June 21, 2010

Mr. Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization
Westinghouse Electric Company
P.O. Box 355
Pittsburg, PA 15230-0355

SUBJECT: AUDIT REPORT FOR LIFECYCLE PHASES ONE AND TWO DOCUMENTATION VALIDATION RELATED TO PROTECTION AND SAFETY MONITORING SYSTEM AND DIVERSE ACTUATION SYSTEM FOR THE AP1000 DESIGN CERTIFICATION AMENDMENT APPLICATION

Dear Mr. Sisk:

On April 12 through 16, 2010, the U.S. Nuclear Regulatory Commission (NRC) conducted an audit to verify information related to the safety-related Protection and Safety Monitoring System (PMS) and the important-to-safety Diverse Actuation System (DAS) at the applicant's facility in Warrendale, Pennsylvania. The intent of this audit was to gain understanding with regard to the applicant's implementation of programs and processes which track ongoing work or completion of development tasks or stages related to the Westinghouse AP1000 Design Certification Amendment application. In particular, this regulatory audit focused on two Instrumentation and Controls (I&C) systems; the system responsible for Reactor Trip, Engineering Safety Features Actuation System (ESFAS), and Post Accident Monitoring functions as well as safety-related component control, which Westinghouse describes as the PMS. The second system serves as the separate and diverse system that backs-up the PMS in the event of a software common-cause failure of the PMS. Westinghouse describes this system as the DAS.

The audit examined and evaluated proprietary technical, procedural, and process information related to the PMS and DAS. The specific areas of review dealt with the first two phases of the PMS and DAS developmental lifecycles, which Westinghouse refers to as the Design Requirements (or Conceptual) phase and the System Definition phase. Branch Technical Position (BTP) 7-14 within Chapter 7 of NUREG 0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: Light-Water Reactor Edition," SRP refers to these two phases of development as the "Planning Activities" phase and the "Requirements Activities" phase of the PMS software lifecycle and the DAS programmable technology lifecycle. The NRC audit staff reviewed the documents provided to verify compliance with the Commission's rules and regulations.

The applicant proposed in Revision 17 of the AP1000 Design Control Document (DCD) to remove the first two phases, (Design Requirements and System Definition), of the developmental lifecycles for both the PMS and DAS. The attached enclosure provides the NRC staff's audit results of the topical areas listed above. In summary, the staff concluded that:

- Due to the significant number of missing or inconsistent requirements specifications for the PMS, the System Definition Phase from the PMS Tests, Analyses and Acceptance Criteria (ITAAC) should not be removed. In addition, the staff found a number of instances where the traceability of the requirements specifications was not clear and sufficient decomposition and provision of acceptance criteria were not observed.

- The staff was unable to identify adequate Component Interface Module planning and development documentation, particularly with regards to independent verification and validation. The staff was also unable to identify a vulnerability assessment for the secure development and operational environment for the PMS. These issues prevent the removal of the PMS Design Requirements Phase from the PMS ITAAC.

- The staff was unable to identify adequate design information regarding the DAS setpoint methodology for automatic DAS functions and the operator action timing requirements. This issue prevents the removal of the DAS Design Requirements and System Definition Phases from the DAS ITAAC.

You and your staff are welcome to contact me regarding the audit report.

Sincerely,

/RA/

Eileen M. McKenna, Branch Chief
AP1000 Projects Branch 2
Division of New Reactor Licensing
Office of New Reactors

Enclosure:
As stated

- Due to the significant number of missing or inconsistent requirements specifications for the PMS, the System Definition Phase from the PMS Tests, Analyses and Acceptance Criteria (ITAAC) should not be removed. In addition, the staff found a number of instances where the traceability of the requirements specifications was not clear and sufficient decomposition and provision of acceptance criteria were not observed.

- The staff was unable to identify adequate Component Interface Module planning and development documentation, particularly with regards to independent verification and validation. The staff was also unable to identify a vulnerability assessment for the secure development and operational environment for the PMS. These issues prevent the removal of the PMS Design Requirements Phase from the PMS ITAAC.

- The staff was unable to identify adequate design information regarding the DAS setpoint methodology for automatic DAS functions and the operator action timing requirements. This issue prevents the removal of the DAS Design Requirements and System Definition Phases from the DAS ITAAC.

You and your staff are welcome to contact me regarding the audit report.

Sincerely,

/RA/

Eileen M. McKenna, Branch Chief
AP1000 Projects Branch 2
Division of New Reactor Licensing
Office of New Reactors

Enclosure:
As stated

Distribution
PUBLIC
RidsNroDnrlNwe2 TJackson WRoggenbrodt SKMitra EMcKenna
RidsOgcMailCenter JZhao KDMott RBeacom DZhang
DSantos JKent
RidsAcrsAcnwMailCenter
ADAMS Accession Number: ML101740602 (LTR) ML101380259 (Report) NRC-001
ML101380277 (PKG)

OFFICE	NRO/DNRL/NWE2:LA	NRO/DNRL/NWE2:BC	NRO/DNRL/ICE1:PM	NRO/DE/ICE1: BC	NRO/DNRL/NWE2: BC
NAME	RButler	SKMitra	WARoggenbrodt	TJackson	EMcKenna for JCruz
DATE	05/26/2010	06/14/2010	06/16/2010	06/16/2010	06/21/2010

OFFICIAL RECORD COPY