Industry Comments – DI&C-ISG-06

Location	Original Text	Proposed text	Comments
Global	"It should be noted…" "It is important to note"	delete	
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.
Global	Software operator	Replace software "operator" with "user". Since there may be many others who interface with the system, not just operators.	
Global	documents	information	Replace "documents" with "information".
Global	Failures	errors	Software 'failures' should be replaced by 'errors'.
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.
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	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	Should agree with last sentence in paragraph.

Location	Original Text	Proposed text	Comments
	associated guidance including ISGs.	ISGs.	
B.1 Background	actives	activities	Typo 'actives ' for 'activities'
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
B.1 Background	process's	processes	Typo 'process's' for 'processes'
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.

Location	Original Text	Proposed text	Comments
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
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	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

Location	Original Text	Proposed text	Comments
	quality assurance program.		
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".
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.
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.

Location	Original Text	Proposed text	Comments
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.
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.
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		Change 'site' to supplier's or licensee's facility.

Location	Original Text	Proposed text	Comments
	for audit 12 months prior requested approval date).		
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.

Location	Original Text	Proposed text	Comments
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.
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		Appendix B says FAT must be submitted, not audited.

Location	Original Text	Proposed text	Comments
	build documentation) will likely cover information from both Phase 1 and Phase 2, and may result in further requests for information to be docketed.		
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.
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'

Location	Original Text	Proposed text	Comments
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.
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.,

Location	Original Text	Proposed text	Comments
			microprocessors). The text should define the areas of specific interest to the staff.
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").
D.1.3 Regulatory Evaluation	D.1.3 Regulatory Evaluation		Poor title words, since there is no Regulatory requirement, just information for reviewer.
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

Location	Original Text	Proposed text	Comments
			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.
D.2.2 Information to be Provided	Any deviations or revision changes should be identified and adequately justified.		Deviations in docketed information only.
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.
D.3.1 Scope of Review	Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In		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

Location	Original Text	Proposed text	Comments
	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.		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.
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.
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	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

Location	Original Text	Proposed text	Comments
	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		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. 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

Location	Original Text	Proposed text	Comments
			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.
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.
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.
D.4.4.1 Software Management Plan (SMP)	The SMP should include sufficient information about the security requirements		Since it is in a state of change, guidance should reference the appropriate revision of RG 1.152.

Location	Original Text	Proposed text	Comments
	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.		
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."

Location	Original Text	Proposed text	Comments
			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."
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'
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		Since Cyber-Security is now separated from Digital Security, this should be reworded for clarity. Regulatory Guide 5.71 vs. Regulatory Guide 1.152.

Location	Original Text	Proposed text	Comments
	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.		
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.
D.4.4.2 Software Development Plan (SDP)	Software Configuration Management Plan (SCMP0,	Software Configuration Management Plan (SCMP),	Typo '(SCMP0' for '(SCMP)'
D.4.4.2 Software Development Plan (SDP)	Coding standards should be compared to the suggestions contained in NUREG/CR-6463, "Review	Coding standards should follow the suggestions contained in NUREG/CR-6463, "Review Guidance for Software languages	New requirement imposed here.

Location	Original Text	Proposed text	Comments
	Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.	for Use in Nuclear Power Plant Safety Systems".	
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'.
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'
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.
D.4.4.2 Software Development Plan (SDP)	Coding standards should be compared to the suggestions contained in NUREG/CR-6463, "Review		There are 432 pages in this NUREG/CR-6463. Justifying deviations goes well beyond regulatory precedence for NUREG compliance.

Location	Original Text	Proposed text	Comments
	Guidance for Software languages for Use in Nuclear Power Plant Safety Systems," and any deviations should be justified.		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.
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.
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		Typo 'SQP ' for 'SQAP'

Location	Original Text	Proposed text	Comments
	to determine not only that the SQP exhibits		
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.
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.
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	Delete footnote 9	Footnote 9 repeats the second paragraph text.

Location	Original Text	Proposed text	Comments
	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.		
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'
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	

Location	Original Text	Proposed text	Comments
		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.	
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.
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'.
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.
D.4.4.6 Software	In many instances, the	In many instances, the software	Both maintenance activities can be

Location	Original Text	Proposed text	Comments
Maintenance Plan (SMaintP)	software maintenance will be done by the original system vendor. In this case, two maintenance plans are required.	maintenance will be done by the original system vendor. In this case, two maintenance plans may be required.	covered in the same plan.
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)?
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'
D.4.4.8 Software Operations Plan (SOP)	The Software Operations Plan is not intended describe		Conflicts with BTP 7-14 guidance and contradicts

Location	Original Text	Proposed text	Comments
	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.		(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.
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)?
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		Replace software "operator" with "user". Since there may be many others who interface with the system, not just operators.

Location	Original Text	Proposed text	Comments
	described, including the time sequencing of any extended conversations.		
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."
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.,		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

Location	Original Text	Proposed text	Comments
	intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.		Use Security controls instead of cyber risk
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		Not the same definitions as IEEE 1012-1998 and IEEE Std 610.12-1990.

Location	Original Text	Proposed text	Comments
	determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.		
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.
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".
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."

Location	Original Text	Proposed text	Comments
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.
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)?
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
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		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

Location	Original Text	Proposed text	Comments
	by V&V personnel.		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
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."
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. Fix list in Appendix B to match.

Location	Original Text	Proposed text	Comments
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.
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.
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		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.

Location	Original Text	Proposed text	Comments
	vendor build documentation).		
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.
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
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.
Footnote 22; D.4.4.18	This section states that a	This section states that a	Replace sentence for clarity.

Location	Original Text	Proposed text	Comments
Requirements Traceability Matrix	requirements traceability matrix, that needs to show every requirement, should be broken down in to sub-requirements as necessary.	requirements traceability matrix needs to show every requirement and should be broken down in to sub-requirements as necessary.	
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.
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"
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 FMEA24, 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		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.

Location	Original Text	Proposed text	Comments
	determine if the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures.		
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		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.

Location	Original Text	Proposed text	Comments
	mode. The FMEA is also used as an input to the diversity and defense in depth analysis.		
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."
D.4.4.19 Failure Modes	The key attribute which the	The key attribute which the staff	Delete 'software' failures. Delete "and

Location	Original Text	Proposed text	Comments
and Effects Analysis (FMEA)	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.	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.	accuracy" or explain it. FMEA should also demonstrate that all failures are detectable.
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
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.
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		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".

Location	Original Text	Proposed text	Comments
	correctly, and in such a manner as to produce high quality software suitable for use in safety-related applications at nuclear power plants.		
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
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.
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).
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

Location	Original Text	Proposed text	Comments
			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
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.
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.
D.5.4 Technical	The testing should include		Temp and humidity testing is not required

Location	Original Text	Proposed text	Comments
Evaluation	exposure to expected extremes of temperature, humidity, radiation, electromagnetic and radio interference, and seismic input.		for mild environments.
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		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)?

Location	Original Text	Proposed text	Comments
	should be preconditioned sufficient to account for the acceptance criteria of the surveillance plus the expected aging until the next performance of the surveillance.		
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.
D.5.4.2 Radiation	(i.e., it does not return to its original state up removal of the stressor)		Typo "up" for 'upon'
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.
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. OE shows no problems in mild

Location	Original Text	Proposed text	Comments
			environments. This guidance restates the obvious. What is expected? This appears beyond the scope of a digital LAR.
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.
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.
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'
D.6.2 Information to be Provided	A list of all manual operator actions credited for diversity.	…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.

Location	Original Text	Proposed text	Comments
	Detailed justification for operator actions with limited margin.		
D.6.2 Information to be Provided	using Branch Technical Position 7-19,	using Branch Technical Position 7-19, revision 5,	
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.
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.
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.
D.6.2 Information to be Provided	A list of all manual operator actions credited for diversity.		Credited for coping with CCF, not diversity.

Location	Original Text	Proposed text	Comments
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
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'
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.
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		For correctness use DI&C-ISG-02 throughout to avoid confusion with any non DI&C ISG-2.

Location	Original Text	Proposed text	Comments
	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		
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.
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.
D.7.1 Scope of Review	Omitted text		This section should clarify the extent of failures to be assumed in this evaluation.

Location	Original Text	Proposed text	Comments
			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?
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.
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.
D.7.3 Regulatory	Additional Guidance on	Additional Guidance on	Correct ADAMS reference for DI&C-ISG-04

Location	Original Text	Proposed text	Comments
Evaluation	interdivisional communications is contained in ISG-4, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML072540138).	interdivisional communications is contained in DI&C-ISG-04, "Highly-Integrated Control Rooms – Communication Issues, revision 1," (ADAMS Accession No. ML083310185).	R1 is ML083310185.
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).
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.
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		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

Location	Original Text	Proposed text	Comments
	submitted for approval before a LAR is submitted referencing the TR.		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.

Location	Original Text	Proposed text	Comments
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		This is more restrictive control criteria than either 10CFR50.59 or 10CFR52.63(b).

Location	Original Text	Proposed text	Comments
	those of the existing approval.		
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.
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.
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,		RG 1.153, revision 2 endorses IEEE Std 379-2000.

Location	Original Text	Proposed text	Comments
	"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."		
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)
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.

Location	Original Text	Proposed text	Comments
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.
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.
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'
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		A better way to describe this is that licensees need to meet their licensing basis commitments using RG 1.97.

Location	Original Text	Proposed text	Comments
	of IEEE Std. 479-1981.		
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.
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.
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?
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		At platform level, 10% of vendor material goes out of shop to customer. Limit 'nuclear safety items' to items sent

Location	Original Text	Proposed text	Comments
	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).		to customer. Identification should be application dependent: safety vs. non-safety
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.
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.
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.
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		NRC has not endorsed either IEEE Std 352 or IEEE Std 577. Neither should be imposed as expectations here.

Location	Original Text	Proposed text	Comments
	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."		
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.
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		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

Location	Original Text	Proposed text	Comments
	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.		required to meet requirements in IEEE 603.

Location	Original Text	Proposed text	Comments
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'
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'
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.
D.10.2 Information to be Provided	Commercial Grade Dedication Plan Commercial		This list exceeds the list of documents submitted in support of the Oconee

Location	Original Text	Proposed text	Comments
	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		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

Location	Original Text	Proposed text	Comments
			list is necessary.
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'.
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'.
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.
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 first paragraph implies software metrics are required and the next says not required. Conflicts. What is a diverse metric? Why is it needed?

Location	Original Text	Proposed text	Comments
	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.		This is a repeat of Software Quality earlier; no metrics mentioned there. If expected, then it should be in BTP 7-14 section too.
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.
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	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.

Location	Original Text	Proposed text	Comments
	regulatory requirements for software developed under an Appendix B program.		
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'
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.
D.10.4.2.3.5 IEEE 7-4.3.2, Clause 5.3.5, Software configuration	The reviewer of the software configuration management system should evaluate that	The software configuration management system should be evaluated to ensure that the	Reworded to apply to submitter and reviewer.

Location	Original Text	Proposed text	Comments
management	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.	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.	
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.
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

Location	Original Text	Proposed text	Comments
			listing risks. Part of software design process D.4.4.1 (SMP) already; not necessary here.
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'
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."
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		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.

Location	Original Text	Proposed text	Comments
	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		

Location	Original Text	Proposed text	Comments
	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.		
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.
D.10.4.2.4.2 IEEE 7-4.3.2, Clause 5.4.2, Qualification of	Commercial Grade Dedication Plan Commercial Grade Dedication Report	Commercial Grade Dedication Plan Commercial Grade Dedication Report	Remove duplicate line.

Location	Original Text	Proposed text	Comments
commercial computers	Commercial Grade Dedication Reports Final Report on Acceptance of Commercial Grade Dedication	Final Report on Acceptance of Commercial Grade Dedication	
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.
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	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	Reworded to apply to submitter and reviewer. Typo 'Factory' for 'Failure'

Location	Original Text	Proposed text	Comments
	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 failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.	

Location	Original Text	Proposed text	Comments
	software watchdog will fail to operate if the processor freezes and no instructions are processed.		
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.
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.
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	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	Missing the word 'that'

Location	Original Text	Proposed text	Comments
	determine whether or not those methodologies are acceptable.	those methodologies are acceptable.	
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
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.	
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	

Location	Original Text	Proposed text	Comments
		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.	
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.	
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	

Location	Original Text	Proposed text	Comments
		will be in place prior to installation.	
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.	
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.
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.
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.
Enclosure B	Final Logic Diagrams (D.9.2)		Assuming you have a 12 month SLC, then

Location	Original Text	Proposed text	Comments
Documents to be Submitted in Support of a Digital I&C Upgrade License Amendment Request			the SER will be 3 years from initiation of the project.
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.
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.
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)?