Westinghouse

Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 43-374-6206
Direct fax: 724-940-8505
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP_NRC_002774

February 11, 2010

Subject: AP1000 Response to Proposed Open Item (Chapter 7)

Westinghouse is submitting the following responses to the NRC open item (OI) on Chapter 7. These proposed open item response are submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in these responses is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application.

Enclosure 1 provides the response for the following proposed Open Item(s):

OI-SRP7.2-ICE-02

Questions or requests for additional information related to the content and preparation of this response should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Very truly yours,

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Enclosure

1. Response to Proposed Open Item (Chapter 7)

D063
NRO

cc:	D. Jaffe	-	U.S. NRC	1E
	E. McKenna	-	U.S. NRC	1E
	S. Mitra	-	U.S. NRC	1E
	T. Spink	-	TVA	1E
	P. Hastings	-	Duke Power	1E
	R. Kitchen	-	Progress Energy	1E
	A. Monroe	-	SCANA	1E
	P. Jacobs	-	Florida Power & Light	1E
	C. Pierce	-	Southern Company	1E
	E. Schmiech	-	Westinghouse	1E
	G. Zinke	-	NuStart/Entergy	1E
	R. Grumbir	-	NuStart	1E
	B. Seelman	-	Westinghouse	1E

ENCLOSURE 1

AP1000 Response to Proposed Open Item (Chapter 7)

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.2-ICE-02
Revision: 0

Question: OI-SRP7.2-ICE-02

Clause 5.3 of IEEE Std. 603-1991 and Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 require safety-related I&C systems to be designed, manufactured, inspected, installed, and tested under an acceptable quality assurance program. SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2"; Section 5.3; and BTP 7-14 specifically address the criteria for a quality software development process. Additionally, the staff evaluated the documentation in the SLC against the guidance in the following documents:

- Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits"
- Regulatory Guide 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans"
- Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 829-1983, "IEEE Standard For Software Test Documentation"
- Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing"
- Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications"
- Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Lifecycles and Processes"

In Section 7.2.2.2, the staff discusses the approval of the Common Q platform topical report. However, additional requirements were placed on the SLC for the AP1000 safety system, as described in the Software Program Manual (SPM), WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," Revision 1A, dated January 21, 2005 (ADAMS Accession No. ML050350234); and WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Revision 0. The certified design (Revision 15) of the AP1000 DCD designated the SPM and WCAP-15927 as Tier 2* documents, requiring NRC approval before altering WEC commitments. The staff recently received and reviewed WCAP-15927, Revision 2 (ADAMS Accession No. ML091890752).

In AP1000 DCD Tier 1, Table 2.5.2-8, Item 11, WEC removed the design requirements and system definition phases of the PMS SLC ITAAC. The design requirements phase corresponds to the planning activities phase of the SLC in SRP BTP 7-14, and the system definition phase corresponds to the requirements activities phase in the same SRP BTP. WEC made available for audit the software planning documents to support removal of the design requirements phase. The staff audited those software planning documents on several occasions. WEC describes its quality software development process for the AP1000 project in the Common Q SPM and WCAP-15927, Revision 2. The staff reviewed the proprietary and nonproprietary documentation associated with the first two phases of the SLC as it relates to PMS system development.

WEC originally provided 11 documents that comprise the design requirements phase of the AP1000 SLC. On April 9–11, 2008; October 9–16, 2008; January 22–30, 2009; and July 30, 2009, the staff conducted site visits at the Twinbrook WEC location in Rockville, MD, to review the proprietary documents associated with the design requirements phase. WEC continues to modify design and technical information in the documents affecting the supervisory, subordinate, and peer-to-peer relationships of the design requirements phase documents. In RAI-SRP7.1-ICE-03, the NRC asked WEC to explain in the DCD how it meets the requirements of the planning ITAAC. This may include a diagram of the planning process and planning documents related to cyber security and other project-specific documents. **The NRC staff identified this issue as OI-SRP-7.2-02.**

Westinghouse Response:
Westinghouse will revise the DCD as described below to explain how WEC meets the requirements of the planning ITAAC, also known as the design requirements phase of the software lifecycle.

Design Control Document (DCD) Revision:

7.1.2.14.1 Design Process

[*WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:*

- *Conceptual phase (may also be referred to as design requirements phase)*
- *Requirements phase (may also be referred to as system definition phase)*
- *Design phase (may also be referred to as hardware and software development phase)*
- *Implementation phase (may also be referred to as hardware and software development phase)*
- *Test phase (may also be referred to as system integration and test phase)*
- *Installation and checkout phase (may also be referred to as installation phase)*]*

~~The conceptual phase (design requirements phase) has been completed for AP1000.~~

[*WCAP-16096-NP-A (Reference 9) and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.*]*
NABU-DP-00014-GEN (Reference 20) provides lower-level process implementation details.

The planning (or design requirements) phase documents are listed below. Figure 7.1xxxxx shows the relationship of the same documents.

Document 1: WNA-PN-00043-WAPP, "NuStart/DOE Design Finalization Program."

Document 2: WNA-PQ-00201-WAPP, "NuStart/DOE Design Finalization Program Project Quality Plan."

Document 3: WNA-PN-00045-WAPP, "NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan."

Document 4: WNA-PD-00042-WAPP, "NuStart/DOE Design Finalization Protection and Safety Monitoring System So, "ftware Development Plan."

Document 5: WCAP-16096-NP-A, "Software Program Manual for Common Q Systems"

Document 6: NABU-DP-00014-GEN, "Design Process for Common Q Safety Systems"

Document 7: WNA-PV-00009-GEN, "Verification & Validation Process for the Common Q Safety Systems"

Document 8: WNA-PT-00058-GEN, "Testing Process for Common Q Safety Systems"

Document 9: NABU-DP-00015-GEN , "Common Q Software Configuration Management Guidelines"

Document 10: 00000-ICE-3889, "Coding Standards & Guidelines for Common Q Systems"

Document 11: WNA-VR-00213-GEN, and is now APP-PMS-GER-020, "Protection and Safety Monitoring System Concept Phase V&V Summary Report."

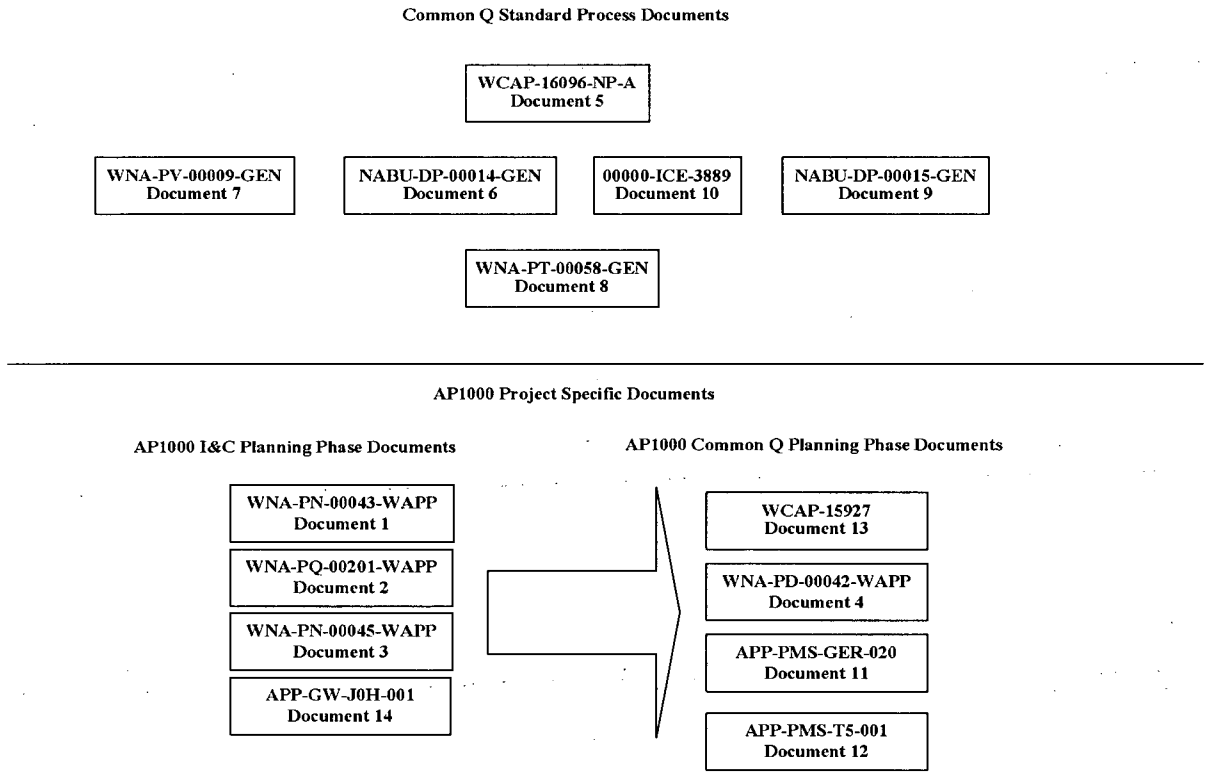
Document 12: APP-PMS-T5-001, "AP1000 Protection and Safety Monitoring System Test Plan"

Document 13: WCAP-15927, "Design Process for AP1000 Common Q Safety Systems"

Document 14: APP-GW-J0H-001, "AP1000 I&C Systems Cyber Security Plan"

PRA Revision:
None

Technical Report (TR) Revision:
None



Westinghouse Proprietary Class 2