August 27, 2002

Mr. Michael M. Corletti
Passive Plant Projects & Development
AP600 & AP1000 Projects
Westinghouse Electric Company
Post Office Box 355
Pittsburgh, Pennsylvania 15230-0355

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION LETTER NO. 3 - AP1000 DESIGN CERTIFICATION REVIEW (TAC NO. MB4683)

Dear Mr. Cummins:

By letter dated March 28, 2002, Westinghouse Electric Company (Westinghouse) submitted its application for final design approval and standard design certification for the AP1000.

The Nuclear Regulatory Commission (NRC) staff is performing a detailed review of your design certification application to ensure that the information is sufficiently complete to enable the NRC staff to reach a final conclusion on all safety questions associated with the design before the certification is granted.

The NRC staff has determined that additional information is necessary to continue the review. Enclosure 1 contains requests for additional information (RAIs) regarding the instrumentation and control and electric power systems portions of the AP1000 design certification application. These RAIs were sent to you via electronic mail on August 14 and August 19, 2002. We also discussed on August 19, 2002, that Westinghouse would provide a response to these RAIs by December 2, 2002. Receipt of the information by December 2, 2002, will support the schedule documented in our letter dated July 12, 2002.

Enclosure 2 contains a summary of previously-issued RAI correspondence.

If you have any questions or comments concerning this matter, you may contact me at (301) 415-3053 or at ljb@nrc.gov.

Sincerely,

/RA/

Lawrence J. Burkhart, AP1000 Project Manager
New Reactor Licensing Project Office
Office of Nuclear Reactor Regulation

Docket No. 52-006

Enclosure: As stated

cc: See next page

August 27, 2002

Mr. Michael M. Corletti
Passive Plant Projects & Development
AP600 & AP1000 Projects
Westinghouse Electric Company
Post Office Box 355
Pittsburgh, Pennsylvania 15230-0355

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION LETTER NO. 3 - AP1000 DESIGN CERTIFICATION REVIEW (TAC NO. MB4683)

Dear Mr. Cummins:

By letter dated March 28, 2002, Westinghouse Electric Company (Westinghouse) submitted its application for final design approval and standard design certification for the AP1000.

The Nuclear Regulatory Commission (NRC) staff is performing a detailed review of your design certification application to ensure that the information is sufficiently complete to enable the NRC staff to reach a final conclusion on all safety questions associated with the design before the certification is granted.

The NRC staff has determined that additional information is necessary to continue the review. Enclosure 1 contains requests for additional information (RAIs) regarding the instrumentation and control and electric power systems portions of the AP1000 design certification application. These RAIs were sent to you via electronic mail on August 14 and August 19, 2002. We also discussed on August 19, 2002, that Westinghouse would provide a response to these RAIs by December 2, 2002. Receipt of the information by December 2, 2002, will support the schedule documented in our letter dated July 12, 2002.

Enclosure 2 contains a summary of previously-issued RAI correspondence.

If you have any questions or comments concerning this matter, you may contact me at (301) 415-3053 or at ljb@nrc.gov.

Sincerely,

/RA/

Lawrence J. Burkhart, AP1000 Project Manager
New Reactor Licensing Project Office
Office of Nuclear Reactor Regulation

Docket No. 52-006

Enclosure: As stated
cc: See next page
DOCUMENT NAME: C:\ORPCheckout\FileNET\ML022390103.wpd
ACCESSION NO. ML022390103

OFFICE	NRLPO/PM	EEIB/BC	NRLPO/DD
NAME	LBurkhart:cn	JCalvo	MGamberoni
DATE	8/21/02	8/21/02	8/26/02

OFFICIAL RECORD COPY

Distribution for letter to M. Corletti dated August 27, 2002

Hard Copy

PUBLIC
NRLPO R/F
LBurkhart
JLyons
MGamberoni
JWilson
JSebrosky

E-Mail

SCollins/JJohnson
RBorchardt
ACRS
OGC
JCalvo
HLi
NTrehan
EMarinos
WJensen
CHolden
CGraham

Request for Additional Information
AP1000 Standard Plant Design
Series 420 Instrumentation and Control
and 435 Electric Power Systems

Series 420 - Instrumentation and Controls

420.001 (Design Control Document (DCD) Section 7.1)

DCD Section 7.1 states that the design certification of AP1000 focuses upon the process used to design and implement instrumentation and controls (I&C) systems for the AP1000. DCD Chapter 7 for the AP1000 has been written to permit the use of either the protection system hardware described in the AP600 DCD or the Common Q system. The U.S. Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP), Chapter 7, Branch Technical Position (BTP) HICB-14, "Guidance on Software Review for Digital Computer-Based Instrumentation and Control Systems," identified certain information that needs to be reviewed with respect to digital I&C design process and implementation. It states that the information should include, but not be limited to, the following areas:

A. Software Life Cycle Process Planning

1. Software management plan
2. Software development plan
3. Software quality assurance plan
4. Integration plan
5. Installation plan
6. Maintenance plan
7. Training plan
8. Operations plan
9. Software safety plan
10. Software verification and validation plan
11. Software configuration management plan

B. Software Life Cycle Process Implementation

1. Safety analyses
2. Verification and validation analysis and test reports
3. Configuration management reports

C. Software Life Cycle Process Design Outputs

1. Software requirements specifications
2. Hardware and Software architecture description
3. Software design specifications
4. Code listing
5. Build documents
6. Installation configuration tables
7. Operations manuals

8. Maintenance manuals
9. Training manuals

In the AP600 design certification, Westinghouse has stated that the process described in WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design Verification and Validation Process Report," is the basis for the associated I&C system inspection, test, analysis and acceptance criteria (ITAAC) which allows the NRC to review the phased implementation of the I&C system design. WCAP-13383 has been designated as a Tier 2* item. AP1000 DCD Section 7.1.7 Reference 9, "CE-CES-195, Rev.01 - Software Program Manual for Common Q Systems," may serve a similar purpose as WCAP-13383 for the AP600 design certification. However, review points should be established in the document to allow NRC to review and audit the design process. A formal commitment is required to include both WCAP-13383 and CE-CES-195 as Tier 2* documents. Any change to these documents will require NRC approval.

Because DCD Chapter 7 for the AP1000 has been written to permit the use of either the protection system hardware described in the AP600 DCD or the Common Q system, Tier 1 Description 2.5.2, "Protection and Safety Monitoring System," should be modified to accommodate the design features in the Common Q system (items related to Questions 420.028 and 420.029 should also be included in the ITAAC). Please provide an updated Tier 1 description of Section 2.5.2 for staff review.

420.002 (DCD 7.1)

One of the characteristics that is identified in BTP 14 is "security." It is applicable as a management characteristic for the software management, maintenance, and operations plan; a functional characteristic for the software requirement specifications, software architecture, software design specifications, codes, system build documents, and installation tables. Please describe how the security aspects are addressed in the AP1000 planning and implementing plant-specific application software in generic digital platforms.

The specific regulations and guidance are as follows:

A. IEEE 603 Section 5.9 requirements addressing "Control of Access."
B. SRP Chapter 7, Section 7.1-C states that controls should address access via network connections or via maintenance equipment.
C. SRP Chapter 7, Section 7.9, "Data Communication (DCS)," states that the DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators.

420.003 (DCD 7.1)

Discuss how the AP1000 I&C "Fail-safe" mode requirement complies with General Design Criterion (GDC) 23, "Protection System Failure Modes," IEEE279, Section 4.5, "Channel Integrity," IEEE603, Section 5.5, "System Integrity," for reactor protection system (RPS), engineered safety feature actuation system (ESFAS), and supporting data communication systems.

420.004 (DCD 7.1)

Discuss the AP1000 I&C system manual control at a system-level provision per requirement of IEEE279 (Section 4.17) for RPS and ESFAS, including associated parameter displays.

420.005 (DCD 7.1.3.3)

DCD 7.1.3.3 states that each soft control device can control safety-related and non-safety-related equipment. Describe how the soft control devices interface with the redundant safety-related components. What type of safeguard in the design can prevent unauthorized or erroneous data entry into the protection system? Discuss the qualification process for the soft control device.

420.006 (DCD 7.1.2.14.2)

Please provide the Commercial Dedication process ITAAC for staff review.

420.007 (DCD 7.1.2.5)

Describe the Qualified Data Processing Subsystems (QDPS) in more detail. DCD takes credit on the QDPS in the Defense-in-Depth and Diversity analysis. Describe the relationship between the QDPS and the reactor trip system (RTS)/ESFAS. Are the QDPS sharing sensors with the RTS or the ESFAS? (Figure 7.1-1 shows some sensors feed into plant protection subsystem directly while some sensors feed into QDPS subsystem). If the QDPS has separate sensors, do they have the same qualification requirement as RTS/ESFAS?

420.008 (DCD Figure 7.1-2)

Describe the “GATEWAY” design and its interface with the Protection and Safety Monitoring System.

420.009 (DCD 7.4.3.1.1)

DCD 7.4.3.1.1, ”Remote Shutdown Workstation,” states that control of non-safety-related components is available, allowing operation and control when alternating current (ac) power is available. ANSI 58.6 - 1996, “Criteria for Remote Shutdown for Light Water Reactors,” Criterion 4.9 states that remote shutdown systems and components, comprising the means to achieve and maintain safe shutdown conditions within 72 hours after a fire-induced evacuation occurrence, shall be capable of being powered by both onsite and offsite electric power systems. Otherwise, an independent onsite power system shall be provided. Discuss the AP1000 design compliance with this criterion.

420.010 (DCD 7.1.2.8)

Provide the Data Communication System (DCS) ITAAC for staff review. SRP Chapter 7, Section 7.9, “Data Communication System,” may be used as guidance.

420.011 (DCD 7.1.7, Item 5)

DCD 7.1.7, Item 5, listed the AP600 protection system setpoint study (WCAP-14605, "Westinghouse Setpoint Methodology for Protection Systems, AP600)" to be applicable for AP1000 design. Explain how the AP600 protection system setpoint study can be used to address all the setpoint concerns for the AP1000 design when the Common Q system will be used as AP1000 protection system hardware.

420.012 (DCD 7.1.7, Item 7)

DCD 7.1.7, Item 7, WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Section 4.10.2, states that the protection and monitoring system (PMS) provides both system-level and component-level manual means of actuating ESF functions, and the diverse actuation system (DAS) provides manual means of actuating selected ESF functions. To support manual ESF actuation, both the PMS and the DAS provide plant information to the operator. Identify all the PMS and the DAS system-level and component-level manual actuation devices for every ESF function and the related supporting indications to the operator.

420.013 (DCD 7.1.7, Item 7)

DCD 7.1.7, Item 7, WCAP-15775, Section 4.11, states that the signal conditioning and data acquisition functions associated with these signals are performed by an independent subsystem in the PMS, not associated with the reactor trip or ESF actuation functions. Describe the system configuration with respect to this statement for both the AP600 system hardware and the Common Q system hardware.

420.014 (DCD 7.1.7, Item 7)

WCAP-15775 has not addressed specific compliance with BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," in SRP Chapter 7. Discuss the AP1000's compliance with the four point positions listed in BTP HICB-19.

420.015 (DCD 7.1.2.12)

Describe the design features of the graphic displays on the workstation and the wall panel. Discuss the interface between the workstation display, the wall panel display, and the qualified display processing system (QDPS).

420.016 (DCD 7.1.2.12)

Describe the design features of the AP1000 alarm system such as alarm setpoint determination, alarm display, alarm message queues, and all the software and hardware to support the alarm systems. Discuss the ITAAC for the alarm management system. Describe how the operating procedures are implemented (computer-based procedures and alarm responses).

420.017 (DCD 7.2.1.1.3)

Describe the reactor coolant hot leg and cold leg temperature measurement arrangement from the sensor to the plant protection system. Describe how the average coolant temperature (Tavg), Delta T, Overtemperature Delta T, and Overpower Delta T setpoint software is developed in the Common Q system.

420.018 (DCD 7.1.2.10)

Describe the ITAAC for the isolation devices to be used in the AP1000 I&C system design.

420.019 (DCD Figures 7.1-3, 7.1-5, 7.1-6, 7.1-8, and 7.1-9)

DCD Section 7.1 states that DCD Chapter 7 for the AP1000 has been written to permit the use of either the protection system hardware described in the AP600 DCD or the Common Qualified Platform (Common Q) described in Reference 8. Justify the deletion of Figures 7.1-3, 7.1-5, 7.1-6, 7.1-8, and 7.1-9 in the AP1000 DCD. These figures are related to the integrated protection cabinets, the ESF actuation cabinets, the protection logic communication cabinets, the qualified data processor, and the protection logic cabinet architecture. Since Reference 8, "CENPD-396-P, Rev.1 - Common Qualified Platform," is a proprietary document, the equivalent information should be provided for both the AP600 design and the Common Q design in the AP1000 DCD.

420.020 (DCD Figures 7.1-2 and 7.1-10)

Describe the multiplexer configuration in the AP1000 design, where the multiplexer will be used in the protection and control systems, how many are used, and how to maintain channel separation. Describe the ITAAC for the multiplexer devices to be used in the AP1000 I&C system design.

420.021 (DCD Figure 7.1-10)

Describe the signal selector in the AP1000 design. Also, describe the ITAAC for the signal selector devices to be used in the AP1000 I&C system design.

420.022 (DCD 7.1.2.11)

The AP600 protection and safety monitoring system performs surveillance testing via a portable tester. Describe the provision provided for the AP1000 surveillance testing. Identify the tasks tested by a portable tester and the tasks tested by the built-in circuit in the protection cabinets.

420.023 (DCD 7.1.7, Items 8, 9, and 10)

During the AP600 review, Westinghouse stated that the process to design, manufacture, install, operate, maintain, and modify the I&C systems is described in DCD Chapter 7 and WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design Verification and Validation Process Report." These procedures are available for NRC review. Provide a formal design implementation process with a phased ITAAC for the 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*).

420.024 (DCD Figure 7.1-4)

In the AP600 design, there is an interface between the Remote Shutdown Workstation and the Reactor Trip Switchgear. Explain why the AP1000 design has not shown this interface. Discuss procedure changes from the AP600 design to the AP1000 design with respect to the control transfer from the main control room to the remote shutdown workstation following an evacuation of the control room.

420.025 (DCD 7.1.7, Item 8)

Describe the program language to be used for the Common Q system (if information has been provided in Reference 8, please identify the specific section). Justify why that language was chosen for the safety system application.

420.026 (DCD 7.1.7, Item 8)

Describe the software system architecture planned for the AP1000 by the Common Q platform. Describe the test methods and test tools that will be used to verify the design of the software program and code for this software architecture feature, and describe the tests performed on the program at run time to verify that it is correct.

420.027 (DCD 6.3.9)

To support the AP600 review, Westinghouse performed a failure mode and effects analysis (FMEA) on Core Makeup Tank (CMT) level instrumentation as documented in WCAP-13594 (proprietary), “FMEA of Advanced Passive Plant Protection System.” This reference is not listed in the AP1000 DCD 6.3.9. Provide this reference for the AP1000 docket if the analysis is still applicable.

420.028 (DCD 7.1.7 item 11)

In the NRC’s safety evaluation report (SER) dated August 11, 2000, on Common Q design (Reference 11 in DCD 7.1.7), the staff identified the following plant-specific action items for the licensee to follow when the Common Q design is implemented in a specific plant. Please address each of these items applicable to the AP1000. If the action item cannot be implemented during the design certification stage, then the action should be included in the Tier 1 Material (ITAAC).

A. Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 input/output modules to be used in the design against its plant-specific input/output requirements (See Common Q SER Section 4.1.1.1.2).

B. A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the Flat-Panel Display System (FPDS). The review of the implementation of such a hardware user interface would be a plant-specific item (See Common Q SER Section 4.1.2).

C. If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and is not to be used such that it is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant-specific FMEAs (See Common Q SER Section 4.2.1.2).

D. Each licensee implementing a Common Q application must verify that its plant environment data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests (See Common Q SER Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3).

   CE Nuclear Power (CENP) configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots (See Common Q SER Section 4.2.2.1.2).

E. On the basis of its review of the CENP's software development process for application software, the staff concludes that the Software Program Manual (SPM) specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of a life cycle activity that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design output for specific application on a plant-specific basis (See Common Q SER 4.3.2).

F. When implementing a Common Q safety system (i.e., post-accident monitoring system (PAMS), core protection calculator system (CPCS), or digital plant protection system (DPPS)), the licensee must review CENP's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report (See Common Q SER Sections 4.1.1.4, 4.4.1.3, 4.4.2.3, and 4.4.3.3).

G. The Operator's Module (OM) and the Maintenance Test Panel (MTP) provide the human machine interface for the Common Q platform. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis (See Common Q SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 4.4.4.3.6).

H. If the licensee installs a Common Q PAMS, CPCS, or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is replaced, and meets the functionality requirement applicable to those systems (See Common Q SER Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3).

I. Modifications to plant procedures and/or technical specifications due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for a license amendment with attendant justification (See Common Q SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 5.0).

J. A licensee implementing any Common Q application (i.e., PAMS, CPCS, or DPPS) must prepare its plant-specific model for the design to be implemented and perform the FMEA for that application (See Common Q SER Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 5.0).

K. If a licensee installs a Common Q PAMS, CPCS, DPPS, or integrated solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital I&C systems and meet the requirements of HICB BTP-19 in the NRC SRP, Chapter 7 (See Common Q SER Sections 4.1.6, 4.4.2.3, 4.4.3.3, 4.4.4.3.3, and 5,0).

L. A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing (See Common Q SER Section 4.4.3.3).

M. The analysis of the capacity of the shared resources to accommodate the load increase due to sharing (See Common Q SER Section 4.4.4.3.1).

N. The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished Three-Mile Island (TMI) action items (See Common Q SER Section 5.0).

420.029 (DCD 7.1.7, Item 11)

In the NRC's SER on Common Q design (Reference 11 in DCD 7.1.7), the staff identified 10 Generic Open Items. Provide a discussion on the resolution on each of those open items for AP1000. If a specific item cannot be resolved during the design certification stage, then the action should be included in the Tier 1 Material (ITAAC).

420.030 (DCD 7.1.7, Item 10)

DCD 7.1.7 Reference 10, NABU-DP-00014-GEN, Rev. 0, "Design Process for Common Q Safety Systems," has not been reviewed by the NRC staff. Please provide this document for staff review.

420.031 (DCD 7.1.7, Item 8)

DCD 7.1.7 Reference 8, CENPD-396-P, Rev. 01, "Common Qualified Platform," May 26, 2000, has four Appendices. Appendix 4 states that the purpose of this appendix is to describe the implementation of the Common Q Platform for an integrated configuration when digital

upgrades are incorporated for multiple safety systems. However, the original intent of the Common Q design is for digital upgrade on an active operating plant, and not for a passive plant. In order for Reference 8 to become more useful for a passive plant application such as the AP1000, please provide another appendix document specifically describing the implementation of the Common Q Platform for a passive plant with multiple safety systems.

420.032 (DCD 7.7.1.8.1)

In the AP1000 DCD Highlight/Strikeout Version from the AP600 DCD (Revision 0 of the AP1000 DCD), there is an indication on design change at the Feedwater Control System. Describe the changes made from the AP600 design to the AP1000 design. Discuss the reasons for the change.

420.033 (DCD Table 7.5-8)

Explain the reason for deleting “Post-Accident Sampling Station Area Radiation Monitor.”

420.034 (DCD Table 7.5-1 & TS Table 3.3.3-1)

Explain the reason for downgrading the “Hydrogen Concentration Monitor” from Category C1 to Category C3 and deleting it from Technical Specification Table 3.3.3-1, “Post-Accident Monitoring Instrumentation.”

420.035 (DCD 7.7.1.11)

DCD Section 7.7.1.11, “Diverse Actuation System,” provides diverse protection in the low probability case where a common mode failure occurred at the PMS. Describe the interface design between the safety-grade PMS channels and the non-safety-grade DAS channels and the arrangement at the actuated devices. Is the Component Interface Module (CIM) of the Common Q design utilized in the AP1000 design?

420.036 (DCD 7.2.2.2.6)

Explain the design difference between the AP600 and the AP1000 with respect to conformance to Requirements on Multiple Setpoints used for Reactor Trips (Paragraph 6.8.2 of IEEE 603-1991). The AP600 does not use multiple setpoint for reactor trips; why does the AP1000 need to use multiple setpoints for a particular mode of operation?

420.037 (DCD 7.3.1.2.17)

DCD Figure 7.2-1 Sheet 13 Functional Diagram indicates that the Control Room Isolation and Air Supply Initiation logic has a signal to actuate main control room (MCR) Pressure Relief Valves. There is no discussion in DCD 7.3.1.2.17 for this provision. Describe the design of the MCR isolation system in DCD 7.3.1.2.17.

420.038 (DCD 2.5.1, Table 2.5.1-4, 3.h)

AP600 DCD 2.5.1, Table 2.5.1-4 Design Commitment 3.h) states that the DAS equipment can withstand the room ambient temperature and humidity conditions that exist at the plant locations in which the DAS equipment is installed. However, in AP1000 DCD 2.5.1, Table 2.5.1-4 Design Commitment 3h) has been changed to "The DAS equipment can withstand the room ambient temperature and humidity conditions that will exist at the plant locations in which the DAS equipment is installed at the times the DAS is required to be operational." The staff considers that the DAS should be available all the time while the plant is in operation. Justify the wording changes in the Design Commitment.

420.039 (DCD 2.5.2, Item 9.c)

DCD 2.5.2 Design Description 9.c) states that the PMS does not allow simultaneous bypass of two redundant channels. Describe the design provision to implement this requirement.

420.040 (DCD 2.5.2, Item 11)

DCD 2.5.2 Design Description 11 states that the PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during specific life cycle stages. "Specific life cycle" should be defined in this Tier 1 material to allow the staff to perform audit and review.

420.041 (DCD 16.1, TS LCO 3.3.1)

Technical Specification (TS) Limiting Condition of Operation (LCO) 3.3.1 Conditions N and O has added new Required Actions, N.2.2 and O.2.2, respectively, which states that "With two interlock channels inoperable, place the Functions associated with one inoperable interlock channel in bypass and with one inoperable interlock channel in trip." Explain why this Action is required for the AP1000 design, but was not required for the AP600 design. Are all the interlock logics using 2-out-of-4 coincident logic? Why is the wording in Required Actions for N.2.1 and O.2.1 different?

420.042 (DCD 16.1, TS LCO 3.3.2)

TS LCO 3.3.2 Condition J has added a new Required Action J.2.2 which states that "With two interlock channels inoperable, place the Functions associated with one inoperable interlock channel in bypass and with one inoperable interlock channel in trip." Explain why this Action is required for the AP1000 design and was not required for the AP600 design. Are all the interlock logics using 2-out-of-4 coincident logic?

420.043 (DCD Tier 1, Section 2.5.2)

As mentioned in ITAAC No. 3 of Table 2.5.2-8, describe the report that exists or will exist and concludes or will conclude that Class 1E equipment will be able to withstand surge withstand capability (SWC), electromagnetic interference (EMI), radio frequency interface (RFI) and electrostatic discharge (ESD) conditions.

420.044 (DCD Tier 1, Section 2.5.2)

Provide a copy of the Software Requirements Specification for the PMS software including the safety requirements that the software is to perform.

420.045 (DCD Tier 1, Section 2.5.2)

Describe the method of safety analysis that will be performed on the PMS and its components to ensure the PMS will perform as specified and that failures have been identified.

420.046 (DCD Tier 1, Sections 2.5.1, 2.5.3, 2.5.4, 2.5.5, 2.5.6, and 2.5.7)

Describe the architecture of the real-time data network and how the information is used to control and monitor the plant. This includes the network in the precautions, limitations, and setpoints (PLS) and the one that interfaces with the digital data service (DDS), document control system (DCS), PLS, in-core instrumentation system (IIS), special monitoring system (SMS) and the DAS.

Series 435 - Electric Power Systems

435.001

Appendix 1A, “Conformance With Regulatory Guides,” of the AP1000 Design Control Document (Tier 2) lists the applicable regulatory guides (RGs) with referenced IEEE Standards. The column, “Clarification/Summary Description of Exceptions,” states that, for several IEEE Standards, the AP1000 uses the latest version of the industry standards which are not endorsed by a RG. However, Westinghouse states that their use should not result in a deviation from the design philosophy otherwise stated in the RG. For each of these standards, discuss (1) the difference between the latest version of the industry standard used in the design of the AP1000 and the standard endorsed by the regulatory guide, and (2) the conformance of the AP1000 to the standard.

435.002

Section 3.1, “Conformance with Nuclear Regulatory Commission General Design Criteria,” states the AP1000 plant design supports an exemption to the requirements of GDC 17 for two physically independent offsite circuits by providing safety-related systems for core cooling and containment integrity.

Section 8.2.3, “Conformance to Criteria,” refers to Section 3.1 as described above. Section 8.2, “Offsite Power System,” does not describe the exemption to GDC 17 regarding two independent offsite circuits. The exemption should be discussed in detail in the main body of the offsite power system.

435.003

The frequency of catastrophic failures of the main step-up transformers due to lightning or solar storms has been greater than what was previously anticipated. Describe the design for lightning and solar storm protection for the main step-up transformers. Note that the solar storm cycle is 11 to 12 years.

435.004

Discuss the assumptions used in sizing the Class 1E batteries to include the simultaneous starting of all connected loads with the maximum inrush for the first minute.

435.005

Per IEEE Std 485, “Recommended Practice for Sizing Lead-Acid Batteries for Stationary Application,” discuss whether battery sizing calculations have taken into account (1) temperature correction factor; (2) design margin; and (3) aging factor.

435.006

Standard molded-case breakers can be used in direct current (dc) circuits. However, the dc interrupting rating will generally be one-half to one-third of the alternating current (ac) value. Many manufacturers do not publish dc application data for these breakers. Discuss how the design will ensure that molded-case breakers will have adequate dc interrupting ratings.

435.007

Discuss the operating voltage range for the safety-related dc power system as described in IEEE Std 946. Discuss the design to ensure that the voltage range will envelope the design-basis accident conditions and that the batteries are sized to provide adequate voltages at the end of the battery duty cycle.

435.008

Failures of the uninterruptible power supply (UPS) system constitute one of the main causes of forced plant outages. Discuss the design to ensure that the failure or unavailability of a single battery, battery charger, or inverter will not result in a plant trip.

435.009

Discuss the design to ensure that each safety-related battery charger has sufficient capacity to meet the largest combined demands of the various steady-state loads plus the charging capacity to restore the battery charger from the design minimum charge to the fully charged state in less than 12 hours (in accordance with IEEE Std 946) regardless of the state of the plant during which these demands occur.

435.010

Inverter and charger failures have been reported to be age-related. Capacitors, transformers, and semiconductors are affected by increase in ambient temperature. Discuss the conservatism used in the AP1000 design as it relates to these components.

435.011

Discuss the design features or operating practices used to reduce the risk of simultaneous failures (common cause failures) affecting all of the battery divisions.

435.012

Discuss the aspects of the AP1000 design that preclude the ac power supply source (offsite) from becoming a load on the safety-grade batteries.

435.013

Are the battery cells provided with explosion-resistant vent caps that would prevent the ignition of gases within the cell from an ignition source outside the cell? Please describe.

435.014

The loads used for digital control power supplies and computers in the AP1000 design are inherently non-linear in nature. Also variable speed drives and fluorescent lighting blasts introduce harmonics into the plant distribution system. Discuss the measures taken so that the total harmonic distortion (THD) due to non-linear loads on power system will not affect the current and voltage waveform of the UPS system.

435.015

Discuss the protection provided in the AP1000 design to suppress voltage spikes that may result from surges caused by de-energizing highly inductive loads.

HISTORY OF PREVIOUSLY ISSUED
REQUESTS FOR ADDITIONAL INFORMATION

Letter No.	Date issued	ADAMS Accession No.	RAI Nos.	Date of response	ADAMS Accession No.
1	6/26/2002	ML021780568	440.001 - 440.008	7/24/2002	ML022110430
2	8/16/2002	ML022280379	720.001		

AP 1000

cc:

Mr. W. Edward Cummins
Advanced Plant Safety & Licensing
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355

Mr. Michael Corletti
Advanced Plant Safety & Licensing
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230-0355

Mr. H. A. Sepp
Westinghouse Electric Company
P.O. Box 355
Pittsburgh, PA 15230

Lynn Connor
Doc-Search Associates
2211 sw 1ST Ave - #1502
Portland, OR 97201

Barton Z. Cowan, Esq.
Eckert Seamans Cherin & Mellott, LLC
600 Grant Street 44th Floor
Pittsburgh, PA 15219

Mr. Ed Rodwell, Manager
Advanced Nuclear Plants' Systems
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94304-1395

Charles Brinkman, Director
Washington Operations
Westinghouse Electric Company
12300 Twinbrook Parkway, Suite 330
Rockville, MD 20852

Mr. R. Simard
Nuclear Energy Institute
1776 I Street NW
Suite 400
Washington, DC 20006

Mr. Thomas P. Miller
U.S. Department of Energy
Headquarters - Germantown
19901 Germantown Road
Germantown, MD 20874-1290

Mr. David Lochbaum
Nuclear Safety Engineer
Union of Concerned Scientists
1707 H Street NW, Suite 600
Washington, DC 20006-3919

Mr. Paul Gunter
Nuclear Information & Resource Service
1424 16th Street, NW., Suite 404
Washington, DC 20036

Ms. Wenonah Hauter
Public Citizen's Critical Mass Energy
Project
215 Pennsylvania Avenue, SE
Washington, DC 20003

Mr. Tom Clements
6703 Guide Avenue
Takoma Park, MD 20912

Mr. James Riccio
Greenpeace
702 H Street, NW, Suite 300
Washington, DC 20001

Hugh Jackson, Policy Analyst
Public Citizen's Critical Mass Energy
and Environment Program
1724 Duarte Drive
Henderson, NV 89014

Mr. James F. Mallay, Director
Regulatory Affairs
FRAMATOME, ANP
3315 Old Forest Road
Lynchburg, VA 24501

Mr. Ed Wallace, General Manager
Project Management
Lake Buena Vista Bldg., 3rd Floor
1267 Gordon Hood Avenue
Centurion 0046
Republic of South Africa
PO Box 9396 Centurion 0046

Mr. Vince Langman
Licensing Manager
AECL Technologies, Inc.
901 15th Street, NW., Suite 440
Washington, DC 20005-2301

Mr. Glenn R. George
PA Consulting Group
Chrysler Building, 34th Floor
405 Lexington Avenue
New York, NY 10174