UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

May 10, 2010

MEMORANDUM TO: Lois M. James, Chief
Probabilistic Risk Assessment Op Support Branch
Division of Risk Assessment
Office of Nuclear Reactor Regulation

FROM: G. Edward Miller, Project Manager
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

SUBJECT: TASK WORKING GROUP NO. 6 – SUPPORTING DOCUMENT FOR PUBLIC MEETING TO ADDRESS DEVELOPMENT OF DIGITAL I&C LICENSING PROCESS DRAFT COMMENT RESOLUTION

The purpose of this memorandum is to provide you with, and make publically available, the proposed NRC Staff resolution of the comments received from the Nuclear Energy Institute (NEI) regarding the draft version of Interim Staff Guidance 6, "Digital Instrumentation and Controls, Licensing Process," in support of the public meeting on May 20, 2010. The public meeting notice, which included the draft guidance is available under Agencywide Documents Access and Management System Accession No. ML101120993. The resolution of the comments were provided via e-mail to Gordon Clefton, NEI, on Friday May 7, 2010. Subsequent to providing them, a typographical error was noted in Comment 34. Specifically, on page 8 or 38, Comment 34, "NRC Comment/Disposition column," the number of was listed as 6,134 while it should have been 16,134. The error has been corrected in the version attached to this memorandum.

Enclosure: As stated

May 10, 2010

MEMORANDUM TO: Lois M. James, Chief
Probabilistic Risk Assessment Op Support Branch
Division of Risk Assessment
Office of Nuclear Reactor Regulation

FROM: G. Edward Miller, Project Manager /RA/
Plant Licensing Branch I-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

SUBJECT: TASK WORKING GROUP NO. 6 – SUPPORTING DOCUMENT FOR PUBLIC MEETING TO ADDRESS DEVELOPMENT OF DIGITAL I&C LICENSING PROCESS DRAFT COMMENT RESOLUTION

The purpose of this memorandum is to provide you with, and make publically available, the proposed NRC Staff resolution of the comments received from the Nuclear Energy Institute (NEI) regarding the draft version of Interim Staff Guidance 6, "Digital Instrumentation and Controls, Licensing Process," in support of the public meeting on May 20, 2010. The public meeting notice, which included the draft guidance is available under Agencywide Documents Access and Management System Accession No. ML101120993. The resolution of the comments were provided via e-mail to Gordon Clefton, NEI, on Friday May 7, 2010. Subsequent to providing them, a typographical error was noted in Comment 34. Specifically, on page 8 or 38, Comment 34, "NRC Comment/Disposition column," the number of was listed as 6,134 while it should have been 16,134. The error has been corrected in the version attached to this memorandum.

Enclosure: As stated

DISTRIBUTION:

Public RidsNrrPMGMiller LPL1-2 R/F

ADAMS Accession No.: ML101270108

OFFICE	LPL1-2/PM	EEIB/BC
NAME	GEMiller	WKemper
DATE	5/10/10	5/10/10

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
1	Global	"It should be noted…" "It is important to note"	delete		Agree	Globally - 'It should be noted" and "It is important to note" have been removed.	Closed
2	Global	When does the Staff start writing the SER?	Suggest commencing in Phase 1	Best to write SER in first 12 months and use second 12 month for confirmation.	Agree - Wording added to Section C.3.	During Phase 1, the NRC staff will draft the SE and issue requests for additional information (RAI) for the information that is necessary to complete the review of the docketed material.	Closed
3	Global	Software operator	Replace software "operator" with "user". Since there may be many others who interface with the system, not just operators.		Agree in part. Where this ISG describes the requirements in IEEE 603 or 7-4.3.2, and the IEEE standard uses the term "operator" this term is generaly maintained.	Globally - "operator" replaced with "user" where appropriate.	Closed
4	Global	documents	information	Replace "documents" with "information".	(see Comment 185) Disagree - No change. There are two types of information that is required: (1) The regulations contain certain fiunction requirements (e.g., single-failure criterion) and the information required to review the acceptability of the design can be in many forms, but is basically a description of how the design meets the requirement. (2) BTP 7-14 requires that the staff evaluate certain documents. These documents should be docketed per LIC-101 (LIC-101 Revision 3, "Licese Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.2, "Using Precedent Safety Evaluations & References to Topical Reports," states: "If a licensee in their application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its SE for the plant-specific license amendment application."). Section B.1.2 added.	(See "Final Text" of Comment No. 34 for the new text.)	Closed
5	Global	Failures	errors	Software 'failures' should be replaced by 'errors'.	Agree	Globally - "failures" replaced by "errors" were appropriate.	Closed
6	C.1 Process Overview	Missing	Tier 1- address Application Specific Action Items (ASAI) and post-SE regulatory guidance (DI&C-ISG-04) Tier 2 – addresses ASAI and any deviations from approved SE or Topical Report Tier 3 – new application (what DI&C-ISG-06 addresses in detail)	Mis-match between guidance amount and probability of use.	Agree	Tier one generally address: (1) Application Specific Action Items (ASAI) identified in the safety evaluation of the digital I&C platform, (2) post-SE regulatory changes, (3) post-SE regulatory guidance changes (e.g., DI&C-ISG-04), and (4) evaluation of the equipment for performing application or plant specific requirements. ... Tier two evaluations generally include Tier 1 review scope and any deviations from the approved SE or Topical Report. ... Tier three evaluations generally include Tier 1 review scope and Topical Report review scope.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
7	B. PURPOSE	The NRC staff will review proposed digital I&C upgrades against the design basis of the plant and the guidance in the Standard Review Plan (NUREG-0800), Chapter 7, and other associated guidance including ISGs.	The NRC staff will review proposed digital I&C upgrades against the licensing basis of the plant and the guidance in the Standard Review Plan (NUREG-0800), Chapter 7, and other associated guidance including ISGs.	Should agree with last sentence in paragraph.	Agree	The NRC staff will review proposed digital I&C equipment to ensure that there is reasonable assurance that the equipment will perform the required functions; this review will use the guidance in the Standard Review Plan (NUREG-0800), Chapter 7, and other associated guidance including ISGs. Licensees should provide a description of the licensing basis functions of the I&C equipment and include a description of the equipment that implements the functions. Additionally, licensees should clearly identify those parts of the licensing basis they are updating as a result of the proposed change.	Closed
8	B.1 Background	actives	activities	Typo 'actives ' for 'activities'	Agree	The NRC oversight includes different types of activities performed by the NRC staff in the oversight of design, construction and operation of a nuclear power plant (NPP).	Closed
9	B.1 Background	The NRC staff does not perform an independent design review of the DSS. Instead, the staff reviews the design process and design outputs to determine that the process is of sufficient high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants.	The NRC staff does not perform an independent design review of the DSS. Instead, the staff reviews/audits the design process and design outputs to achieve reasonable assurance that the process is of sufficient high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants.	'reviews/audits' for 'reviews' throughout	Disagree - The paragraph has been reworded to add clarity. The term "review" will be used throughout to refer to staff activitied associated with a Licensee amendment request conducted in accordance with LIC 101 Revision 3, "License Amendment Review Procedures". The NRC must assure appropriate safety functions have been included in the design, there is sufficient redundancy in the design, justifications for/against diverse actuation systems are justified by the design, etc. To state that the NRC will no longer review the details of safety system designs is counter to the requirements of the Atomic Energy Act.	The NRC staff does not perform an independent design review of the DSS. Instead, the staff reviews the design process and design outputs to determine that the process is of sufficient high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants. In addition the staff may perform thread audits to verify that the DSS implementation activities are consistent with the DSS planning activities in accoradance with LIC 111, "Regulatory Audits".	Closed
10	B.1 Background	process's	processes	Typo 'process's' for 'processes'	Agree	Therefore, a major portion of the NRC staff review is of documentation of plans and processes which describe the life-cycle development of the software to be used by and/or in support of the digital I&C system.	Closed
11	B.1 Background	For this reason, the DSS design must be complete and the system tested to demonstrate that it will perform its safety function.	For this reason, the DSS design must be complete to the system level to demonstrate that it will perform its safety function.	This sentence is ambiguous, since to what extent the design must be "complete" and the system must be "tested" are not defined. It also conflicts with the sentence above which says "The NRC staff then depends on the proper application of this high quality design process to produce acceptable systems and software." If the NRC depends on the process, then the design does not need to be complete and the system does not need to be tested.	(see comment 189) Disagree - No Change. The sentence is clear. The NRC dependence on a high quality design procees is related to another issue.	In the March 24, 2010 public meeting it was decided that this issue was outside the scope of this ISG6 meeting (i.e. no change to text).	Closed
12	B.1.1 High Quality Process is a Critical Characteristic of Software	"High Quality Process is a Critical Characteristic of Software"	"Principals of Review"	Change title	Agree	B.1.1 Principles of Review	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
13	B.1.1 High Quality Process is a Critical Characteristic of Software	It is generally accepted in the software industry that no non-trivial software can be completely tested (or be bug free), which means that (by strict interpretation) the critical characteristics of software cannot be verified. The result would be that no commercially developed software could be used in any safety related application, but that software developed under a quality assurance program could be. To reconcile this apparent contradiction, the NRC staff determined that a high quality software development process is a critical characteristic of all safety-related software. A high quality software development process is one that is equivalent to the development process for software developed under a quality assurance program.	Since the critical characteristics of software cannot be verified, no commercially developed software could be used in any safety related application. Software developed under a 10CFR50 Appendix B quality assurance program could be, since even commercial software is developed under "a quality assurance program". The NRC staff determined that a high quality software development process is a critical characteristic of all safety-related software. A high quality software development process is one that is equivalent to the development process for software developed under a quality assurance program.	Delete first sentence of last paragraph in Section Not guidance; training reviewer. Industry knows how to dedicate. This paragraph does not relate to the use of the NRC approved Commercial Off The Shelf (COTS) dedication in EPRI TR-106439. The discussion refers to developed-under-a-QA-program but does not include dedicated-under-a-QA-program	Agree - Last paragraph changed. Disagree - The industry does not have much experience related to commercial dedication of software. Software currently used in NPP safety systems has been specifically developed by industry vendors for safety applications. Reference to EPRI TR 106439 and associated SE have been added. Commercial grade dedication must be done under an approved Appendix B program. It is assumed that industry knows this and that this does not need to be repeated here.	Since the critical characteristics of software cannot be verified, no commercially developed software could be used in any safety related application; however, software developed under a 10CFR50 Appendix B quality assurance program could be. This position seems to conflict with the fact that some commercially available software is highly reliable. Therefore, the NRC staff has determined that a high quality software development process is a critical characteristic of all safety-related software. A high quality software development process is one that is equivalent to the development process for software developed under an Appendix B quality assurance program. " Consistent with this principle, the Safety Evaluation (SE) for EPRI TR-106439, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," the staff stated (see Section 2.0, "Background," subsection "Commercial Dedication per CFR Part 21"): "The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests.	Closed
14	C. DIGITAL I&C REVIEW PROCESS	However, verification that the as-built facility conforms to the approved design is performed through the inspections, tests, analyses, and acceptance criteria (ITACC) verification process.		There should be a corresponding statement for the Part 50 process. Otherwise the implication is that the Part 50 process requires approval of the "as-built facility"; however, there is nothing in the SRP that requires approval of the "as-built facility".	Disagree with comment. - The scope of this licensing process is Part 50, not Part 52. The paragraph has been removed.	(paragraph removed)	Closed
15	C. DIGITAL I&C REVIEW PROCESS	Specifically, Enclosure B identifies the documents to be submitted in a License Amendment Request (LAR) that seeks to install a digital I&C safety system.		The Staff previously agreed to replace "documents" with "information". The Licensee should have the option to submit actual design documents or other submittals that include the required information. This should also state that Appendix B identifies the information that must be available for inspection.	(see Comment Nos. 4, 185, & 186) Agree - Text modified. In the March 24, 2010 public meeting the staff took the action to investigate the possibility of using sharepoint or other such technology as a way to view the information requird, and the staff could then inform the applicat of what would need to be docketed.	Specifically, Enclosure B identifies the documents <u>and/or information</u> to be submitted in a <u>typical</u> License Amendment Request (LAR) that seeks to install a digital I&C safety system.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
16	C.1 Process Overview	The NRC staff recognizes that some information may not be available upon initial submittal of the LAR, thus it is not expected that information sufficient to address all review topics be submitted until at least 12 months prior to the requested approval date.		Should add: Some information may be submitted after the 12 month cut-off based on prior NRC agreement in an agreed Project Schedule, without delaying the approval.	Agree - Wording changed in C.1 Wording added to C.2.	...; the timing of specific exceptions may be a topic for discussions during the Phase 0 meetings. All proposed deviations from the document list and associated schedule described in Enclosure B should be discussed in the Phase 0 meeting(s). Any associated agreements should be documented in the Phase 0 meeting minutes. Delays by an applicant in honoring these commitments can result in a application be denied (see 10 CFR 2.108, "Denial of application for failure to supply information") or delay the final evaluation completion date. The NRC is currently considering development of office level procedures for the use of data portals (e.g., electronic reading rooms) to verify information within various documents referenced by the submittal and to determine if the documentation (or some portion thereof) should be submitted on the docket. When this procedure is available, it is expected that it's use will enhance the efficiency of digital I&C reviews as well.	Closed
17	C.1 Process Overview	Tier one is applicable to license amendments proposing to reference a previously approved topical report completely within the envelope of its generic approval as described in the topical report.		Tier 1 should also be applicable to a license amendment proposing to reference a previously approved license amendment, not just a previously approved Topical Report. Anything previously approved by precedence should apply.	Agree in part - Words added to Section C to clarify the use of precedence.	Precedent licensing actions are those with a similar proposed change and regulatory basis for the SE. Searching for, identifying, and using precedents in the review process maximizes staff efficiency, minimizes the need to issue requests for additional information and ensures consistency of licensing actions. However, approval of a function or DSS at one plant does not serve as the basis for approving the same at another plant. Each LAR is a plat specific licensing action.	Closed
18	C.1 Process Overview	The list of documents that would typically need to be submitted by the licensee in support of a tier two review are contained in Enclosure B, column 2, however it should be noted that for any particular submittal, the actual list of documents needed will be determined by the changes from the previously approved topical report.		Column 2 is not typical, but rather based on specific changes identified in the Note at the end of the table.	Agree	The list of documents that would typically need to be submitted by the licensee in support of a <u>typical</u> tier two review are contained in Enclosure B, column 2, however for any particular submittal, the actual list of documents needed will be determined by the changes from the previously approved topical report as determined in the Phase 0 meetings.	Closed
19	C.3 Initial Application (Phase 1)	As further discussed in Section C.4, the NRC staff and licensee should be aware that some information needs may be best met by documentation available at site (e.g., Enclosure B, table of documents to be available for audit 12 months prior requested approval date).		Change 'site' to supplier's or licensee's facility.	Agree - A licensee is responsible for maintaining adequate documentation. Change "site' to "licensee's facility".	As further discussed in Section C.4, the NRC staff and the licensee should be aware that some information needs may be best met by documentation available at licensee's facility (e.g., Enclosure B, table of documents to be available for audit 12 months prior requested approval date).	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
20	C.3 Initial Application (Phase 1)	It should be noted that one of the reasons for a publically available safety evaluation is so members of the public can have confidence in the review process by understanding what was approved, and the basis for that approval. This is addressed, in part, in Information Notice 2009-07. Sufficient non-proprietary information, including some system design details and design methods, should be provided as non-proprietary by the licensee and vendor to make this possible. To satisfy this concern, non-proprietary versions of documents should limit the material that is redacted to only specific portions that are necessary (i.e., containing proprietary information does not make an entire document proprietary).		This is a major burden. Make information available for audit---NOT submitted/docketed that must be kept up to date. It is awkward for the list of design documents in enclosure B required to be submitted before finalized and in P and non-P versions. In effect it doubles the documentation and configuration management work, since P and non-P version of design documents must now be produced and maintained. The audit approach is a much more workable approach. If these documents get revised in the future via some CFR50.59-like process, do these documents need to be resubmitted since these were initially docketed? Also, docketing and providing redacted versions of detailed documentation will add cost and schedule delays to a project. If the purpose of the NRC review is to ensure that the licensee (vendor) is following his process via audit, there is no justification for docketing detailed design information.	(See Comment No. 1 & 185.) Disagree - Change made per comment No. 1, and text added for clarification. LIC-101 Revision 3, "Licensee Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.0, "Safety Evaluation," states: "Given that the SE serves as the record of the staff's disposition of a license amendment request, the information relied upon in the SE must be docketed correspondence." No. The information/documents used to approve a license amendment will be referenced in the safety evaluation. Changes made to a DSS under 10CFR50.59 after it is installed may require trvision to these documents; however, that is the licensee's responsibility to maintain configuration control of these design documents and they need not be resubmitted to the staff for review. Even if the staff reviews information during an audit, the documentation will still need to be submitted on the docket if the activity is addressed in the safety evaluation as the basis for verifying a DSS complies with the regulations.	One of the reasons for a publically available safety evaluation is so members of the public can have confidence in the review process by understanding what was approved, and the basis for that approval. This is addressed, in part, in Information Notice 2009-07. Sufficient non-proprietary information, including some system design details and design methods, should be provided as non-proprietary by the licensee and vendor to make this possible. To satisfy this concern, non-proprietary versions of documents should limit the material that is redacted to only specific portions that are necessary (i.e., containing proprietary information does not make an entire document proprietary). It is recognized that it is a burden to licensees and vendors to maintain proprietary and non-proprietary versions of DSS documents; therefore, the staff will make every effort to minimize the use of proprietary information in safety evaluations. Conversely licensees and vendors are encouraged to exercise discipline in marking documents as proprietary. The final determination of which documents should be redacted and submitted as non-proprietary will be made after the draft safety evaluation has been reviewed by the licensee or vendor for proprietary information.	Closed
21	C.4 Continued Review and Audit (Phase 2)	It should be noted that some documentation (e.g., factory acceptance testing results) may not be available 12 months prior to the anticipated issuance of the amendment. Although the plans and other available information should be submitted at early as possible, it is acceptable to submit the results when available but prior to the SER.		The Staff should allow later submittals based on agreements at the Phase 0 review meetings. This approach increases the economic justification challenge because it requires considerable investment while significant regulatory acceptance and schedule performance risk exits. The NRC track record has not engendered confidence in either predictable outcomes or predictable schedules. This is inconsistent with the table in Appendix B. Asterisks should be placed on those items that can be accepted after the LAR.	No change. The staff agrees that some documentation may not be available within 12 months of the safety evaluation date. This was addressed in comment no. 16, which is sufficeint to address this comment also.	(no change)	Closed
22	C.4 Continued Review and Audit (Phase 2)	Any audits (e.g., of completed factory acceptance test procedure and results, configuration management reports, detailed system and hardware drawings, final circuit schematics, final software integration report, individual completed test procedures and reports, Individual V&V problem reports up to FAT, software code listings, and vendor build documentation) will likely cover information from both Phase 1 and Phase 2, and may result in further requests for information to be docketed.		Appendix B says FAT must be submitted, not audited.	Agree with industry comment; documentation must be submitted in accordance with Enclosure B. Specific audit examples have been removed from the body of this ISG to avoid inconsistencies.	Globally - Specific references to audited documentation have been removed.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
23	C.4 Continued Review and Audit (Phase 2)	It should be noted that some documentation (e.g., factory acceptance testing results) may not be available 12 months prior to the anticipated issuance of the amendment. Although the plans and other available information should be submitted at early as possible, it is acceptable to submit the results when available but prior to the SER.		This tends to contradict previous NRC statements regarding 12 months prior and supports delivering according to an agreed project plan.	Agree	Globally - Examples have been removed to ensure consistency.	Closed
24	C.5 Implementation and Inspection (Phase 3)	Following regulatory approval of the digital I&C system, licensees will implement the upgrade by installing the system, effecting associated procedural and technical specification changes, and completing startup testing.	Following regulatory approval of the digital I&C system, licensees will implement the upgrade by installing the system, implementing associated procedural and technical specification changes, and completing startup testing.	'implementing' vs. 'effecting'	Agree	Following regulatory approval of the digital I&C system, licensees will implement the upgrade by installing the system, implementing associated procedural and technical specification changes, and completing startup testing.	Closed
25	D.1.2 Information to be Provided	…The hardware items should be identified to the revision level…. Any deviations or revision changes should be identified and adequately justified…. These descriptions should include a description of all assemblies (e.g., Cabinet, Channel, Train) and sub-assemblies (e.g., nineteen inch rack and associated sub-racks), down to the field replaceable units (e.g., power supply, display, circuit board), the required behavior of each, and how they work together to accomplish the various system functions.		This results in submission of a very detailed design document.	Disagree - The predominate regulatory interest is in digital equipment. Wording has been clarified.	Enclosure B is only an example list of information which has been explained throughout this ISG and is needed to review a DSS. An applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation and description to allow the NRC staff to identify what hardware is being used in this application, how the hardware items function, how the various hardware items are interconnected, and any software which runs on that hardware. The digital hardware items should be identified to the revision level. In those cases where the hardware has previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation, including the ADAMS accession numbers if available. Any deviations or revision changes should be identified and adequately justified.	Closed
26	D.1.2 Information to be Provided	Any deviations or revision changes should be identified and adequately justified.		The review should be giving credit to Appendix B processes to control significant design changes (function changes) from information previously docketed. Justification should be an audit item of the Appendix B process. Revisions are often due to supplier changes or minor design changes due to component obsolescence. These are controlled by the supplier's Appendix B program. The Staff should only review significant changes (e.g., microprocessors). The text should define the areas of specific interest to the staff.	Disagree - Certain credit is given for an approved Appendix B program and the reactor oversight process implemented by the regions; however, it is assumed that the licensee followed a 10CFR50.59 process and determined that the proposed changes is outside of the current licensing basis; the licesee is applying to amend its licensing basis. The NRC is currently considering development of guidance for determining the regulatory significance of changes to topical report. Wording added to Section D.1.2. In the March 24, 2010 public meeting the staff took the action to investigate the possibility of using sharepoint as a way to view the information requird. (See comment No. 16)	LIC-101 Revision 3, "License Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.2, "Using Precedent Safety Evaluations & References to Topical Reports," states: "If a licensee in their application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its SE for the plant-specific license amendment application." ... As stated previously, electronic access portals may be used for the staff to evaluate these changes and request information for significant changes to be docketed.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
27	Footnote #2; D.1.2 Information to be Provided	These descriptions should include a description of all assemblies (e.g., Cabinet, Channel, Train) and sub-assemblies (e.g., nineteen inch rack and associated sub-racks), down to the field replaceable units (e.g., power supply, display, circuit board), the required behavior of each, and how they work together to accomplish the various system functions. It is expected that this architecture description include both text and diagrams.		Size is not appropriate for reasonable assurance ("nineteen inch rack").	Agree - Comment Incorporated. Footnote moved to glossary.	Hardware Architecture Description: A description of the manner in which the hardware components of a digital I&C system are organized and integrated. These descriptions should include a description of all assemblies (e.g., Cabinet, Channel, Train) and sub-assemblies down to the field replaceable units (e.g., power supply, display, circuit board), the required behavior of each, and how they work together to accomplish the various system functions. It is expected that this architecture description include both text and diagrams.	Closed
28	D.1.3 Regulatory Evaluation	D.1.3 Regulatory Evaluation		Poor title words, since there is no Regulatory requirement, just information for reviewer.	Disagree - No change. These section contain direction for the reviewer to follow in performing regulatory evaluations.	(no change)	Closed
29	D.2.2 Information to be Provided	Quality Assurance Plan for Digital Hardware		No one has seen such a plan. QA for digital hardware is the same as QA for any other hardware. It is within the supplier's/licensee's Appendix B Quality Assurance Manual; therefore, this section should clearly state that a separate QAP for Digital Hardware is not required.	Agree. 'Quality assurance plan for Digital Hardware" has been removed from D.2.2 and Enclosure B. The remaining text in D.2.2 is adequate for describing desired documentation:	This information would typically be in the quality assurance plans and reports, commercial grade dedication plans and reports (if commercial grade dedication is used), the system description, hardware architecture description, theory of operations description, detailed system and hardware drawings, final circuit schematics, vendor build documentation, and the systems and hardware requirements specification.	Closed
30	D.2.2 Information to be Provided	Any deviations or revision changes should be identified and adequately justified.		Deviations in docketed information only.	Agree - No Change. The staff only reviews docketed information.	(no change)	Closed
31	D.2.4 Technical Evaluation	The NRC staff will provide a description of the design process and the quality control which governed that design process. This description will cover both design of the individual functional units and modules and how those units and modules were used in the application specific safety function design. Since this description will be contained in a publically available safety evaluation, portions of the licensee's description will need to be non-proprietary.		If these documents get revised in the future via some 50.59 process, do these documents need to be resubmitted since these were initially docketed? Also, docketing and providing redacted versions of detailed documentation will add cost and schedule to a project. An auditing process is suggested, rather than 2nd party review of design.	(see Comment No. 20) Disagree - No change. The 50.59 process is a separate process and will be addressed by a revision to RIS 2002-22. The NRC performs Licensee Reviews not 2nd party reviews.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
32	D.3.1 Scope of Review	Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In these situations, the NRC staff's scope of review will include the software (including all aspects of the life-cycle) used to generate, implement, and maintain the hardware logical functions.		Per IEEE 7-4.3.2, software tools do not require qualification, if there is sufficient Verification & Validation (V&V) to confirm the quality of the tool output. (RG 1.168 endorses 7-4.3.2.) These tools should be handled the same as piping-analysis, code-compliers, function-libraries, etc. Staff need not review tools used to manage software. Use OE for confidence of performance. This is a new NRC position; should not be in guidance document.	Disagree - Wording changed to add clarity. Please see the Wolf Creek MSFIS SER (ML090610317). Reference to NUREG/CR-7006, "Review Guidelines for Field Programmable Gate Arrasy in Nuclear Power Plant Safety Systems," has been added.	Some digital technologies, such as a field-programmable gate array (FPGA), do not utilize software while the system is in operation (BTP 7-14 will be used to review the associated development process). Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In these situations, the NRC staff's review of the software tools used to generate, implement, and maintain the FPGAs will be guided by IEEE Std 7-4.3.2-2003 Clause 5.3.2. EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," states that operating history alone is not sufficient for commercial dedication of equipment. Operating history must be used in combination with one or more of the other three commercial dedication approaches (i.e., special tests and inspections, source evaluations, and supplier surveys). Please see also NUREG/CR-7006, "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems."	Closed
33	D.3.2 Information to be Provided	The software should be identified to the revision level. In those cases where the software has previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation. Any deviations or revision changes should be identified and adequately justified.		This results in submission of a very detailed design document.	(See Comment No. 185) Disagree - No change. Knowing what version of software is in the equipment is not detailed design information. LIC-101 Revision 3, "License Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.2, "Using Precedent Safety Evaluations & References to Topical Reports," states: "If a licensee in their application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its SE for the plant-specific license amendment application."	(no change)	Closed
34	D.4.2 Information to be Provided	Software Management Plan Software Development Plan Software Quality Assurance Plan Software Integration Plan Software Installation Plan Software Maintenance Plan Software Training Plan Software Operations Plan Software Safety Plan Software Verification and Validation Plan Requirements Traceability Matrix Software Configuration Management Plan Software Test Plan System Requirements Specification Platform Software Requirements Specification Application Software Requirements Specification Software Design Specification System Build Documents Configuration Lists Configuration Tables FMEA	Delete	Adds no value and does not match Section D.4.4 nor Appendix B which gives needed document list. This list duplicates the list of documents submitted in support of the Oconee RPS/ESPS LAR review without benefit of lessons learned. As reported in the trade press: In an August 27 meeting on a future Diablo Canyon digital I&C amendment, the NRC said it had not "specifically requested" over 25,000 pages of supporting information to be submitted on the docket, but the information it was looking for was simply "buried in lengthy documents that were submitted in whole." To satisfy the NRC's information needs, Duke submitted numerous supplements to its January 31, 2008 submittal.	Section B.1.2 has been added. This document list and similar document list have been deleted. Approximately 28, 025 pages of documents were docketed in the Oconee RPS/ESPS LAR and associated supplements; 16,134 pages of which were either not applicable to the staff review or were corrections to errors and inconsistencies.	B.1.2 Documentation Reviewed As a general rule, the organization responsible for the review of I&C (i.e., EICB) does not review procedures; however, EICB must review sufficient information to make an evaluation against the review criteria in the SRP. If the only place such information exists is inside procedures, then the EICB will request and review those procedures. As a general rule, the EICB reviews only the information required to make an evaluation against the review criteria in the SRP; EICB will require that information to be docketed. If the information required is contained in proprietary or larger documents, then EICB will request those documents. If a licensee chooses, the information may be extracted or reproduced in another format convenient for docketing. This ISG does not describe the design process; an applicant	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
				The sad fact is that NRC required the submission of these documents in the same manner as specified in this guidance. The submission creates another document management problem. Since the design is moving through a software development lifecycle, the list can be revised multiple times as the design progresses. NRC required that subsequent revisions be submitted on the docket, upping document page count. If these documents get revised in the future via some CFR50.59 process, do these documents need to be resubmitted since these were initially docketed? Also, docketing and providing redacted versions of detailed documentation will add cost and schedule to a project. An auditing process is suggested, rather than 2nd party review of design.	In the January 31, 2008 LAR submittal, Duke did not docket any deisgn documents; Duke provided a CD containing many documents to the NRC for information purposes only. Since the NRC normally requires tht information be provided on the docket, under oath and affirmation, the NRC engaged in internal discussio of how to handle this information. In order to expidite the NRC internal processes, Duke (via the first LAR suplement) docketed all of the information on the CD. The NRC did not require all the documents that Duke chose to submit. Duke made a business decision regarding the format they chose to submit documentation required to suport the review of the LAR due to the short time remaining from when their LAR was submitted, until the next outage in which they intended to implement the modification. Agreed - The NRC would prefer that the applicant submit final documentation. It would save both parties much time and effort. 394 pages were revisions to previosuly docketed information. For example, there was a conflict between: (1) the response time specified by Duke and calculated by Areva, and (2) the factory acceptance testing. Therefore Duke changed the required response time and Areva changed the calculated response time. It would not have been possible for the NRC to accept a system with such a discrepancy on the docket. See comment No. 20. See comment No. 20.	is allowed to determine their own design process (e.g., per RG 1.73 and IEEE Std 1074). However, this ISG makes certain assumptions (consistent with 10 CFR 50 Appendix B), about that design process. For example, if there exists a regulatory requirement that a safety-system has a certain property (e.g., IEEE 603-1991 Clause 5.1, "Single-Failure Criterion"), then it is assumed that there is a documented design analysis that demonstrates that the safety system meets this regulatory requirement. It is also assumed that the V&V team evaluates this design documentation and documents their evaluation. In order to minimize regulatory burden, Enclosure B sometimes asks for this analysis using a generic name. In some cases it may be appropriate to summarize this analysis (in sufficient detail for the regulator to independently determine that the regulatory requirement is met) in the LAR. A statement made under oath and affirmation that the regulatory requirement is met is necessary but not sufficient for the regulator to determine that the system is designed to meet the regulations.	
35	D.4.2 Information to be Provided	Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:	If you have an approved Software Program Manual, you do not need to re-submit the following plans but you need to address ASAIs in the SPM:	This section could discuss the submittal of a generic Software Program Manual, in lieu of individual Software Plans. The SPM would include the critical technical characteristics of each plan to demonstrate regulatory compliance. Resources, budgets and schedules are typically included in project specific documentation.	Agree - Text added to D.4.	In some cases an applicant has combined many of the generic aspects of the twelve plans, described in BTP 7-14, into a software program manual (SPM). In these cases project specific aspects (e.g., budget and schedule) are described in project plans. These SPMs can be reviewed and approved independent of a specific project, and any approval will generally contain application specific action items to address project specific aspects.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
36	D.4.4.1 Software Management Plan (SMP)	Text within: D.4.4.1 Software Management Plan (SMP)		The descriptions for each of these plans include a lot of repetition from BTP 7-14. This ISG should only add clarification or emphasis ("of particular interest to the Staff"), not repetition. The entire section should be scrubbed to eliminate simple repetition.	Disagree - No Change. Previously, industry wanted text to be copied and not to be referenced.	(no change)	Closed
37	D.4.4.1 Software Management Plan (SMP)	The SMP should include sufficient information about the security requirements for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 and that the methods are used effectively. This needs to be an actual description of the security requirements enumerated in RG 1.152, and not just a statement that all security requirements will be met.		Since it is in a state of change, guidance should reference the appropriate revision of RG 1.152.	Agree - The new revision of RG 1.152 (DG-1249) will be referenced after it is publically available.		Open
38	D.4.4.1 Software Management Plan (SMP)	Generally, these are the quality assurance organization, the software safety organization, and the software verification and validation organization. It is important that these groups maintain independence from the development organization, by both organization and function. The independence of the quality assurance organization, the software safety organization, and the software verification and validation organization should be described in terms of management, schedule, and finance.		Regulatory requirements exist for independent design verification and QA originations in 10 CFR Part 50 Appendix B. Formal regulatory guidance exists for the V&V organization in RG 1.152 R2 (which endorses IEEE Std 7-4.3.2-2003 and RG 1.168 R1 (which endorses IEEE 1012-1998). No requirements or guidance exist for a software safety organization and none should be imposed here. NRC has not endorsed IEEE 1228-1994. Delete Software Safety Organization. IEEE Std. 7-4.3.2 only requires separate organizations for Design and V&V. The responsibilities for software safety may be divided among the Design Team and V&V Team. NUREG6101 states "The software safety organization referred to in the list could be part of the system safety organization." The Oconee SER states: "AREVA NP Inc., does not have a dedicated software safety team and does not have a designated individual to be responsible for performing software safety activities other than the project technical manager who provides oversight for all of the project activities. Each software safety activity is the responsibility of the overall project organization. The software V&V organization is, however, tasked with specifically documenting and addressing the safety issues of the digital RPS/ESPS system."	Agree	Another important aspect of the SMP is the relationship between the software development group and the group(s) that check the quality of both the software development program and the software. Generally, these checking functions are quality assurance, software safety, and verification and validation. It is important that these functions maintain independence from the development organization. The independence of quality assurance, software safety, and verification and validation should be described in terms of management, schedule, and finance. If these independence aspects are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan or QA plan, the SMP should provide a pointer to the appropriate section of those plans.	Closed
39	Footnote 6; D.4.4.1 Software Management Plan (SMP)	Without an SPMP, the probability is high that…	Without an SMP, the probability is high that	Typo 'SPMP' for 'SMP'	Agree - Comment incorporated and Footnote move to Glossary.	Without an SMP, the probability is high that some safety concerns will be overlooked at some point in the project development period, that misassignment of resources will cause safety concerns to be ignored as deadlines approach and funds expire, and that testing will be inadequate.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
40	D.4.4.1 Software Management Plan (SMP)	The SMP should include sufficient information about the security requirements for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 and that the methods are used effectively. This needs to be an actual description of the security requirements enumerated in RG 1.152, and not just a statement that all security requirements will be met. The review of how those requirements are being met will be addressed in separate NRC guidance on this issue, as indicated in Section D.12.		Since Cyber-Security is now separated from Digital Security, this should be reworded for clarity. Regulatory Guide 5.71 vs. Regulatory Guide 1.152.	Agree RG 1.152 is bing revised to remove "cyber" considerations. Globally - Cyber has been removed from this ISG.	The SMP should include sufficient information about the secure environment for the reviewer to determine that the methods used are consistent with Regulatory Guide 1.152 and that the methods are used effectively. This needs to be an actual description of the secure environment described in RG 1.152, and not just a statement that all secure environment requirements will be met. The review of how those requirements are being met will be addressed in separate NRC guidance on this issue, as indicated in Section D.12.	Closed
41	D.4.4.1 Software Management Plan (SMP)	The adequacy of the budget and personnel for the quality assurance organization, the software safety organization, and the software verification and validation organization is of interest, and should ensure that those groups have adequate resources to support a high quality design effort. This will require some judgment, and it may require a justification by the licensee or vendor. In addition, software safety and V&V personnel		Guidance should not imply the need for separate software safety organization nor personnel.	See Comment No. 38.	(See "Final Text" of Comment No. 38 for the new text.)	Closed
42	D.4.4.2 Software Development Plan (SDP)	Software Configuration Management Plan (SCMP0,	Software Configuration Management Plan (SCMP),	Typo '(SCMP0' for '(SCMP)'	Agree	The NRC staff review of the software development is primarily intended to determine that use of the SDP results in a careful and deliberate process which will result in high quality software, suitable for use in safety-related systems in nuclear power plants. The details on how this will be done may be found in other plans, such as the Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP). If this is done, the SDP should provide pointers to the appropriate sections of those other plans.	Closed
43	D.4.4.2 Software Development Plan (SDP)	Coding standards should be compared to the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.	Coding standards should follow the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems".	New requirement imposed here.	Agree - Change "should be compared to" to "should follow". See also Coment No. 47.	Coding standards should follow the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.	Closed
44	D.4.4.2 Footnote 7 Software Development Plan (SDP)	Some of the topics that should be discussed in this plan were also listed for the SPM. The SPM document is directed at the project management personnel, so emphasizes the management aspects of the development effort.		Typo 'SPM' for 'SMP'.	Agree - Footnote moved to Glossary. Comment incorporated.	The Software Development Plan (SDP) provides necessary information on the technical aspects of the development project, that are used by the development team in order to carry out the project. Some of the topics that should be discussed in this plan were also listed for the SMP.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
45	D.4.4.2 Footnote 7 Software Development Plan (SDP)	The SDP will specify the life cycle that will be used, and the various technical activities that take place during that life cycle	The SDP will specify the life cycle model that will be used, and the various technical activities that take place during that life cycle	Missing the word 'model'	Agree - Footnot moved to Glossary. Comment incorporated.	The SDP will specify the life cycle model that will be used, and the various technical activities that take place during that life cycle. Methods, tools, and techniques that are required in order to perform the technical activities will be identified.	Closed
46	D.4.4.2 Software Development Plan (SDP)	...is that software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities.		Incomplete sentence partially copied from BTP 7-14.	Disagree - No change. Beginning of this sentence is on the previous page, before the footnote.	(no change)	Closed
47	D.4.4.2 Software Development Plan (SDP)	Coding standards should be compared to the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.		There are 432 pages in this NUREG/CR-6463. Justifying deviations goes well beyond regulatory precedence for NUREG compliance. Instead this should be replaced by the words used in the Oconee SER: "The Code Listing (CL) should have sufficient comments and annotations that the intent of the code developer is clear. This is not only so the reviewer can understand and follow the code, but also so future modifications of the code are facilitated. Undocumented code should not be accepted as suitable for use in safety-related systems in nuclear power plants. The documentation should be sufficient for a qualified software engineer to understand." It is not appropriate to use a NUREG/CR as a licensing standard or to impose requirements.	(See also Comment 43. Wording changed to add clarity. Disagree. While NUREG/CR-6463 may have many pages, NUREG/CR-6463 does not have to be read front to back. NUREG/CR-6463 has some general (informative material) and nine (9) laguage specific sections; only 20 to 70 pages are required to be read for any given language. For example, Section 11, "Function Block Diagrams," has 21 pages, and a three-page table in Appendix A that summarizes the guidance. Secton 2, "Generic Safe Programming Attributes," provides generic information in approximately 30 pages. While NUREGs do not impose requirements and thereby require compliance, they do provide NRC staff guidance on what is appropriate.	Coding standards should follow the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages for Use in Nuclear Power Plant Safety Systems." Any deviations from NUREG/CR-6463 should be identified in the LAR; all significant deviations should be explained.	Closed
48	Footnote 8; D.4.4.3 Software Quality Assurance Plan (SQAP)	For example, the section on code control may reference the Software Configuration Management Plan (SCMP), and describe the methods by which the SQA organization will ensure that this plan is followed.		There should be no implication that a separate SQA organization is required. SQA can be the responsibility of the overall QA organization.	Agree - No change. The guidance does not say that there shall be four organizations that are independent of each other. Rather it says that three of them be independent of the fourth. The guidance does not require that organizational entities with specific names exist, just that the organizational entities that perform certain functions have certain characteristics (e.g., QA is independent).	(See "Final Text" of Comment No. 38 for the new text.)	Closed
49	D.4.4.3 Software Quality Assurance Plan (SQAP)	The SQAP is one of the more important plans which will be reviewed by the staff. The staff reviewer will need to determine not only that the SQP exhibits		Typo 'SQP ' for 'SQAP'	Agree	The SQAP is one of the more important plans which will be reviewed by the staff. The staff reviewer will need to determine not only that the SQAP exhibits	Closed
50	D.4.4.3 Software Quality Assurance Plan (SQAP)	The software QA organization should be described in sufficient detail to show that there is sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised.		There should be no implication that a separate software QA organization is required. SQA can be the responsibility of the overall QA organization.	(See "NRC Comment / Disposition" of comment No. 48.)	(See "Final Text" of Comment No. 38 for the new text.)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
51	D.4.4.4 Software Integration Plan (SIntP)	The planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.		When a generic software program manual is used, it is typical to include the technical portion of the plan in the SPM, but resources, budgets, and schedules are included in project specific documentation. The ISG should acknowledge this method of documentation.	Agree - Words added to D.4.	In some cases an applicant has combined many of the generic aspects of the twelve plans, described in BTP 7-14, into a software program manual (SPM). In these cases project specific aspects (e.g., budget and schedule) have been described in project plans. These SPMs can be reviewed and approved independent of a specific project, and any approval will generally contain application specific action items to address project specific aspects.	Closed
52	D.4.4.4 Software Integration Plan (SIntP)	The software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. In the first phase, the various object modules are combined to produce executable programs. The second phase is when these programs are then loaded into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems, and instrumentation. The final phase consists of testing the results.	Delete footnote 9	Footnote 9 repeats the second paragraph text.	Agree - Comment incorporated and Footnote moved to Glossary.	Software Integration Plan (SIntP): Software integration actually consists of three major phases: (1) integrating the various software modules together to form single programs, (2) integrating the result of this with the hardware and instrumentation, and (3) testing the resulting integrated product. During the first phase, the various object modules are combined to produce executable programs. These programs are then loaded in the second phase into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems and instrumentation. The final phase consists of testing. Multiple levels of integration may be necessary, depending on the complexity of the software system that is being developed. Several integration steps may be required at some levels.	Closed
53	D.4.4.5 Software Installation Plan (SInstP)	The SIP should include the method by which these errors are identified, corrected, and documented, and should confirm that these corrections are subject to the same quality and configuration control as the rest of the system.		Typo 'SIP' for 'SInstP'	Agree	The SInstP should include the method by which these errors are identified, corrected, and documented, and should confirm that these corrections are subject to the same quality and configuration control as the rest of the system.	Closed
54	D.4.4.6 Software Maintenance Plan (SMaintP)	Omitted	It should be noted that the implementation of the maintenance plan will not be reviewed or commented upon in the staff SER. Licensee training is not a part of the licensing process. Instead, it falls under the regional inspection purview. The licensee should be prepared to support any regional inspections of the maintenance done in preparation for use of the proposed system prior to the system being put into operational use.		Text added to D.4.4.6	The Software Maintenance Plan will not be reviewed in the staff SE. Licensee maintenance are not a part of the licensing process, and therefore may be inspected by the regional inspectors. The licensee should be prepared to support any regional inspections of the maintenance plan prior to the system being put into operational use.	Closed
55	Footnote 11; D.4.4.6 Software Maintenance Plan (SMaintP)	Software maintenance is the process of correcting faults in the software product that led to failures during operation.	Software maintenance is the process of correcting faults in the software product before they lead to failures during operation.	Software faults are often corrected before they lead to failures. Fixing and enhancing things occur, after putting in service.	Agree - Footnote moved to Glossary. Wording modified.	Software maintenance is the process of correcting errors in the software product.	Closed
56	Footnote 11; D.4.4.6 Software Maintenance Plan (SMaintP)	The software maintenance plan describes three primary activities: reporting of failures that were detected during operation, correction of the faults that caused those failures, and release of new versions of the software product.	The software maintenance plan describes three primary activities: reporting of errors that were detected during operation, correction of the faults that caused those errors, and release of new versions of the software product.	Software 'failures' should be replaced by 'errors'.	Agree	The software maintenance plan describes three primary activities: reporting of errors that were detected during operation, correction of the errors that caused failures, and release of new versions of the software product.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
57	D.4.4.6 Software Maintenance Plan (SMaintP)	The Software Maintenance Plan should have some provisions for qualifying a new revision of the tool if the original version of the tool is no longer available.	The Software Maintenance Plan should have some provisions for determining acceptability of a new revision of the tool, if the original version of the tool is no longer available.	Change qualifying to "determining acceptability of" since the original tool may not have been qualified.	Agree	The Software Maintenance Plan should have some provisions for determining the acceptability of a new revision of the tool if the original version of the tool is no longer available.	Closed
58	D.4.4.6 Software Maintenance Plan (SMaintP)	In many instances, the software maintenance will be done by the original system vendor. In this case, two maintenance plans are required.	In many instances, the software maintenance will be done by the original system vendor. In this case, two maintenance plans may be required.	Both maintenance activities can be covered in the same plan.	Disagree - No change. Do not see how two plans would not be required.	(no change)	Closed
59	D.4.4.7 Software Training Plan (STrngP)	It should be noted that the implementation of the training plan will not be reviewed or commented upon in the staff SER. Licensee training is not a part of the licensing process. Instead, it falls under the regional inspection purview. The licensee should be prepared to support any regional inspections of the training done in preparation for use of the proposed system prior to the system being put into operational use.		"will not be reviewed" If this is the case, why is it submitted on the docket with the LAR (phase 1 submittal)?	Text changed per comment No. 1. Agree - Item removed from Enclosure B. Words added to D.4.4.7.	The software training plan will not be reviewed in the staff SE. Licensee training is not a part of the licensing process. Instead, it falls under the regional inspection purview. The licensee should be prepared to support any regional inspections of the training done in preparation for use of the proposed system prior to the system being put into operational use.	Closed
60	Footnote 11; D.4.4.7 Software Training Plan (STrngP)	The software training plan will describe the methods that will be used to train the operators of the software system.	The software training plan will describe the methods that will be used to train the users of the software system.	'users' for 'operators'	Agree - Text changed and moved to glossary.	The software training plan will describe the methods that will be used to train the users of the software system.	Closed
61	D.4.4.8 Software Operations Plan (SOP)	The Software Operations Plan is not intended describe how the software is intended be used; the requirements for how the software is intended to be used should be included in the design documentation so that the software can be designed for its intended use.		Conflicts with BTP 7-14 guidance and contradicts (1) BTP 3.8.1 which requires a description of operation and (2) BTP 3.8.1's footnote which requires an operations description. Too many 'intended'; 4 times in one sentence.	Agree - This plan will be reviewed in the same manner as this plan was reviewed in the Oconee RPS/ESPS upgrade LAR. These two sentences have been removed. Agree - Three "intended"s removed.	The Software Operations Plan will be reviewed for completeness, and therefore the plan needs to address all operations of the system and the plant after it is installed.	Closed
62	D.4.4.8 Software Operations Plan (SOP)	It should be noted that the implementation of the Software Operations Plan will not be reviewed or commented upon in the staff SER. Licensee operations are not a part of the licensing process, and therefore may be inspected by the regional inspectors. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.		"not a part of the licensing process " If this is the case, why is it submitted on the docket with the LAR (phase 1 submittal)?	Text changed per comment No. 1. Agree - Item removed from Enclosure B. Words added to D.4.4.8.	The Software Operations Plan will not be reviewed in the staff SE. Licensee operations are not a part of the licensing process, and therefore may be inspected by the regional inspectors. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.	Closed
63	Footnote 13; D.4.4.8 Software Operations Plan (SOP)	Start-up and shut-down of the computer system should be discussed. All communications between the computer system and the operator should be described, including the time sequencing of any extended conversations.		Replace software "operator" with "user". Since there may be many others who interface with the system, not just operators.	Agree - Footnote move to glossary. Text changed.	All communications between the computer system and the user should be described, including the time sequencing of any extended conversations.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
64	D.4.4.9 Software Safety Plan (SSP)	The Software Safety Plan should describe the boundaries and interfaces between the software safety organization and other company organizations. It should show how the software safety activities are integrated other organizations and activities. It should also designate a single safety officer that has clear responsibility for the safety qualities of the software being constructed.		Delete Software Safety Organization. Delete single safety officer. Oconee SER states:"AREVA NP Inc. does not have a dedicated software safety team and does not have a designated individual to be responsible for performing software safety activities other than the project technical manager who provides oversight for all of the project activities. Each software safety activity is the responsibility of the overall project organization. The software V&V organization is, however, tasked with specifically documenting and addressing the safety issues of the digital RPS/ESPS system."	See Comment No. 38.	(See "Final Text" for Comment No. 38.)	Closed
65	D.4.4.9.1 Safety Analysis	The safety analysis activities also includes the cyber security risk, and the methods used to ensure that the standards and procedures used ensure that the design products do not contain undocumented code, malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.		This ISG is by NRR. NRC NRR tells us they have no jurisdiction on review criteria for cyber security, yet it is included here. Security controls include tech, ops, and management controls Appendix C of RG 5.71; C-12 Configuration Management Appendix C of RG 5.71; C-12 Configuration Management Use Security controls instead of cyber risk	Agree - "Cyber" has been removed.	The safety analysis activities also includes the security risk, and the methods used to ensure that the processes used ensure that the design products do not contain undocumented code, malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.	Closed
66	D.4.4.10 Software Verification and Validation Plan (SVVP)	Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements. Combined, V&V is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.		Not the same definitions as IEEE 1012-1998 and IEEE Std 610.12-1990.	Do not understand the motivation for making such a comment. IEEE Std 1012-1998 is 73 pages long and describes verification and validation. This standard (in normative Annex I) includes a definition of both Verification and Validation; combined these two definitions should include all normative material in the standard. The intent of the text in this ISG was to clarify staff understanding; therfore because industry finds some of these words confusing, they have been removed.	Verification and Validation (V&V) is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.	Closed
67	D.4.4.10 Software Verification and Validation Plan (SVVP)	Per IEEE Std 1012-1995, the V&V team should be independent in management, schedule, and finance.	Per IEEE Std 1012-1998, the V&V team should be independent in management, schedule, and finance.	1998 version endorsed in RG 1.168 R1.	Agree - Comment incorporated.	Per IEEE Std 1012-1998, the V&V team should be independent in management, schedule, and finance.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
68	D.4.4.10 Software Verification and Validation Plan (SVVP)	The plan should specifically show how the V&V team is independent, and why the V&V personnel are not subject to scheduling constraints or to pressure from the software designers or project managers for reports or review effort.	The plan should specifically show how the V&V team is independent, and how the V&V personnel are not subject to scheduling constraints or to pressure from the software designers or project managers for reports or review effort.	There is no need to justify the need for independence; therefore, change "why" to "how".	Agree - Changed "why" to "how".	The plan should specifically show how the V&V team is independent, and how the V&V personnel are not subject to scheduling constraints or to pressure from the software designers or project managers for reports or review effort.	Closed
69	D.4.4.10 Software Verification and Validation Plan (SVVP)	In general, the SVVP needs to document how the requirements of IEEE 1012 will be meet, and for any IEEE 1012 requirement which is not being meet, what compensatory actions are being used to demonstrate an equivalent level of verification and validation.		RG 1.168 states, "IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," provides methods that are acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 as they apply to the verification and validation of safety system software, *subject to the exceptions* listed in these Regulatory Positions."	Agree - Propsed text added.	Regulatory Guide 1.168, "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants," Revision 1, endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed in these Regulatory Positions.	Closed
70	D.4.4.11 Software Configuration Management Plan (SCMP)	The Software Configuration Management Plan should specify how modified software or documentation should be tested and verified, and who is to do this.	Delete sentence	These are in the 'Software Validation & Verification Plan' and 'Software Test Plan', not the SCMP. Page 42 of BTP 7-14.	Agree - Paragraph has been removed.	(Removed)	Closed
71	D.4.4.11 Software Configuration Management Plan (SCMP)	The plant specific SCMP will not be reviewed and approved with the LAR, but may be subject to regional inspection of the system.		"will not be reviewed " If this is the case, why is it submitted on the docket with the LAR (phase 1 submittal)?	(See Comment No. 72): Disagree - No Change. The SCMP that will be docketed is the one that is used to manage the configuration while the software is being developed, not the one that is used to manage the configuration after it is installed in the plant.	(no change)	Closed
72	D.4.4.11 Software Configuration Management Plan (SCMP)	The Software Configuration Management Plan may be two different plans, one used by the software vendor during the development of the software, and one used by the licensee during the operational phase of the project.		This is true of all plans. A previous section implies there could be three different plans for each - vendor, licensee corporate office, & licensee plant. 3 referenced in D.4 Software Design Processes	Agree - No change proposed.	(no change)	Closed
73	D.4.4.12 Software Test Plan (STP)	The NRC staff will specifically be reviewing the test plan to ensure that the required V&V test is actually generated and performed by the V&V group, and not done by a design or test group, and merely checked by V&V personnel.		This is not consistent with the Oconee SER which states that the testing was developed and performed by the developers, but then independently verified by the Independent V&V team (Appendix B allows): "Instead, the functions of preparing test specifications and procedures and test scripts were assigned as responsibilities of the software engineers who may be members of the design and development organization. Test engineers are matrixed as members of the V&V organization during performance of the FAT activities. ...the IVV organization performed an acceptance review of the test specifications and procedures prior to release for performance. The NRC staff considers this to be an acceptable method for maintaining the independence of the V&V organization." ...and did not prepare the design to be a tester at Oconee...per Areva	Disagree - No Change. The Staff's position is that the normative material of IEEE Std 1012-1998 (as endorsed by RG 1.168 Rev. 1) is an acceptable way of meeting the regulations. IEEE 1012 requires that the testing be done by the V&V team. Exceptions may be appropriate on a case by case basis; significant additional effort was involved in reviewing the Oconee deviation form IEEE 1012.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
74	Footnote 19; D.4.4.13 Software Requirements Specification (SRS)	A hazard analysis of the safety system should be available.	Delete sentence	Oconee SER states: "Although no specific hazards analysis was performed for the digital RPS/ESPS, the cumulative effect of performing D3, Criticality, Failure Modes and Effects, and Response Time Analyses ensures the high degree of reliability necessary for safety-related software." Fix list in Appendix B to match.	Disagree - Hazard Analysis and Software Hazard Analysis are now defined in the glossary. The staff's position is that a Hazard Analysis should be done. Exceptions may be appropriate on a case by case basis. No change in Appendix B as explained above.	Software Hazard Analysis: eliminates or controls software hazards and hazards related to interfaces between the software and the system (including hardware and human components). It includes analyzing the requirements, design, code, user interfaces and changes. (NUREG/CR-6430, "Software Safety Hazard Analysis", describes a method for performing a software hazards analysis.)	Closed
75	D.4.4.13 Software Requirements Specification (SRS)	It should be noted that the NRC staff will not be able to completely review the SRS, but will only sample a limited number of requirements during the thread audit.		If the NRC staff does not plan to review the SRS, it does not need to be submitted. It should be made available only for audit.	Disagree - Wording changed to more clearly reflect the NRC position. The NRC does not perform design reviews, that is to say the NRC does not completely review design documents. The NRC performs a licensing review in accordance with LIC-101 and the SRP.	The NRC staff will not independently review the SRS, but will review the SRS against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit(s). The NRC staff will expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.	Closed
76	D.4.4.14 Software Architecture Design (SAD)	The SAD must explain how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software.		Software architecture may be generically described at the platform level; therefore, it should not need to be addressed again for each application.	Disagree. Each application has its own architecture, based on modules whose architecture were previously reviewd. Wording changed to clarify NRC position.	The SAD must explain how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software. This is further addressed in Section D.3, "Software Architecture." There may be SAD for both the platform and the application, if appropriate.	Closed
77	D.4.4.15 Software Design Specification (SDS)	It should be noted that the NRC staff will not be able to completely review the SDS, but will only sample a limited number of requirements during the thread audit (e.g., of software code listings).		If the NRC staff does not plan to review the SDS, it does not need to be submitted. It should be made available only for audit. Fix list in Appendix B to match.	Disagree - Wording changed to more clearly reflect the NRC position. The NRC does not perform design reviews, that is to say the NRC does not completely review design documents. The NRC performs a licensing review in accordance with LIC-101 and the SRP.	The NRC staff will not independently review the SDS, but will review it using the criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit(s). The NRC staff will expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software design by the V&V organization.	Closed
78	D.4.4.16 System Build Documents (SBDs)	It should be noted that the NRC staff will not be able to completely review the SBDs, but will only sample a limited number of requirements during the thread audit (e.g., of configuration management reports, final software integration report, and vendor build documentation).		If the NRC staff does not plan to review the SBD, it does not need to be submitted. It should be made available only for audit. Fix list in Appendix B to match.	Disagree - Wording changed to more clearly reflect the NRC position. The NRC does not perform design reviews, that is to say the NRC does not completely review design documents. The NRC performs a licensing review in accordance with LIC-101 and the SRP.	The NRC staff will not independently review the SBDs, but will review against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit(s). The NRC staff will, however, expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.	Closed
79	D.4.4.17 Installation Configuration Tables (ICT)	Any item that is changeable should have the intended configuration recorded in the Installation Configuration Tables, and the staff reviewer will sample these configuration items to verify that they are correct.		Sampling in the Installation Configuration Tables means it does not need to be submitted. It should be made available only for audit. Fix list in Appendix B to match.	Disagree - Wording changed to more clearly reflect the NRC position. The NRC does not perform design reviews, that is to say the NRC does not completely review design documents. The NRC performs a licensing review in accordance with LIC-101 and the SRP.	Any item that is changeable should have the intended configuration recorded in the Installation Configuration Tables. The NRC staff will not independently review the ICT, but will review against the acceptance criteria in BTP 7-14 and will sample a limited number of requirements during the thread audit(s). The NRC staff will, however, expect to find sufficient V&V documentation to show that there was a 100% verification and validation of the software requirements by the V&V organization.	Closed
80	D.4.4.18 Requirements Traceability Matrix	D.4.4.18 Requirements Traceability Matrix	D.4.4.18 Requirements Software Traceability Matrix	Add 'Software' to title	Disagree - No change.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
81	D.4.4.18 Requirements Traceability Matrix	The traceability should be possible both forwards and backwards, that is, the staff and the V&V teams should be able to take any requirement, and trace it through the SRS, SDS, and the actual code. Tracing backwards, it should be possible to take any portion of code and determine what requirement is responsible for that code.		Traceability starting point is functional requirement specification or any requirement from the licensing basis. Testing traceability should be added.	Agree	The licensee should ensure that the Requirements Traceability Matrix (RTM) is written such that each requirement and sub-requirement is traceable through the entire design process. The traceability should be possible both forwards and backwards, that is, the staff and the V&V teams should be able to take any requirement, and trace it through the SRS, SDS, the actual code, and test documentation. Tracing backwards, it should be possible to take any portion of code and determine what requirement is responsible for that code. One of the things this will be used for is to determine that there is no unnecessary code contained in the final product. Any application code which is not traceable back to a system or plant requirement is unnecessary, and should be removed.	Closed
82	Footnote 22; D.4.4.18 Requirements Traceability Matrix	This section states that a requirements traceability matrix, that needs to show every requirement, should be broken down in to sub-requirements as necessary.	This section states that a requirements traceability matrix needs to show every requirement and should be broken down in to sub-requirements as necessary.	Replace sentence for clarity.	Agree	See Comment No. 81.	Closed
83	D.4.4.18 Requirements Traceability Matrix	One of the things this will be used for is to determine that there is no unnecessary code contained in the final product.		The Oconee SER states: "The RTM reports were made available for NRC staff review during the two NRC staff audits." Thus, it should be clarified that the RTM is a living document that may be audited by the staff at any stage of the life cycle. It does not need to be submitted.	Disagree - No change. An RTM is mentioned several times in BTP 7-14 as SRP acceptance criteria, which per LIC-101 must be docketed. In many locations, IEEE Std 1012-1998 identifies traceability analysis as a V&V task; an RTM is one way to document this anslysis. It is believed that the RTM can be updated at the completion of every life cycle phase. This updating is what makes the RTM a living document. There are also many commercially-available software tools that support such analysis. It is also possible to make all documents both forward and backward traceable as defined by IEEE Std 830-1993 Clause 4.3.8 a) and b), as endorsed by RG 1.172.	(no change)	Closed
84	D.4.4.18 Requirements Traceability Matrix	Any application code which is not traceable back to a system or plant requirement is unnecessary, and should be removed.	Application code that is not traceable back to a system or plant requirement should be evaluated for its potential impact on safety functions.	Too prescriptive. Does not allow generic platform software with un-used parts. remove "and should be removed"	Disagree - No change. This is the existing guidance. BTP 7-14 states: "Correctness - One of the often overlooked aspects of correctness is simplicity. The system and specifically the software should be no more complex than required to perform the needed functions. Unused or unneeded functions and code should not be in the safety-related software, even if the software developer wishes to include them for ease of use, future development, or other reasons. The system and software requirements and the final code should be examined to insure that only those features need to implement the safety functions and to perform system and software testing are included."	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
85	D.4.4.19 Failure Modes and Effects Analysis (FMEA)	There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA, however IEEE Std 1228-1994 and MIL-Std-882B identify techniques which can be used for identifying hazards. Each system must be independently assessed to determine if the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures.		FMEA is used to demonstrate compliance with IEEE 379-2003, as endorsed by RG 1.53. IEEE Std 1228-1994 and MIL-Std-882b have not been endorsed by NRC.	Agree - FMEAs can be used for many purposes, one of with is to document a single failure analysis.	There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA. Each system must be independently assessed to determine if the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures. For example, an FMEA is a method for documenting a single failure analysis which is conducted in accordance with IEEE Std 379-2000 as endorsed by RG 1.53 Rev. 2.	Closed
86	D.4.4.19 Failure Modes and Effects Analysis (FMEA)	The FMEA is a method of analysis of potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure. The overall staff expectation is that each potential hardware and software failure will be identified, and the effect of that failure will be determined. For a complex system, this is expected to be a complex analysis. The key attribute which the staff will be reviewing is completeness, where all hardware and software failures are identified, and accuracy, where the analysis reaches an understandable reason for what the failure effect is for each failure mode. The FMEA is also used as an input to the diversity and defense in depth analysis.		It is wrong to state an expectation that each potential software failure be identified and its effect determined. If that were possible, then Software CCF could be eliminated and DAS would be unnecessary.	Agree	The FMEA is a method of analysis of potential failure modes within a system for determination of the effects on the system. This information can then be used to assess the potential for an undetectable failure. The overall staff expectation is that each potential hardware failure mode will be identified, and the effects will be determined. For a complex system, this is expected to be a complex analysis. The key attribute which the staff will be reviewing is completeness, where all failures are identified, and accuracy, where the analysis reaches an understandable reason for what the failure effect is for each failure mode.	Closed
87	D.4.4.19 Failure Modes and Effects Analysis (FMEA)	The overall staff expectation is that each potential hardware and software failure will be identified, and the effect of that failure will be determined.		There is no precedence for identifying potential software failures. Oconee SER states: "In the AREVA FMEA, software faults are characterized as being design errors that are introduced to the system during development activities. As such, software failures were not included as failure modes of the system. It is not practical to list and evaluate the impact of all possible software errors, so a software error that prevents the system from performing its safety function, when required, is postulated (see Section 3.9 of this SE). IEEE Std. 379-2000 specifically allows exclusion of design deficiencies from consideration. The effects of random external interactions that can affect memory values within the system were considered in the FMEA and were determined to be bounded by the propagation effect of either causing a spurious trip or lack of trip from the SVE2. Such a failure would result in an alarm indication and operator response is credited for the mitigation of such a failure."	See also comment No. 85 & 86. There is literature in the software development community that addresses using FMEAs to analyse software failures. Wording was modified to address nuclear industry specific comment and allow for the nuclear industry to follow accepted conventions in the software industry.	The overall staff expectation is that each potential failure mode will be identified, and the effects will be determined.	Closed
88	D.4.4.19 Failure Modes and Effects Analysis (FMEA)	The key attribute which the staff will be reviewing is completeness, where all hardware and software failures are identified, and accuracy, where the analysis reaches an understandable reason for what the failure effect is for each failure mode.	The key attribute which the staff will be reviewing is completeness, where all hardware failures are identified and where the analysis reaches an understandable reason for what the failure effect is for each failure mode.	Delete 'software' failures. Delete "and accuracy" or explain it. FMEA should also demonstrate that all failures are detectable.	Agree - See comment No. 86.	The overall staff expectation is that each potential failure mode will be identified, and the effects will be determined.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
89	Footnote 24; D.4.4.19 Failure Modes and Effects Analysis (FMEA)	FMEA is a systematic method of identifying the affects of single failures.		A software error is not a single failure, unless the error is caused by a hardware failure. Software errors are design errors. IEEE 379	Agree - No change. The stateement is true. An FMEA is a systemetic way of documenting the analysis of the effects of single failures.	(no change)	Closed
90	D.4.4.20 Operations Manual			It is not clear why the Staff needs this for review, since they require the SOP for review. It should be sufficient to make this available for audit.	Agree - Text added to D.4.4.20.	The Operations Manual will not be reviewed in the staff SER. Licensee operations are not a part of the licensing process, and therefore may be inspected by the regional inspectors. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.	Closed
91	D.4.5 Conclusion	The NRC staff will sample the design process actually used during the design of the software under review, with the intent of determining that the process described is the process that was used, and that the process was used was used correctly, and in such a manner as to produce high quality software suitable for use in safety-related applications at nuclear power plants.		If this “sample the design process” is the case, then why does the NRC require all the design information be docketed? Sample, implies audit; therefore, all software design documents identified in Table B should be re-categorized as "for audit".	Disagree - Wording changed to more clearly reflect the NRC position. The NRC does not perform design reviews, that is to say the NRC does not completely review design documents. The NRC performs a licensing review in accordance with LIC-101 and the SRP.	The NRC staff will need to find that the information describes a well-defined, disciplined process which will produce a high quality product. The NRC staff will also need to find that the V&V process described will provide acceptable analysis, evaluation, review, inspection, assessment, and testing of the products and processes. The NRC staff will review the design process information/documents produced during the development of the DSS. The NRC staff will also perform thread audits of the software under review, with the intent of confirming that the process described was the process that was used, and that the process was used correctly and in such a manner as to produce high quality software suitable for use in safety-related applications at nuclear power plants.	Closed
92	D.5 System Qualifications			D.5 duplicates D.9.4.2.4 IEEE 603 section should reference this section; purge D.9.2.4.2	Agree - No change. Comment does not affect meaning.	(no change)	Closed
93	D.5.1 Scope of Review	The system is tested with respect to a wide range of parameters including temperature, humidity, seismic, and electromagnetic.		Temp and humidity testing is not required for mild environments.	Agree	The system is tested with respect to a wide range of parameters, such as temperature, humidity, seismic, and electromagnetic, based on the environment in which the equipment is located.	Closed
94	D.5.2 Information to be Provided	Equipment Qualification Testing Plans Qualification Test Methodologies		‘Qualification Test Methodologies‘ should be included in ‘Equipment Qualification Testing Plans‘ (line before).	Agree. List removed due to prior comment.	Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee’s submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is adequately robust to perform its safety function within its design-basis normal and adverse environments. This information should be found in the equipment qualifications test plans, methodologies, and test reports. The results of the qualification testing should be documented in the summary. The information necessary to address the various aspects of environmental qualification are elaborated in Section D.5.4.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
95	D.5.2 Information to be Provided	Summaries of Final EMI, Temperature, Humidity, and Seismic Testing Results		Temp and humid testing is not required for mild environments. IEEE 323 states "For equipment located in a mild environment for meeting its functional requirements during normal environmental conditions and anticipated operational occurrences, the requirements shall be specified in the design/purchase specifications. ... The documents required to demonstrate the qualification of Class 1E equipment located in a mild environment are the design/purchase specifications, seismic test reports (if applicable), and an evaluation and/or certificate of conformance. The design/purchase specifications shall contain a description of the functional requirements for a specific environmental zone during normal environmental conditions and anticipated operational occurrences." Point to IEEE 323 or CFR50.49	Agree in part - Text changed to indicate that the equipment qualification summaries are required for the environment that the equipment is located in.	See final text for comment No. 94.	Closed
96	D.5.2 Information to be Provided	The results of the qualification testing should be documented in the summary of final EMI, temperature, humidity, and seismic testing.		Temp and humidity testing is not required for mild environments.	Agree in part - Text changed to indicate that the equipment qualification summaries are required for the environment that the equipment is located in.	See final text for comment No. 94.	Closed
97	D.5.3 Regulatory Evaluation	RG 1.89, Revision 1, that endorses and provides guidance for compliance with IEEE Std. 323-1974;		The correct reference for digital I&C is RG 1.209, which endorsed IEEE Std 323-2003.	Agree - Reference added.	RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses IEEE Std. 323-2003 subject to five enhancements and exceptions.	Closed
98	D.5.4 Technical Evaluation	The testing should include exposure to expected extremes of temperature, humidity, radiation, electromagnetic and radio interference, and seismic input.		Temp and humidity testing is not required for mild environments.	Agree in part - Text changed to indicate that the equipment qualification summaries are required for the environment that the equipment is located in.	See final text for comment No. 94.	Closed
99	D.5.4 Technical Evaluation	Prior to the performance of testing, the system shall be reviewed to identify any potential aging mechanisms. An aging mechanism is significant if in the normal and abnormal service environment, it causes degradation during the installed life of the system that progressively and appreciably renders the equipment vulnerable to failure. If the system has one or more significant aging mechanisms, preconditioning is required prior to testing to the degree that the mechanism is not accounted for by surveillances and maintenance. For example, if an aging mechanism exists and there is a surveillance performed to quantify the progress of the aging mechanism, the system should be preconditioned sufficient to account for the acceptance criteria of the surveillance plus the expected aging until the next performance of the surveillance.		This paragraph is very complicated. The Staff should provide real guidance on what they expect to be aged prior to qualification testing. Accept past precedence? Mechanical relays only (seismic testing only)?	Agree Disagree - The staff expects the aplicant to perform this review, and make this determination. Comment unclear.	Prior to the performance of testing, the system shall be reviewed to identify significant aging mechanisms. An aging mechanism is significant if in the normal or abnormal service environments, cause degradation during the installed life of the system (e.g., aging mechanisms that progressively and appreciably renders the equipment vulnerable to failure). If the system has one or more significant aging mechanisms, preconditioning is required prior to testing to the degree that the mechanism is not accounted for by surveillances and maintenance. For example, if an aging mechanism exists and there is a surveillance performed to quantify the progress of the aging mechanism, the system should be preconditioned sufficient to account for the acceptance criteria of the surveillance plus the expected aging until the next performance of the surveillance. Additional criteria pertinent to environmental qualification arereferenced in D.5.3.	Closed
100	D.5.4.1 Atmospheric	The system must be qualified in the most severe environment to which it will be exposed and is relied upon to perform its safety function.		Testing is not required for mild environments.	Disagree - No change. Statement is still applicable to all environments.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
101	D.5.4.2 Radiation	(i.e., it does not return to its original state up removal of the stressor)		Typo "up" for 'upon'	Agree	(i.e., it does not return to its original state upon removal of the stressor)	Closed
102	D.5.4.2 Radiation	… radiation exposure equivalent to the total dose expected during the system's service life should be applied as an aging mechanism.		There is no requirement in IEEE323 for radiation aging for mild environments--only for harsh environments.	Agree in part - Reference to RG 1.209 was added. This is reflecting existing guidance. As such, no new requirements are being imposed by the ISG. Exemptions for Mild environments would still be applicable as are GDC 4 criteria.	RG 1.209 dated March 2007 contains guidance regarding the significant differences between analog and digital technologies with respect to radiation. The system must be qualified in the most severe environment to which it will be exposed and is relied upon to perform its safety function.	Closed
103	D.5.4.2 Radiation	The information provided should provide adequate references to support this conclusion.		Historically there has been no radiation qualification for areas outside the containment. This guidance restates the obvious. OE shows no problems in mild environments. What is expected? This appears beyond the scope of a digital LAR.	Agree in part - Reference to RG 1.209 was added.	See "Final Text" of comment No. 102.	Closed
104	D.6.1 Scope of Review	The principle of defense-in-depth may be thought of as requiring a concentric arrangement of protective barriers or means that are sequentially challenged by the failure of a preceding system.		DI&C-ISG-02 already dismissed this explanation of concentric rings.	Disagree - No change. The industry response is a misinterpretation of ISG2. The principles of DinD are still valid. ISG 2 only provided an acceptable means of combining echelons of defense when certain conditions are met. "The RTS and ESFAS functions may be combined into a single digital platform if the criteria of Staff Positions 1 and 2 of this ISG are addressed."	(no change)	Closed
105	D.6.2 Information to be Provided	Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information, for example:		Delete ', for example:' D3 Analysis is a requirement not an example.	Disagree - Text has been revised to explain why the Enclosure is an example. Enclosure B is still just an example but the D3 analysis submittal is a requirement.	Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's D3 analysis submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is diverse and sufficiently robust against CCF.	Closed
106	D.6.2 Information to be Provided	Interim Staff Guidance DI&C-IGS-02.	Interim Staff Guidance DI&C-ISG-02.	Typo 'IGS' for 'ISG'	(see Comment 116): Agree	Globally - "ISG2" replaced by "DI&C-ISG-02"	Closed
107	D.6.2 Information to be Provided	A list of all manual operator actions credited for diversity. Detailed justification for operator actions with limited margin.	…and Interim Staff Guidance DI&C-ISG-05.	With the reference to operator actions, DI&C-ISG-05 should also be mentioned in this section.	Agree - A reference to ISG-5 has been added.	Refer to DI&C ISG-5 for further guidance on the use of manual operator actions.	Closed
108	D.6.2 Information to be Provided	using Branch Technical Position 7-19,	using Branch Technical Position 7-19, revision 5,		Agree - BTP 7-19 Rev. 6 is ML093490771.	Globally - "BTP 7-19" replaced by 'BTP 7-19 Rev. 6"	Closed
109	D.6.2 Information to be Provided	An analysis of the diversity of the system with respect to the six areas (human diversity, design diversity (hardware), software diversity, functional diversity, signal diversity, and equipment diversity) discussed in Section D.6.1.		This analysis is for the aggregate of I&C systems, not for any single system. There is no need to address diversity within a single system unless the diversity within that system is the only diversity credited.	Agree - It is recognized that NUREG/CR-6303 requires that the applicant analyze each postulated common-mode failure 9of the digital system) for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best estimate (using realistic assumptions) methods. Reference to BTP 7-19 Rev. 6 added. BTP 7-19 Rev 6 (ML093490771) Contains the latest guidance on D3.	...NRC staff will evaluate the licensee's proposed amendment using Branch Technical Position 7-19 Rev. 6 (ML093490771)...	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
110	D.6.2 Information to be Provided	An evaluation of all common elements or signal sources shared by two or more system echelons.		It is not clear why this is needed, since the analysis above (1st bullet) covers all CCFs.	(see Comment No. 111): Agree - The staff wants to understand the degree to which the echelons of defense have been merged or combined. I do agree that this should be a part of the D3 analysis however and agree that it may be removed. Relocate referenced item as a sub bullet of item 1	See Final Text for Comment No. 111	Closed
111	D.6.2 Information to be Provided	Identification of all interconnections between the RTS and ESFAS provided for system interlocks and justification that functions required by 10 CFR 50.62 are not impaired by the interconnection.		Agreed, the staff needs to know all interconnections, but the evaluation is covered by the AOO and PA analysis above.	(see Comment No. 110): Agree - Bulleted item moved. Relocate referenced item as a sub bullet of item 1.	An analysis of the diversity of the system with respect to the six areas (human diversity, design diversity (hardware), software diversity, functional diversity, signal diversity, and equipment diversity) discussed in Section D.6.1. o An evaluation of all common elements or signal sources shared by two or more system echelons. o Identification of all interconnections between the RTS and ESFAS provided for system interlocks and justification that functions required by 10 CFR 50.62 are not impaired by the interconnection.	Closed
112	D.6.2 Information to be Provided	A list of all manual operator actions credited for diversity.		Credited for coping with CCF, not diversity.	Agree	A list of all manual actions credited for coping with a common cause failure.	Closed
113	D.6.2 Information to be Provided	Detailed justification for operator actions with limited margin.	Detailed justification for operator actions.	Remove "with limited margin" Reference DI&C-ISG-05	Agree	Detailed justification for manual actions.	Closed
114	D.6.3 Regulatory Evaluation	As discussed in BTP 7-19, The NRC staff's review considered the following regulatory requirements:	As discussed in BTP 7-19, the NRC staff's review considered the following regulatory requirements:	Capitalization typo 'The' for 'the'	Agree	As discussed in BTP 7-19, the NRC staff's review considered the following regulatory requirements	Closed
115	D.6.3 Regulatory Evaluation			Most of this section simply repeats prior guidance; it adds no value. The staff should identify addition focus areas: · Demonstration that failures in credited non-safety systems will not impair normal safety functions, including remote shutdown. · Demonstration that any shared elements between safety and credited diverse systems are not subject to CCF.	Agree - No change. Part of what this ISG is trying to accomplish is to bring various review guidance from diferent sources into one place. As such much of the ISG does repeat existing guidance.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
116	D.6.4 Technical Evaluation	ISG-2 provides guidance to the NRC staff on performing an evaluation of the defense-in-depth and diversity of a digital I&C system. D.6.4.1 Adequate Diversity and Manual Operator Actions Section 1 of ISG-2 provides guidance to the NRC staff for reviewing the defense-in-depth and diversity of a digital I&C upgrade with respect to adequate diversity and manual operator actions. D.6.4.2 Branch Technical Position 7-19, Position 4 The NRC staff, in ISG-2, has recommended		For correctness use DI&C-ISG-02 throughout to avoid confusion with any non DI&C ISG-2.	(see Comment 106): Agree	Globally - "ISG2" replaced by "DI&C-ISG-02"	Closed
117	D.6.5 Conclusion	...staff will specifically address the positions in BTP 7-19 and ISG 2 to determine adequate diversity exists.		For correctness use DI&C-ISG-02 throughout to avoid confusion with any non DI&C ISG-2.	Agree - Comment incorporated throughout.	Globally - "ISG2" replaced by "DI&C-ISG-02"	Closed
118	D.7.1 Scope of Review	These reviews will be done by examination of the communication methods used, and comparing them to each staff position within ISG #4.		For correctness use DI&C-ISG-04 throughout to avoid confusion with any non DI&C ISG-4.	Agree	Globally - "ISG4" replaced by "DI&C-ISG-04"	Closed
119	D.7.1 Scope of Review	Omitted text		This section should clarify the extent of failures to be assumed in this evaluation. Add: Failures from interconnected systems should be limited to credible single failures as defined in IEEE 379. For example for D3 that Staff requires that we assume a CCF, even if it isn't credible. For this analysis are we to assume multiple spurious signals generated by non-safety systems, even if we demonstrate they are not credible. If so, how does this affect the current AOOs?	Disagree - No change. Any failure that would have the potential to affect a safety function would fall into the perview of this review. The ISG defines this as the criteria. If the failure of one channel could impair the safety function of a safety processor in another channel, then it is a credible single failure as is defined. The agency policy for software common cause failures (SWCCFs) is that they are credible and therefore the I&C systems must be designed to cope with (SWCCFs).	(no change)	Closed
120	D.7.2 Information to be Provided	Footnote 26: This report may include an ISG#6 compliance matrix.		For correctness use DI&C-ISG-06 throughout to avoid confusion with any non DI&C ISG-6.	Agree	Globally - "ISG6" replaced by "DI&C-ISG-06"	Closed
121	D.7.2 Information to be Provided	This documentation should also show where in the documentation of design details this compliance can be verified. Submission of this document is not absolutely required, but since the NRC staff will then have to do this verification themselves, submission of this document will have the effect of reducing the time and effort required for NRC staff review.		"Submission of this document is not absolutely required" - Why not? This conflicts with itself. Nothing here is absolutely required in guidance. Just add that it can be part of FMEA or other hazard analysis documentation.	Agree - The sentences identified have been deleted.	The information needed by the NRC staff to reach a determination of adequate data isolation should be contained in the system, hardware and software specifications, architecture, and descriptions. Depending on the complexity of the proposed communications, the NRC staff may also have to examine the actual circuitry as described in the final circuit schematics and in the software code listings, and in detailed system and hardware drawings. The licensee should provide documentation on how each clause in DI&C-ISG-04 has been met, or what alternative is proposed when an individual clause is not meet.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
122	D.7.3 Regulatory Evaluation	Additional Guidance on interdivisional communications is contained in ISG-4, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML072540138).	Additional Guidance on interdivisional communications is contained in DI&C-ISG-04, "Highly-Integrated Control Rooms – Communication Issues, revision 1," (ADAMS Accession No. ML083310185).	Correct ADAMS reference for DI&C-ISG-04 R1 is ML083310185.	Agree	Additional Guidance on interdivisional communications is contained in DI&C-ISG-04 Rev. 1, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML083310185).	Closed
123	D.8.1 Scope of Review	This review area describes how the NRC staff determines the significance of deviations from previously approved systems, hardware, software, or methodologies.		This section should identify and analyze change that would affect previously approved LARs, SEs, or TRs (excluding other docketed material).	Agree - No change. This is generally application specific. LIC-101 (LIC-101 Revision 3, "Licese Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.2, "Using Precedent Safety Evaluations & References to Topical Reports,") states: "If a licensee in their application or the NRC staff during its review identifies a deviation from the process or limitations associated with a topical report, the staff should address the deviation in its SE for the plant-specific license amendment application."). 10 CFR 50.59 does not aply to topical reports and there is currently no screen criteria for changes to topical reports.	(no change)	Closed
124	D.8.2 Information to be Provided	The information provided should identify any and all deviations to the system, hardware, software, or design lifecycle methodology from a previous NRC approval of a digital I&C system or topical report.		Examples should be provided to clarify the use of the criteria for determining what should and should not be reported.	Agree - No change. The NRC is considering this under a separate venue. DI&C-ISG-06, "Licensing Process," may be revised at a later date to reflect this process.	(no change)	Closed
125	D.8.2 Information to be Provided	Completion of this review will essentially result in an update of the previous digital I&C system; however, for topical reports (TRs), it is strongly encouraged that the updated TRs be submitted for approval before a LAR is submitted referencing the TR.		Using LIC-109, the Staff will reject an application that references an unapproved TR. The TR and LIC-109 processes together are unworkable to support evolving technology. It takes too long to get a TR approved and it is likely to be out-of-date (when controlled at the HW/SW version level) before an LAR can be assembled to reference it and a digital system built.	Disagree - The approval of an updated topical report (TR) will not require near as much NRC staff effort and time as was required to approve the original TR. An updated TR is currently under review by the NRC staff and the level of effort required to approve this TR is expected to be approximately one quarter of that for the original TR.	(no change)	Closed
126	D.8.4 Technical Evaluation	The NRC staff considers significant changes to hardware such as a new microprocessor requiring re-compiling of software, changes in software which would modify the software design description, or changes in methods which would result in a different way of complying with regulatory guidance, even if the licensee or vendor believes the change will continue to comply with regulatory requirements to be major. The NRC staff assumes that if the licensee or vendor believes the change would result in the new system, hardware, software, or design lifecycle methodology would not meet regulatory requirements, the change would not have been made. In each of these instances discussed above, the new documentation should be submitted to the NRC staff for review. Additionally, the licensee should justify how the pertinent features of the subject plant conform to those of the existing approval.		This is more restrictive control criteria than either 10CFR50.59 or 10CFR52.63(b).	(see Comment 123): Disagree - No change. Part 50 and Part 52 are different licensing processes, and connot be compared directly. Also to properly evaluate replacement digital safety systems (DSS) under 10CFR50.59 the extent of its hardware and software and design lifecycle methodology should be evaluated in the 50.59 safety evaluation to determine that the new DSS still conforms with the existing approval SER. Otherwise, the DSS modification should be submitted as a LAR for staff approval. NEI 01-01 provides guidance and recomended practices for performing these type of reviews.	See "Final Text" of comment No. 26.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
127	D.9.2 Information to be Provided	… for example: Design Analysis Report Design Report on Computer Integrity, Test and Calibration, and Fault Detection Theory of Operation Description Software QA Plan System Description Quality Assurance Plan for Digital Hardware Safety Analysis System Test Plan Final Design Description Final Logic Diagrams Reliability Analysis Final Factory Acceptance Test Reports Installation Test Plans and Methodologies Operation Manuals Summary of Test Results		Make list accurate or eliminate list. FMEA not in list. 'Final' anything is ridiculous. 'FAT Reports' are not required for regulatory compliance determination. 'Installation Test Plans' should only be required if tests after installation are credited for validation testing, i.e., cannot test in the factory, only at site.	Agree - List eliminated. Text references Enclosure B.	D.9.2 Information to be Provided Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system meets the requirements of IEEE Std. 603-1991. To assist the NRC staff in making the determination that the licensee submittal meets the requirements of IEEE 603, the licensee may submit a document showing where within the other documentation submitted the confirmatory information can be found. While this is not an absolute requirement, it will result in a faster review requiring less NRC staff time. The information necessary to address the various clauses of the standard are elaborated in Section D.9.4.	Closed
128	D.9.4.1.5 IEEE 603-1991, Clause 4.5, Criteria for manual protective actions	Additionally, ISG-5 addresses this issue.		For correctness use DI&C-ISG-05 throughout to avoid confusion with any non DI&C ISG-5.	Agree - Comment incorporated throughout.	Globally - "ISG5" replaced by "DI&C-ISG-05"	Closed
129	D.9.4.2.1 IEEE 603-1991, Clause 5.1, Single Failure Criterion	Guidance in the application of the single-failure criterion is provided in RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std. 379-1988, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."		RG 1.153, revision 2 endorses IEEE Std 379-2000.	Agree - The IEEE standard referenced by RG 1.53 will be corrected.	RG 1.53 Rev. 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std. 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."	Closed
130	D.9.4.2.1 IEEE 603-1991, Clause 5.1, Single Failure Criterion	This is addressed further in Section D.6 and ISG-4.		This should be DI&C-ISG-02 "Diversity and Defense-in-Depth Issues", revision 2 (ML091590268)	Agree	This is addressed further in Section D.6 and DI&C-ISG-02.	Closed
131	D.9.4.2.4 IEEE 603-1991, Clause 5.4, Equipment Qualification	Regulatory Guide 1.89 Revision 1, endorses guidance for compliance with IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." And Mild environment qualification should conform with the guidance of IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."		The correct reference for digital I&C is RG 1.209, which endorsed IEEE Std 323-2003.	Agree	Globally - reference to RG 1.89 change to RG 1.209. "323-1974" changed to "323-2003".	Closed
132	D.9.4.2.4 IEEE 603-1991, Clause 5.4, Equipment Qualification	Regulatory Guide 1.151 addresses review of mild environment qualifications. The reviewer should also confirm that the environmental protection of instrument sensing lines is addressed.	Regulatory Guide 1.151 addresses review of mild environment qualifications. The RG may be used to ensure that the environmental protection of instrument sensing lines is addressed.	Reworded to apply to submitter and reviewer.	Agree	Regulatory Guide 1.151 dated July 1983, "Instrument Sensing Lines," may be used to ensure that the environmental protection of instrument sensing lines is addressed.	Closed
133	D.9.4.2.6.3 IEEE 603-1991 Clause 5.6.3, Other Systems	The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1981.		RG 1.75 Revision 3 endorses IEEE Std 384-1992.	Agree	Gobally - "384-1981" changed to "384-1992" in several places.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
134	D.9.4.2.8 IEEE 603-1991, Clause 5.8, Information Displays	… of IEEE Std. 479-1981	… of IEEE Std. 497-1981	Typo '479' for '497'	Agree	IEEE Std. 497-1981	Closed
135	D.9.4.2.8 IEEE 603-1991, Clause 5.8, Information Displays	Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions will be part of the safety systems and will meet the requirements of IEEE Std. 479-1981.		A better way to describe this is that licensees need to meet their licensing basis commitments using RG 1.97.	Disagree - RG 1.97 does not state that it addresses Clause 5.8.1. IEEE 603 Clause 5.8.1 includes instrumentation to avoid or prevent accidents. RG 1.97 applies to post accident monitoring instrumentation (PAMI), and provides guidance for this instrumentation as required by associated Post-TMI action plans. Paragraph wording revised to clarify.	Clause 5.8.1 requires that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions will be part of the safety systems. The design should minimize the possibility of ambiguous indications.	Closed
136	D.9.4.2.11 IEEE 603-1991 Clause 5.11, Identification	…of a safety system in accordance with IEEE Std. 384-1981		RG 1.75 Revision 3 endorses IEEE Std 384-1992.	See comment No. 133.		Closed
137	D.9.4.2.11 IEEE 603-1991 Clause 5.11, Identification	…and IEEE Std. 420-1982. Further, the safety system equipment must be distinguishable from any identifying markings placed on the equipment for other purposes, that the identification methods not require the frequent use of reference materials (i.e., be "user friendly"), and that the associated documentation be distinctly identified in accordance with IEEE Std. 494-1974 (R1990).		NRC has not endorsed either IEEE Std 420 or IEEE Std 494. Neither should be imposed as expectations here.	Agree	Globally - Reference to standards that have not been endorsed have been removed.	Closed
138	D.9.4.2.11 IEEE 603-1991 Clause 5.11, Identification			This paragraph should identify what documentation needs to be marked "nuclear safety related". It should provide guidance as to what is the appropriate level of identification?	Agree - No change. This clause contains requirements on the safety system, not identification requirements for documentation. Caluse 5.11 of IEEE 603 implies all "associated documentation" be distinctly identified. It is generally required (by all Appendix B compliant QA programs) that all design inputs to safety-related documentation be safety-related or verified; therefore, one must be able to identify which documents or information is safety-related or verified. Traditionally this is done by some textual means on the front of the document. These requirements are not specific to DSS and therefore are not addresed in this ISG.	(no change)	Closed
139	D.9.4.2.11 IEEE 603-1991 Clause 5.11, Identification	Further, the safety system equipment must be distinguishable from any identifying markings placed on the equipment for other purposes, that the identification methods not require the frequent use of reference materials (i.e., be "user friendly"), and that the associated documentation be distinctly identified in accordance with IEEE Std. 494-1974 (R1990).		At platform level, 10% of vendor material goes out of shop to customer. Limit 'nuclear safety items' to items sent to customer. Identification should be application dependent: safety vs. non-safety	See comment No. 138.	(no change)	Closed
140	D.9.4.2.13 IEEE 603-1991 Clause 5.13, Multi-Unit Stations	…contained in IEEE Std. 308-1980		RG 1.32 Revision 3 endorses IEEE Std 308-2001.	Agree - The IEEE standard referenced by RG 1.32 have been corrected.	Guidance on the sharing of electrical power systems between units is contained in RG 1.32 Revision 3, "Criteria for Power Systems for Nuclear Power Plants," which endorses IEEE Std. 308-2001, and guidance on application of the single-failure criterion to shared systems is contained in RG 1.53 Rev. 3 IEEE Std. 379-2000.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
141	D.9.4.2.13 IEEE 603-1991 Clause 5.13, Multi-Unit Stations	… contained in IEEE Std. 379-1988		RG 1.153 Revision 2 endorses IEEE Std 379-2000.	Agree - The IEEE standard referenced by RG 1.153 have been corrected.	Guidance on the sharing of electrical power systems between units is contained in RG 1.32 Revision 3, "Criteria for Power Systems for Nuclear Power Plants," which endorses IEEE Std. 308-2001, and guidance on application of the single-failure criterion to shared systems is contained in RG 1.53 Rev. 3 IEEE Std. 379-2000.	Closed
142	D.9.4.2.14 IEEE 603-1991 Clause 5.14, Human Factors Considerations	…in accordance with IEEE Std. 1023-1988.		NRC has not endorsed IEEE Std 1023 and it should not be imposed as an expectation here.	Agree - Reference to standards that have not been endorsed have been removed.	Clause 5.14 requires that human factors be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operators and maintainers can be successfully accomplished to meet the safety system design goals. The information provided should also be sufficient to demonstrate that the guidance contained in DI&C-ISG-05 has been met.	Closed
143	D.9.4.2.15 IEEE 603-1991 Clause 5.15, Reliability	The information provided should include a detailed Failure Modes and Effects Analysis and a reliability analysis in accordance with IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," and IEEE Standard 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities."		NRC has not endorsed either IEEE Std 352 or IEEE Std 577. Neither should be imposed as expectations here.	Agree - Sentence has been removed.	Clause 5.15 requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. The information provided should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is...	Closed
144	D.9.4.3.2 IEEE 603-1991 Clause 6.2, Manual Control	RG 1.62 provides further guidance on this topic.		This guidance must match RG 1.62, "Manual Initiation of Protective Actions", which is in state of flux in spring of 2010. This guidance should not guess on what it might say here. What needs to be submitted or available-for-audit (hardware architecture schematic and system description/requirements) should be clarified.	Disagree - No change. There is currently an approved version of RG 1.62. Also, the new version of RG 1.62 is available. DG-1190 (ML080720443).	(no change)	Closed
145	D.9.4.3.2 IEEE 603-1991 Clause 6.2, Manual Control	It is important to note that the manual control required by Clause 6.2 is different from a manual action which may be used as an acceptable diverse actuation required by BTP 7-19 as defense against common cause software failure (CCSF). The manual initiation and indicators to tell the operator when to use the manual initiation required by Clause 6.2 are required to be at a system level and safety-related. These controls may not be the ones used in the event of CCSF, and therefore the CCSF controls should be independent and therefore downstream of the digital portion of the safety system. The SRM to SECY 93-087, as reflected in BTP 7-19, has the requirement for diverse automatic or manual controls in the event of CCSF. The CCSF manual controls may be system level or component level, and may be non-safety, but must be independent of any CCSF, and therefore downstream of any digital portion of the digital safety system. It is possible for one set of manual controls to meet both of these requirements, by making those controls safety-related, system level, and downstream of any digital portion of the safety system.		Consider eliminating this paragraph. This paragraph should reflect the resolution of public comments on DG-1190. This conflicts with DG-1190 contents discussed with ACRS. Adequate guidance will be in RG 1.62 - method of compliance of IEEE 603. This introduces new concept: diversity not required to meet requirements in IEEE 603.	Disagree - No change. This paragraph is pointing out the an interesting way of meeting the regulations. A safety-related system-level manual actuation is required by IEEE Std 603-1991 Clause 6.2. RG 1.62 may allow this manual control to be a input into the computer system. Then another nonsafety-related manual control may be required by D3. However, this paragraph has been revised to clarify this.	The manual control required by Clause 6.2 is different from a manual action which may be used as an acceptable diverse actuation required by BTP 7-19 Rev. 6 (ML093490771), as defense against common cause software failure (CCSF). The manual initiation and indicators to tell when to use the manual initiation required by Clause 6.2 are required to be at a system level and safety-related. These controls may or may not be the ones used in the event of CCSF (due to the design of these manual controls and their susceptibility to CCF), and therefore the CCSF controls should be independent and therefore downstream of the digital portion of the safety system. The SRM to SECY 93-087, as reflected in BTP 7-19 Rev. 6 (ML093490771), has the requirement for diverse automatic or manual controls in the event of CCSF.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
146	D.9.4.3.4 IEEE 603-1991 Clause 6.4, Derivation of System Inputs	Further, for both direct and indirect parameters, the characteristics of the instruments that product the safety system inputs, such as range, accuracy, resolution, response time, and sample rate.	Further, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate.	Typo 'product' for 'produce'	Agree	Further, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate.	Closed
147	D.9.4.3.5 IEEE 603-1991 Clause 6.5, Capability for Testing and Calibration	Clause 6.5 requires that is must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, including the availability of each sense and command feature required during the post-accident period.	Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, including the availability of each sense and command feature required during the post-accident period.	Typo 'is' for 'it'	Agree	Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, including the availability of each sense and command feature required during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for Clause 6.5. The information provided should confirm that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. Additionally, when only two channels of a readout are provided, the information provided must justify why it is expected that an operator will not take incorrect action if the two channel readouts differ.	Closed
148	D.9.4.4 IEEE 603-1991, Clause 7, Execute Features	In addressing clauses 7.1 through 7.5, the additional considerations should be taken into account:	Delete	Sentence unnecessary.	Agree - Sentence deleted.	(Sentence deleted.)	Closed
149	D.10.2 Information to be Provided	Commercial Grade Dedication Plan Commercial Grade Dedication Report Design Analysis Report Design Report on Computer Integrity, Test and Calibration, and Fault Detection Theory of Operation Description System Description Reliability Analysis Vendor Software Plan Software Development Plan Software Installation Plan Software Integration Plan Software Maintenance Plan Software Management Plan Software Operations Plan Software Project Risk Management Program Software Safety Plan Software Test Plan Software Tool Verification Program Software Training Plan Software V&V Plan Software Configuration Management Plan Commercial Grade Dedication Report Final System Configuration Documentation Software Project Risk Management Report System Test Procedures Software Test Procedures V&V Reports		This list exceeds the list of documents submitted in support of the Oconee RPS/ESPS LAR review. As reported in the trade press: In an August 27 meeting on a future Diablo Canyon digital I&C amendment, the NRC said it had not "specifically requested" over 25,000 pages of supporting information to be submitted on the docket, but the information it was looking for was simply "buried in lengthy documents that were submitted in whole." To satisfy the NRC's information needs, Duke had submitted numerous supplements to its January 31, 2008 submittal. NRC required the submission of these documents in the same manner as specified here. The submission creates another document management problem. Since the design is moving through a software development lifecycle, the can be revised multiple times as the design progresses. NRC required that subsequent revisions be submitted on the docket, upping document page count. Up to this point the guidance requires individual 'design analysis reports' (e.g., P.40 - Communication, P. 42 - Modifications, etc.). An explanation/clarification of the content of this item (Design Analysis Report) in this list is necessary.	Agree - List eliminated. Text references Enclosure B.	D.10.2 Information to be Provided Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is consistent with IEEE Std. 7-4.3.2-2003. The information necessary to address the various clauses of the standard are elaborated in Section D.10.4.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
150	D.10.3 Regulatory Evaluation	While compliance with IEEE Std. 7-4.3.2 is not required by regulation, it is a defacto standard used by the NRC staff in evaluating digital I&C upgrades and is endorsed by RG 1.152 Rev. 2 dated 2003.	While compliance with IEEE Std. 7-4.3.2 is not required by regulation, it is the Standard used by the NRC staff in evaluating digital I&C upgrades and is endorsed by RG 1.152 Rev. 2 dated 2003.	It is the Standard; not 'defacto'.	Agree - text revised to clarify.	D.10.3 Regulatory Evaluation While IEEE Std. 7-4.3.2 is not codified in 10CFR50.55a, it is the principal standard used by the NRC staff in evaluating digital I&C upgrades and is endorsed by RG 1.152 Rev. 2 dated 2003 (i.e., RG 1.152 & IEEE 7-4.3.2 are SRP acceptance criteria). To demonstrate conformance with another standard in lieu of IEEE Std. 7-4.3.2, the licensee should include an evaluation that allows the NRC staff to conclude that conformance provides reasonable assurance of a high quality system. This activity should be expected to take a significant amount of additional review time and effort.	Closed
151	D.10.4.2.3.1 IEEE 7-4.3.2, Clause 5.3.1, Software development	SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff will used when assessing the quality criteria of this clause.	SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff will use when assessing the quality criteria of this clause.	Typo 'used' for 'use'.	Agree	SRP BTP 7 14 describes the characteristics of a software development process that the NRC staff will use when assessing the quality criteria of this clause.	Closed
152	D.10.4.2.3.1 IEEE 7-4.3.2, Clause 5.3.1, Software development	IEEE Std. 1061-1998 discusses software quality metrics methodology and methods by which various metrics systems can be evaluated.		NRC has not endorsed IEEE Std 1061 and it should not be imposed as an expectation here.	Agree in part - No change. IEEE Std 1061-1998, "IEEE Standard for Software Quality Metrics Methodology," is referenced in both SRP Chapter 7 BTP 7-14 and Appendix 7.1-D.	(no change)	Closed
153	D.10.4.2.3.1 IEEE 7-4.3.2, Clause 5.3.1, Software development	The metrics methodology should use diverse software measures that appropriately aggregate the measurement data to provide a quantitative assessment of the quality of the outputs. This recommends but does not require the use of software quality metrics. If metrics are used to justify software quality, the licensee must demonstrate how those metrics actually measure software quality, and how use of the metrics will demonstrate that the quality requirements of 10 CFR Appendix B are being met.		The first paragraph implies software metrics are required and the next says not required. Conflicts. What is a diverse metric? Why is it needed? This is a repeat of Software Quality earlier; no metrics mentioned there. If expected, then it should be in BTP 7-14 section too.	Disagree - No change. RG 1.152 endorses IEEE 7-4.3.2 as an acceptable way of meeting the regulations. Disagree - No change. The meaning of diverse used here is similar to the meaning used in BTP 7-19. Disagree - No change. BTP 7-14 does mention metrics and measures, as does RG 1.152 and RG 1.74.	(no change)	Closed
154	D.10.4.2.3.2 IEEE 7-4.3.2, Clause 5.3.2, Software tools	The tools shall either be developed to a similar standard as the safety-related software or the tool shall be used in a manner such that defects not detected by the tool will be detected by V&V activities.		The original software may undergo full V&V, but copies made by the tool will not. This section should address the level of qualification needed for replication by tools after V&V.	Disagree - Even if the a tool is qualified to copy software correctly, a human can make an error in the use of the tools; therefore, copies need to be checked either way. Qualification of a tool to perform copying may be able to reduce the degree of checking of the copy.	(no change)	Closed
155	D.10.4.2.3.2 IEEE 7-4.3.2, Clause 5.3.2, Software tools	If, however, it can not be proven that defects not detected by software tools or introduced by software tool will be detected by V&V activities, the software tool should be designed as Appendix B quality software itself, with all the attendant regulatory requirements for software developed under an Appendix B program.	If software tool cannot be demonstrated with reasonable assurance, the software tool should be designed...	Very awkward language. Forces tools to be safety-related qualified.	Disagree - No change. It is clear. The guidance does not require tools to be safety related, but does require that they be developed to same standards if their output is unverifiable.	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
156	D.10.4.2.3.3 IEEE 7-4.3.2, Clause 5.3.3, Verification and validation	It should be noted that review of the V&V plan, and the determination that the V&V effort meets regulatory requirement is one of the most significant part of the NRC staff review of the design life cycle, and therefore will receive a through review.	It should be noted that review of the V&V plan and the determination that the V&V effort meets regulatory requirements is one of the most significant part of the NRC staff review of the design life cycle, and therefore will receive a thorough review.	Typo 'requirement' for 'requirements'. Typo 'through' for 'thorough'	Agree	Review of the V&V plan, and the determination that the V&V effort meets regulatory requirements is one of the most significant part of the NRC staff review of the design life cycle, and therefore will receive a thorough review. It should also be noted that the V&V testing should be described in the system and software test plans, and the results of this testing should be contained in the final test reports. The NRC staff will review these test plans and associated documentation to ensure that the testing done was adequate to support the V&V effort, and meets the requirement of RG 1.168 and IEEE Std. 1012.	Closed
157	D.10.4.2.3.3 IEEE 7-4.3.2, Clause 5.3.3, Verification and validation	As described in section D.4.4.10 of this ISG, the licensee will need to submit the V&V plan actually used during the development of the platform and the applications software. If the V&V effort used documents which are not included as part of the V&V plan, those documents must also be submitted for NRC staff review.	As described in section D.4.4.10 of this ISG, the licensee will need to submit the V&V plan actually used during the development of the platform and the applications software. If the V&V effort used documents which are not included as part of the V&V plan, those documents must be available for NRC audit.	The V&V plan is likely to reference procedures that are not part of the plan and not submitted. SPM has all plans that reference procedures that may NOT be submitted. This implies submit all procedures. Delete sentence or say: ...must be available for NRC audit.	Disagree - Text revised to calrify. LIC-101 Revision 3, "Licensee Amendment Review Procedures," Appendix B, "Guide for Processing License Amendments," Section 4.0, "Safety Evaluation," states: "Given that the SE serves as the record of the staff's disposition of a license amendment request, the information relied upon in the SE must be docketed correspondence."	As described in section D.4.4.10 of this ISG, the licensee will need to submit the V&V plan (which is consistent with NRC endorsed standards) actually used during the development of the platform and the application software. If the V&V effort used documents which are not included as part of the V&V plan (i.e., V&V planning activities are contained within other documents), those documents must also be submitted for NRC staff review.	Closed
158	D.10.4.2.3.5 IEEE 7-4.3.2, Clause 5.3.5, Software configuration management	The reviewer of the software configuration management system should evaluate that the system used by both the vendor and the licensee ensures that any software modifications during the design process and after acceptance of the software for use will be made to the appropriate version and revision of the software.	The software configuration management system should be evaluated to ensure that the system used by both the vendor and the licensee ensures that any software modifications during the design process and after acceptance of the software for use will be made to the appropriate version and revision of the software.	Reworded to apply to submitter and reviewer.	Agree	The reviewer of the software configuration management system should evaluate that the system used by both the vendor and the licensee ensures that any software modifications during the design process and after acceptance of the software for use will be made to the appropriate version and revision of the software. This will involve not only a review of the Software Configuration Management documentation, but also a review of the actual methods being used at both the vendor and licensee facilities, to ensure that the methods discussed in the plans are properly implemented.	Closed
159	D.10.4.2.3.5 IEEE 7-4.3.2, Clause 5.3.5, Software configuration management	There may be two different software configuration management programs to evaluate, that being used by the software vendor during the design process, and that used by the licencee after the software has been delivered and installed in the nuclear power plant. Both of these programs should be evaluated.		Typo 'licencee' for 'licensee' There could be more than two, since configuration management of the Basic Software and Application Software may be unique: Configuration management of platform, application, customer, etc.	Agree	There may be two or more different software configuration management programs to evaluate, that being used by the software vendor(s) during the design process, and that used by the licensee after the software has been delivered and installed in the nuclear power plant. All of these programs should be evaluated.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
160	D.10.4.2.3.6 IEEE 7-4.3.2, Clause 5.3.6, Software project risk management	Software project risk management differs from hazard analysis.		"Software project risk management" is new; not described. Text only says what it is not. 'Software project risk management' could be commercial information that is not shared. Guidance to limit to process of planning and managing risk would work without listing risks. Part of software design process D.4.4.1 (SMP) already; not necessary here.	Disagree - No change. BTP 7-14 uses the word "risk" 43 times (e.g., "A.3.1.1 Definition of Management Characteristics .... Risks - The method used to identify, assess and manage risks that may interfere with achieving the purpose of the planning document."). ("risk" is also in IEEE 7-4.3.2, which was endorsed by RG 1.152.) The NRC is very careful to ensure that all proprietary materail is not compromized. This comment conflicts with the second comment.	(no change)	Closed
161	D.10.4.2.3.6 IEEE 7-4.3.2, Clause 5.3.6, Software project risk management	The software and hardware safety plan addresses the identification, evaluation and resolution of hazards.		'hardware safety plan' is not identified; it is a new term. Eliminate words 'and hardware safety plan'	This section addresses software project risk management, which is different than hazard analysis; therefore, most material regarding hazard analysi has been removed. Only one statement remains that state that risk management is not hazard analysis.	Clause 5.3.6 defines the risk management activities required for a software project. Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems should be addressed to assure that software quality goals are achieved. Risk management should be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety-related functions. Risk factors that should be addressed include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of pre-developed software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.). Software project risk management differs from hazard analysis.	Closed
162	D.10.4.2.3.6 IEEE 7-4.3.2, Clause 5.3.6, Software project risk management	The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems.		Give examples of "abnormal events and plant operations with degraded equipment and plant systems". Oconee SER states: "Although no specific hazards analysis was performed for the digital RPS/ESPS, the cumulative effect of performing D3, Criticality, Failure Modes and Effects, and Response Time Analyses ensures the high degree of reliability necessary for safety-related software."	See comment No. 161.	(See "Final Test" for Comment No. 161)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
163	D.10.4.2.3.6 IEEE 7-4.3.2, Clause 5.3.6, Software project risk management	A hazard is a condition that is prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. The software and hardware safety plan addresses the identification, evaluation and resolution of hazards. Hazard analysis is the process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. The software safety plan should include the safety analysis implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried out in their entirety. Documentation should exist that shows that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the system safety requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety.		This information is redundant to section D.4.4.9.1 and not relevant to section D.10.4.2.3.6. It should be deleted.	See comment No. 161.	(See "Final Test" for Comment No. 161)	Closed
164	D.10.4.2.3.6 IEEE 7-4.3.2, Clause 5.3.6, Software project risk management	The reviewer, when analyzing the risk management program, should keep in mind that licensee acceptance of risk is not necessarily sufficient or acceptable. As an example, if the licensee decides to use highly complex software in lieu of a simpler system, the licensee should demonstrate that the complexity is acceptable. The reviewer should look for alternative solutions, and analysis of those alternatives, and a reason why the complexity offered sufficient advantages to outweigh the disadvantages.	When analyzing the risk management program, it should be kept in mind that licensee acceptance of risk is not necessarily sufficient or acceptable. As an example, if the licensee decides to use highly complex software in lieu of a simpler system, the licensee should demonstrate that the complexity is acceptable. Alternative solutions, and analysis of those alternatives, should be considered and a reason why the complexity offered sufficient advantages to outweigh the disadvantages.	Reworded to apply to submitter and reviewer.	Agree	When analyzing the risk management program, it should be kept in mind that licensee acceptance of risk is not necessarily sufficient or acceptable. As an example, if the licensee decides to use highly complex software in lieu of a simpler system, the licensee should demonstrate that the complexity is acceptable. Alternative solutions, and analysis of those alternatives, should be considered and a reason why the complexity offered sufficient advantages to outweigh the disadvantages.	
165	D.10.4.2.4.2 IEEE 7-4.3.2, Clause 5.4.2, Qualification of commercial computers	Commercial Grade Dedication Plan Commercial Grade Dedication Report Commercial Grade Dedication Reports Final Report on Acceptance of Commercial Grade Dedication	Commercial Grade Dedication Plan Commercial Grade Dedication Report Final Report on Acceptance of Commercial Grade Dedication	Remove duplicate line.	Agree - The text has been revised to reference Enclosure B.	Enclosure B contains an example list of documents that the NRC staff would expect to provide sufficient information.	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
166	D.10.4.2.6 IEEE 7-4.3.2, Clause 5.6, Independence	The interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.		Past interpretations have also considered the effect of the failure. A failure that does not challenge the protection system does not need to leave the protection system fully intact to meet the single failure criteria. Ref D.7 that has detail already. Nothing more needed or supplied.	Agree - No change. The text is accurate and provided for clarity.	(no change)	Closed
167	D.10.4.2.7 IEEE 7-4.3.2, Clause 5.7, Capability for test and calibration	The reviewer should carefully examine the capability of the software to test itself. From experience with a number of digital failures, the failures, were not in the operational code but in the diagnostic code. One of the reasons for this may be that the diagnostic code may be much more complex than the operational code. The reviewer should examine the portion of the analysis in the Factory Modes Effects Analysis (FMEA) on diagnostic code failure. Assertions that failure of the operation code is not credible because the system and software diagnostics will find every failure should be carefully examined. The total amount of software code should be compared to the amount of operational code. Large amounts of test and diagnostic software increase the complexity of the total software, and this increase in complexity should be balanced against the potential gain in confidence in the system provided by that test and diagnostic software. This may also be balanced by the extensive previous use of these diagnostic routines. The test and diagnostic software may have been well tested and extensively used in the past, while the operational code is likely new for this application. The reviewer's judgment should be used. A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog will fail to operate if the processor freezes and no instructions are processed.	The capability of the software to test itself should be considered. An analysis in the Failure Modes Effects Analysis (FMEA) on diagnostic code failure should be conducted. Judgment should be used. A search should be conducted for a hardware watchdog timer whose only software input is reset after the safety processor completes its function. There should be no possibility of a software failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.	Reworded to apply to submitter and reviewer. Typo 'Factory' for 'Failure'	Agree	The capability of the software to test itself should be clearly described. From experience with a number of digital failures, the failures, were not in the operational code but in the diagnostic code. One of the reasons for this may be that the diagnostic code may be much more complex than the operational code. The Failure Modes Effects Analysis (FMEA) should include diagnostic code failure. Large amounts of test and diagnostic software increase the complexity of the system, and this increase in complexity should be balanced against the potential gain in confidence in the system provided by that test and diagnostic software. This may also be balanced by the extensive previous use of these diagnostic routines. The test and diagnostic software may have been well tested and extensively used in the past, while the operational code is likely new for this application. A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog will fail to operate if the processor freezes and no instructions are processed.	Closed
168	D.10.4.2.7 IEEE 7-4.3.2, Clause 5.7, Capability for test and calibration	The reviewer should look for a hardware watchdog timer whose only software input is reset after the safety processor completes its function. Even then, the reviewer should look to ensure that there is no possibility of a software failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.		This is impossible to prove. If it were possible, there would be no need for a CCF analysis for systems that have hardware watchdogs. Eliminate sentence.	Disagree - No Change. It is generally agreed that one can not predict the behavior of a software based system unde CCF; the system may still partially function (e.g., reset the watchdog), but not in a completly corect manner (e.g., fail to trip).	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
169	D.11.1 Scope of Review	The scope of review includes the information necessary to ensure compliance with 10 CFR 50.36.		This section should discuss credit for self-diagnostics in extending and eliminating manual surveillances for setpoints and functional logic verification. BTP 7-17 applies.	Agree - This text is already included in this section. Agree - Reference to BTP 7-17 has been added.	The scope of review includes the information necessary to ensure compliance with 10 CFR 50.36. SRP Chapter 7 BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," will be used by the staff in these evaluations. As discussed previously, the complex nature of digital I&C systems allows for individual channels to be aware of other channels and system functions. This ability has the potential to obviate the need for some of the Surveillance Requirements (SRs) classically associated with I&C. Specifically, the need for channel checks, channel calibrations, etc, may no longer be necessary if these functions can be performed internally by the digital I&C system. While utilization of digital I&C systems may allow the deletion of some existing SRs, those that are necessary to assure that the quality of the system and its components is maintained need to be retained in or proposed for addition to the TSs.	Closed
170	D.11.5 Conclusion	Additionally, the NRC staff will review the methodologies have been proposed for incorporation into the administrative section of the TSs and will determine whether or not those methodologies are acceptable.	Additionally, the NRC staff will review the methodologies that have been proposed for incorporation into the administrative section of the TSs and will determine whether or not those methodologies are acceptable.	Missing the word 'that'	Agree - Comment incorproated.	Additionally, the NRC staff will review the methodologies that have been proposed for incorporation into the administrative section of the TSs and will determine whether or not those methodologies are acceptable.	Closed
171	D.12 System and Software Security	System and software security will be addressed following the issuance of separate NRC guidance on this issue.		The document has 'system and software security' guidance in D.4.4.1, D.4.4.8, D.4.4.9, D.9.4.2.9, and D.10.4.2.3.6	Agree - The guidance for secure environment will be updated per Rev.3 of RG 1.152. Documentation requirements will be stated. Some requirements may be contained within the existing documents.	(Later)	Open
172	D.12.1 Scope of Review	None--System and software security will be addressed following the issuance of separate NRC guidance on this issue.	The scope of review includes information necessary to ensure compliance with 10 CFR 73.54 for this specific modification. As background, the NRC approved licensee Cyber Security Plan is a part of the Physical Security Plan and contains several security controls that are applicable to modifications and additions of digital assets. The NRC approved Cyber Security Plan provides high assurance of adequate protection from cyber attacks up to and including the design basis threat.		Disagree - Cyber security is not part of Part 50 and will not be addressd during the Part 50 DSS licensing review.	To ensure that the development processes and documentation are secure (from non-malicious acts or events) such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system. Review of secure software design and development processes will be limited to and including the factory acceptance tests. To ensure that any credible failure of the connected non-safety system shall not prevent the safety system from performing its safety function. To ensure that access to safety systems is controlled such that inadvertent access and or operator error will not adversely impact the safety system functionality. (To be completed later.)	Open

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
173	D.12.2 Information to be provided		Licensee affirms in the LAR that the security control elements contained in its NRC approved Cyber Security Plan either have been completed or will be completed for this modification prior to its installation in the plant. Security controls include various technical, operational and management controls.		See Comment No. 172.	Enclosure B is only an example list and an applicant may have different names for similar documents. The licensee's submittal should provide sufficient documentation to support the assertion that a proposed digital I&C system is adequately robust to perform its safety function within its design-basis normal and adverse environments. The vulnerability assessment should address vulnerabilities due to hardware, software, access control, network connectivity etc. and it forms the basis for the overall system secure environment approach. To address regulatory positions 2.1, Concepts Phase through 2.5, Test Phase of regulatory guide 1.152 the following documents should be provided: Vulnerability Assessment Secure Environment Concepts Secure Environment Requirements Design Phase Requirements Implementation Phase Requirements Test Phase Requirements	Open
174	D.12.3 Regulatory Evaluation		10 CFR 73.54 states: (d) (3) As part of the cyber security program, the licensee shall: Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained. With the approved Cyber Security Plan, the NRC has determined the adequacy of these processes for all modifications and additions. The NRC approved Cyber Security Plan provides high assurance of adequate protection from cyber attacks up to and including the design basis threat.		See Comment No. 172.	GDC 21, "Protection system reliability and testability", requires ... Appendix B to Part 50, ... delineates the requirements for a quality assurance program. Criterion III of Appendix B, "Design Control" ... 10 CFR 50.55a(h) requires ... IEEE Std. 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603. IEEE Std. 603-1991 in Clause 5.6.3.1(2) ... IEEE Std. 603-1991 in Clause 5.9 ... (To be completed later.)	Open
175	D.12.4 Technical Evaluation		The NRC staff review should verify that the security controls for this modification have been identified and either are already in place or will be in place prior to installation.		See Comment No. 171.		Open
176	D.12.5 Conclusion		The NRC staff affirms that the process prescribed by the approved Cyber Security Plan has been implemented for this plant modification.		See Comment No. 172.	(no change)	Open
177	Enclosure B Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request	Software Design Specification (D.4.4.15)		The prerequisite to a SDS is the functional requirements and the system design and the software requirements specification listed after the SDS. To include the SDS in the LAR delays the submission of the LAR 6 - 12 months after the initiation of the project.	Disagree - No change. The NRC licenses designs. The SDS may be the first design document produced. There is a 2-year NRC clock on issuing SERs. The licensing guidance requires that an LAR cannot be submitted for staff review without a design for review (i.e., the SDS and daughter products).	(no change)	Closed

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
178	Enclosure B Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request	Software Training Plan (D.4.4.7)		It is unrealistic for the licensee to have a software training plan with the LAR submittal when the software is not designed and implemented yet.	Document removed from Enclosure B.	(Document removed from Enclosure B.)	Closed
179	Enclosure B Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request	Requirement Traceability Matrix (D.4.4.18)		The RTM goes throughout the whole SLC. That means an unacceptable delay of the LAR submittal until all SLC phases are complete.	See Comment Nos. 80-84.	(no change)	Closed
180	Enclosure B Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request	Final Logic Diagrams (D.9.2)		Assuming you have a 12 month SLC, then the SER will be 3 years from initiation of the project.	Agree - No change proposed.	(no change)	Closed
181	Enclosure D, Table of Contents	3.5.1 Environmental Qualification of System - IEEE Std 323-1974/1983.....4		The more correct reference for DI&C is RG 1.209, which endorsed IEEE Std 323-2003.	Agree - Reference removed.	3.5.1 Environmental Qualification of System...	Closed
182	Enclosure D, 3.5.1 Environmental Qualification of System - IEEE Std 323-1974/1983	3.5.1 Environmental Qualification of System - IEEE Std 323-1974/1983		The more correct reference for DI&C is RG 1.209, which endorsed IEEE Std 323-2003.	Agree - Reference removed.	3.5.1 Environmental Qualification of System…	Closed
183	Enclosure E, Table of Contents	5.2.2.6 Software Maintenance Plan (See Section D.4.4.6 of ISG #6) 5.2.2.7 Software Training Plan (See Section D.4.4.7 of ISG #6) 5.2.2.8 Software Operations Plan (See Section D.4.4.8 of ISG #6)		If the SER does not intend to address these topics, why are the: Maintenance Plan Software Training Plan Software Operations Plan submitted on the docket with the LAR (phase 1 submittal)?	Agree - Documents removed from Enclosure B.		Closed
184	ISG6 Parking Lot			Industry commented that Enclosure B includes documents that were not reviewed as part of the Oconee RPS/ESPS digital upgrade.	The NRC Staff will continue to review the utilization of documents from the Oconee RPS/ESFAS upgrade to inform the list of documents to be submitted.		Open
185	ISG6 Parking Lot			Industry wanted to reduce the amount of material docketed, particularly proprietray documents.	The staff noted that there is a tendency in industry to produce fewer, but larger documents. The staff suggested that industry review their documentation practices and consider producing more but smaller docuements that were modular and cohesive. The NRC Staff will explore the feasibility of using information technology to review documents.		Open

No.	Location	Original Text	Proposed text	Industry Comments	NRC Comment / Disposition	Final Text	Status
186	ISG6 Parking Lot			Industry stressed that the most important information in this ISG was a clarification of what was needed and when.	In the March 24, 2010 public meeting the staff took the action to investigate the possibility of using sharepoint as a way to view the information requird. The NRC Staff will clarify both the information needed and when, in the review process it is needed. Text added to Section C.2.	(Later: The NRC is currently investigating the potential of using data portals (e.g., electronic reading rooms) to review information within various documents and determine if the documentation (or some portion thereof) should be submitted on the docket.)	Open
187	ISG6 Parking Lot			Industry expressed an interest in guidance that would clarify the type of information needed to describe and justify changes to a Digital platform approved in a topical report.	The staff pointed out that two vendors are trying to address this in a revision to their topical report, and that the staff had discussed this internaly, but that no final position has yet been reached. If agreement can be reached on this process then this ISG will be revised to include it as appropriate. The NRC Staff will clarify what documentation is needed to describe and justify changes made to a previously reviewed platform when the previous approval is used as precedent.	(Later)	Open
188	non-ISG6 Parking Lot			Industry wanted the staff to change the review process using ISG6.	The scope of a Digital I&C Review (Would need to be addressed by a revision to Chapter 7 of the Standard Review Plan). This may be considered as a separate task in the future.	(N/A)	Open
189	non-ISG6 Parking Lot			Industry wanted the staff to consider the use of license conditions to review acceptance testing.	The current NRC position is that the licensing process includes factory acceoptance testing and associated documentation. Reactor oversight includes, site acceptance testing, installation, operation & maintenance.	(N/A)	Open
190	non-ISG6 Parking Lot			Industry wanted a clarification of the scope of licensing basis with respect to a digital I&C review.	Please read LIC-100, "Control of Licensing Bases for Operating Reactors," (ML033530249).	(N/A)	Open