Canada Comments on
DS431: Design of Instrumentation and Control Systems for Nuclear Power Plants (Draft K)

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Canadian Nuclear Safety Commission Country/Organization: CANADA			Date: 2013/05/31				
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
1	General	Possibly at clause 1.9 (wording is suggested only…please edit as required to meet IAEA writing style) "The guidance provided in this document may also be applied to the design of instrumentation and control systems for SMRs in a manner that is commensurate with the risks presented by the facility"	This document is very well written, comprehensive and the requirements (shalls) and guidance (shoulds) are written in a technology neutral fashion. The scope of this document, however, requires a clarification to be added to confirm whether the document is applicable to near-term deployable SMRs. This is particularly true for integrated light water reactor (ILWR) designs that are at a reasonably advanced state of design such as, but not limited to the: ▪ Korean SMART ▪ Generation mPower ▪ NuScale With that said, the document was reviewed from the point of view of how it might be applied to a very small SMR (e.g. 10 MWe). The conclusion is that the contents of DS431 are actually written at a level where the requirements and guidance can be applied as-is to SMR I&C design as long as consideration is given to risks presented by the facility. (i.e. recognize that the requirements and guidance can be met by alternative means) CNSC is aware that the IAEA is at the initial DPP development stages for a possible document to cover "Instrumentation and Control for Advanced Small Modular Reactors". Based on the CNSC's review of DS431, CNSC suggests that this new DPP be developed to <u>supplement</u> DS431 rather than lead to the development of parallel requirements and guidance. That is, the new proposed document should seek to identify address those SMR issues that differ significantly from what is found in DS431 such as shared I&C architectures between multiple units, increased use of automation and remote monitoring and control				

			and unique environmental conditions that require novel I&C solutions.				

DS431 Design of Instrumentation and Control Systems for Nuclear Power Plants, draft K 25th April 2013

COMMENTS BY REVIEWER Reviewer: M-L Järvinen/Heimo T takala Page1 of 2 Country/Organization: Finland Date: 31.5.2013							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	General	The proposed new draft version K of DS431 incorporates a large number of changes based on comments made on the previous version of the draft guide. Finland supports the new version of the draft and proposes the following technical comments to be considered by the Agency for the preparation of the next version of the document.	Finland thanks the IAEA Technical Officers and the expert team responsible this draft and appreciate the quality of the draft and how the many improvements are carried out.				
	General	The draft guide should be reviewed against the IAEA safety classification document DS367 rev. 8 April 2013 and revised where necessary	The new IAEA safety classification draft safety guide DS367 rev. 8 is accepted by CSS for submission to Publication Committee and is not expected to change. The new guide will propose somewhat different safety classification and categorization as the old IAEA safety classification guide. This new safety grading is more appropriate for nuclear I&C and the I&C document draft DS431 should support it.				

	Configuration management: 2.38 – 2.55	The hierarchical levels of configuration management should be presented more clearly in the text about configuration management. Eg. in para 2.40, 7 th bullet could be: “To define configuration baselines i.e. configuration of mutually compatibel and consistent items in every hierarchical level of configuration under configuration management”	The hierarchical levels of the configuration items are inevitable in plannig of the configuration management.				
	Para 6.72, spurious action/operation	At the end of para: “..., cause spurious action by error in (SW) design or parametrization.”	The chapter 4 address design of architecture against CCF taking account design errors too (para 4.27). But in paras 6.66 – 6.78 failure mode “spurious action” caused by e.g. design or such a common reasons was not yet addressed.				

May 2013 Comments on IAEA Draft Safety Guide "Design of Instrumentation and Control Systems for Nuclear Power Plants" (DS431)

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
1	2.18	Human Factors Engineering and **establishment of computer security** are examples of such activities.	"Computer Security" is not an activity. Instead, it is an established characteristic of a system. The activity is efforts to establish this characteristic.				
2	2.19	Replace "computer security" with "Cyber Security.", or change Figure 1 term to "Computer Security."	Terminology is not consistent with the terms used in Figure 1. Figure 1 uses "cyber security."				
3	2.25	Add Bullets for : • System Training, and • System Operation	Plans should also be developed for providing system training to operators and maintenance personnel. Planning should include operations plan.				
4	2.25	Consider adding a new bullet for "Cyber Security Plan.	Later in clauses 2.34, 2.35, and 2.36 the guide refers to a computer or cyber security plan but it is not included in 2.25 as an I&C planning topic.				
5	2.61	Add the following clause to the end of the sentence:	The guide should include the objective of addressing the potential for introducing new hazards into the system during				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		"… to ensure that hazards introduced to the system during the development process are adequately addressed."	development.				
6	2.85	Change last sentence to: "Claims for better reliabilities than this are not precluded, however, special justification should be provided, taking into account all of the factors mentioned."	Except for the last sentence, the clause can be viewed as informative guidance. Inclusion of the last sentence (as written) makes this a mandatory clause				
7	2.125a	Rewrite to say: "Challenge all integration interfaces, including hardware to software, software module to module, **and overall I&C system with plant systems**;	The current integration aspects omit the concept of integrating the I&C system into the plant systems.				
8	2.130	Replace the first sentence with: "For the purpose of this guide, the **majority of system validation is**	The second sentence contradicts the previous sentence.				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		complete when the system has been installed into the plant."					
9	3.14.d (Design Basis)	**The equipment protective provisions that could prevent the safety systems from accomplishing their safety functions**	Limitations of equipment preventing safety functions to be performed are a realistic constraint. "Limitations on materials to be used" is identified, 3.15.d.5, but this should not be the same.				
10	4.22	Change last phrase to: "…of paragraphs 6.26 to 6.58"	Additional clauses have been added since this reference was created. I believe the reference is intended to be to the whole independence section which is 6.26 through 6.58.				
11	4.40	Probabilistic studies should not treat I&C items important to safety as fully independent unless they are diverse, and meet the guidance for functional independence <u>given in this document, including</u> electrical isolation,	The final clause could be read as "internal events given in this document," implying a list of events that is not found in the document. Relocating the clause makes it clear that the guidance is "given in this document."				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		communications independence, environmental qualification, seismic qualification, electromagnetic qualification, physical separation, and protection against internal events ~~given in this document~~.					
12	4.41	Delete the word “simply” from the last sentence. Also reword as follows: “In probabilistic studies, failure probabilities for systems that are fully independent are calculated by taking the product of their individual failure probabilities.” Sentence could also be deleted to resolve this item.	The last sentence in this clause incorrectly implies that simply taking the product of individual failure probabilities is a sufficient means of establishing independence.				
13	5.10	Delete the term “safety related.” Replace with	Clause 5.12 states that this guide will avoid using the term				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		"Items important to safety but not safety systems."	"safety related."				
14	5.12	Re-title the left most list of systems in Figure 3 as "Not Part of Safety System" in order to avoid use of the term "safety-related."	This clause claims that this guide avoids the use of the term "safety related," however; the term is defined within this same clause and is used in Figure 3.				
15	6.5	Delete one of the Clause 6.5's.	Clause 6.5 on page 47 is duplicated.				
16	6.16 through 6.19 / 1 (Single Failure Criterion)	Delete these steps.	There should be no justification within the design for non-compliance with the single failure criterion. The remote likelihood for postulated failures being discounted is an argument the NRC has steadfastly denied. As an example, the CCF in the safety system will require a DAS (regardless of the likelihood of a CCF). Another example is whether LBLOCA should be distinct from SBLOCAs. In this case, ITS systems are less qualified and less developed, making failures more likely than in a safety system. Requirements				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
			and guidance basis: 10 CFR 50 Appendix A Criterion 21 and IEEE Std 379 do not exclude SFC based on likelihood of failure.				
17	6.17	Delete first two bullets.	Allowing SFC exception due to rarity of PIE or when consequences are improbable opens the door to using PRA analysis as a tool for skirting the SFC criteria. SFC criteria should be applied to all safety systems and functions regardless of the likelihood of needing that safety function.				
18	6.49	Add statement: “Member countries may have additional requirements and restrictions on connections of non-safety maintenance systems to safety systems.”	Different member countries have different requirements on connection of lower safety class maintenance systems to safety equipment. This should be pointed out in this guide. For example, the US only allows temporary connections of non-safety maintenance systems to safety systems that is enforced through physical disconnects.				
19	6.165	Change to: “When possible, system	This clause conflicts with clause 6.167 in that Clause 6.165 does not include provision for systems				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		designs should include provisions for testing and calibration of safety system equipment in all modes of normal operations, including power operation, while retaining the capability of the safety systems to accomplish their safety functions.	or components that cannot be feasibly tested during power operation as is accounted for in Clause 6.167.				
20	6.167.b	Delete the word "untested" from this clause.	There can be no interval between tests when the components are "untested."				
21	6.209, 2nd bullet	Revise as follows: "Analytical limit (of setpoint) – . . . The margin between the analytical limit and the safety limit takes into account: the response time of the instrument channel, **analytical inaccuracies, modeling inaccuracies, plant dynamic response, and** the range of transients due to the accident	Analytical Limit definition should include analytical and modeling inaccuracies.				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		considered.					
22	6.213	Revise as follows: "Limiting settings for safety systems should be calculated using a documented methodology that provides sufficient allowance between the trip setpoint and the analytical limit to account for measurement and channel biases, uncertainties, **including those associated with random and bias terms,** and any changes to these values which occur over time."	Uncertainties should include those uncertainties that are associated with random and bias terms.				
23	7.52	"should satisfy all ~~reliability, redundancy, and independence~~ **safety** requirements in the presence of a failure of any component …"	No justification to limit or identify just these few requirements; all safety requirements should be maintained by the safety system in the presence of any non-safety system failure.				
24	7.62	Replace "… the associated interruption in supply" with "… any	Transfers of power supply do not always have an associated interruption in supply.				

COMMENTS BY REVIEWER Reviewer: Country/Organization: US Nuclear Regulatory Commission Date: 6/05/2013				RESOLUTION			
Comment No. / Reviewer	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/ rejection
		associated interruption in supply".					
25	7.81	Replace the word "recommendations" with "guidance." Guidance was the term used in 7.101.	Reference to Independence section is inconsistent with the reference provided in 7.101.				
26	7.122	Recommend deleting clause 7.122.	Since operators could in fact pose an insider threat, I do not understand why the criteria of 7.119 through 7.121 should not also apply to their activities. I see no down side to monitoring and logging control room operator activities.				
27	8.23	Change reference to "… 8.22 items a, b, c, **and e** should be classified as safety …"	In the reference to 8.22, letter e should also be classified as safety because the protection / safety function depends on it.				

Design of instrumentation and control systems for NPP, DS431 draft K

COMMENTS BY REVIEWER Reviewer: Page.1. of..x Country/Organization: FRANCE/IRSN Date: 2013/05/09				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
FR 1	General	See other comments	France thanks the project leader for the many improvements made to solve the open items and the "some member states" issues. In particular the treatment of these issues in a unique place (annex 3) clarifies the whole document. In its current writing the annex III could sometimes lack some clarification about what is consensual and what is not. -some practices are presented as applied by "some MS"; this is correct; -but some practices, also only applied by these Member States, are presented in general statements, which by contrast with the first case could give the wrong impression that such practices are accepted by all MS. Thus some modifications (see comments about annex 3) are needed to distinguish what is consensual from what is recognized by some Member States and to reflect the practice of other Member States. We have limited the corresponding comments to the minimum in number and scope, in order to ease and accelerate the resolution process.				
FR2	General	See other comments	The two comments about annex 3 (FR12 and FR13) are considered to be important. The other comments are suggestions to further increase the technical quality of the guide.				
FR 3	2.138	Replace with: "The functional tests should be designed to cover all behaviours allowed by the functional requirements and their structural coverage, resulting from this	A system has several functional behaviours; each of them may correspond to many internal execution cases. The test campaign must provide assurance that : A1) all required behaviours are (correctly) implemented A2) no other behaviour is present A3) all execution cases corresponding to a given behaviour				

		functional design, should be justified."	involve the same structural part of the software (thus testing this behaviour gives information for all corresponding execution cases). Whatever the number of tests performed in practice, this number will always be infinitely small compared to the number of possible execution cases. Thus, if the tests are not correctly designed they can miss some behaviour: their number does not guarantee their adequacy. As a result, the only way to fulfil A1, A2 and A3 is a sound analysis, not the brute-force; so the testing strategy promoted in domains concerned by safety (nuclear, avionics, etc.) is: -design the tests to cover all behaviours allowed by the functional requirements. This must be done by an independent team, who makes its own analysis of the functional requirements (i.e. independent from the analysis of the requirements made by the development team). -only after the tests have been formalized, analyse how they cover the internal structure of the software. If the coverage is not correct, this may indicate that the software has behaviours not required (infringes A2) or implemented with extraneous complexity (infringes A3). -perform the tests and check whether the system responds as specified by the test scenario (guarantees A1)				
FR4	7.70 1rst sentence	Full verification and validation of such complex components could be very difficult or even practically impossible, **if they were not correctly designed**.	This general statement is a conditional: "could". Given its importance for safety it is mandatory to mention the corresponding condition. If not limited in scope, the statement would also be inconsistent with clauses 2.67 and 2.69 which require full verification and validation. In fact, the design requirements for safety systems (see e.g. IEC 60880) are elaborated primarily to allow full V&V. The safety guide must reflect this to be up to date.				
FR5	7.70 2nd sentence	Unidentified errors ~~are likely to~~ **might** exist and they might exist in all redundant components	"are likely to exist" is too strong for safety systems properly developed. This is confirmed by more than 30 years of positive experience feedback. Otherwise, the guide should definitely ban digital safety systems to fulfil the overall safety objectives (see e.g. 1.7).				

FR6	7.71 2nd and 3rd sentences	Add to both sentences: "**if they were not correctly designed"**	All safety systems must be designed to avoid the mentioned adverse effects. This is explicitly required by the safety standards; see e.g. IEC 60880 or IEC 62340. The safety guide must reflect this to be up to date.				
FR7	7.76	Response time and accuracy of digital systems ~~are heavily influenced by~~ **functionally depend on the** sample rate **and on the processing** ~~processor~~ cycle time. **In systems not correctly designed, these parameters could depend on the** ~~and~~ processor speed.	The sampling rate and the processing cycle time (not to be confused with "processor" cycle time) are part of the functional requirements. The safety systems must be designed so that these parameters do not depend on variations of the intrinsic processor speed. Otherwise the clause 7.74 of the guide (deterministic behaviour) could not be fulfilled, especially with "modern" processors (i.e. posterior to 1995…) of which the intrinsic speed is essentially unpredictable, including for successive iterations of the same loop. This design property is explicitly required by the safety standards; see e.g. IEC 60880 or IEC 62340. The safety guide must reflect this to be up to date.				
FR8	(*7.145 and 7.147*)	Provide the definition of "HPD" in the relevant location of the guide: HDL-Programmed Device: integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools. (IEC 62566)	The term "HPD" is correctly used in the guide, but not defined.				
FR9	7.145.a and f; 7.148	Replace "HDL Programmed Device" with "HPD"	For editorial consistency.				
FR10	7.148.a	Confirm that no ~~hidden circuits~~ **unspecified function** ~~exist~~ **has been programmed**	The wording "hidden circuits exist" is ambiguous in this context. It could be interpreted as referring to the basic micro-electronic circuits embedded in the silicon itself: the verification process cannot address this. It only addresses what is programmed in HDL. Probably the intent is to match the software verification process (which verifies the code, not the low-level circuits of the microprocessor).				
FR11	8.60.e	(should…) be ~~the simplest design~~ consistent with	A "should" requirement for the "simplest design" implies that the designer has to provide a justification based on a measure of				

		function…	simplicity, but no such metrics is widely recognized.				
FR12	Annex III-2, 2nd sentence	Thus to estimate digital system reliability it is necessary to estimate the probability of system failure due to ~~both~~ hardware failure and, **for some Member States,** software error. **For other Member States design errors (including software errors) and their consequences are not adequately treated by probabilities but only by qualitative analyses of the architecture and of the design.**	Needed to: -clarify what is consensual and what is not -reflect the view of other Member States				
FR13	Annex III-4	Add at the beginning: "**For the Member States who apply numerical reliability to software**, …"	Needed to clarify what is consensual and what is not.				

Design of instrumentation and control systems for NPP *(DS431)*

COMMENTS BY REVIEWERS Reviewer: IEC/SC45A Secretariat and experts Page.1. of..7 Country/Organization: IEC/SC45A Date:2013/05/27				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	General	IEC/SC45A supports draft K dated 25th of April 2013 submitted for comments for the 35th NUSSC meeting and proposes the following technical comments prepared by IEC/SC45A experts to be considered by the Agency for the preparation of the next version of the document.	**IEC/SC45A experts acknowledged the work done by the IAEA Technical Officers and the expert team which produced this draft and recognized the high quality of this document and the high level of consensus it reached.** IEC/SC45A noted that the vast majority of the numerous comments formulated on the previously circulated versions of DS431 were taken consensually into account according the NUSSC members recommendations in particular the ones formulated during the 34th NUSSC meeting. IEC/SC45A will use and reference this IAEA Safety Guide as a basic document to develop IEC/SC45A				

			standards, as soon as it will be published.				
2	1.15 pages 9-10	Reword the last sentence: “Examples of I&C systems to which this guide may apply include:”	Effluent monitoring systems and I&C for fuel handling are important to safety in some member states and not important to safety in some others member states.				
3	Fig. 1 (mentioned in 2.19 & 2.29)	In Fig. 1, Add a bracket “cybersecurity activities” next to “individual system life-cycle level”. Change CDA in “graded approach to security” or “security level/degree assignment”	Cybersecurity related parts (right side) of Fig. 1 are misleading: - They give the false impression that there is no cybersecurity activity at the individual system life-cycle level, which is wrong; - Overall terminology and concepts are inconsistent with IAEA NSS17. In particular, the identification of Critical Digital Asset is a US (NRC RG5.71) concept. IAEA NSS17 concepts should be privileged.				
4	2.82	Security testing usually involves vulnerability assessment and respect of security good practice.	The terms “know vulnerabilities/unknown vulnerabilities” are not clear. Moreover, penetration testing is useful only when the system is in place in the target architecture.				
5	2.85	...when all of the potential sources of failures” (excluding cybersecurity related ones)...	Presently, it is not possible to quantify attack probability on I&C systems: we suggest adding a parenthesis to exclude this aspect.				
6	6.5 page 47	Recommendation 6.5 is written twice.	Typo				

7	6.50 page 52	Add the following sentence: “Monitoring systems of lower safety classification may be connected to safety systems provided that it is demonstrated that they cannot disturb them.”	As per clause 6.168. I&C systems should have self-supervision or monitoring features that allow regular confirmation of their continued correct operation. Considering the functionality to be implemented in the monitoring systems, it is common that the terminal which displays the detailed state of the safety systems to the maintenance operators cannot be safety systems. A demonstration that such monitoring systems of lower safety classification cannot disturb the safety systems to which they are connected has to be provided in this situation.				
8	6.72 page 55	The failures that might result from software errors are difficult to predict. Nevertheless, it is not necessary to know how the software fails to determine the possible failure states as seen at device terminal. The most likely possible failure modes could be identified and classified into a manageable set of possibilities, e.g. wrong output, delayed output, frozen output.	The identification of all possible failure modes for a PLC based systems, which includes thousands of variables, several internal states, and multiple interfaces and outputs, cannot be done. This is in line with the first sentence of recommendation 6.72. However, expectable failure modes can be identified and addressed.				
9	7.126	Remove “such as scanning for security vulnerabilities”	It is proposed to group specific considerations on security scanning in 7.129, as right now, it is split between 7.126 and 7.129.				

10	7.129	Remove “for safety systems”	Scanning should be made on off-line system for all I&C systems, not only safety ones.				
11	7.99 page 82	Delete	IEC/SC45A experts do not understand why the clause removed in revision J has been reintroduced. IEC/SC45A experts noted that communication between safety divisions concern essentially the votes. Each division typically sends its partial trip to the others and receive partial trip from the others to do the votes. In such a case, it is unclear how one-directional communication is possible between safety divisions.				
12	7.140 page 86	Delete	IEC/SC45A experts noted that there is no definition of what is “IP cores” and in this context this recommendation would be extremely difficult to apply. In the frame of the elaboration of the IEC 62566 standard, IEC/SC45A experts have concluded that it was not possible to provide a viable definition for IP core because the terminology widely differs between vendors. IEC/SC45A experts noted also that from a formal perspective it is difficult to				

			have a recommendation to avoid IP cores that is directly followed by a clause that contradicts this recommendation. Simply deleting clause 7.140 resolves the contradiction.				
13	9.41+	(additional section, set at the end of the design section, or close to 9.35) The software design should take into account the best practices in terms of information security, in order to avoid the creation of vulnerabilities by design, that are easy to exploit by malware or hackers, and difficult to fix.	IEC/SC45A experts noted that there can only be one software design process: this guide must refer to software secure development methodologies, that may be further developed in another document (dedicated to cybersecurity). A large number of vulnerabilities for I&C systems was made public during the years 2011 to 2013. Many of those are caused by design, that addressed well safety & reliability, but ignored security. We now have many unfixable devices in the field, with “exploits” easy to use and publicly available. The requirement could be “shall” for safety systems actually (and “should” for non safety)				
14	9.59 page 106	Move the sentence “There are many different sources of potential coincident software failures and statistical independence cannot always be assumed; this would need to be accounted for in any claim for the reliability achieved. » in appendix III	IEC/SC45A experts noted that this sentence is applicable only for some member states that use numerical reliability target for software. Consequently, it is suggested to move this				

			sentence in appendix III.				
15	9.60+	(additional section, set at the end of the implementation section, or close to 9.53) Implementation teams should be trained on secure development techniques. Development methodologies and tools should include the best practices in terms of secure development.	IEC/SC45A experts noted that as for comment #1, the same rational applies to software development. Although in theory software security vulnerabilities that are caused during the development are easier to fix (patches), in reality, patching (especially of I&C) is difficult to perform.				
16	9.90+	(two additional sections, set at the end of the verification section, or close to 9.78 for code review, and 9.89 for pen tests) The code should be reviewed to check for software security vulnerabilities, using automated tools and complemented by manual review of the critical sections of the code (I/O handling, exception handling) For safety systems, the resulting application should be submitted to security-specific testing (such as pen testing), to make sure that common security vulnerabilities are not easy to detect, and to allow for continuous improvement of the software design and implementation.	(same rational as #2 and #3)				
17	III – 6 page 125	Add the following sentence: Some member states use a qualitative approach for determining SW reliability. Such qualitative approach is typically based on strong requirements on the deterministic behaviour of the software to allow a full verification and validation. Such combination of strong design requirements that allow full V&V gives a high confidence in the reliability of the software.	A description of the qualitative approaches used in some other member states is proposed by IEC/SC45A experts for consideration.				
18	III – 7 page 125	Paragraph 4.32 recommends that an analysis should be done of the consequences of each PIE in combination with CCF that will prevent ~~the I&C safety~~	IEC/SC45A experts noted that this sentence was modified to match recommendation 4.32				

		~~systems~~ a protection system from performing the needed safety functions.	which it refers to.				

Design of instrumentation and control systems for NPP *(DS431)*

COMMENTS BY REVIEWER				RESOLUTION			
Reviewer: Page.1 of 1 Country/Organization: Switzerland/ENSI Date:2013/05/29							
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1	2.79 / 1	(Add Reference for GS-R-4)	Reference is missing				
2	3.6 / 3	The objective of these functions, corresponding to the concept of defence in depth, are to	the relation to the concept of defence in depth is not mentioned				
3	6.72 / 5	, spurious output actions.	spurious output actions are not mentioned				