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: 412-374-6206
Direct fax: 724-940-8505
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP_NRC_002950

July 8, 2010

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-SRP7.0-ICE-11 R2
RAI-SRP7.1-SHA-01 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 Strategy

/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. K. 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-SRP7.0-ICE-11
Revision: 2

Question:

WCAP-17179-P should state that the CIM and SRNC are programmable technology devices and not imply they are hardware devices and therefore be treated as discrete or analog technology. The report should describe the high quality lifecycle development process for the devices.

Westinghouse Response:

The following wording will be updated throughout the AP1000 Component Interface Module Technical Report, WCAP-17179 Revision 1.

The CIM and SRNC are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on programmable technology. The logic is implemented using field programmable gate array (FPGA) technology.

Section 2.7 of "AP1000 Component Interface Module Technical Report," WCAP-17179, Revision 1, will be updated to more thoroughly describe the high quality development process for the CIM and SRNC modules.

NRC Question from 6/24/10 Email:
The CIM TR should describe logic being treated as software.

Westinghouse Amended Response Based on 6/28/10 Conference Call with the NRC:
The CIM development process, as described in Section 2.7 of "AP1000 Component Interface Module Technical Report," WCAP-17179, will be deleted in Revision 2 of the WCAP. Additionally, all references to the MSFIS project and/or Wolf Creek Generating Station will be removed from WCAP-17179.

The following sentences will be updated in Section 1.1.

The CIM system components are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on FPGA technology. FPGA-based systems employ software tools to configure and test the resulting customized circuitry. As a result, the CIM will be developed following a high-quality software lifecycle development process.

Westinghouse will scrub all CIM related documents to ensure wording consistency with Section 1.1 of WCAP-17179 that CIM system components are logic based modules that do not use

microprocessors or software for operation. The following document is just one example of a document that will be revised:

- WCAP-16675 (APP-GW-GLR-071), "AP1000™ Protection and Safety Monitoring System Architecture Technical Report"

In addition, the DCD revision 18 will include an ITAAC to describe the CIM development process. The following words are added as Item 14 to DCD Tier 1 Subsection 2.5.2 and Table 2.5.2-8.

Design Control Document (DCD) Revision:

2.5.2 Protection and Safety Monitoring System

Design Description

14. The Component Interface Module CIM) is developed using a planned design process which provides for specific design documentation and reviews.

Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.2-8 specifies the inspections, tests, analyses, and associated acceptance criteria for the PMS.

Table 2.5.2.-8
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14. The Component Interface Module CIM) is developed using a planned design process which provides for specific design documentation and reviews.	An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.	A report exists and concludes that CIM meets the below listed life cycle stages and is approved for use in the AP1000 safety related PMS. Life cycle stages: a. Design requirements phase, may be referred to as conceptual or project definition phase b. System definition phase c. Hardware and software development phase, consisting of hardware and software design and implementation d. System integration and test phase e. Installation phase

PRA Revision:
None

Technical Report (TR) Revision:
WCAP-17179, Revision 2

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: RAI-SRP7.1-SHA-01 (OI-SRP7.1-ICE-02)
Revision: 1

Question:

Westinghouse submitted WCAP 16592-P, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System, (SHA) Revision 1. The report fails to mention any potential failures introduced into the PMS as a result of a design or programming error of the Component Interface Module (CIM). While the CIM uses no software during its operation, a programming language is used extensively during the device's development.

Westinghouse committed to follow IEEE Standard (Std.) 603–1991, ""Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995," that is an incorporate by reference standard within 10 CFR 50.55a, "Codes and Standards". IEEE Std. 603–1991 requires among other things that, safety systems within nuclear power plants be designed and constructed with sufficient Quality, Clause 5.3; and Reliability, Clause 5.15. Westinghouse also committed to following the guidance within Branch Technical Position BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," of NUREG – 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light Water Reactor Edition," (SRP). Within the "Acceptance Criteria for Resources Characteristics of Planning Documents," of BTP 7-14, it relates the applicant should address the use of methods or tools employed for use or development of the safety system. Additionally, Section B.3.1.9, Software Safety Plan discusses the use of a Software Safety Plan and the discussion of risks and hazards the software, or programmable technology, is expected to control. The staff understands the AP1000 PMS SHA is intended to address these hazards and, as such, the staff requires discussion within the AP1000 PMS SHA to focus upon the issue of software hazards encountered, and successfully mitigated or eliminated during the CIM development process.

Westinghouse Amended Response Based on 6/28/10 Conference Call with the NRC:

WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System" will be revised as follows:

Section 2.4:

The ILC cabinet contains redundant ILP process stations, in two separate subracks, each receiving HSLs from the two LCL process stations that generate the system-level automatic commands. The two ILP process stations output the component actuation commands via independent HSLs through a safety remote node controller (SRNC). The SRNC is described in WNA-DS-01272-GEN, "Safety System Remote Note Controller Hardware Requirements Specification" (Reference 9). The commands then go via the SRNC to a component interface module (CIM) for air-operated valve (AOV), hydraulic-operated

valve (HOV), motor-operated valve (MOV), solenoid-operated valve (SOV), switchgear, and squib operated valves. The CIM is described in detail in WNA-DS- 01271-GEN, "Component Interface Module (CIM) Hardware Requirements Specification" (Reference 10). The two ILP process stations use a unidirectional HSL to the CIM via the SRNC. The CIM actuation logic is a logical AND to prevent spurious actuations on single failures.

The following sentence will be removed from the last paragraph of Section 2.4:

"The SRNCs and CIMs contain no processors and execute no code and will not be discussed in this analysis."

The following paragraph is added to the end of Section 2.4:

"The SRNCs and CIMs are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on FPGA technology. FPGA-based systems employ software tools to configure and test the resulting customized circuitry. As a result, the SRNC and CIM software development tools are considered in the software hazard analysis for AP1000."

The following table will be added to Section 5:

Name	Hazard Description	Hazard Cause	Method of Detection	Potential Consequences	Safety Hazard Mitigation	Safety Hazard Control Verification Method
CIM or SRNC	Logical programming error of the CIM or SRNC.	Programming error during creation of the FPGA logic in the software tool.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	DAS for common mode failure affecting CIMs in multiple divisions	IV&V review of the functional logic. IV&V testing to functional requirements.

	Error in software tool used to configure FPGA.	An error in the FPGA software tool results in the wrong FPGA configuration.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	If random tool error failure, then other PMS divisions will perform function. CCF covered by DAS.	IV&V testing to functional requirements.
	Error in software tool used to test FPGA.	An error in the simulation tool used to test the FPGA results in improper indication that FPGA design is correct.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	If random tool error failure, then other PMS divisions will perform function. CCF covered by DAS.	IV&V review of the FPGA logic to functional requirements. Two independent test benches are developed on two independent simulation tools.
	Incorrect image programmed into the CIM or SRNC FPGA.	Human error during the use of the software tool.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	CIM programmed with SRNC FPGA: The CIM would not respond to X bus messages and appear as not installed. This condition is monitored and indicated within PMS. SRNC programmed with CIM image: The SRNC would not respond to HSL messages and appear as not installed. This condition is monitored and indicated within PMS.	Functional testing of module before installation into PMS.

References:

1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

Design Control Document (DCD) Revision:
None

PRA Revision:
None

Technical Report (TR) Revision:
1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"