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/NRC2467

May 13, 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-03 R1
RAI-SRP7.9-ICE-11 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,

D. A. Lindgren / FOR

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

/Enclosure

1. Response to Request for Additional Information on SRP Section 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

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-03
Revision: 1

Question (Revision 0):

Provide a roadmap describing the relationship between the eleven documents that comprise Design Requirements Phase.

Westinghouse provided eleven documents that comprise the design requirements phase of the AP1000 software development lifecycle. On April 9-11, 2008, the NRC staff conducted a site visit to Westinghouse's Rockville, MD office to review the eleven documents. However, the staff had difficultly navigating through the eleven documents as there were multiple references in a single document to one of the other eleven documents, or references to documents that were not present at the office. Therefore, a roadmap is needed that shows the peer-to-peer relationship, as well as, what documents serve as subordinates to others and what documents serve as supervisory documents to others.

Westinghouse Response (Revision 0):

The eleven documents provided by Westinghouse were presented to NRC during the AP 1000 NuStart PMS Design Requirements Phase Meeting/Inspection October 3, 4, 5, 2006 and provided at the Rockville, MD office are:

1. RRAS AP1000 NuStart I&C Program Project Plan (WNA-PN-00031-GEN)

2. RRAS AP1000 NuStart I&C Program Project Quality Plan (WNA-PQ-00166-GEN)

3. AP1000 NuStart Protection and Safety Monitoring System Project Plan (WNA-PN-00035-GEN)

4. AP1000 NuStart Protection and Safety Monitoring System Software Project Plan (WNA-PJ-00071-GEN)

5. Software Program Manual for Common Q Systems (WCAP-16096-NP-A)

6. Design Process for Common Q Safety Systems (NABU-DP-00014-GEN)

7. Verification & Validation Process for the Common Q Safety Systems (WNA-PV-00009-GEN)

8. Testing Process for Common Q Safety Systems (WNA-PT-00058-GEN)

9. Common Q Software Configuration Management Guidelines (NABU-DP-00015-GEN)

10. Coding Standards & Guidelines for Common Q Systems (00000-ICE-3889)

11. AP1000 NuStart Protection and Safety Monitoring System Project Concept Phase V&V (WNA-VR-00213-GEN)

Documents 1 and 2 (WNA-PN-00031-GEN and WNA-PQ-00166-GEN respectively) are plans that identify information necessary to manage and execute the overall I&C design program/project (the design of the AP 1000 Instrumentation and Control) This includes items such as the project scope, deliverables, project milestones, project stages, project inputs and review, key personnel, quality requirements and project interfaces. These documents are at the top level of the hierarchy.

Documents 3 and 4 (WNA-PN-00035-GEN and WNA-PJ-00071-GEN respectively) are plans that identify information necessary to manage and execute the design of the AP1000 Protection and Safety Monitoring System (PMS) and similarly discuss items such as the project scope, deliverables, project milestones, project stages, project inputs and review, key personnel, quality requirements and project interfaces. These specific PMS documents are subordinate to the top-level documents described above.

Document 5 (WCAP-16096-NP-A) represents Westinghouse's licensing commitments to the NRC for the design life cycle activities for any application developed using the Common Q Platform. This document is imposed on the project by Document 4 (WNA-PJ-00071-GEN)).

Documents 6 through 10 are process and methodology documents which are followed in the design and implementation of the Protection and Safety Monitoring System (using the Common Q platform), to ensure compliance to Document 5 (WCAP-16096-NP-A). Documents 6 and 7 (NABU-DP-00014-GEN and WNA-PV-00009-GEN respectively) are the top level documents for process and methodology in Westinghouse for Common Q systems. Document 6 is the process to be followed by the design team, and Document 7 is the process to be used by the V&V team. Documents 8-10 (WNA-PT-00058-GEN, NABU-DP-00015-GEN and 00000-ICE-3889 respectively) are more detailed instructions, standards and guidelines in the area of testing, configuration control and coding standards.

Document 11 summarizes the verification and validation activities, reviews performed and the results of these reviews during the design requirements phase of the AP 1000 Protection and Safety Monitoring System project.

The attached figure shows the document hierarchy reflecting the relationship between the eleven documents.

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

The attached figure shows the relationship of the eleven planning documents. Since the October 2006 meeting, the AP1000 planning documents (Documents 1-4 and 11) have been revised and their document numbers have changed as follows:

Document 1, the RRAS AP1000 NuStart I&C Program Project Plan, was WNA-PN-00031-GEN, and is now WNA-PN-00043-WAPP, "NuStart/DOE Design Finalization Program."

Document 2, the RRAS AP1000 NuStart I&C Program Project Quality Plan, was WNA-PQ-00166-GEN, and is now WNA-PQ-00201-WAPP, "NuStart/DOE Design Finalization Program Project Quality Plan."

Document 3, the AP1000 NuStart Protection and Safety Monitoring System Project Plan, was WNA-PN-00035-GEN, and is now WNA-PN-00045-WAPP, "NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan."

Document 4, the AP1000 NuStart Protection and Safety Monitoring System Software Project Plan, was WNA-PJ-00071-GEN, and is now WNA-PD-00042-WAPP, "NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan."

Document 11, the AP1000 NuStart Protection and Safety Monitoring System Project Concept Phase V&V, was WNA-VR-00213-GEN, and is now APP-PMS-GER-020, "Protection and Safety Monitoring System Concept Phase V&V Summary Report."

Westinghouse has revised the original figure attached to the RAI response to more accurately reflect the relationship of the eleven documents with one another.

Design Control Document (DCD) Revision:
None

PRA Revision:
None

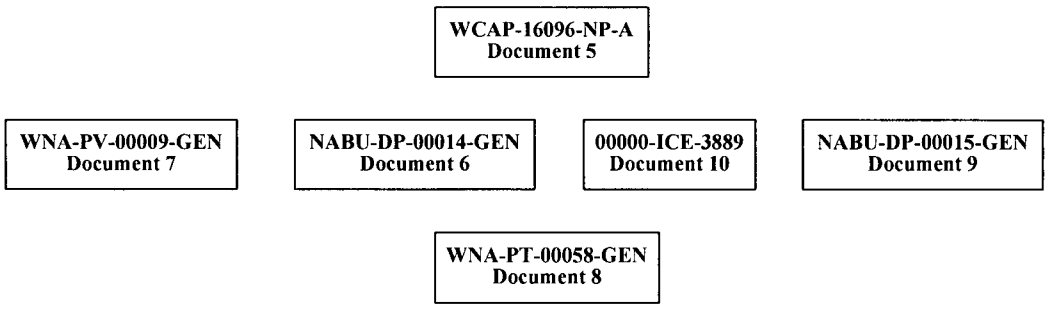
Technical Report (TR) Revision:
None

AP1000 TECHNICAL REPORT REVIEW

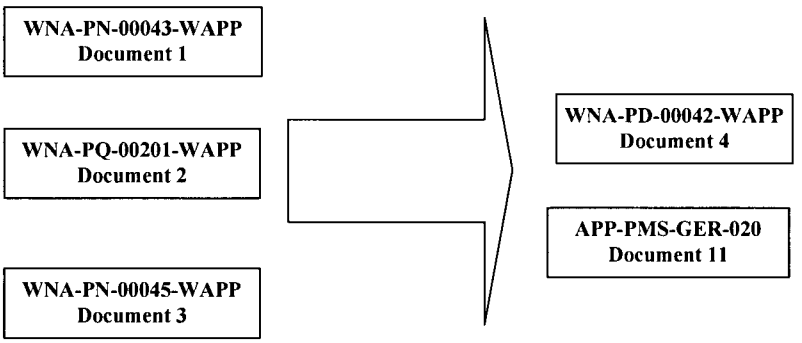
Response to Request For Additional Information (RAI)

RAI-SRP-7.1-ICE-03 Attachment

Common Q Standard Process Documents



AP1000 Project Specific Documents



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.9-ICE-11
Revision: 1

Question (Revision 0):

Provide additional information on the implementation of cyber security measures for the non-safety data network. Demonstrate how the network design prevents unauthorized access of the non-safety network.

In Section 3.1.3 of WCAP-16774-P, Westinghouse commits to providing off-site access security via the use of multilayered firewalls, with the Ovation System providing only unidirectional access to higher and higher levels in the hierarchy. Demonstrate via text and schematics how this hierarchy is defined. For example, where are the firewalls placed? What types of firewalls will be used (e.g. stateful, stateless)? How will Westinghouse prevent workstations within higher security levels from downloading malicious code (either intentionally or unintentionally) from devices at lower security levels?

Westinghouse Response (Revision 0):

WCAP-16791-P Revision 1 demonstrates the hierarchy of how data is passed, unidirectional from the highest levels of security (Safety and Non-Safety Control Systems) to lower levels of security. Security will be accomplished through a combination of cutwire gateways and firewalls. The cutwire gateways are placed between the Cyber Security Level 4 network and the Cyber Security Level 3 network, and firewalls are placed between the Cyber Security Level 3 network and the Cyber Security Level 2 Site Business LAN. Workstations in Levels 3 and 4 will not have internet access to download malicious code. Physical access to all input devices except keyboard and mice is secured in locked / alarmed cabinets. Physical access to keyboard and mice is also controlled via site authorization program. Design implementation details such as the firewall types will be completed as part of the ongoing design finalization effort completing 2010.

Reference:

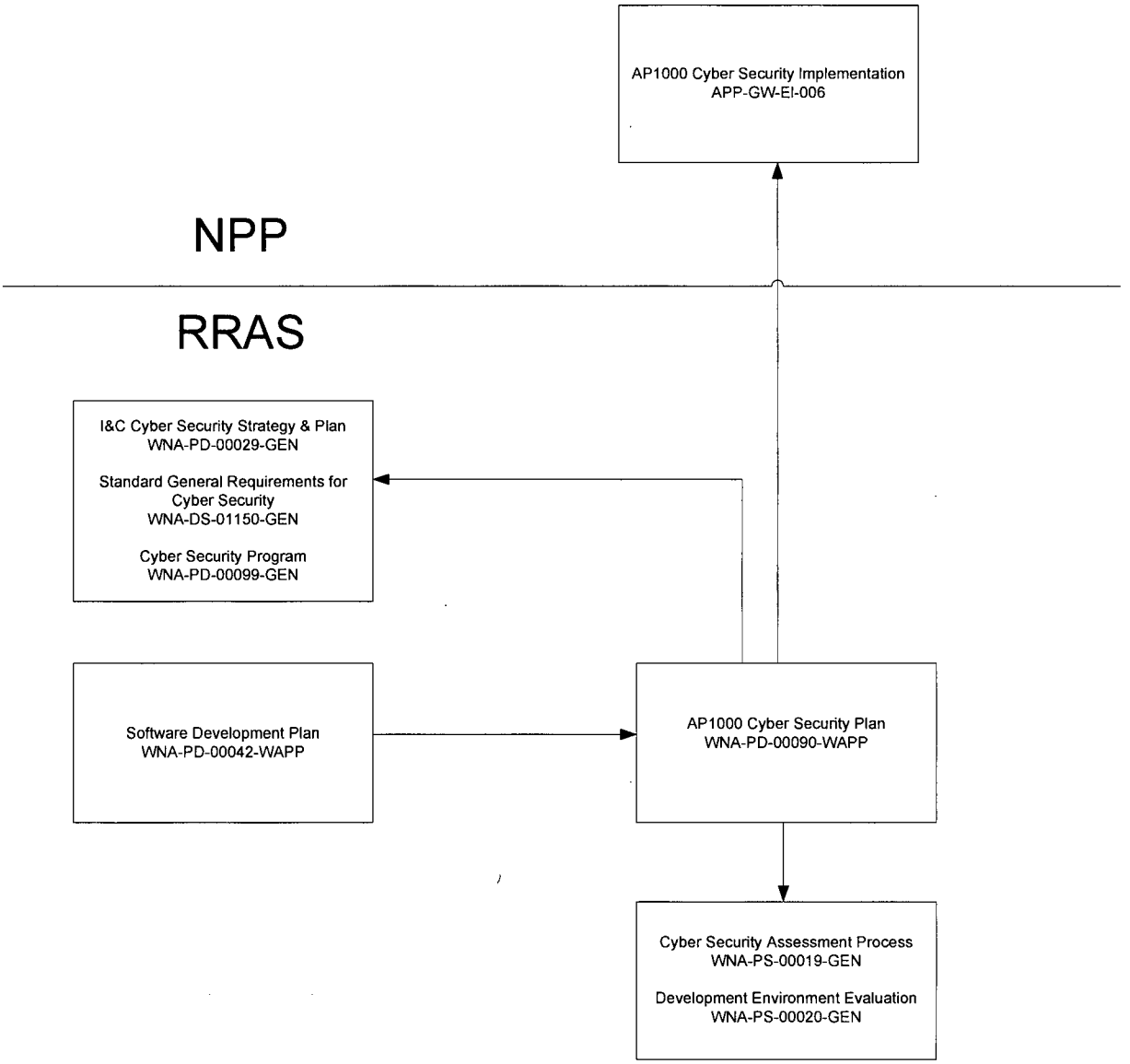
WCAP-16791-P Revision 1, AP1000 Cyber Security Implementation

Westinghouse REVISED Response based on NRC comments from the January 29-30, 2009 and April 21, 200 meetings (Revision 1):

At the January 29-30 meeting, the NRC stated that there was inadequate information regarding the cyber security assessments in WNA-PD-00042-WAPP, Rev. 1, "NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan." The description should include the systems that will be assessed and the criteria used to assess the systems.

Westinghouse has developed an AP1000 Cyber Security Plan (WNA-PD-00090-WAPP) that will be provided to the NRC for audit. It will describe the cyber security program for AP1000 and reference the cyber security criteria, program description, and procedures that will be employed. The AP1000 PMS Software Development Plan (WNA-PD-00042-WAPP) will be revised to reference this AP1000 Cyber Security Plan. The attached figure illustrates the relationship of the AP1000 PMS Software Development Plan, the AP1000 Cyber Security Plan, and the criteria, program description and procedures that will be employed.

Figure 1
Relationship Between PMS Software Development Plan and the AP1000 Cyber Security Plan and its References



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

References:

WNA-PD-00042-WAPP, Rev. 1, "NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan," Westinghouse Electric Company LLC.

NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," U.S. Nuclear Regulatory Commission, October 2004.

WNA-DS-01150-GEN, Rev. 0, "Standard General Requirements for Cyber Security," Westinghouse Electric Company LLC.

APP-GW-GLR-104, Rev. 1, "AP1000 Cyber Security Implementation," Westinghouse Electric Company LLC.

APP-GW-E1-006, Rev. 0, "AP1000 Cyber Security Implementation," Westinghouse Electric Company LLC.

WNA-PD-00029-GEN, Rev. 0, "I&C Cyber Security Strategy & Plan," Westinghouse Electric Company LLC.

WNA-PD-00099-GEN, "Cyber Security Program, "Westinghouse Electric Company LLC.

WNA-PD-00090-WAPP, Rev. 0, "AP1000 I&C Cyber Security Plan," Westinghouse Electric Company LLC.

WNA-PS-00019-GEN, Rev. 0, "Cyber Security Assessment Process," Westinghouse Electric Company LLC.

WNA-PS-00020-GEN, "Development Environment Evaluation," Westinghouse Electric Company LLC.

Design Control Document (DCD) Revision:
None

PRA Revision:
None

Technical Report (TR) Revision:
None