testing should be strictly based on the assumptions in the SAR and limited to parameters that require special consideration for response time because their timely response is critical to facility safety.		accepted it will be added a foot note to clarify the issues page 27 footnote 3		
50.	4.85	Confirm that design basis functional and performance requirements are met **by documenting the success of a test showing compliance with tolerance requirements.**	Clarity	accepted	4.85		
51.	4.85	Add: Provide post maintenance testing to ensure that systems are returned to operation correctly.	Tightening the requirements on the testing program.	accepted	4.85		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
52.	4.90	For testing purpose, temporary modification of computer code in systems and components **must only be done under strict administrative control with return to service checking**.	Sometimes the adjustment of variables (setpoints) is used to verify the function of a channel. Code modification does not include temporary alteration of variable values or disabling of input/output points. This should always be done under strict administrative control with return to service checking.			rejected	Variables or set points can be modified during testing. What it is not allowed is the temporary modification of the computer code.
53.	4.92	Add: Preference should not be given for whole channel testing when equivalent overlapping tests are more practical to perform.	The meaning of single online is not clear.			rejected	Single online refers to the capability to test a whole channel with a test procedure. Equivalent overlapping tests are acceptable when single online test is not possible due to practical reasons.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
54.	4.94	Add: ... with consideration taken for the wear on actuators when tested excessively.	Although this would be ideal, credit should be given for individual or overlapping parts tested separately. There are multiple functions to test – calibration, trip setpoint function, voting logic, sensor calibration so it is the experience at OPAL that separable parts are tested.	accepted	New 4,92		
55.	4.98	Provision of test panels, instrument isolation and draining and test connections.	An additional consideration is to maintain the area around the instrumentation when future modifications occur.	accepted	4.98		
56.	4.100	Delete a or b. Delete e or f. g) include mean time between failure. h) ... for permanently installed test equipment k) and after/during test conditions and during startup/commissioning when the plant is not operating under normal conditions (e.g. trips due to low flux with fresh core). Delete i or j.	Paragraphs a and b are the same. Paragraphs e and f are the same. Clarity Clarity Clarity Paragraphs i and j are the same.	accepted	4.100 Deleted a) and f) Deleted i)		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
57.	4.101		A guide or standard should be provided. The tools for the analysis also need to be defined.			rejected	The definitions of specific international standards and tools are out to the scope of the current safety guide
58.	4.103		The OLCs should include consideration of limiting safety system settings when determining the limiting value to insert in the OLC. Limiting safety system settings are nominal and require acceptance criteria for testing.			rejected	The comment is correct but does not require the modification of the paragraph
59.	4.104	Dot point 1: Recommend text change to "physical parameters". Dot point 2: Analytical limit (of **measured value**) Dot point 3: ... limiting **actuation** value ...	The definition of safety limits given in standards refers to a physical limit on the plant design for example fuel meat temperature. The Safety Limit drives the analytical limits. Analytical limit is not "of safety system setting", it is of measured value. Allowable Value is a limiting actuation value of the safety system given a particular setting. Safety system setting is fixed/ideal. Specifies least conservative value at which actuation must occur.			rejected	Paragraph 4.104 generically describes the relationship between the parameters associated with the determination of the safety system settings in an I&C system.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
60.	Fig. 4.1	Insert **limiting** above and **setting** below "Safety system".	Missing the word "limiting" above and "setting" below "safety system".		accepted It will rephrased as *safety system setting*		Safety system setting is the right word
61.	4.105		Components inside cabinets may not require labelling but if the organisation employs a computerised maintenance planning system, components may need labelling for tracking purposes (e.g. spare parts).			rejected	The paragraph is not mandatory. Only mentions that it may not be necessary if the component or modules are clearly identified.
62.	5.7	The final location also needs to be tested to verify the design assumptions and whether associated setpoints, limiting conditions and allowable values should be reassessed.	Clarity.	accepted			

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
63.	5.13	Add: In addition, the reactor protection system should remain latched at least until the protective action is completed. Reset actions should be manually initiated by the operator and only allowed once the latching time has passed.	Clarity		accepted It will be rephrased as: *The action initiated by the reactor protection system should be latched so that once an action is started, it will continue* until its completion*, even if the initiating state ceases to be present.*		The modification is proposed for clarity
64.	5.20	Ensure that the term "safety system setting" is used consistently (capitalised or not).	Consistency (see 5.31 for example)	accepted	New 5.19		
65.	5.20	Ensure that the term "reactor protection system" is used consistently (capitalised or not).	Consistency (see 5.19 for example)	accepted	New 5.19		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
66.	5.21		"High quality" should be described as meeting acceptable standards for safety or high reliability systems (either national or international standards) as deemed by the operating organisation or the national regulator. Lifecycle issues can be built into the maintenance plans. For example proactive maintenance could involve replacement of items deemed to be end of life.			rejected	The paragraph does not need clarifications on the meaning of high quality and the way in which lifecycle can be implemented.
67.	Section 5 **Reactor Protection System**	**General comment**	For computer based systems, consider shorter life cycles/earlier obsolescence.				A paragraph will be included in Section 8, COMPUTER BASED SYSTEM AND SOFTWARE, GENERAL CONSIDERATIONS
68.	5.31		Appears to be a repeat of earlier statements.			rejected	The paragraph has consistency in this section
69.	5.32		Satisfactory conditions should comprise appropriate ranges for the parameters listed in 5.33.			rejected	Specifying appropriate ranges is out of the scope of the current safety guide

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
70.	5.33	Include **radiation dose** and **dust**.	Completeness.	accepted	Listed in 7.25		
71.	5.37	Include **ergonomic factors**	Completeness, although it is included later in the HMI section.			rejected	It is not necessary to duplicate concepts that are included in other sections
72.	Section 5 **Control rooms**	**General comment**	Indication of safety parameters should be designed, extending the defence in depth principle so that there is suitably qualified indication if systems of a lower classification used for indication are not operational.				Each safety system should have its own safety parameter command and display consoles and panels. Refer to 2.10: Instrumentation and control for Command and Monitoring: Safety parameter command and display consoles and panels

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
73.	5.38	Add: The supplementary control room instrumentation and control systems should be appropriately independent from the main control room to avoid common cause failures diminishing the operability of the supplementary control room systems. For example design of control system networking should be such that there is minimal chance of being unable to use the system from both control rooms. Another example is the separation of power supplies for the control rooms.	Completeness	accepted	New 5.32		
73.	Section 5 **Main control room**	**General comment**	The ability to operate the main facility systems should be restricted to the main and supplementary control rooms. Local control of plant should be restricted to only those tasks not required to be performed by reactor operators for example operation of experimental or production equipment. Actions allowed from the Supplementary Control Room should be considered as required by the facility operation/emergency plans.				

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
74.	Section 5 **Provisions for fire detection and extinguishing**	**General comment**	National or state requirements should be noted as inputs for the design. Gas suppression systems are a good alternative to water sprinkler systems for rooms containing power and instrumentation and control systems. Requirements for periodic testing should be considered.				
75.	5.59	Failure modes for power supplies also need to be considered.	Completeness		accepted It will add a last sentence phrased as: *In addition failures modes for power supplies should be considered.*	New 5.53	
76.	5.60 Note 2	Consider effect on failure modes for centralised DC instead of distributed DC conversion.	Completeness			rejected	The comment is too specific for this section

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
77.	Section 6 **Operational Limits and Conditions**	Include the definition of Allowable Value as these values are often chosen for inclusion in the OLCs. Include mention of the need for a well-defined trip setpoint methodology which ties all these definitions together.	The Allowable Value is the least conservative value at which a trip may actuate during a test. Its calculation is based on the instrument and test equipment uncertainties associated with doing the test. A means for calculating the trip setpoints and allowable values should be established and a means of controlling these values should be implemented in the operating organisation.			rejected	Paragraph 104 already deals with the uncertainties associated with the safety system settings.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
78.	6.2	Rephrase for clarity.	This paragraph is unclear. The protection system contributes to keeping the values of reactor parameters within the limits determined for facility safety.		accepted The paragraph will be rephrased as: *The design of the instrumentation and control systems of the reactor should assure that, during the operational states of the reactor, the instrumentation and control systems contribute to keep the reactor parameter values and system conditions within the original selected operational limits and condition;* REF [10].		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
79.	6.3		The systems should prevent reaching the Analytical Limits as these are measureable parameters. It is the value of these limits that prevent reaching the safety limit.		accepted The paragraph will be rephrased as: *The instrumentation and control systems should include those safety functions and safety related functions that prevent the exceeding of safety limits during the operational states of the reactor by means of the selected safety system settings, during design basis accident and, …*		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
80.	6.4	Use analytical limit instead of safety limit.	Clarity	accepted			
81.	6.4	Explain what is meant by "capability of storing these safety system settings".	If the computerised RPS is powered off, is it expected to keep the setting in memory?		Accepted The last sentence of the paragraph will be rephrased as: *The required instrumentation and control systems to provide these functions should include the capability of storing or recovering these safety systems settings.*		
82.	6.5	Add: Acceptable margins must be allowed for expected drift in measured signals and all expected variations during normal operation.	Completeness	accepted			

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
83.	6.9	Add: National regulations/standards may be used to define the requirements for control system security as the control system/IT technologies become more alike.	Although the purpose of security is to prevent unauthorised access to the system, it has to be ensured that legitimate access is not prevented in any circumstance so that safe operation of the plant is maintained.		accepted It will be added as the last sentence of the paragraph: *National regulations/standards may be used to define the requirements for control system security.*		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
84.	Section 6 **Maintenance, Testing, Surveillance** ...	**General comment**	What is the agency's position on routine testing of software (replicating equivalent tests that are normally done on hardware logic)? For example logic testing of software based systems where the logic is programmed rather than hardwired? Hardware fails but software does not change unless reprogrammed.				Clarification: Once the system based on software is commissioned there is not recommended practice to perform routine testing of software at regular intervals because the software is not allowed to be modified after the commissioning stage.
85.	6.18	Add: For example, tripping one redundancy of a 2oo3 system leaves a 1oo2 system remaining during the test. Administrative controls on availability of safety systems should keep operation within design bases.	Completeness.	accepted			
86.	6.19	... or any other reason.	Completeness.	accepted			

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
87.	6.20	... and also what instrumentation is required to restart the reactor after a long shutdown when normal instrumentation may be out of range.	Completeness.			rejected	To restart the reactor after an extended shutdown should be applied a restart programme for the research reactor approved by the reactor manager, the safety committee and also by the regulatory body.
88.	7.4	Add: The safety classification of the HMI will determine the level of qualification required and could limit the technology available.	Completeness.			rejected	It is out of the scope of paragraph 7.4.
89.	7.9	Consider clarifying in accordance with the comment provided (right).	Does this statement refer to modernisation projects within an organisation or is it expected that for a new installation, a review of other plants is conducted?	Accepted	New 7.6		Clarification This statement refers to new projects as well as modification projects.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
90.	7.10	... and should be part of architecture considerations	Completeness		Accepted New 7.7 It will be rephrased as: *and should be part of architectural consideratio ns during the design stage*		
91.	7.13	"..should **take into account the** time needed by operators…"	Clarity	accepted	New 7.16		
92.	7.14	Consider revising to: The instrumentation and control system should protect against operator errors by implementing range limits, interlocks or trips to protect the plant from unsafe operation.	It is impossible to prevent operator error for actions that are undefined. Some clarity is required on this statement. Caution should be taken when implementing inhibits on operation unless these inhibits are always applicable. Operator actions can usually be monitored through system logs on computerised systems.	accepted	New 7.17		
93.	7.15	Consider deleting.	This statement is similar to 7.10 and should also be considered in architecture.	accepted	deleted		
94.	8.16	Delete	Repeat of 8.9.	accepted	deleted		
95.	8.36	**Clarification required**	A different organisation could also be used to complete V&V activities.	accepted			

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
96.	8.48	**Clarification required**	Does this refer to software errors? The term software hazard is unfamiliar. Is there a suitable reference for identifying and dealing with software hazards and software safety analyses? Or can this point be expanded here?		accepted Paragraph deleted by other MS comment		
97	8.75	**Clarification required**	The requirement for verification of maintenance is unclear. Does this mean that maintenance instructions are tested on the plant?	accepted	New 8.73		"*maintenance*" will be removed from the paragraph
98.	8.79	**Clarification required**	It is recommended in American standards that partial download of software modules is not performed for safety systems. Complete downloads are done instead.			rejected	Partial modification does not mean partial download of the modified module. A complete download must be done after a modification.
99.	9.2	• maintenance (e.g. maintenance plans, instructions for preventative and breakdown maintenance);	Completeness			rejected	Maintenance is already mentioned as an example in "measures for improvements" bullet
100.	9.4	... or generation of new documentation to describe the existing installation.	Completeness	accepted	Inserted to 10.8 but deleted after		

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
101.	10.3	Example is not clear and the example should include an example of an effect.	Clarity	accepted	New 10.5		
102.	10.5	Change "competition" to "completion".	Grammar	accepted	New 10.7		
103.	10.17	The second statement is unclear.	Clarity	accepted	New 10.18		
104.	Annex 1 1.3	"..compare them with allowable values…" should be "…compare them with **safety system settings** ...".	Clarity	accepted			
105.	Annex 1 1.11	(See also point 2.14 above.)	It is the experience at OPAL (Australia) that specifying the Vibration Monitoring System as a separate system does not add any value. The vibration sensors are part of the process system to which they are connected. Seismic sensors are not included in the VMS at OPAL.			rejected	The intention of the annex is to show all the systems that can be included in a generic design. In this case, the vibration monitoring system is considered as a data acquisition system to collect information of all the relevant vibration parameters of the facility.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
106.	Annex 1 1.13	Delete duplication of requirements where these occur in the list.	Seems to be some duplication in the list		accepted The ninth bullet will be rephrased as follow to eliminate possible duplication: *keep the reactor in a safe shutdown; and*		
107.	Annex 1 1.18	**Clarification required**	Would recommend not mixing security and operational CCTV. They are for different requirements. Reactor Operators should not be responsible for responding to physical security incidents.	accepted			The paragraph will be rephrased to eliminate any reference to security staff or security use of the CCTV

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
108.	Annex 1 1.20	**Clarification required**	Unless the reactor operators are required to respond to physical access situations, would not recommend an access control panel in the control room. If the reactor operators are required to know about access to particular areas of the plant, then dedicated sensors should be made part of the reactor control system or safety system. For example at OPAL, the containment area air lock doors are controlled by the separate physical security system but have dedicated sensors for the reactor control system and PAM system.		Accepted The last sentence will be rephrased as: *Access control panels <u>may</u> be located in the control rooms to provide the reactor operators with relevant information.*		The paragraph will be rephrased to eliminate the strong requirement.

Comment No.	Para/ Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
109.	2.7/1,2	Functions of safety systems are to ensure timely detection of deviation from the normal operation and automatically initiate reactor shutdown; emergency core cooling and residual heat removal to prevent violation of safety limits, and confinement of radioactive materials and/or limitation of accident releases.	'Limits and conditions for safe operations' used in the draft could be misinterpreted as OLCs. Safety systems e.g. automatic trips are setup in such a way the parameters during anticipated transient states do not violate the OLCs.	accepted			

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

Canada

COMMENTS BY REVIEWER Reviewer: Country/Organization:			Page.... of.... Date:	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	General		We highly welcome and acknowledge this initiative that will hopefully help in clarifying guidance for facilities we regulate. Although, no research reactors are contemplated to be constructed in Canada in any near future, changes to existing facilities have, or are expected to take place.				Noted
2.	1.1	It supplements and elaborates upon the safety requirements for design and operation of the instrumentation and control ~~system~~ (I&C) systems for research reactors…	1. Suggest to use I&C in the main body of the text 2. Plural should be used. This comment is applicable to the whole document where both "instrumentation control system" and "instrumentation and control systems" are used.			Rejected	Acronyms are omitted in the safety guide
3.	1.2	… caused by ~~intelligent~~ smart	To be consistent with	accepted	Sentence deleted		

		devices …	DS431				
4.	1.3	The objective of this ~~safety guide~~ Safety Guide	Safety Guide should be capitalized. This comment is applicable to the whole document			Rejected	Capital letters are omitted in the text safety guide within the paragraphs
5.	1.3	… including I&C architecture,…	Section 2 is devoted to I&C architecture, therefore, one of the objectives of DS436 is given guidance on I&C architecture	accepted			
6.	1.3	.. the regulatory body, I&C equipment and system suppliers and other …		accepted			
7.	1.4	This safety guide provides guidance on the design, implementation, …	Missing activity "implementation" which has been used 18 times in the DS436	accepted			
8.	1.5	~~Post-Accident Monitoring System (PAMS)~~ Accident Monitoring System ~~Post-accident monitoring instrumentation~~ Accident monitoring instrumentation is becoming an important feature of nuclear facilities.	Suggest changing "post-accident monitoring" to reflect the fact that these instrumentation plays an important role in the accident management. This comment is applicable to the whole document	accepted	Accident monitoring is mentioned only in the Annex not in para 1.5		
9.	Section SCOPE		The document is intended to apply specifically to research reactors. However, the document			Rejected	Please refer to Ref. NS-R-4 for these issues, in particular paragraph 1.3 and

			does not define research reactors, explain the specific challenges / differences posed by such facilities and how it addresses such differences. In that, it is unclear that the proposed document is indeed a graded version of NS-G-1.3 (same document for NPPs), and brings specific information and guidance applicable to "research reactors". Research reactors cover a wide span of power and complexity. I&C requirements vary from very minimum for inherently safe reactors (e.g. SLOWPOKE reactors), to even more complex than what is expected in NPPs for test reactors (e.g. NRU) where changes are frequent due to flexibility in core configurations, and in view of constraints and additional trips signals to				1.9

			ensure core / personnel protection from operation of test (loops) / experimental (beams, neutron sources) / production (targets) systems / sites. The scope being unclear, it is difficult to comment on completeness and adequacy of the document. In that, the objective of the document and what it needs to accomplish (e.g. provide guidance for a given type of reactor) are unclear and do not clearly provide incremental guidance from that provided in NS-G-1.3, except may be for introduction of more modern concepts (e.g. computer based systems and software).				
10.	Section SCOPE	Add a paragraph to reflect the fact that DS436 also gives recommendations to security	DS436 also given guidance to computer security, for example, Para. 4.42 to 4.49 are	accepted	In 1.4		

			dedicated to security. Phrase “security” is used 37 times in the document				
11.	2.4	Remove this clause	The clause reads as “Systems not important to safety are those systems that do not belong to systems important to safety. » This clause adds nothing; also, it constitutes its own rationale.	accepted and deleted	recursive definition.		
12.	2.5 and 2.6		Graded approach is discussed in Para 2.5. It states that “*for instrumentation and control systems important to safety, graded approach to the requirement of Ref [1] can be applied but the extent of grading should be clearly justified in the safety analysis report*.” The graded approach is a method in which the stringency of the design measures and analyses applied are commensurate		accepted . new 2.4 Reference is made to the IAEA Safety Guide on application of graded approach		

			with the level of risk posed by the reactor facility. Designs using the graded approach shall demonstrate that the all safety objectives and the requirements are met. Clarification is required for the “graded approach to the requirements” stated in Para. 2.5.				
13.	2.8	Restrict last bullet to “Mitigate the consequences of beyond design basis accidents”, and remove note 1.	Design extension conditions is not the same as BDBAs, as the latter includes severe accidents. To this reviewer’s knowledge, severe accidents are those concerned with core degradation and are considered to be beyond design extension conditions.			Rejected	In accordance with the new terminology introduced by IAEA SSR 2/1
14.	Fig 1, Paras 2.17 to 2.23		One of the unique characteristics of a research reactor is the experimental devices. Therefore, it is expected that guidance should be given to the safety classification of	Accepted			Classification of I&C for experimental devices follows same methodology as for the reactor itself.

			experimental devices I&C systems in this document. Para. 2.16 listed I&C of experimental devices and irradiation installations that do not affect reactor safety as one of the systems not important to safety. The question is whether there are I&C of experimental devices and irradiation installations that do affect reactor safety. Annex 1.16 states that "*Experimental and irradiation installations may have an impact to the reactor safe operation, so main parameters of the experimental devices that affect the safety of the reactor should be displayed in the main control room. Also trip signals from IEFCMS to RPS could be provided as demanded*." It states also in Para 1.11				

			of NS-R-4 that "*design and operating characteristics of research reactors may vary significantly since the use of experimental devices may affect the performance of reactors. In addition, the need for flexibility in their use requires a different approach to achieving and managing safety*." In view of the above quoted statements from this document and NS-R-4, guidance should be given in this document on how to classify I&C systems for experimental devices and irradiation installations.				
15.	2.8		To be consistent with 2.7, please consider adding emergency core cooling in Bullet 3	accepted	Paragraph deleted following comments from other MSs		
16.	2.21 to 2.23	DESIGN, CONTRUCTION, OPERATION AND MAINTENANCE OF INSTRUMENTATION AND CONTROL SYSTEMS	To be balanced with the text of Para. 2.21	accepted			

17.	2.21	All instrumentation and control systems and equipment should be designed, constructed, operated and maintained in ….	Missing ","	accepted	Paragraph deleted following comments from other MSs		
18.	3.2	… should fulfil safety objectives and design requirements described in paragraphs 2.2 to 2.7; …..	1. It is better to describe what the I&C architecture design will fulfil, even at high level.	accepted			
19.	3.2		By checking the paragraphs listed, we are expected the architecture design will address requirements listed. Para. 6.43 of NS-R-4 requires that the design of research reactor should consider ease of testing and maintenance. I&C architecture design plays an important role to fulfil this requirement. Clarification is required why " " described in Para. 6.43 is not addressed in the I&C architecture design.	accepted			The requirement will be addressed in section 3
20.	3.2		Research reactors are flexible in nature and they may be in various different states. Para. 6.65 of NS-R-4 requires that "*special precautions shall*	accepted			The requirement will be addressed in section 3

			be taken in the design in relation to the utilization and modification of the research reactors to ensure that the configuration of the reactor is known at all times." Clarification is required for why I&C architecture design will not address this unique and important requirement of research reactor.				
21.	3.2 and 3.3	Move to Section "OVERALL ARCHITECTURAL DESIGN OF THE INSTRUMENTATION AND CONTROL SYSTEM", which currently starts with clause 3.18	Clauses 3.2 and 3.3 explicitly concern I&C architecture.			rejected	They are general requirements and it is correct that they remain in the GENERAL section
22.	3.5	The facility design should incorporate the defence in depth <u>strategy</u>.		accepted	"concept" is used		
23.	3.5	Remove this clause.	The clause reads as "The facility design should incorporate the defence in depth. The levels of defence should be independent as far as is practicable. See also Ref. [6]. ». This Safety Guide is about I&C, not about facility. This clause has no business being here.		accepted "facility" will be replaced by "instrumentation and control system		

24.	3.11	~~Items important to safety should be environmentally qualified for the effects of the design basis accidents to which they must respond.~~	It is a legitimate requirement but might be in wrong place (I&C architecture design), because section 3 is dedicated to overall architecture design of I&C systems. Suggest moving EQ of ITS to other Section.	accepted			
25.	3.13	A common cause failure is defined as ~~the concurrent~~ failure of two or more structures, systems or components due to a single event or cause.	"Concurrent" is not in both IAEA safety glossary (2007) and NS-R-4 definition of common cause failure. Consistent with other IAEA documents is required	accepted	New 3.11		
26.	3.15	The design of equipment should take due account of the potential for common cause failures of items important to safety to determine how the concepts of diversity, redundancy, physical separation, electrical and functional isolation have to be applied to achieve the necessary reliability.	This paragraph is dedicated to CCF. It should be noted that redundancy is used for meeting SFC, not for CCF. In addition, physical separation, electrical and functional isolation are means to achieve independence which is described from paras 3.8 to 3.12.	Accepted	new 3.14		With the exception of redundancy that will be removed from the paragraph, the other elements are suitable to eliminate common cause failures.

			Clarification is required				
27.	3.17		For computer-based reactor protection system, the software CCF can be identified but could not be completely eliminated. However, the consequences can be mitigated by adding diversified reactor protection system(s). Clarification is required.	accepted			This issue is addressed in 5.21
28.	3.18 Bullet 2	Provide systems necessary to support the defence in depth ~~concept~~ <u>strategy</u> of the facility	DiD is a general concept, but is becomes strategy to be implemented in the facility design	accepted	New 3.15		
29.	3.24		Para. 6.42 of NS-R-4 states that "*The principle of fail-safe design shall be considered and shall be adopted in the design of systems and components important to safety, as appropriate: systems at research reactor facilities shall be designed to pass into a safe state, with no necessity for any action to be initiated, if a system or component fails.*"			rejected	There are no gaps between between Para 3.24 of DS-436 and Para 6.42 of NS-R-4. The paragraphs are written with the same meaning but using different wording.

			Similar statement can be found in Para 4.37 of DS-436. It looks like there are gaps between Para 3.24 of DS-436 and Para 6.42 of NS-R-4. Clarification is required.				
30.	4.2	Careful review of the rational for each requirement is one effective means for avoiding ~~inessential~~ unnecessary complexity.		accepted	Paragraph deleted following comments from other MSs		
31.	4.2	The design of the instrumentation and control systems should as simple as possible to achieve its imparted goals. Simplicity leads to fewer components, simpler interfaces, easier verification and validation and easier maintenance for the hardware and software. Proper requirement analysis is an effective means to achieve design simplicity.	Simpler guideline, same purpose, easier to read and understand.	accepted	Added to the new 4.2		
32.	4.16	The design of instrumentation and control system important to safety should minimize the possibility of common cause failures by ~~means~~ applying principle of independence, ~~physical separation~~ and diversity		accepted	New 4.13		

		strategy ~~of equipment~~. Especially, safety systems should be designed in such a way that ~~occurrence of~~ common cause failures are ~~safely~~ prevented or safely mitigated.					
33.	4.17	The principle of independence (e.g. functional ~~independent~~ independence, electrical isolation, physical separation by means of distance, barriers or a special layout ~~for reactor components~~ as well as ~~independent~~ independence of ~~communication~~ data transfer) should be applied, as appropriate and as far as reasonably practicable, to enhance the reliability of systems.	There are many forms of communication. The independence of communication specifically refers to data transferring	accepted	New 4.15		
34.	4.21	Electrical and data connections between redundant systems, and ~~connections~~ between safety systems and systems of a lower safety classification should be designed so that no credible failure in one system will prevent the other system(s) from meeting their performance and reliability requirements.	Clarifications are required: 1) It looks like redundant systems should be redundant divisions 2) when there is a form of connection between safety and system with a lower safety classification, the design should ensure that the failure of the lower safety classification shall not affect the safe operation of the safety system, not vice versus 3) there is no guideline given for connection between two safety systems	accepted	New 4.19		

35.	4.25	If data communication channels are used in safety systems they should satisfy the recommendations for independence (functional isolation, electrical isolation and physical separation).	First it is unclear what is the definition of “data communication channels” Second, it is not cleat how physical separation could be applied to data communication channels. Unless wireless communication is used, otherwise, they will be physically connected to cables. Clarification is required.			rejected	Data communication channels are those used for data transfer. Physical separation is achieved using different paths for redundant communication channels.
36.	4.26		Size of equipment was listed as a diverse attribute. It is not clear how the size of I&C systems plays a diverse role. Clarification is required	accepted	New 4.24		
37.	4.37	The principle of fail-safe design should be considered and adopted as appropriate in the design of instrumentation and control systems to fail into a safe state, with no necessity for any action to be initiated for any system in failure.	The fail safe design of system for shutting reactor down might require initiating trip the reactor. This might be conflicted with the statement as highlighted. Clarification is required for the highlighted statement			rejected	This paragraph complies with paragraph 6.42 of NS-R-4.
38.	4.50 (new)	“The taking in account of security should not impede the achievement of accident management by the safety systems nor by the operator”.	To avoid security requirements leading to a safety concern. It is useless to have a secure facility if it is not also a safe facility.			rejected	The issue is addressed in 4.45
39.	4.67	The types of electromagnetic interference to be considered in the	It is true that immunity to electromagnetic disturbances should be considered in the			rejected	Clarification: Electromagnetic

		design of instrumentation and control systems and components should include: • Emission of and immunity to electromagnetic disturbances;	design of I&C, however, immunity to electromagnetic disturbance is not one of the types of EMI. Clarification is required.				interference is a disturbance that affects an electrical circuit due to either electromagnetic induction or electromagnetic radiation emitted from an external source
40.	4.100	(b) Failure mode and effects analysis 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.	FMEA is a systematic analysis of the systems to demonstrate that no single failure will cause an undesired event. However, FMEA is not used to confirm compliance with the SFC as suggested by the quoted statement. Clarification is required.	accepted	4.100 (a)		
41.	FIG 4.1	Label “Safety system” should be “Safety system <u>trip setpoint</u>”	Missing “trip setpoint”		Accepted It will be completed as Safety system setting		
42.	5.14	Add to end of clause “These assumptions should be thoroughly validated in simulations using representative end users”	The assumptions stated in the clause are often made without realistic or credible basis; since the operator is expected to play a crucial role in safety, as assumed in the	accepted	It will be included as a foot note.		

			clause, a credible validation (beyond "engineering judgement") is required.				
43.	5.17	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	Paragraph deleted following comments from other MSs		
44.	5.21	If a computer based system is intended to be used in reactor protection system the following requirements should be applied: - Hardware should meet specified reliability requirements. - Software should be specified using formal methods, or equivalent. …..	First bullet is vague (who will admit not to use quality stuff and best practices?).			rejected	The rec formulation of the ommendation is valid
45.	5.25	Unclear why this clause is in italics.					Clarification: Because it is an extract from NS-R-4, par. 6.104, (c)
46.	5.28	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive	accepted	Paragraph deleted following comments from other MSs		

			set of guidelines that will lead to a broader and robust design.				
47.	5.30	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	New 7.14		
48.	5.31	Add consideration for research-related tasks, and for accident handling.	The mission of the system is to support research-related tasks, so requirement definition and analysis should consider it.	accepted	new 5.26		“accident handling” will not be considered as the paragraph deals with normal operation of the reactor
49.	5.33	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted			
50.	5.35	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations	accepted	New 7.26		

			contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.				
51.	5.36	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	New 5.27-5.28		
52.	5.37	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	new 7.27		
53.	5.41	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	New 5.34		

54.	5.42	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.	accepted	New 7.29		
55.	5.43	Remove clause and incorporate its intent to Section 7 on Human Factors.	This is too specific as a guideline, as well as too restrictive. The Human Factors considerations contained in Section 3 provide a comprehensive set of guidelines that will lead to a broader and robust design.			rejected	The clause in question is very important and specific for the main control room.(requested to be included by another MS)
56.	7.1	An effective human factors engineering process should be embedded into the overall design process for every aspect of the design.	Such a process will typically incorporate a screening step that will guarantee that human factors will be considered, as appropriate, wherever it is warranted.	accepted			
57.	7.2	Remove.	The essence of this clause is subsumed by clauses 7.9 to 7.20 in section titled “PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HMI DESIGN”.	accepted			

58.	7.3	Reword to “Appropriate design standards and guidelines should be identified and used throughout the design process”.	The suggested wording is to broaden the usefulness of this Section. The wording for the original clause is specific to HMI design. Its content will be subsumed in a new wording for clause 7.11.	accepted			
59.	7.4	Move over to section titled “PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HMI DESIGN”	The clause is specific to HMI design.	accepted	New 7.8		
60.	7.5	Move over to section titled “PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HMI DESIGN”	The clause is specific to HMI design.	accepted	New 7.10		
61.	7.7	Move over to section titled “PRINCIPLES FOR HUMAN FACTORS ENGINEERING AND HMI DESIGN”	The clause is specific to HMI design.	accepted	New 7.15		
62.	7.11	Design requirements for HMI designs should be specified based on all of the tasks to be supported by the HMI, including normal and abnormal operations, for operators as well as the maintenance staff, experimenters and emergency response staff.		accepted	New 7.9		
63.	7.18	Remove.	While this is the “textbook” way to do things, the content and intent of this clause are	accepted			

			subsumed by the newly worded clause 7.11.				
64.	7.19	Remove.	The content and intent of this clause are subsumed by the newly worded clause 7.11.	accepted			
65.	7.20	Remove.	The content and intent of this clause are subsumed by the newly worded clause 7.11.	accepted			
66.	7.24	Remove.	The content and intent of this clause are subsumed by the newly worded clause 7.11.	accepted			
67.	7.25	Remove.	The content and intent of this clause are subsumed by the newly worded clause 7.11.	accepted			
68.	8.8	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 is required for top-down development process.	accepted	It will be clarified by a foot note. Footnote 6		
69.	8.56	The production of software code should be verifiable against the software specifications.	Clarification is required on how to verify the production of software code against software specifications	accepted	New 8,54		
70.	8.57	A system for requesting formal change and controlling modifications should be in place in the implementation phase to deal	Is this a software specific requirement or it is applicable to all I&C systems?				Clarification: It is an specific clause for software based systems

		with omissions and inconsistencies.					
71.	ANNEX I Fig AI.1		It is indicated that VMS is linked to reactor control and monitoring system (RCMS). What are the purposes of such link? Is there any information from produced in the VMS be used in RCMS or RCMS is used for passing the information from the VMS to the control rooms? Clarification is required. In the meantime, HVAC system is linked to RCMS as well. It shows that there are information exchanges between RCMS and HVAC. What are the information send from RCMS to the HVAC system? Clarification is required.	accepted			

Draft Safety Guide DS436 „Instrumentation and Control and Software Important to Safety for Research Reactors “
Status: SPESS Step 8 – Consultation of MS for comments.
Deadline for comments: 31 May 2013

	COMMENTS BY REVIEWER Reviewer: **Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)** (with comments of TÜV Süd) Page 1 of 4 Country/Organization: **Germany** Date: 2013-05-14				RESOLUTION			
Rele-vanz	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/reject ion
2	1	2.9	“The safety system should automatically initiate [???] the required protective actions for the full range of postulated initiating events to terminate the event safely.” Add Footnote: [???] Manual operator action is permitted accordingly to §5.14	See §5.14	Accepted	Paragraph deleted following comments from other MSs		
1	2	2.17 3rd bullet	Delete 3rd bullet	→2.18 / 1st bullet	Accepted	Paragraph deleted following comments from other MSs		
1	3	2.18 1st bullet	~~The estimated frequency or probability (if available) of postulated initiating events and the potential severity of their consequences if the instrumentation and control system provided fails (e.g.: high, medium or low probability, with high, medium or low consequences (e.g. radiological consequences));~~	The frequency/probability of PIE should be considered in the safety analysis. The I&C classification bases on this analysis and the specified design basis accidents and design extensions.		Paragraph deleted following comments from other MSs	Rejected	1st bullet of 2.18 considers the potential severity if the instrumentation and control system fails upon a request to perform a safety function. This safety guide does not include the reference to the

			In case of comparable severity of consequences the instrumentation and control functions needed to mitigate consequences of design extension conditions could be assigned to a lower safety class than functions needed to control anticipated operational occurrences and design basis accidents to reach a controlled state (cf. para. 3.15 and Tab. 1 of Ref. [???]). [???] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standard, IAEA, Vienna, in preparation.					draft "Safety classification of Structures, Systems and Components in Nuclear Power Plants (DS367)"
2	4	2.18 bullet 4	… can be detected by the operational behavior and remedied. Make a footnote to the remedy	The detection by self supervision and the maintainability can be not addressed in the phase of the classification. A possible factor may be the permissible downtime associated with typical usual repair time.	Accepted	Accepted Paragraph deleted following comments from other MSs		
2	5	2.19	clarify	It is not clear which criteria are meant.	accepted	Paragraph deleted following comments from other MSs		

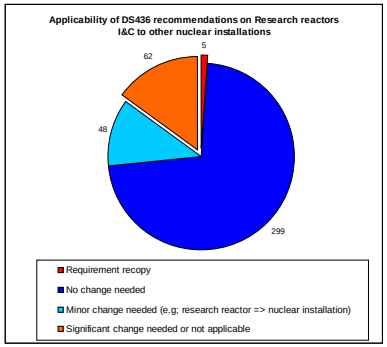
1	6	2.21	… constructed commissioned operated …	The important phase of commissioning is missing.	accepted	Old 2.21 new 2,7		
2	7	2.23	… as the process-engineering system or equipment ….	There may be a contradiction to 2.14, bullet 4	accepted	Paragraph deleted following comments from other MSs		
2	8	3.1	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 [1] reactor shutdown, emergency core cooling, residual heat removal, and the confinement of radioactive materials and/or limitation of accidental releases during and after accident conditions. Add Footnote: [1] Manual operator action is permitted accordingly to §5.14	See §5.14	accepted			
2	9	3.3	… A well designed architecture is characterized by a rational ….	There are a lot reasons for complexity (see 4.2). The functional allocation is no relevant factor for complexity of modern computer based I&C systems.	accepted			
2	10	3.13	… ~~concurrent~~ failure …	See safety glossary	accepted	New 3.11		
1	11	3.14	"Justification that a common cause	A important factor of	accepted	New 3.12		

			failure need not be considered may, for example, be based on the assigned level of defence in depth of the instrumentation and control function, the component dependability, or technology~~, or feedback gained over its wide usage~~."	the consideration of CCF or not is the associated level of the defense in depth (graded approach). Operational feedback cannot give reliable forecasts for the potential for CCF.				
3	12	3.17	The 2. Sentence should be moved as 1. Sentence.	No logical order of the sentences	accepted	Paragraph deleted following comments from other MSs		
2	13	3.18, bullet 3	clarify	The meaning of the sentence is not clear: what is meant by "a hierarchical system design"? Which design features "keep the highest priority"?	Accepted	New 3.15The paragraph will be rephrased as: • *provide preferably a hierarchical system design where instrumentation and control systems that belong to safety systems keep the highest priority to perform the safety functions for which they have been designed. In this way, other systems of lower safety class are not able to prevent the*		

						actions initiated by safety systems. (i.e. shutdown of the reactor)		
1	14	4.28	Delete this aspect	The factor of the conservatism should be only the consequence of PIE not their frequency.		accepted Paragraph deleted following comments from other MSs		
2	15	5.60	… be connected to uninterruptible ~~alternative~~ current power supplies …	The requirement and the footnote don't fit together.	Accepted "	footnote deleted		
3	16	8.16	delete	The requirement is doubled (see 8.9)	accepted			

TITLE : DS 436 Instrumentation and Control and Software Important to Safety for Research Reactors Draft 3

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.		Change the scope of DS436 to make it applicable to all facilities, with an appendix specific to research reactors or delete items not specific to research reactors	Lots of paragraphs (3 out of 4) than in DS436 are not really specific to research reactors and could apply to any I&C system, for example to Fuel cycle facilities or NPP. (see graphs at the end of the table) 			Rejected	DS436 supplements and elaborates the safety requirements for Instrumentation and Control (I&C) systems and software important to safety for research reactors which are established by the Safety Requirements NS-R-4. The scope of the Safety Guide covers: All components of I&C systems from sensors to human-machine interface; research reactors of all types and sizes; research reactor experimental facilities and utilization of RR and I&C modernization projects. In preparation of the DS436, the guidance provided by DS431 was taken into consideration. Where appropriate, certain provisions of the DS431 were adapted, considering the differences in potential hazards and in complexity of systems between NPP and RRs. This issue was already discussed and solved during the NUSSC meeting held in November 2012 and it was obtained the clearance to send the draft to MS for comments.

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
2.	1.1	This safety guide ~~is part of the set of publications developed within the framework of the IAEA research reactor safety programme, which covers all of the important areas of research reactor safety. It~~ supplements and elaborates upon the safety requirements for design and operation of the instrumentation and control system for research reactors that are established in Section 6 and 7 of Ref. [1].	Superfluous	accepted			
3.	1.2	~~The rate of ageing and obsolescence of research reactor instrumentation and control systems has increased due to the technological advancements in the field of electronics.~~	Superfluous. Next sentences (as modified) is enough	accepted			
4.	1.2	During the lifetime of a research reactor one or more refurbishments of instrumentation and control system can be predicted. There are different reasons demanding instrumentation and control modernization projects such as obsolescence or ageing, improvement of maintainability and reliability, new utilization or experiments in research reactors, enhancement of safety, etc.	To take into account deletion of prevrious sentence	accepted			

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
5.	1.2	~~The advances in technology will require special attention to the safety classification of instrumentation and control systems, to the development in the use of computer based instrumentation and control systems, to the significant structural changes of instrumentation and control systems caused by the intelligent devices, and to the software development including verification, validation and quality assurance.~~	Superfluous	accepted			
6.	1.5	The guidance applies to both, the design and configuration management of instrumentation and control systems for new research reactors and to the modernization of the instrumentation and control of existing facilities.	To take into account para 1.7 (which deletion is proposed)	accepted			
7.	1.7	Delete 1.7	Superfluous considering modified 1.5	accepted			
8.	1.9	Transfer 1.9 to section 10	More appropriate location	accepted	New 10.1		
9.	1.9	Additional aspects supporting a positive decision for modernization is ~~evidently~~ the technological progress in instrumentation and control systems leading to higher reliability of instrumentation and control systems, improvement of human-system interface and extensive and fast data collection and processing.	Superfluous	accepted	New 10.1		
10.	1.10	Transfer 1.10 to section 10	More appropriate location	accepted	New 10.2		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
11.	2.1 Bullet list	~~Functions, systems, and components important to safety are further categorized as either safety systems or safety-related items;~~	This would better fit at the beginning of 2.2	accepted			
12.	2.1 Bullet list	~~• The main safety functions for a research reactor are:~~ ~~i. Control of reactivity;~~ ~~ii. Cooling of radioactive material; and~~ ~~iii. Confinement of radioactive material.~~	Delete bullet as it does not bring additional information on the separation between items important to safety and items not important to safety (which is the topic addressed in 2.1	accepted			

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
13.	2.2 2.3	2.2 <u>Functions, systems, and components important to safety are further categorized as either safety systems or safety-related items:</u> <u>•</u> Safety systems consist of the protection system, the safety actuation systems and the safety system support features. 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. The design premise should be to prevent the addition of any component or function not strictly required by the highest safety classification. • ~~2.3~~ Safety related systems are systems important to safety performing other safety functions not mentioned in paragraphs 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.	Merge 2.2 and 2.3 so that: - 2.1 set distinction between items important to safety and items not important to safety and make links with functions (not) important to safety - New 2.2 deals with items important to safety See previous comment on 2.1	accepted			

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
14.	2.4	Locate 2.4 in 2.1 bullet list 2.1 For the purposes of this guide the following classification scheme is used to grade recommendations according to safety significance: • All instrumentation and control functions, systems, and components fit into one of two categories: items important to safety or items not important to safety (see Fig.1); • Functions, systems, and components important to safety are those which contribute to: i. Safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions; ii. Remove residual heat from the reactor core after shutdown, and during and after appropriate operational states and accident conditions; iii. Prevent or 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 accidents; and iv. Permit the safe operation of the reactor. • Systems not important to safety are those systems that do not belong to systems important to safety. • Instrumentation and control systems important to safety are those instrumentation and control systems used to accomplish functions important to safety.	To be consistent with the content of 2.1 which discuss classification	accepted	Not implemented due to other MS comments		
15.	2.5	Locate 2.5 after Figure 1	More logical location.	accepted	New 2.4		
16.	2.6	Merge 2.5 and 2.6	Both are making link with IAEA safety standards	accepted	New 2.4		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
17.	2.7	Delete 2.7	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
18.	2.8	Delete 2.8	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
19.	2.9	Delete 2.9	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
20.	2.10	Delete 2.10	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
21.	2.11	Delete 2.11	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
22.	2.12	Delete 2.12	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
23.	2.13	Delete 2.13	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			.
24.	2.14	Delete 2.14	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			.
25.	2.15	Delete 2.15	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			
26.	2.16	Delete 2.16	Fig 1 is enough (classification of SSC is not the purpose of the guide)	accepted			

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
27.	2.17	The method for classifying the safety significance of a structure, system or component should be based primarily on deterministic methods and engineering judgment, complemented where appropriate by available probabilistic safety assessment. <u>For I&C,</u> The basis for such classification should consider:	Only I&C classification is encompassed in the scope of the guide, not all SSCs classification.	accepted	Old 2.19 new 2.5		
28.	2.18 bullet lisr	~~• The estimated frequency or probability (if available) of postulated initiating events and the potential severity of their consequences if the instrumentation and control system provided fails (e.g.: high, medium or low probability, with high, medium or low consequences (e.g. radiological consequences));~~	Already taken into account in 2.17	accepted	Old 2.20 deleted		
29.	2.19	Delete 2.19	Superfluous considering 2.20	accepted	Old 2.21		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
30.	2.23	Instrumentation and control system ~~or equipment safety class~~ should have the same safety class as the system or equipment they control/monitor.	Superfluous	accepted	New 2.9The paragraph will be rephrased as: *The safety class of the instrumentation and control system should be based on the safety class of the function of the parameters being controlled/monitored. .If an instrumentation and control system or equipment controls or monitors several process systems or equipment, its safety class should be the same as the highest safety class of these parameters being controlled/monitored.*		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
31.	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 ~~.~~(including shut down, refuelling, maintenance) and accident conditions. In particular, I&C should enable to automatically initiate reactor shutdown, emergency core cooling, residual heat removal, and the confinement of radioactive materials and/or limitation of accidental releases during and after accident conditions.	To explicitly mention I&C should be appropriate for accident management	accepted			
32.	3.6	Merge 3.5 and 3.6	Both deals with DiD	accepted	Paragraph 3.6 deleted following comments from other MSs		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
33.	3.9		First part of the sentence ("to compromise the independence of a SSC safety class") is unclear . A safety class is achieved (or not) but what means compromising its independence ?		accepted The paragraph will be rephrased as: *The overall instrumentation and control architecture should not compromise the independence implemented at the different levels of defence in depth*		.
34.	3.11	Merge 3.11 with 4.50	Same topic (qualification)	accepted	Paragraph 3.11 deleted following comments from other MSs		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
35.	3.14 and 3.16	The second part of 3.14 ("The consequences of a postulated initiating event in combination with a common cause failure that prevents necessary reactor protection system response to the postulated initiating event should be no greater than those tolerated for design basis accidents. The accident sequences and consequences resulting from the combination of a postulated initiating event and common cause failure of the reactor protection system may be analysed using best estimate methods.") should be merge with 3.16		accepted	New 3.13		
36.	Fig 3.1	Locate Fig 3.1 before 3.21	More logical place	accepted	New 3.19		
37.	Heading before 4.7	Redundancy <u>and single failure</u>	4.7, 4.13, 4.14 and 4.15 are dealing with redundancy but 4.8 to 4.12 are dealing with single failure. Having all these paragraphs under one heading would be better…	accepted			
38.	4.7	The last sentence of 4.7 ("The design should ensure, on the basis of analysis that the redundancy will provide a backup to assure that no single failure could result in a loss of the capability of a system to perform its intended safety function.") should be located after 4.9	The sentence deals with single failure	accepted	New 4.10		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
39.	4.8	4.8 should be located after the heading "Single failure"	4.8 deals with single failure	accepted			
40.	4.12	Merge 4.12 with 4.10	Same topic (resistance to single failure)	accepted	New 4.11		
41.	4.16	Especially, safety systems should be designed in such a way that occurrence of common cause failures are ~~safely~~ prevented.	Superfluous	accepted	New 4.13		
42.	4.20	Merge 4.20 with 4.17: 4.17 The principle of independence (e.g. functional independent, electrical isolation, physical separation by means of distance, barriers or a special layout for reactor components as well as independent of communication) should be applied, as appropriate and as far as reasonably practicable, to enhance the reliability of systems. <u>For example,</u> ~~4.20~~ Different safety functions should be performed by different modules, components or systems to avoid the effect of the failure of these items on each other.	Same topic	accepted	New 4.15		
43.	4.30	In any application, it should be ensured that <u>required</u> diversity is achieved in the implemented design and preserved throughout the life of the facility.	Clarification	accepted	New 4.27		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
44.	4.32 bullet list	• Equipment diversity: achieved by sensors and systems using different technology or produced by different manufacturers.	Equipment diversity is also provided by different manufacturer (not using the same equipment as explained in 4.33)	accepted	New 4.29 The bullet will be rephrased as: *equipment diversity: achieved by sensors and systems using different technology or designed and produced by different manufacturers*.		
45.	4.33	In assessing claimed diversity, attention should be paid 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, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers' names are insufficient without consideration of this possibility.	Superfluous	accepted	New 4.30		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
46.	4.33	~~To minimize common failure modes, the design should preferably consider the option of different processors with different operating systems.~~	This may be a too strong recommendation. The issue of "true" diversity is adequately addressed in the previous sentences in 4.33	accepted	New 4.30		
47.	4.34	Delete 4.34	Redundant with beginning of 4.35	accepted			
48.	4.43	As the instrumentation and control system is, in general, a combination of hardware and software modules that execute the overall functional and performance requirements to keep the research reactor in safe status in all of its plant states, the architectural and functional vulnerabilities and their consequences on the instrumentation and control system should be assessed ~~and quantified~~.	Quantification may not be feasible.	accepted	New 4.41		
49.	4.49	Delete 4.49	There is no equivalent recommendations on safety aspects.			rejected	The paragraph is valid for Security. There is not a similar section for safety.
50.	4.56	Examples of functional requirements ~~should~~ include:	Typo	accepted	New 4.55		
51.	4.57	Examples of performance requirements ~~should~~ include:	Typo	accepted	New 4.56		
52.	4.58	Examples of reliability requirements ~~should~~ include:	Typo	accepted	New 4.57		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
53.	4.61	Systems and components should be designed to withstand the effects of, and be compatible with the environmental conditions associated with normal operation, ~~and~~ anticipated operational occurrences and ~~or postulated~~ accidents when they are required to function.	clarification	accepted			
54.	4.64	Merge 4.64 and 4.63	Same topic	accepted	New 4.62		
55.	4.64	Significant sources of electromagnetic interference ~~should~~ include,	Typoc	accepted	New 4.62		
56.	4.69	The contribution of electromagnetic emissions from all equipment, not only equipment important to safety, ~~must~~ should be evaluated as to its impact on the performance of instrumentation and control systems important to safety.	Guidance, not a requirement	accepted	New 4.67		
57.	4.71	Transfer “Many of the research reactors are operated on relatively short operating cycles therefore provisions for testing during operation on those research reactors may be not necessary.” into a footnote	This is not a recommendation and it weakens the previous sentence…	accepted	Footnote 2		
58.	4.72 g)	Delete bullet g)	Does not fit in the topic addressed.	accepted	4.70 (g) changed		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
59.	4.78	Examples of considerations ~~should~~ include:	Typo	accepted	New 4.76it will be rephrased as: *Considerations for the test should include:*		To keep the paragraph as a recommendation.
60.	4.78 bullet list	• ~~Have~~ communications facilities as needed to support the tests.	Typo	accepted	Bullet copied to a new para 4.77		
61.	4.79	Locate 4.79 in 4.72 e)	Same topic	accepted	New 4.70 (e)		
62.	4.87 4.88	Locate 4.87 and 4.88 after 4.95	Both paragraphs deals with inadequate test results. All other paragraphs deals with test programme and performance.	accepted	New 4.94, 4.95		
63.	4.105	Clear identification of components is necessary to reduce the likelihood of inadvertently performing <u>installation, modification,</u> maintenance, tests, repair or calibration on an incorrect channel.	Clarification	accepted			

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
64.	5.22 5.23 5.24	5.22 Where the necessary 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 fulfilment of the protection functions should be provided. The 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.; and • By a diverse system which may be hardwired or computer-based as long as adequate diversity can be justified*. ~~5.23 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.~~ ~~5.24 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, it is easier to justify diversity between computer-based and hardware-based systems than between two computer-based systems.	No need for separate paragraphs as some modifications to 5.22 (including adding a footnote) accommodate 5.23 and 5.24.	accepted	New 5.21		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
65.	5.35	The design should consider the layout of instrumentation and the mode of presenting information 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. The design of the control room should take into account ergonomic factors and include suitable provisions for preventing unauthorized access and use.	To have a similar recommendation for the control room as for the supplementary control room (5.43)	accepted	New 5.27, 5.28		
66.	5.60	Instrumentation and control systems that are required to be available for use at all times in operational states or ~~design basis~~ accident conditions should be connected to uninterruptible alternate current power supplies that provide the systems with power within the tolerances specified by the instrumentation and control design bases	No reason to limit to DBA	accepted	Old 5.59 New 5.54		
67.	6.2	The design of the instrumentation and control systems of the reactor should assure that, during the operational states of the reactor, the instrumentation and control systems contribute to keep the settings and values ~~of~~ within the original selected operational limits and conditions.	Clarification	accepted			

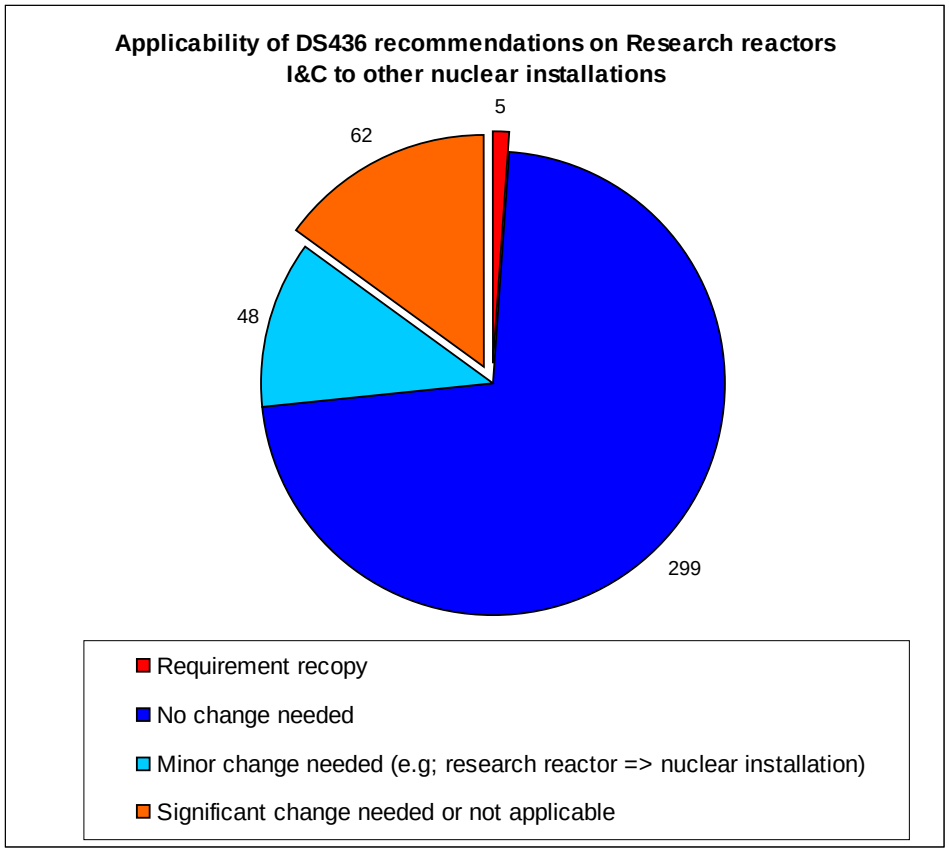
COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
68.	6.4	For each parameter for which a safety limit is required and for other important safety related parameters, an instrumentation and control system should monitor the parameter and, <u>where appropriate,</u> provides a signal that can be utilized in an automatic mode to prevent that parameter from exceeding the set limit.	To allow flexibility	accepted			
69.	6.5	Acceptable margins between normal operating values and the safety system settings should be considered in the functions of the instrumentation and control systems to assure safe operation of the reactor ~~and~~ <u>while</u> avoid<u>ing</u> frequent actuation of safety systems.	Clarification (if a trip is needed, it is needed, even it is frequent)	accepted			
70.	6.9	<u>When computer based systems are part of I&C systems,</u> On the basis of the security policy that has been defined for the computer based system environment, appropriate security procedures - for instance password management - should be implemented (for example to guard against unauthorized access and viruses).	Clarification	accepted			
71.	6.15	Delete 6.15	Redundant with para on pages 28 and 29			rejected	The recommendation is valid in both, Design and Operation Sections

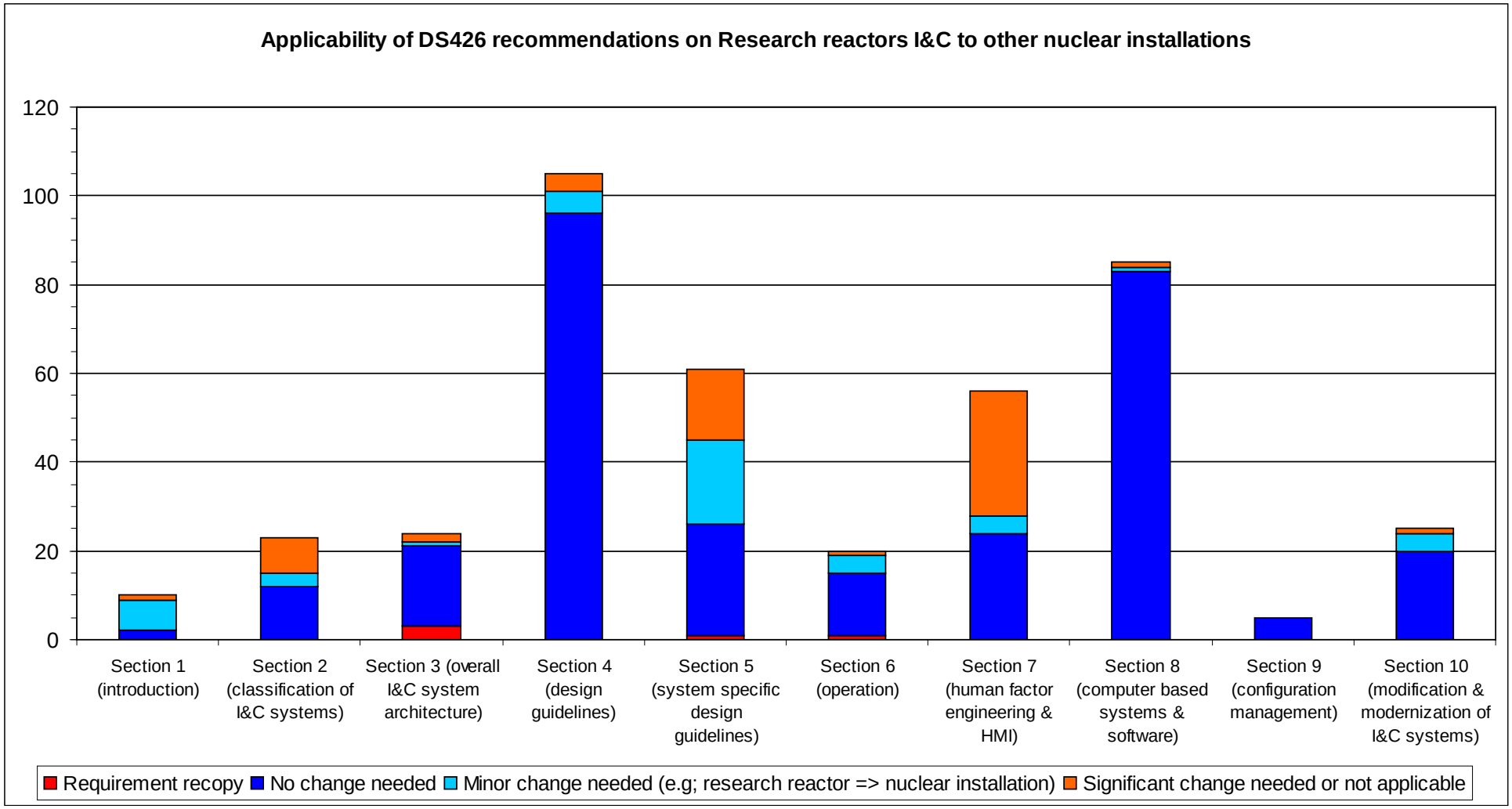
COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
72.	6.18	Delete 6.18	Redundant with 4.76 and 4.85			rejected	The paragraph was modified and completed by other MS comment demanding the paragraph should remain in its modified version.
73.	6.20	Combine 6.20 and 6.19	Same topic.	accepted	New 6.19		
74.	7.13	The instrumentation and control system design should ~~ensure~~ take due account of the time needed by operators to perform their expected tasks.	Typo	accepted	New 7.16		
75.	7.27	Delete 7.27	Redundant with modified 5.35 and 5.43			rejected	The functional isolation and physical separation are not addressed neither in 5.35 nor in 5.43.
76.	7.28	In control room design human factors engineering <u>aspects such</u> as workload, possibility of human error, operator response time and minimization of the operator's physical and mental efforts should be taken into account, in order to facilitate the execution of the operating procedures specified to ensure safety in all operational states and accident conditions.	Clarification	accepted	New 7.24		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
77.	8.1	Computer based systems are of increasing importance to safety in research reactors as their use in both new and older facilities is ~~rapidly~~ increasing.	Superfluous	accepted			
78.	8.2	Computer based systems reliability could be ~~predicted and demonstrated~~ evaluated with a systematic, fully documented and reviewed engineering process.	Less ambitious wording		Accepted The paragraph will be rephrased as: *Computer based systems reliability should be evaluated with a systematic,…*		To convert the paragraph in a recommendation.
79.	8.8	~~The computer system should meet the criteria for the highest safety class of the functions it is implementing.~~	Redundant with 8.9	accepted	New 8.9		
80.	8.16	Delete 8.16	Redundant with 8.8	accepted			
81.	8.24	Data flow from lower to higher classified safety systems should be prevented unless decoupling device is inserted.	Direct data flow should be prevented as far as practicable	accepted			
82.	8.29	~~Also, a verification and validation plan should provide procedures for evaluating risks in each development activity.~~	Superfluous considering 8.34 to 8.37	accepted	Para 8.29 deleted		
83.	8.31	All phases of the development process should be identified. Each phase consists of specification, design, ~~and~~ implementation and verification.	Clarification, to be consistent with end of 8.31	accepted	New 8.30 second sentence deleted		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
84.	8.43	Safety analyses, for example accident analyses, transient analyses or facility safety analyses (based on postulated initiating events and safety criteria), should be an essential part ~~of this design~~. <u>for defining functional safety requirements.</u> In addition to safety requirements, some additional requirements not directly associated with safety are added at this stage of the design, such as: requirements for availability.	Clarification	accepted	New 8.42		
85.	8.44	Locate 8.44 after 8.46	8.44 deals with all requirements, whether functional or not	accepted	New 8.45		
86.	8.45	Delete 8.45	Superfluous as previous paragraph do not mention specifically safety systems.	Accepted	New 8.43 The paragraph will be rephrased as: *A safety analysis should also be made for safety and safety related systems to determine functional safety requirements.*		

COMMENTS BY REVIEWER Reviewer: FF Page Country/Organization: France /ASN Date: 03/05/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
87.	9.4 9.5	Merge 9.4 and 9.5 and locate them with 10.6	Same topic.	accepted	new 10.8		
88.	10.14	When modifying any instrumentation and control system, ~~consideration on~~ development of design guidelines should be considered.	Clarification	accepted	10.16		
89.	10.16	Locate 10.16 before 10.14	10.13 and 10.16 are dealing with safety systems. 10.14 and following or not specific to safety systems	accepted	10.14 1nd 10.16 are merged forming a new 10.16		
90.	10.22	Locate 10.22 after 10.25	Running system in parallel can only occur after functional tests is successfully performed.	accepted	New 10.26		
91.	/						
/	/						


Applicability of DS436 recommendations on Research reactors I&C to other nuclear installations
5
62
48
299
Requirement recopy
No change needed
Minor change needed (e.g; research reactor => nuclear installation)
Significant change needed or not applicable


Applicability of DS426 recommendations on Research reactors I&C to other nuclear installations
120
100
80
60
40
20
0
Section 1 (introduction)
Section 2 (classification of I&C systems)
Section 3 (overall I&C system architecture)
Section 4 (design guidelines)
Section 5 (system specific design guidelines)
Section 6 (operation)
Section 7 (human factor engineering & HMI)
Section 8 (computer based systems & software)
Section 9 (configuration management)
Section 10 (modification & modernization of I&C systems)
Requirement recopy
No change needed
Minor change needed (e.g; research reactor => nuclear installation)
Significant change needed or not applicable

INDIA

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	General	The guide should align with IAEA NS-G-1.3. If there are specific departures, this should be brought out.	Uniformity against other guides of NPP I&C will be maintained.				
2.	2.1	The mapping from IAEA safety classification to IEC may be included in the document.	Safety classification as per IEC is IA, IB, 1C and NINC (not important to safety). To align with IEC61226 which is followed in many countries, including India.			Rejected	Reference to International standards other than the IAEA standards is out of the scope of the current safety guide.
3.	2.14	This section may include an explicit mention of Communication including Emergency Public Annunciation (EPA) & General Public Annunciation (GPA) Systems.	The Radiation Emergency declaration is done by authorized personnel using only EPA. The evacuation/stay-in signals are annunciated using EPA. Its class/requirements may be considered appropriately.	accepted	Paragraph deleted following comments from other MSs		
4.	2.14/2.15/2.1	Following systems may be included	These being important	accepted	Paragraph deleted		

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	6	1. Fail Fuel Detection & Identification System 2. Meteorological and Environment Monitoring Instruments 3. Seismic Monitoring System 4. Effluent Treatment/ Discharge Plant instrumentation	monitors, they may be explicitly considered.		following comments from other MSs		
5.	2.23	Validity of the statement "Instrumentation and control system or equipment safety class should have the same safety class as the system or equipment they control/monitor. If an instrumentation and control system or equipment controls or monitors several systems or equipment, its safety class should be the one of the highest safety class of these systems or equipment" should be checked.	As per IEC 61226, Functions that provide continuous or intermittent tests or monitoring of functions in category A to test and indicate their continued availability for operation are classified as IB. Hence the statement in 2.23 is conflicting with accepted practices.		New 2.7	rejected	Reference to International standards other than the IAEA standards is out of the scope of the current safety guide.
6.	3.17	Replace "..on level of defence 3.." with "..on levels of defence 2 and 3.."	Safety systems span defence in depth levels 2 and 3.	accepted	Paragraph deleted following comments from other MSs		
7.	4.3	Point d: "for each manual protective action the points in time" Not clear. Can be reworded for better clarity.	Not clear and may be clarified in the document.	Accepted	New 4.4 (e)It will rephrased as: *for each manual protective action, the*		

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					plant conditions during which manual control is allowed;		
8.	4.3	Availability requirements may be added in design basis.	Suggestion	accepted	New 4.4 (l)		
9.	4.3	Performance requirements specifying the guaranteed response time for safety functions shall also be included in the DESIGN BASIS	All safety functions demands for timely actions and hence it becomes very important to specify, the time, within which the safety function shall be initiated.	accepted	New 4.4 (d)		
10.	4.10	The statement may be added at the end of this para, "A single failure in the system should be considered along with a) failures as a consequence of postulated initiating event; and b) any credible and undetected fault in the system"	If there are undetected faults in the system, even with a single failure plant safety is not assured.	accepted	New 4.11		
11.	4.12	This para may be deleted	Identical to 4.10	accepted			
12.	4.13	Not clear. Rationale may be added.	Not clear.	accepted	The paragraph will be deleted		
13.	4.31	Calculators word can be changed to "Processors".	Editorial	Accepted	new 4.28The paragraph will be rephrased as: ... signal conditioning devices, signal		

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					processors/calculators to the actuators drivers.		
14.	4.100	In g, fail safeness can also be added in design analysis	Suggestion	accepted	Added in bullet a) "and to check if the system is fail safe)		
15.	5.0	System Specific Design Guidelines.	Sections on "Nuclear Instrumentation" including "Start-up Instrumentation" "Radiation Monitoring System (RMS)" and "Reactor Control & Monitoring System (RCMS)"may be added.			rejected	The comment modify the structure of the document already approved
16.	5.34	Similar to 5.43, "ergonomie factors and suitable provisions for preventing unauthorized access and use" is to be included for main control panel also.	Uniformity between MCR and SCR may be maintained.	accepted	New 5.27, 5.28 take care		
17.	5.95-5.61	Power Supplies for I&C systems.	Guiding requirement during Station Black Out Condition etc. should be included.	accepted	New 5.54		
18.	6.14	Design Guidelines regarding different types of Maintenance, Surveillance including In-Service-Inspection (ISI).	Guidance for basis for surveillance frequency for various systems should be included.	accepted			
19.	8.0	A section containing the following may be added	Safety system settings are very important for correct	Accepted Added in			

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		"Wherever safety system settings are user configurable, changes to these settings shall be allowed only by authorized user and these system settings shall be checked for its integrity."	implementation of safety functions, hence unintentional or unauthorized changes to these need to be guarded.	parahraph 8.47			
20.	8.9, 8.16	Statements given in 8.9, 8.16 are same. May be deleted.	Duplication	accepted	8.16 deleted		
21.	8.31	Following statement is not clear *Each phase consists of specification, design and implementation* Following statement may be modified to make more clear *The design activity of one phase sets the requirements for the next phase* It may be modified as *The activity of one phase sets the inputs for the next phase.*	Suggestive. Specification, design and implementation belong to different phases of SDLC. May be rephrased.	accepted	New 8.30		
22.	8.39	Refer the following statement *The change control procedure should maintain records of the problems that were identified during the development process…* Above may be corrected as *The change control procedure should maintain records of the problems that were identified during the development*	Configuration Management Plan is applicable during development as well as during O&M phase.	accepted			

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		process or during operation of the plant…					
23.	8.46	Performance Requirements, specifying the response time requirements should be put as part of Non-functional requirements.	Response time requirements are very important for safety functions and it comes under the category of non-functional Requirements	accepted	New 8.44		
24.	8.51	In addition to internal interfaces between modules of the software, design shall explicitly specify the external interfaces of the software, such as system calls, hardware interfaces, library, etc. Design shall ensure that each instance of external interface usage is within the constraints imposed by these, if any	The context of external interfaces needs to be clearly specified.	accepted	New 8.50		
25.	8.53	Specification requirements regarding concurrency in software design with any synchronization issues may be included.	It is important to analyse the concurrency behaviour of the software in terms of various task priorities, periodicities. If not analysed properly, it may lead to unpredictable results in terms of response time requirements.	accepted added in paragraph 8.52	New 8.51		
26.	8.72	In the text "In constructing test cases, special consideration should be given to	Requirements for security functionality may be	accepted	New 8.70		

COMMENTS BY REVIEWER Reviewer: **BARC, India** Country/Organization: **India** Date:16/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		the following..."	included.				
27.	1.4 Annex-I	Engineered Safety Features (ESF)	Guiding requirements related to ESF testability, reliability, maintenance & surveillance may be included. IAEA NS-G-1.3 may be referred.			rejected	It is out of the scope of the annex which only identifies typical set of I&C systems and their interrelations. Refer to paragraphs 1.1 and 1.2 of the annex.

Instrumentation and Control and Software Important to Safety for Research Reactors (DS 436)

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Country/Organization: Indonesia/BATAN			Page 1 of.... Date: 26/04/2013	RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	1.2/2	… systems has increased due to loss of device supply in the market generated by technological advancements in the field of …	Increasing of the rate of ageing and obsolescence of research reactor instrumentation and control systems is mainly caused by loss of device supply in the market	accepted	Sentence deleted following comments from other MSs		
2	1.3/3	… and control components, from the sensors ~~allocated to the mechanical systems~~ to the …	the considered sensors are not limited only to the ones which are allocated to the mechanical systems	accepted			
3	2.10/6	… experimental devices and facilities; and …	facilities such as radiation facilities should be considered	accepted	Paragraph deleted following comments from other MSs		
4	2.10/14	safety parameter command and display consoles and panels; ~~and~~	editorial	accepted	Paragraph deleted following comments from other MSs		

5	2.14 Add one other example	• seismic monitoring system	The cause of vibration event should be declared to assure the sensors placement in such a way to catch the vibration signal information as soon as possible	accepted	Paragraph deleted following comments from other MSs		
6	Substantif		Seismic monitoring system has not been covered in this document			rejected	Not all the I&C systems of the reactor are covered in detail. The recommended inclusion as a system in 2.14 (comment no. 5) should be enough. Usually seismic switches are included in the reactor protection system to trip the reactor in case of seismic.
7	2.20	..... and control system, a decision should be made.....	editorial	accepted	Paragraph deleted following comments from other MSs		

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Page 2 of.... Country/Organization: Indonesia/BATAN Date: 26/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
8	3.20/4	… should be allocated at the supervision level; the calculation, ~~algorism~~ algorithm, safety and …	The term of algorism has obsolete and should be replaced by algorithm	accepted	New 3.17		
9	3.22/2	… isolation, in the overall architectural design of the ~~instrumentation and control~~	editorial	accepted	New 3.18		
10	4.2 bis	Design as a whole should consider the safety culture	Safety culture should be included in the whole life cycle of instrumentation and control starting from the design step	Accepted	New 4.3 It will be rephrased as: *Safety culture should be included in the whole life cycle of instrumentation and control system.*		
11	Subtitle 4.3	DESIGN BASIS	editorial	accepted			

12	4.3/17	i)Requirements for periodic testing, self-diagnostic including self-check, prognosis, and maintenance;	requirements for device capability to self-check and prognosis should be considered	accepted	New 4.4 (j)		
13	4.3/27 additiona l line	o) Requirement for instrumentation system to serve the whole life cycle of plant including post-accident condition should be assured	Fukushima accident showed that all critical parameters should be monitored from emergency control room. That's why instrumentation system should serve in a whole life cycle of plant including post-accident condition	accepted	New 4.4 (q) it will be rephrased as: *to serve the whole life cycle of facility including accident and post-accident conditions*		

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Page 3 of.... Country/Organization: Indonesia/BATAN Date: 26/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
14	4.35/2	… be known and properly documented using failure mode and cause-effect analysis …	the term cause-effect analysis is more meaningful comparing with term effect analysis only	accepted	New 4.31		
15	4.35 bis	The failure mode of instrumentation and control systems important to safety should include equipment aspects and human aspect, and the "cooperation" of both.	Instrumentation and control systems important to safety should include equipment aspects and human aspect especially in the human-centered instrumentation and control design.	accepted	New 4.32		
16	4.40 bis	To support the ageing program, hence, the instrumentation material sample should be prepared from the beginning of operation as original comparative material to estimate the remaining life of the instrumentation	the original instrumentation material sample should be prepared for remaining life estimation of the instrumentation	Accepted	Paragraph deleted following comments from other MSsIt will rephrased as: *To support ageing management programs or, sensitive instrumentati*		

					on material samples should be prepared from the beginning of operation as original comparative material to estimate the remaining life of such sensitive materials of the instrumentation and control system		
17	4.42/4	… protected equipment, software and data.	Security system should protect not only equipment, but also software and data	accepted	New 4.39		

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Page 4 of.... Country/Organization: Indonesia/BATAN Date: 26/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
18	4.72/additional line	h) be documented in a quality assurance procedure	the procedure for instrumentation testing should also be documented in the quality assurance document	Accepted	New 4.70 (g) It will rephrased as: *document the results of the testing following quality assurance procedures.*		
19	4.76/3	… function nor introduce the potential for common cause failure. Testing of the safety critical system during operation should consider safety aspect.	Instrumentation and control component and system testing during operation especially for a critical ones should be conducted as well allowing the documented procedure to assure the reactor safety	accepted	New 4.74		

20	4.95/2.	… simulated operating conditions, including sequence of operation. Precaution should be taken in testing sensitive and critical safety system.	A well established provision should be considered when testing of sensitive and critical safety system will be conducted.	accepted	New 4.94		

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Page 5 of.... Country/Organization: Indonesia/BATAN Date: 26/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
21	4.98/6	Leaving sufficient room around the equipment to ensure that the maintenance staff with his supporting tools can …	the sufficient room should be prepared not only for maintenance staff but also for supporting tools which needed to completing the tasks	accepted	New 4.99		
22	5.12/4	… independent and diverse from each other. The second protection system should be more reliable than the primary one.	The primary protection system is designed to accommodate the advancement of technology without compromising the safety. But the second protection system main task is to assure the protection system perform well.			rejected	The requirement for a second protection system depends of the study of the CDF (Core Damage Frequency) for a specific research reactor and not by the technology used in the first reactor protection system. The reliability for the second reactor protection system contributes to the whole reliability protection system considering that they, the first and

							the second are completely independent.
23	5.22	~~Where the necessary 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~~, Even though the computer-based reactor protection system has many advantages, some uncertainties still remain. To enhance the reliability of the reactor protection system as a whole, then, diverse means of ensuring fulfillment of the protection functions should be provided.	a reactor protection system should be demonstrated with a high level of confidence. A reactor protection system which cannot be demonstrated with a high level of confidence is not allowed to be installed in the reactor	accepted	Paragraph deleted following comments from other MSs		

COMMENTS BY REVIEWER Reviewer: Djoko Hari NUGROHO Page 6 of.... Country/Organization: Indonesia/BATAN Date: 26/04/2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
24	5.32/4	… the working environment, and to protect against hazardous conditions. The design of control room includes task analysis, ergonomic, and human factor.	task analysis, ergonomic and human factor should be considered when designing a control room.	accepted	New 5.27		
25	5.43/2	… factors and include suitable provisions for preventing unauthorized access and use. The supplementary control rooms should also be constructed resist from fire and earthquake	The supplementary control rooms is utilized when accident occur, then it should be constructed resist from fire, earthquake	accepted	Not implemented following comments from other MSs		
26	7.9/2	… factors engineering problems and issues experienced in previous designs. The human-machine interface design emphasizes on the incorporation of human and machine and the advantages of applying both.	Human and machine has their own advantages and disadvantages. The human-machine interface design emphasizes on the incorporation and the advantages of applying both .	accepted	Added to para 7.5		

Form for comments
Instrumentation and Control and Software Important to Safety for Research Reactors (DS436)

COMMENTS BY REVIEWER Reviewer: RAMIREZ QUIJADA r. Country/Organization: PERU/INST PERUANO DE ENERGIA NUCLEAR Date: 2013.04.26				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	5.12 / 2	Where two reactor protection systems are provided, these two systems should be independent and diverse from each other	There is a redundancy in the “independent” term of the phrase.	accepted			
2	8.13 / 3	Safety System should not have possibility for easy connection to the other and also it should not be connected to external networks	It would be better avoid the possibility of being connected to other computer by not having easiness for doing it.			rejected	The reason of this recommendation is to avoid the connection of safety system with external networks. The Safety systems have the capability to connect with other instrumentation and control systems of the reactor if suitable isolation devices are used.
3	8.14 / 1	The connection for pen drives should be blocked to avoid being used	It would be better to block the connectors as procedures for controlling could be by passed	accepted	New 8.15It will be rephrased as: *The connections for pen drives should be locked to prevent their use.*		

COMMENTS BY REVIEWER Reviewer: RAMIREZ QUIJADA r. Country/Organization: PERU/INST PERUANO DE ENERGIA NUCLEAR Date: 2013.04.26				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
4	10.5 / 3	… reactor is not restarted without formal approval after the completion of modifications	It seems that the term “competition” is wrong	accepted			
5	Annex I	Remote Reactor Surveillance System (RRMS): This surveillance system is intended for reliable following-up of the reactor shutdown state during unattended periods and giving an alarm if any parameter drifts apart from normal values	Some reactors remain unattended for some long periods but the reactor needs to be under continuous surveillance to assure that it remains in a safe shutdown condition. The remote surveillance through by an Alarm Central Station is advisable			rejected	At least a subset of the instrumentation and control system important to safety should be operative during the mentioned unattended period of time of the reactor. Moreover, the reactor should be supported by a minimum operational and maintenance staff during those periods. Unless a full safety analysis has been completed and implemented for the different research reactor states (e.g. Normal Operations, Shutdown etc.) the minimum

COMMENTS BY REVIEWER Reviewer: RAMIREZ QUIJADA r. Country/Organization: PERU/INST PERUANO DE ENERGIA NUCLEAR Date: 2013.04.26				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
							requirements (protective systems availability, personnel/surveillance, maintenance routines, repair times etc.) remain unchanged for all RR states. Reduction in these or the use of Remote Surveillance systems must be justified by an approved and implemented safety assessment.

TITLE: DS 436 Instrumentation and Control and Software Important to Safety for Research Reactors

COMMENTS BY REVIEWER Reviewer: Country/Organization: SPAIN/UNESA Date: May 17, 2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	2.14	Instrumentation and control for heating, ventilation and air conditioning […]	The acronym HVAC stands for heating, ventilation and air conditioning. Humidity is included in the term air conditioning.	accepted	Paragraph deleted following comments from other MSs		
2	4.48	End User organizations and designers should consider principles of security and cyber security in all phases of the project, namely, requirements specifications, conceptual, preliminary and detail design, procurement, fabrication, integration, installation, commissioning, operation and maintenance of the instrumentation and control systems.	Cyber security controls are carried out by including cyber security enhancing activities in all lifecycle activities, which also include procurement. Cyber security requirements should also be set on vendors and contractors.	accepted	New 4.46		
3	4.104 (Figure 4.1)	Paragraph 4.104 to be fully reviewed according to S67.04-1982 Section 4 or equivalent. Figure 4.1 to be substituted by ISA S67.04-1982 Figure 1 or equivalent.	ISA S67.04-1982 is a widely used standard. Section 4 and figure 1 also address the setpoint, which is of high importance when protection systems are to			rejected	Paragraph 4.104 and Figure 4.1 generically describe the relationship between the parameters associated with the determination of the

COMMENTS BY REVIEWER Reviewer: Country/Organization: SPAIN/UNESA Date: May 17, 2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			be properly initiated.				safety system setting in an I&C system. The recommendation to apply a specific international standard and its nomenclature for that purpose is beyond the scope of the current safety guide.
4	8.13	It should be demonstrated that measures have been taken to protect a computer based system throughout its entire lifetime against physical attack, unauthorized access, fraud, viruses and so on. Access from external networks to safety systems should be prevented by means of physical separation or the use of unidirectional devices such as data-diodes.	Data from safety systems can be useful to assess the performance of certain systems. A data-diode has been proved to be an effective device to avoid access to those systems while maintaining data flow from safety systems to an external network. Thus, the functionality of the safety system can not be affected.			rejected	Historical records or SOE (Sequence of Events) of safety systems allow assessing their performance without the requirement of an on-line connection to an external network which should be prevented even though that are devices that avoid access to those sensitive systems.

COMMENTS BY REVIEWER Reviewer: Country/Organization: SPAIN/UNESA Date: May 17, 2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
5	10.22	When an instrumentation and control system is replaced, the new instrumentation and control system may, when appropriate, be run in parallel with the old system for a probationary period, i.e. until sufficient confidence has been gained in the adequacy of the new system. Procedures should be established to guide the operator to respond adequately in case both I&C systems behave differently.	Typically, the old system will be the primary system, while the new I&C system will be monitored to assure its performance is satisfactory. The operator has to be conscious about this configuration.	accepted	New 10.26The paragraph will be rephrased as: *When an instrumentation and control system is replaced, the new instrumentation and control system may, when appropriate, be run in parallel with the old system for a probationary period, i.e. until sufficient confidence has been gained in the adequacy of the new system. In this configuration, only the old instrumentation system should be able to control the reactor meanwhile, the response of the drivers of the new instrumentation and control system should be registered in an independent acquisition system to*		Clarification: During the probationary period, even with both systems connected in parallel, only the old system should be able to control the reactor. The drivers of the new I&C system should not be connected to the process systems of the reactor. The response of the drivers of the new I&C system should be registered in an independent data acquisition system to have the possibility to assess and compare their response against the response of the old system.

COMMENTS BY REVIEWER Reviewer: Country/Organization: SPAIN/UNESA Date: May 17, 2013				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					have the possibility to assess and compare their response against the response of the old system.		
6	Annex I, 1.2	HVAC: Heating, Ventilation and Air Conditioning for Controlled and Supervised areas;	The acronym HVAC stands for heating, ventilation and air conditioning. Humidity is included in the term air conditioning.	accepted			
7	Annex I, 1.10	Heating, Ventilation and Air Conditioning (HVAC)	The acronym HVAC stands for heating, ventilation and air conditioning. Humidity is included in the term air conditioning.	accepted			

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

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	1.1	Use of acronym for Instrumentation and Control (I&C)	Suggest acronyms be defined at the beginning of the document and used throughout. This includes RPS, SSC, etc. Note that minimal use of acronyms is present in this document, and thus the intent appears to be not to use such acronyms.			Rejected	The use of acronyms are omitted in the safety guide with some minor exceptions as IAEA.
2	1.7	….and control systems of existing facilities.	Clarification	accepted	Paragraph deleted following comments from other MSs		
3	2.3	Safety related systems are systems important to safety performing other safety functions not mentioned in paragraph~~s~~ 2.2, such as monitoring the availability of safety systems or	This paragraph is unclear at the end. The proposed text is a suggested clarification	accepted	Paragraph deleted following comments from other MSs		

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~diminishing~~ eliminating the need~~s~~ of a safety system to actuate ~~performing other smooth~~ by taking compensatory actions ~~in advance~~.					
4	2.8 last bullet	Mitigate the consequences of beyond design basis accidents; also can be considered the new terminology introduced by IAEA for this conditions as design extension conditions[1]. See Ref. [14]. To Mitigate the consequences of beyond design basis accidents; alternately referred to in new IAEA terminology as design extension conditions[1]. See Ref. [14].	Clarification	accepted	Paragraph deleted following comments from other MSs		
5	3.3	Modern instrumentation and control systems are more highly integrated than were the ~~last~~ past generations of instrumentation and control systems.	Last implies only the most recent generation. More correct to refer collectively to past generations.	accepted			

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
6	4.14	….meet reliability and ~~unavailability~~ availability requirements of the design….	Correction	accepted	New 4.12		
7	4.40	Significant ageing effects…. To Potentially significant ageing effects….	Statement initially assumes the ageing effects will occur. That is not correct. However, if they occur, they are potentially significant and should be addressed.	accepted	New 4.37		
8	After 4.46	Add Safety functions should not be adversely affected by elements of design intended to enhance security.	To Add/Clarification	accepted	New 4.44		
9	4.64	….natural sources such as lightning strikes and geomagnetically induced currents, and other man-made….	To Add	accepted	moved to 4.62		
10	4.68	Wireless systems and devices analysed should include….	Clarification	accepted	New 4.66		
11	4.99 Last bullet	Provision of facilities for remote replacement, repair and ~~to put back in operation again~~ return to service.	Clarification	accepted			
12	5.46	….exclusively to the experimental	Clarification	accepted	New 5.38		

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		facilities to keep….					
13	5.60	…. uninterruptible ~~alternate current~~ power supplies…	There is no need to specify such detail with the uninterruptible power supplies. Potentially remove footnote 2 that is in 5.60 as well.	accepted	New 5.54		
14	7.13	The instrumentation and control system design should ~~ensure~~ take due account of the time needed by operators to perform their expected tasks.	Clarification	accepted	New 7.16		
15	8.2	….reliability ~~could~~ should be predicted…	Clarification	accepted			
16	8.4	Depending on the complexity of experimental devices in the research reactor, it should be considered to functionally split the Computer based system in reactor system and experimental devices system. In that way, both systems could be treated with its own set of requirements and objectives.	Clarification	accepted			

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		To Depending on the complexity of experimental devices in the research reactor, consideration should be made to have separate reactor and experimental computer based systems. In that way, each system could be treated with its own set of requirements and objectives.					
17	8.46 Last bullet	That the requirements not directly associated with safety (such as availability or security) will not adversely affect the ability of a safety function to be performed when required.	Clarification	accepted	New 8.44		
18	10.5	…after the ~~competition~~ completion of modifications….	Correction	accepted	New 10.7		
19	10.21	For instance, enhancements to the operator interface features might increase errors by operations and	Clarification	accepted			

COMMENTS BY REVIEWER Reviewer: R. Hardin (RES) Country/Organization: USA Nuclear Regulatory Commission Date: 15 May 2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		maintenance ~~personal~~ personnel for some time after the change. As required, sufficient and proper training programs should be developed and implemented to minimize or eliminate the potential for such errors, if changes are implemented.					