



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: 412-374-6206
Direct fax: 412-374-5005
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP/NRC2418

April 2, 2009

Subject: AP1000 Response to Request for Additional Information (SRP 7)

Westinghouse is submitting a response to the NRC request for additional information (RAI) on SRP Section 7. This RAI response is submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in this response 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 RAI(s):

RAI-SRP7.1-ICE-04 R1
RAI-SRP7.1-ICE-10 R1

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,

A handwritten signature in black ink, appearing to read 'Robert Sisk'.

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

/Enclosure

1. Response to Request for Additional Information on SRP Section 7

cc:	D. Jaffe	- U.S. NRC	1E
	E. McKenna	- U.S. NRC	1E
	S. Mitra	- U.S. NRC	1E
	C. Proctor	- 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

Response to Request for Additional Information on SRP Section 7

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.1-ICE-04

Revision: 1

Question (Revision 0):

Demonstrate to what quality standards the Westinghouse NPP organization will hold its employees, and any subcontractor organizations, throughout the project plan and design process for any AP1000 safety-related software system.

Several documents listed as proof of completion of the Design Requirements Phase are actually documents detailing the relationship between Westinghouse RRAS and Westinghouse NPP (for example, RRAS AP1000 NuStart I&C Program Project Plan (WNA-PN-00031-GEN) and RRAS AP1000 NuStart I&C Program Project Quality Plan (WNA-PQ-00166-GEN)). While the documents reveal how the subcontractor (Westinghouse RRAS) interfaces with the parent organization (Westinghouse NPP), they do not provide information detailing how Westinghouse NPP interfaces, and holds accountable, Westinghouse RRAS, employees, and other subcontractors. The response to this question should outline the standards used by Westinghouse NPP and how it ensures subordinate organizations, or persons, comply with those standards.

Westinghouse Response (Revision 0):

Quality Management System

The Westinghouse quality policy is entitled "Quality Management System" (QMS). It has been developed to comply with regulatory, industry, and customer quality requirements imposed by customers or regulatory agencies for items and services provided by Westinghouse world-wide operations. The QMS describes the Westinghouse commitments to the quality assurance requirements of ISO 9001; ISO 9000-3; 10CFR50, Appendix B; ASME NQA-1; and IAEA 50-C-QA.

The QMS applies to all Westinghouse (including NPP, RRAS, Services, and Fuel) activities that affect the quality of items and services supplied by Westinghouse. It defines the basic requirements applicable to customer contracts and is a commitment to our customers. It serves as a directive for all functions in establishing necessary policies and procedures that comply with the requirements of ISO 9001:2000 and ISO 9000-3:1997; and in addition, as applicable for safety-related activities, 10CFR50, Appendix B; ASME NQA-1-1994 Edition; and IAEA 50-C-QA, Revision 1.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

AP1000 Nuclear Power Plants Program Operating Procedures (APP-GW-GAP-100)

Aligned with the Quality management System is the AP1000 Nuclear Power Plants Program Operating Procedures. This document encompasses all the procedures utilized by NPP for maintaining operational control. Included in those procedures are the following:

- QA Program
- Design Control (including change control)
- Procurement Document Control
- Document Control (including control of document preparation, review, and approval)
- Inspection
- Test Control
- Corrective Action
- Interface Agreements

These are just a sampling of the procedures in place to maintain operational control.

Westinghouse REVISED Response based on NRC comments from the January 29-30 meeting (Revision 1):

In addition to the Revision 0 response, the following information is provided per discussions at the January 29-30 meeting:

- RRAS is the acknowledged expert and sole supplier of the AP1000 safety system. They are held accountable, as an NPP supplier, to comply with all the applicable standards associated with developing a safety system. RRAS is responsible for all aspects of system development, including system design, system licensing, and system delivery. RRAS, as an NPP supplier and as a member of Westinghouse Electric Company, is also governed by and held accountable to the Quality Management System of the Westinghouse Electric Company.
- The requirements for qualifying Commercial-Off-The-Shelf (COTS) software are found in Section 11 of the Common Q Topical Report (WCAP-16096-P-A).

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.1-ICE-10
Revision: 1

Question (Revision 0):

Westinghouse has requested to remove the reference to WCAP-15927, "Design Process for AP1000 Common Qualified Platform Safety Systems," which was submitted in addition to the Software Program Manual WCAP-16096-NP-A, Revision 1A (previously designated as CES-195, Revision 1) to resolve Requests for Additional Information 420.001 and 420.023, posed during the development and certification of the original AP1000 final safety evaluation report. Demonstrate what measures will be taken to ensure information contained in this report are not removed. If another document covers the same information but is not currently on the docket, submit that document on the docket.

Westinghouse Response (Revision 0):

RAI 420.023 requested a description of a formal design implementation process with a phased inspection, test, analysis and acceptance criteria (ITAAC) for AP1000 specific Common Q system design development. The description of the development plan should include details of the hardware and software management plan, the configuration plan, and the verification and validation plan. The detailed description should be non-proprietary. The new document should be part of AP1000 Tier 2 Information Requiring NRC Approval for Change (Tier 2*).

The Software Program Manual for Common Q Systems, WCAP-16096-NP-A (Reference 1), is a Tier 2* document that addresses these items requested in RAI-420.023. The NRC stated in its SER for the Common Q Platform, ML003740165 (Reference 2), "CENP's 'Software Program Manual for Common Q Systems' (SPM) specifies plans for implementing a structured software life cycle process for application software and provides guidance for configuration management of commercial-grade hardware and previously developed software." "The staff finds the software program manual acceptable dependent upon the resolution of an open item related to the scope of module testing. Licensees using the Common Q platform for plant-specific applications will be required to implement the application software in accordance with CENP's software program manual."

The issue regarding module testing was subsequently closed in the NRC SER dated June 2001, ML011690170 (Reference 3), (see RAI response RAI-SRP 7.1-ICE-29).

Therefore the original request for docketed design process information is fulfilled by the Software Program Manual for Common Q Systems (WCAP-16096-NP-A), and NABU-DP-00014-GEN (Reference 4) does not have to be Tier 2*.

Westinghouse will revise the DCD as shown below to further clarify this issue.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

References:

1. WCAP-16096-NP-A, Revision 01A, "Software Program Manual for Common Q Systems," January 2004.
2. "Acceptance for Referencing of Topical Report CENPD 396 P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 1 (TAC No. MA1677)," U.S. Nuclear Regulatory Commission, August 11, 2000. NRC Accession Number: ML003740165.
3. "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD 396 P, Revision 1 and CE CES 195, Revision 1 (TAC No. MB0780)," U.S. Nuclear Regulatory Commission, June 22, 2001. NRC Accession Number: ML011690170.
4. NABU-DP-00014-GEN, Rev. 1 (Proprietary), "Design Process for Common Q Safety Systems," March 2006.

Design Control Document (DCD) Revision:

Revise DCD Rev.16 Subsection 7.1.2.14.1 as follows:

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.

PRA Revision:



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

None

Technical Report (TR) Revision:

None

Westinghouse REVISED response based on NRC comments from the January 29-30 meeting (Revision 1):

WCAP-15927, "Design Process for the AP1000 Common Q Safety Systems" (Reference 1), is intended to describe the design process used by the design team in the development of the AP1000™ Protection and Safety Monitoring System. WCAP-15927 supplements WCAP-16096-NP-A, "Software Program Manual for Common Q Systems" (Reference 2) (the SPM), and mimics the Westinghouse Proprietary document, NABU-DP-00014-GEN, "Design Process for Common Q Safety Systems" (Reference 3), for application development. Therefore, it concentrates on the design team's activities and does not provide any detail on life cycle verification and validation (V&V). The V&V activities are described in the SPM at a higher level and are detailed in WNA-PV-00009-GEN, "Verification and Validation Process for Common Q Safety Systems" (Reference 4).

During the January 2009 meetings between Westinghouse and the NRC, the NRC expressed concerns about what appears to be a changed direction on the Westinghouse application of requirement traceability analysis between the Rev. 0 and not-yet-docketed Rev. 1 of WCAP-15927. The concerns stem from the revision to Figure 1, "Development Process," of WCAP-15927.

The V&V method applied to the life cycle phases (i.e., the side note on Figure 1 of WCAP-15927), is not detailed in WCAP-15927. Therefore, without the benefit of textual description of the lifecycle V&V activities, the figure does not provide enough detail to draw a conclusion on the Westinghouse approach to the requirement traceability process. This approach is defined in the SPM.

The Westinghouse approach to requirement traceability has not changed from Rev. 0 of WCAP-15927 and is described in the SPM. For clarification purposes, however, Westinghouse will revise the figure as depicted below to better describe the approach to requirement traceability, and reference the SPM for more details.

Note: The SPM and the more detailed V&V process for Common Q Safety Systems continues to comply with the applicable industry standard IEEE 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 5), as endorsed by Regulatory Guide 1.168, Rev. 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

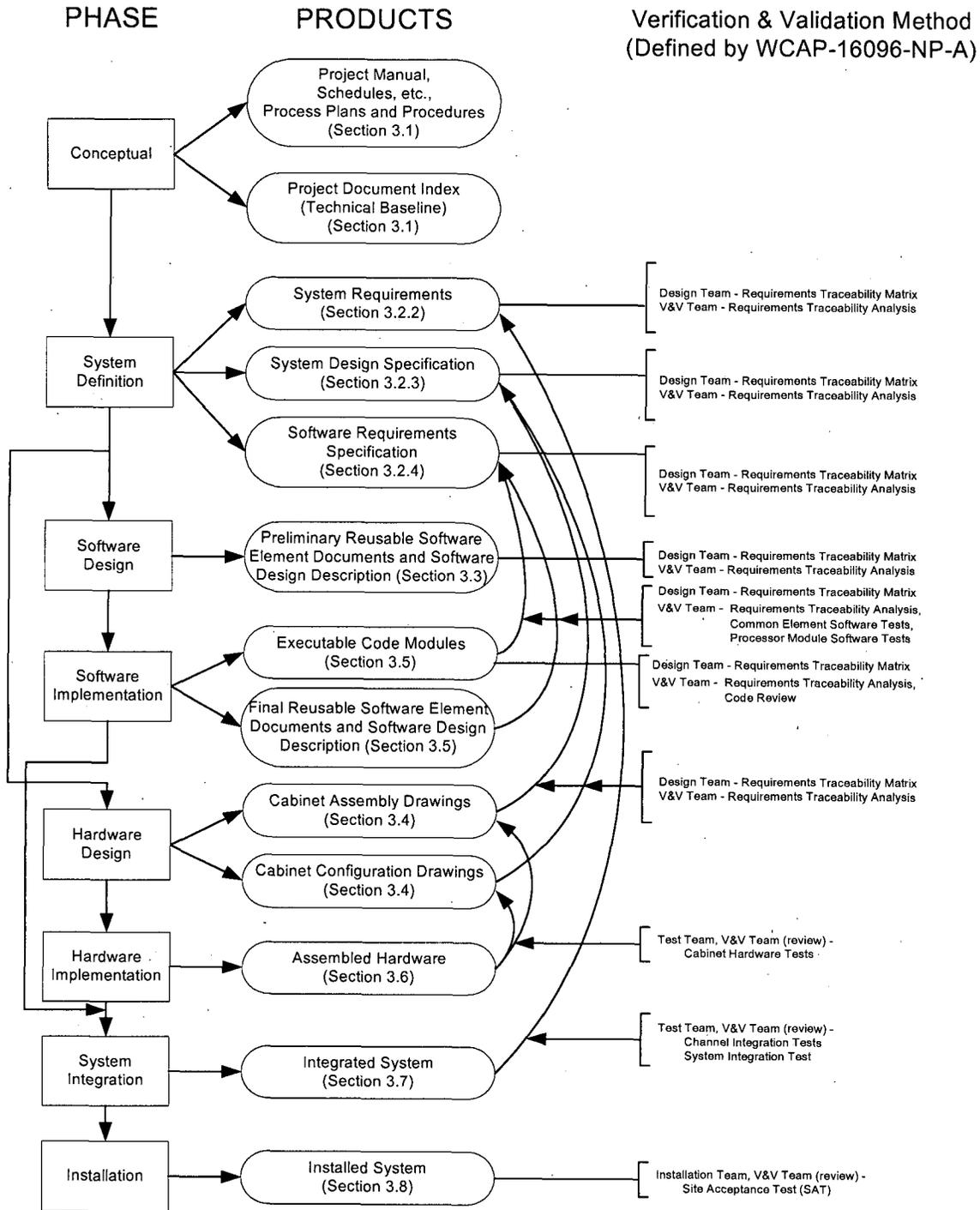
Nuclear Power Plants” (Reference 6), with respect to requirement traceability analysis.

The independent V&V (IV&V) team has always been tasked with the requirement traceability analysis. However, the design team provides the Requirement Traceability Matrix (RTM) as input to IV&V team for analysis. If the IV&V team was also tasked with developing the RTM, there would be nobody to perform a third-party review of the work produced, and the purpose of having IV&V in the first place would be jeopardized.

Westinghouse will reinstate WCAP-15927 in Chapter 7 of the DCD and remove the reference to NABU-DP-00014-GEN. Therefore the only two docketed submittals describing the PMS software life cycle activities will be the Common Q Software Program Manual (WCAP-16096-NP-A) and WCAP-15927-NP-A.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

References:

1. WCAP-15927, Rev. 1 "Design Process for the AP1000 Common Q Safety Systems," Westinghouse Electric Company LLC.
2. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
3. NABU-DP-00014-GEN, Rev. 2, "Design Process for Common Q Safety Systems," Westinghouse Electric Company LLC.
4. WNA-PV-00009-GEN, Rev. 3, "Verification and Validation Process for Common Q Safety Systems," Westinghouse Electric Company LLC.
5. IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation," Institute for Electrical and Electronics Engineers, Inc, 1998.
6. Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Revision 1, February 2004.

Design Control Document (DCD) Revision:
None

PRA Revision:
None

Technical Report (TR) Revision:

WCAP-15927, Rev. 2 will be submitted to the NRC with an updated figure as described in the Rev. 1 response of this RAI.