Comment Resolution Summary

Inspection Procedure (IP) 65001.22
"Inspection of Digital I&C Systems/Software DAC-related ITAAC"

Document date: December 15, 2011

Comment Resolution Summary

Inspection Procedure (IP) 65001.22
"Inspection of Digital I&C Systems/Software DAC-related ITAAC"

No.	Source	Comment	Added	Remarks
1	RI	A1.03.02.a: Add Version Control and Audit Trails to the list. (from IEEE Stds 1012 and 1028)	Yes	
2	RI	A1.03.03.b: Add Backup and Recovery to the list. (from RG 1.209)	Yes	
3	RI	A1.03.04.c.3.b: Change "… probability of error during operation." to "… probability of error during operation and describe the consequences if those errors were to occur."	Yes	
4	RI	A1.03.07.a: Add Regression Testing as an integration strategy of the Software Integration Plan. (from RG 1.170)	Yes	
5	RI	A1.03.08.b.3: Change wording "Include metrics to determine…" to "Include acceptance criteria to determine…"	Yes	
6	RI	A1.03.08.b.5: Change wording "for correct version of software on…" to "for correct version of application software and source code…"	Yes	
7	RI	A1.03.09.b.4: Change "Metrics are included" to "Acceptance Criteria are included"	Yes	
8	RI	A2.03.01.c.5: Change "Critical DI&C System security considerations…" to "Critical DI&C System physical and cyber security considerations…"	Yes	
9	RI	A2.03.01.c: Add "Critical DI&C system boundary value testing requirements are identified."	Yes	
10	RI	A2.03.02.a.4: Add sentence "This includes application software and source code."	Yes	

No.	Source	Comment	Added	Remarks
11	RI	A2.03.02.b.4: Change "…with sensors/actuators…" to "with validation methods of sensors/actuators adequately described."	Yes	
12	RI	A2.03.03.a.3: Change "… (change control)…" to "… (change control, version control, and audit trails)…"	Yes	
13	RI	A3.03.02.b: Add "For commercial off the shelf software (COTS SW) disable all non-required features."	Yes	
14	RI	A3.03.02.b: Add "Auto swap-over to standby backup software are built into the design."	Yes	
15	RI	A3.03.02.b.6: Add "Time critical subroutines."	Yes	
16	RI	A3.03.03.a.1: Change "System code…" to "Application software and system code …"	Yes	
17	RI	A3.03.05.a.1: Add "DI&C must include a failsafe software design." (from RG 1.170)	Yes	
18	RI	A3.03.05.a.1: Add "DI&C must include power loss recovery implementation." (from RG 1.170)	Yes	
19	RI	A3.03.04.b.1: Add individual bullet items for Software Failures, Overrides, Bypasses and Compensatory Measures for Software Failures.	Yes	
20	RI	A3.03.04.b.3: Add Input Validation requirements. (from IEEE Std 829)		Included in A3.03.02b.
21	RI	A3.03.04.b.3: Add Black Box and White Box requirements. (from IEEE Std 829)		Included in A4.03.01b (Integration).
22	RI	A4.03.01.a: Add EMI/RFI requirements and Anti-virus Software requirements.		Included in A4.03.01a.
23	RI	A4.03.01.b.1: Change "Indicators…" to "Acceptance Criteria are used…."	Yes	
24	RI	A5.03.01.a: Add "Software properly scales analog inputs from transmitters."		Included in A3.03.05a.2 (Design Safety Analysis).

No.	Source	Comment	Added	Remarks
25	RI	A5.03.01.a.4: Add sentence "The Failure Modes and Effects Analysis must identify potential errors.	Yes	
26	RI	A6.03.03.b: Change "…security risks…" to "… physical and/or cyber security risks…"	Yes	
27	DE	A1.02: In the Sample Size sections there seems to be no guidance on how to establish an acceptable number of samples. There is also no guidance on altering the sample size based upon inspection findings.		Added general guidelines for sample size of attributes to be selected in the Planning Phase (Appendix 1). There is no quantitative value; the sample size is at the inspector's discretion. Quantitative sampling guidance is provided in the remaining Appendices.
28	DE	When we go to perform this sample based inspection how will we manage the samples? Will we just do as many as we can in the allotted time or will there be a more methodical approach used based on the volume of information we review prior to the inspection. Typically, we in NRR will review the material prior to the site visit and make a determination of how many samples will be needed ahead of time.		Addressed in Comment 35.
29	DE	A1.03: Much of the guidance for conducting the inspection appears to have been derived from BTP 7-14. However, not all of the BTP areas are covered. For example, the IP calls for a review of 8 planning phase documents while the BTP calls out 12. If there is good reason for not including guidance from the BTP then the justification should really be provided. If we are just cherry picking out of the BTP guidance then we will never be able to claim that the same level of safety assurance is being achieved with the inspection process in comparison with the SRP SER processes.		Added justification in A1.03 for not including Operations, Maintenance and Training plans (considered outside of DAC scope). This IP was never intended to replicate BTP 7-14, but is rather a consolidation of guidance from various sources, including BTP, ISGs, NUREGs, RGs, standards, and inspection/audit guidance. Attributes included in this IP were selected based on their value toward verification of design implementation detail, recognizing the limitations of

No.	Source	Comment	Added	Remarks
				ITAAC inspection (time and resources).
30	DE	A1.03.01: It is not clear what the acceptable level of independence between developers, SQA, and V&V groups. BTP 7-14 does provide some guidance on this but this is not reflected in the IP. For example, section B.3.1.10.4 does provide specific guidance for us on how to evaluate the independence characteristics of the SVVP.		Section A1.03.01.3 (SMP) states that independence is required between the design group and V&V group, and the SMP should provide a pointer to the SVVP. Discrete attributes regarding V&V organizational independence, freedom from schedule constraints and reporting are provided in A1.03.04.b.
31	DE	A1.03.02: Often, vendors and licensees do not distinguish between QA and SQA and there is no SQA group or entity. AREVA, for example, did not have any software experts in the QA organization so they relied upon the people in the SVV team to perform SQA related activities. I think that Westinghouse is similar, so we should not include reference to an SQA organization which may not exist.		Removed references to SQA organization, as it may not always be applicable.
32	CCI	Appendix 3, discusses FMEA. Add more guidance on FMEA's and add FMEA references; RG 1.53, "Application of the Single-failure Criteria", maybe RG 1.47 Bypassed and Inoperable Status, ANSI/IEEE 352 , "IEEE Guide for General Principals of Reliability Analysis of NPP, IEEE 379 Application of single failure criteria.		Section A3.03.05.c (FMEA) is modified with references to RG 1.53 (Single Failure) and IEEE-Std-352 (Reliability Analysis). The attributes called out in this section are incorporated from Std 352.
33	CCI	A2.03.02.c: Add static performance requirements.	Yes	See Comment 48.
34	DE	When planning the inspection, the tie in to headquarters staff should be more apparent (i.e., at a minimum consult for specific aspects to inspect and maybe team composition).	Yes	Added to Specific Guidance in 02.02.a. Inspectors will consult with NRO/DE as necessary.
35	DE	For the sample size, there should be more guidance for software planning (i.e., number of samples as well as areas to focus). For the requirements specifications, the sample size should be		Guidance added for sampling during the Planning Phase, which is at the inspector's discretion. Added sampling guidance for each Appendix

No.	Source	Comment	Added	Remarks
		larger. Eight to twelve samples out of ~10,000+ is a small sample. For AP1000, we were able to accomplish 60 samples in one week (in fairness, we had about 5 to 6 people). But, with a good prep week, a smaller team should be able to make the same progress.		(12-15 elements per inspector for Appendices 2, 3, 4 and 6) and 6-10 elements for Appendix 5. This was regarded as a manageable sample given constraints of ITAAC inspection. Recognizing that a typical DI&C software development project may encompass upwards of several thousand requirements, the critical requirements represent a fraction of all requirements, and the sampling strategy contained herein is focused on these critical requirements. This results in a sample that is a "fraction of a fraction" of total requirements. As with all inspection, any sample may be adjusted at the inspector's discretion based on issues/findings.
36	DE	A1.03.04.c.1.d: this item states "SVVP requires that the SRS be evaluated for safety, correctness, consistency, completeness, accuracy, readability, and testability." ACRS will ask: How does an inspector accomplish this? What types of V&V activities do we expect to occur to capture these attributes? Would it be possible to reference certain sections of NUREG/CR-6101 in the inspection procedure? Also, the SVVP section addressed V&V for the requirements stage, but not the other stages. The SVVP should cover all stages.		This is a valid comment. The SVVP should not be assessed for such general and possibly ambiguous attributes. This item is removed. The SRS will be evaluated for these attributes using the IP as guidance. The primary tool used by inspectors to ascertain an adequate level of correctness, consistency, accuracy, etc. is the thread audit and traceability tools. Inspectors are given guidance for tracing software design outputs forward and backward to determine their source and accountability in the overall design. The strategy of thread audits (vertical slice assessment) has been briefed to ACRS on two separate occasions, and will continue to be reinforced. The IP is guidance; careful

No.	Source	Comment	Added	Remarks
				and detailed inspection planning, and use of thread audit techniques, should enable inspectors to reach a conclusion regarding the adequacy of the SRS or any design output. The guidance contained in the IP is derived from NUREG/CR-6101 and other sources. There is no need to reference specific sections of the NUREG. The SVVP section now addresses all life cycle stages.
37	RII/CCI	Appendix 1, Planning Phase: Add guidance stating that compliance with RG 1.173 and IEEE-Std-1074 means mandatory activities are performed, requirements described as "Shall" are met, and all inputs, outputs, activities and pre- and post-conditions mentioned by IEEE-Std-1074 are accounted for in the licensee's/applicant's life cycle model. (Identified during MOX S/W Planning inspection)		Added to A1.03 (Planning Phase General Guidance).
38	RII/CCI	Appendix 1, Planning Phase V&V: Add guidance that a security assessment of safety system software must be part of the minimum set of software V&V activities (according to RG 1.168).		Added task definition to A1.03.04.b to include minimum tasks from RG 1.168.
39	RII/CCI	In the main body of the procedure under "Procedure Completion" an Exhibit 1 is referenced which does not exist.		Deleted reference to Exhibit 1.
40	RII/CCI	Inspection requirement A1.03.01b states that "Project work products and deliverables are well defined." Would like to replace the word "well" with "adequately."	Yes	Editorial- complete.

No.	Source	Comment	Added	Remarks
41	RII/CCI	In inspection requirement A2.03.01a it states that “DI&C System requirements satisfy all applicable codes, standards and requirements”. Recommend removing “all” since we will be only looking at a sample of requirements, which may not encompass all the applicable codes, standards and requirements.	Yes	Editorial- complete.
42	RII/CCI	In inspection requirement A2.03.02a it states “Software functional requirements, taken as a whole, completely specify what the software must do.” The guidance for this section is to take 20-25 samples of functional requirements, which may be relatively small portion of the functional requirements. At the very least take out “taken as a whole, completely.”	Yes	Editorial- complete.
43	RII/CCI	In inspection requirement A2.03.02b the term “fully described” is used. This should be defined somewhere or changed to “adequately described.”	Yes	Editorial- complete.
44	RII/CCI	In inspection requirement A2.03.04a it states “There are no missing or inconsistently specified DI&C system functions or software requirements.” This should be amended with “for the requirements selected for sample”. It’s harder to prove a negative statement with sampling than a positive statement.	Yes	Added “(from the selected sample).”
45	RII/CCI	In inspection requirement A3.03.02b it states that “Static and dynamic structures are simple, with minimal connections between design elements”. What is the definition of “simple?” Is it in one of the references?	Yes	Changed to “exhibit minimal connections.”
46	RII/CCI	Typo on page A4-5, requirement A4.03.03b2 has the words “should are” next to each other. One should be deleted.	Yes	Editorial- complete.

No.	Source	Comment	Added	Remarks
47	RII/CCI	A6.03 has sample size for design elements. Is an ICT a design element? Otherwise there is no sample size included for ICTs.		The ICT is a design output per BTP 7-14. Added a sample size for installation configuration items in Section A6.02.
48	RII/CCI	A2.03.02c Add a bullet for what Static performance requirements are, as follows: -Static performance requirements are fully described: • The number of terminals to be supported; • The number of simultaneous users to be supported; • Amount and type of information to be handled.	Yes	Existing bullet enhanced for clarity.
49	RIV	General Comment: As defined in ANSI/ANS standards, the term "shall" denotes a requirement and the term "should" denotes a recommendation. For the sections of IP 65001.22 that specify the verification of requirements, RIV recommends changing the term "should" to "shall."		For this IP, it is recommended that the term "should" be used unless referring to specific requirements or restatements of criteria in standards committed to by the applicant/licensee. The IP verification items contain the phrase "as committed to in the licensing basis." The inspector has discretion to invoke the "shall" requirement threshold based on the licensing basis.
50	RIV	02.02.a: General Inspection Requirements, first sentence, change the word "should" to "shall..."		See Comment 49.
51	RIV	02.02.a: Specific Guidance, third bullet, following the word "status…" insert the words "and disposition…"	Yes	
52	RIV	02.02.a: Specific Guidance, fourth bullet, following the word "licensee…" insert the word "documented…"	Yes	
53	RIV	02.02.b: Third sentence, following the words "Unexpected events…" insert the phrase "that are identified…"		Third sentence deleted in its entirety.

No.	Source	Comment	Added	Remarks
54	RIV	A1.02: Second sentence, delete the word "high…" and following the word quality, insert the word "affecting…" (Note: the term "high quality…" is not defined in the sense of an explicit quality standard). However, in reference to 10 CFR 50, Appendix B, the term "activities affecting quality …" is synonymous with safety-related.		Deleted "high" and left as "quality design." A "quality design" is well understood as the product of the entire life cycle process.
55	RIV	A1.03: General Guidance, first sentence (see above comment) delete the words "high quality…" and insert the word "effective…" and in the following sentence delete the words "high quality…' and insert the word "scrutable."		Changed to "quality" process and "quality" system. Objective is to avoid using terms such as "scrutable" which may not be understood by personnel engaged in this type of inspection.
56	RIV	A1.03: General Guidance, top of page A1-2, consistent with the first comment, change "should" to "shall," except in the last sentence.		See Comment 49.
57	RIV	A1.03.01a: Inspection Requirements, page A1-2, items 2 & 3, consistent with the first comment, change "should" to "shall."		See Comment 49.
58	RIV	A1.03.02a: Second paragraph, first sentence, delete the word "overall…" and insert "approved…"	Yes	
59	RIV	A1.03.04: Consistent with the first comment, for items 2, 3, 4, 5, & 6, change "should" to "shall."		See Comment 49.
60	RIV	A2.03.04: Consistent with the first comment, for items a. & b., change "should" to "shall."		See Comment 49.
61	RIV	A3.03: General Guidance, third sentence, delete the term "High level…" and insert "Design control…"	Yes	
62	RIV	A3.03.02a: Consistent with the first comment, change "should…" to "shall…" (Note: three places).		See Comment 49.

No.	Source	Comment	Added	Remarks
63	RIV	A3.03.05: For items a., b., & c. change "should…" to "shall…"		See Comment 49.
64	RIV	A4.03: General Guidance, second paragraph, consistent with the first comment, change "should" to "shall" (two places).		See Comment 49.
65	RIV	A4.03.01a: System/Software Integration, consistent with the first comment, change "should" to "shall" (two places).		See Comment 49.
66	RIV	A4.03.01b: Consistent with the first comment, change "should" to "shall."		See Comment 49.
67	RIV	A4.03.03a: Integration Safety Analysis, change "should" to "shall" (two places).		See Comment 49.
68	RIV	A05.03: General Guidance, third paragraph, consistent with the first comment, change "should" to "shall."		See Comment 49.
69	RIV	A5.03.01a. & b: Verification and Validation, change "should" to "shall."		See Comment 49.
70	RIV	A5.03.03: Documentation, change "should" to "shall."		See Comment 49.
71	RIV	A6.03.01a & b: Installation Configuration Tables, change "should" to "shall."		See Comment 49.
72	RIV	A6.03.04a & b: Installation Testing, change "should" to "shall."		See Comment 49.
73	DE	Add "Test Plan" to A1.	Yes	Test Plan attributes added to Appendix 1.
74	RII/CCI	Life Cycle should be consistently capitalized throughout the document.		"Life Cycle" is capitalized only to emphasize the formality of the process.

No.	Source	Comment	Added	Remarks
75	RII/CCI	A1.03.03: Spell out acronym CCB.	Yes	Editorial – complete.
76	RII/CCI	A3.03.02b: typo- “Static and dynamic structures are exhibit . . .” Remove “are.”	Yes	Editorial – complete.
77	DE	Under the framework of 10 CFR 73.54, the terms cyber and security should not be used in ITAAC or DAC DI&C guidance. Recommend replacing with “Secure Development and Operational Environment” or SDOE consistent with RG 1.152.	Yes	