Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NTD-NRC-94-4038
NSRA-APSL-94-0008
Docket No.: STN-52-003

January 12, 1994

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ATTENTION: R. W. BORCHARDT

SUBJECT: WESTINGHOUSE RESPONSES TO NRC REQUESTS FOR ADDITIONAL INFORMATION ON THE AP600

Dear Mr. Borchardt:

Enclosed are three copies of the Westinghouse responses to NRC requests for additional information on the AP600 from your letter of October 8, 1993 and November 2, 1993. This transmittal completes the responses to the October 8, 1993 letter. A listing of the NRC requests for additional information responded to in this letter is contained in Attachment A. Attachment B is a complete listing of the questions associated with the October 8, 1993 letter and the corresponding letters that provided our reponse.

These responses are also provided as electronic files in WordPerfect 5.1 format with Mr. Hasselberg's copy.

If you have any questions on this material, please contact Mr. Brian A. McIntyre at 412-374-4334.

Nicholas J. Liparulo, Manager
Nuclear Safety & Regulatory Activities

/nja

Enclosure

cc: B. A. McIntyre - Westinghouse
F. Hasselberg - NRR

240032

E004

1433A

NTD-NRC-94-4038
ATTACHMENT A
AP600 RAI RESPONSES
SUBMITTED JANUARY 12,1994

RAI No.	Issue
420.107	Protection System ITAAC
420.108	Industrial Standards
420.109	Conformance with RG 1.152
420.111	Vidio Display Qualification Methods
420.112	DAS ITAAC
420.113	Correct Description of DAS Inputs
420.114	DAS Reactor Trip Sensor CM Failure
420.115	Diverse ESF-Containment Isolation
420.117	Bypass Logic for Int Protection System
420.118	Describe DMINS
420.119	Describe Program Language for I&C Systems
420.120	Describe software system architecture
420.121	Describe software develpoment process
420.122	Describe software review & confirmatory activities
480.046	Igniter in Technical Specifications

Printed: 01/13/94

ATTACHMENT B
CROSS REFERENCE OF WESTINGHOUSE RAI RESPONSE TRANSMITTALS TO NRC LETTER OF OCTOBER 8,1993

Question No.	Issue	NRC Letter	Westinghouse Transmittal Date
420.107	Protection System ITAAC	10/08/93	01/12/94
420.108	Industrial Standards	10/08/93	01/12/94
420.109	Conformance with RG 1.152	10/08/93	01/12/94
420.110	Design Basis for "Monitor Bus"	10/08/93	11/30/93
420.111	Vidio Display Qualification Methods	10/08/93	01/12/94
420.112	DAS ITAAC	10/08/93	01/12/94
420.113	Correct Description of DAS Inputs	10/08/93	01/12/94
420.114	DAS Reactor Trip Sensor CM Failure	10/08/93	01/12/94
420.115	Diverse ESF-Containment Isolation	10/08/93	01/12/94
420.116	EMI Test on Protection Cabinet	10/08/93	11/30/93
420.117	Bypass Logic for Int Protection System	10/08/93	01/12/94
420.118	Describe DMINS	10/08/93	01/12/94
420.119	Describe Program Language for I&C Systems	10/08/93	01/12/94
420.120	Describe software system architecture	10/08/93	01/12/94
420.121	Describe software develpoment process	10/08/93	01/12/94
420.122	Describe software review & confirmatory activities	10/08/93	01/12/94

Records printed: 16

Question 420.107

The staff has concluded that Westinghouse's February 9, 1993 response to Q420.8 (regarding ITAAC for the protection system) is not acceptable. SECY-92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews," dated February 19, 1992, describes the staff's approach for using design acceptance criteria (DAC). SECY-90-377, "Requirements for Design Certification Under 10 CFR Part 52," dated November 8, 1990, describes the level of detail required for design certification. The concept of requiring detailed design acceptance criteria would enable the staff to make a final safety determination, subject to satisfactory design implementation and verification by the combined license (COL) licensee, through appropriate ITAAC. The staff believes that to ensure the high quality of the Instrumentation and control (I&C) system in the design certification, the following information should be provided in the Tier 1 submittal for the instrumentation and control systems of the AP600:

a. The instrumentation and control system architecture of the AP600.

b. A description of the configuration of the digital I&C equipment. Block diagram type of information should be used to support the system description.

c. A description of the hardware and software development process used in the design, testing, and installation of digital I&C equipment. As a minimum, the ITAAC submittal should address the software management plan, the configuration management plan, and the verification and validation (V&V) plan.

d. A description of I&C system qualification processes that include programs to mitigate the effects of electromagnetic interference, establish set points for instrument channels, and ensure the qualification of the installed equipment.

e. The ITAAC/DAC for software quality that requires the following design stages (the software life cycle) with appropriate documentation for the development of both safety-related and non-safety-related software. No particular life cycle is endorsed; however, an example of these activities includes the following stages:

1. planning stage
2. requirement stage
3. design stage
4. implementation stage
5. integration stage
6. validation stage
7. installation stage
8. operation and maintenance stage

The ITAAC/DAC should specify criteria (constraints and limits) that describe the method for developing plans and procedures that guide the design process throughout the life cycle stages. The activities and documentation that should be included are listed below:

1. Planning activities result in a number of documents that are used to control the development process. Six documents are recommended to be developed at this stage: a Software Management Plan, a Software Development Plan, a Software Quality Assurance Plan, a Software Safety Plan, a Software V&V Plan, a Software Configuration Management (CM) Plan. These plans are discussed in detail in the ANSI/IEEE standards IEEE-828, IEEE-1012 and IEEE-1033.

2. There are six documents that are recommended to be developed during the requirements activities stage for the software system: the Requirements Specification, the Interface Specifications, a Requirements Safety Analysis, a V&V Requirements Analysis Report, a V&V Anomaly Report, and a CM Requirements Report. These documents will fully capture the requirements of the software project, and relate these requirements to the overall protection system functional requirements and protection system safety requirements.

3. Design activities include the recommended development of eight documents: the Unit Test Plan, the Hardware & Software Architecture, a Design Specification, a Interface Design Specification, a Design Safety Analysis, a V&V Design Analysis Report, a V&V Anomaly Report, and a CM Design Report. The Hardware and Software Architecture will describe the computer system design at a fairly high level, including hardware devices and mapping of software activities to those devices.

4. Implementation activities include writing and analyzing the actual code using some programming language. Documents that should be developed include the actual Code Listings, a Code Safety Analysis, an Integration Plan, an Integration Test Plan, a V&V Unit Test Report, a V&V Test Anomaly Report, and a CM Implementation Report.

5. Integration activities are those activities that bring software, hardware and instrumentation together to form a complete computer system. Documents that should be developed at this stage include the System Build Documents, a Validation Plan, a Validation Test Plan, an Integration Test Safety Analysis, a V&V Integration Test Report, a V&V Test Anomaly Report, and a CM Integration Report.

6. Validation is the process of ensuring that the final complete computer system achieves the original goals that were imposed by the protection system design. The final system is matched against the original requirements, and the protection system safety analysis. Documents that should be developed at this stage include the Installation Plan, an Installation Test Plan, a Training Plan, an Operations Plan, a Validation Test Safety Analysis, a V&V Test Analysis Report, a V&V Test Anomaly Report, and a CM Validation Report.

7. Installation is the process of moving the complete computer system from the developer's site to the operational environment. At the completion of the installation, the operator is provided with a documented operational computer system, including tests following installation. Nine documents are recommended to be developed to support this stage: the Operations Manuals, the Installation Configuration Tables, Training Manuals, Maintenance Manuals, the Maintenance Plan, an Installation Safety Analysis, a V&V Installation Test Report, a V&V Anomaly, and a CM Installation Report.

8. Operations and maintenance activities involve the actual use of the computer system in the operating reactor, and making any required changes to it. Changes may be required due to errors in the system that were not found during the development process, changes to hardware, or requirements for additional functionality. Safety analyses, V&V analyses and CM activities are all recommended as part of the maintenance process.

Implementation of the software ITAAC will be audited by the NRC to verify conformance with the requirements at several phases during the design process for the safety-related digital control system. The documents that demonstrate satisfactory implementation of the ITAAC will be available for inspection at the completion of each of the above stages. The audit phases and conformance review are shown in Enclosure 2 of this package, "Flow of Documents through the Software Life Cycle," and correspond to the completion of the various design development stages. The COL applicant/holder will be required to satisfactorily complete each ITAAC phase and may proceed to subsequent stages without approval from the NRC audit. However, should the NRC audit indicate failure to successfully complete a phased ITAAC, the COL applicant/holder may be required to repeat an earlier ITAAC and/or change the system design. The NRC staff will conduct a conformance review and issue an inspection report for each phased ITAAC and identify any open issues which require resolution. Significant open issues which are not resolved could result in the NRC staff concluding that the ITAAC had not been satisfactorily completed.

At each phased ITAAC, the design development must be verified to be in accordance with the certified design process, and must demonstrate that the detailed design developed (through that stage) meets the certified design. Upon completion of each phased ITAAC, the COL holder will certify to the NRC that the stage has been completed, and that the design and construction completed up through that stage is in compliance with the certified design. The COL applicant/holder will also provide a description of the next stage of design development and associated testing, analysis, and acceptance criteria in sufficient detail that the NRC staff can determine whether or not the proposed design development and testing is consistent with the certified design process and the ITAAC. This phased process will continue until all ITAAC stages for the safety-related software are completed.

A sample of the ITAAC for the ABWR I&C system is provided in Enclosure 3 as an example to consider while preparing the response to this question.

Response:

The instrumentation and control system hardware and software design, verification, and validation process is summarized in WCAP 13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and

Validation Process Report". The procedures for implementing the process summarized in WCAP 13383 are available for NRC review. The commitment to provide the documentation described in WCAP 13383 is a Tier 2 regulatory commitment provided in SSAR Chapter 7.

SSAR Revision: NONE

Question 420.108

The staff has concluded that Westinghouse's May 28, 1993 responses to Q420.9 and Q420.10 (regarding industrial standards) are not acceptable. 10 CFR 52.47 requires that the application for design certification must contain a level of design information sufficient to enable the Commission to make its safety determination. Since the AP600 I&C system design is still in a conceptual phase, reference to industrial standards is an appropriate method to describe the design approach. The staff regards the application of acceptable standards throughout the production process as an important element to demonstrate the quality of the design.

The document that describes the standards and codes applicable to AP600 I&C systems design (referenced in Section 5.2, C&PGSTD-001, "System Development/Implementation Process," of WCAP-13392, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report") has not been submitted for staff review. Provide the information regarding the system development/implementation process with appropriate references to industrial standards.

Response:

Reference 5.2 of WCAP-13392, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report", C&PGSTD-001, "System Development/Implementation Process," is an internal, proprietary Westinghouse document. This document does not list the codes and standards as requested; rather, it defines the requirements for the project-related documents that identify and invoke specific codes and standards on a project.

The following standards are used as design standards for the instrumentation and control systems that are to be used for the safety-related AP600 instrumentation and control equipment.

ANSI/IEEE Std 100-1077	IEEE Standard Dictionary of Electrical and Electronic Terms
IEEE Std 336	Installation, Inspection, and Testing Requirements for Class 1E Instrumentation and Electric Equipment at Nuclear Power Generating Stations (1980)
IEEE Std 352-1975	IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems
IEEE Std 381	Criteria for Type Tests of Class 1E Modules used in Nuclear Power Generating Stations (1977)
IEEE Std 472-1974	IEEE Guide for Surge Withstand Capability (ANSI C37.90a-1974) (SWC) Tests
IEEE Std 488	Standard Digital Interface for Programmable Instruments (1978)

ANSI/IEEE Std 497-1981	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations
IEEE Std 498	Requirements for the Calibration and Control of Measuring and Test Equipment Used in the Construction and Maintenance of Nuclear Power Generating Stations (1980)
ANSI/IEEE Std 677-1976	IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Station
ANSI/IEEE Std 729-1983	IEEE Standard Glossary of Software Engineering Terminology
ANSI/IEEE Std 730-1984	IEEE Standard for Software Quality Assurance Plans
IEEE 796-1983	Standard Microcomputer Bus
IEEE/ANSI 802.3-1985	Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Bus Access Method (Process Bus/Logic Bus)
IEEE Std 828-1983	IEEE Standard for Software Configuration Management Plans
ANSI/IEEE Std 829-1983	IEEE Standard for Software Test Documentation
IEEE Std 1012	Standard for Software Verification and Validation Plans
ANSI/ISA Std R55.1	Recommend Practice Hardware Testing of Digital Process Computers (1975, Reaffirmation May 5,1983)
ANSI/ISA Std S51.1	Process Instrumentation Terminology (1979)
ANSI/EIA Std RS-407-A	Testing Procedures for Relays for Electrical and Electronic Equipment (1978)
RS-232-C	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange (Aug. 1969, Reaffirmed June 1981)
RS-422-A	Electrical Characteristics of Balanced Voltage Digital Interface Circuits (Dec. 1976)
EIA RS-310-C	Racks, Panels, and Associated Equipment (Nov. 1977)
EIA-485	Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems (Apr. 1983)

IEC 529:1976	Specification for Classification of Degrees of Protection Provided by Enclosures
IEC 880	Software for Computers in the Safety Systems of Nuclear Power Stations
ISO 3309-1979	Data Communications - High Level Datalink Control Procedures - Frame Structure
ISO 4335-1979	Data Communications - High Level Datalink Control Procedures - Elements of Procedures, Appendix 1
AEEW R919	Interference Immunity Tests for Nucleonic Instrumentation (Apr. 1974)
ANSI X3.166-1990	Physical Layer Medium Dependent (PMD)
ANSI X3.184-1990	Single-Mode Fiber Physical Layer Medium Dependent (SMF-PMD)
ANSI X3.148-1988	Physical Layer Protocol (PHY)
ANSI X3.139-1987	Media Access Control (MAC)
ANSI X3T9.5/88-139 Rev-2	Media Access Control (MAC-M) (Maintenance Revision)
ANSI X3T9.5/84-49 Rev-6.2	Station Management (SMT)
MIL-HDBK-217E	Reliability Prediction of Electronic Equipment (Oct. 1986) (Revision D; Jan 1983 also Referenced)
MIL-STD-1472C	Human Engineering Design Criteria for Military Systems, Equipment, and Facilities
ANSI N45.2.2-1978	Standard for Packaging, Shipping, Receiving, and Storage of Items for Nuclear Power Plants.

SSAR Revision: NONE

Question 420.109

Clarify the statement in Appendix 1A of the SSAR that describes the conformance of the AP600 with Regulatory Guide 1.152 (RG) "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants," as "Acceptable." Does the AP600 design conform to this RG? RG 1.152 endorses American National Standard ANS-7-4.3.2, 1982, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." However, ANS-7-4.3.2 has been revised in 1992/1993. NRC will endorse the latest revision (Draft 8) in the near future. Will the AP600 design conform to this new draft standard? Identify exceptions, if any, that will be taken for the AP600 design.

Response:

The AP600 conforms to Reg. Guide 1.152, (Task 1C 127-5), Rev. 0, 11/85 - Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants.

Westinghouse will review the revision of ANS-7-4.3.2, determine applicability to the AP600, and identify any exceptions by 3/31/94.

SSAR Revision: NONE

Question 420.111

In the April 29, 1993 response to Q420.50, Westinghouse states that the qualification methods for the qualified video display units used in the AP600 will be similar to the qualification methods described in Supplements EQDP-ESE-63A and EQDP-ESE-63B of WCAP-8587. Provide the specific qualification method for the qualified video display system. If the qualification test results will not be available for design certification, then this system should be included in the ITAAC submittal.

Response:

The qualification program that will be applied is discussed in SSAR Sections 3.10 and 3.11. The program complies with 10 CFR 50.49. Conformance to the guidance provided by Regulatory Guides 1.89 and 1.100 is addressed in SSAR Appendix 1A. The equipment qualification of the AP600 instrumentation and control systems components beyond that discussed in SSAR Sections 3.10 and 3.11 is dependent upon component selection and, therefore, the specific qualification methods are beyond the scope of design certification. Qualification results will not be available for design certification. However, since equipment qualification is a regulatory requirement in 10 CFR 50.49, a tier 1 ITAAC commitment is not required to assure compliance.

SSAR Revision: NONE

Question 420.112

Section 3.5.1, "Diverse Actuation System (DAS)" of the Tier 1 submittal for the AP600 states that the diverse actuation system serves no safety related functions. However, Section 7.7.1.11 of the SSAR states that the DAS provides a diverse backup to the protection systems. Based on WCAP-13633, "AP600 Instrumentation and Control Defense-in-Depth and Diversity Report," the DAS serves very important safety-related functions. The statement in the Tier 1 submittal should be revised accordingly.

In WCAP-13633, Westinghouse states that the DAS diversity is achieved by the use of a different architecture, different hardware implementations, and different software from that of the Protection and Safety Monitoring System (PMS). Software diversity is achieved by running different operating systems and programming in different language. In the April 29, 1993 response to Q420.54, Westinghouse states that the DAS will be devised from the verification and validation processes performed for the PMS and PLS, and will be performed by different people. The design, verification, and validation process for the DAS consists of hardware verification, software verification, system verification, and system validation. The hardware verification consists of inspections and tests to verify that the hardware meets design specifications. The software verification consists of functional tests to verify that the software meets design requirements at the module and subsystem levels. The system validation test consists of a factory acceptance test to verify it meets system functional requirements. These type of design commitments should be included in the ITAAC submittal for DAS.

Response:

SSAR Subsection 3.2.2.1 defines safety-related as those functions relied upon to remain functional during or following a design basis event to provide for the following:

- The integrity of the reactor coolant pressure boundary
- The capability to shut down the reactor and maintain it in a safe shutdown condition
- The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR 100.

Actuation of functions by the diverse actuation system is not a safety-related function since the diverse actuation system is not relied upon to function during or following a design basis event as analyzed in SSAR Chapter 15.

The regulatory commitments identified in the question are considered to be Tier 2 and are addressed in WCAP 13633, "AP600 Instrumentation and Control Defense-in-Depth and Diversity Report," and SSAR Section 7.7. The functionality of the diverse actuation system will be verified by the inspections and tests described in the diverse actuation system ITAAC.

SSAR Revision: NONE

Question 420.113

The description of the inputs for the Diverse Actuation System (DAS) described in Section 7.7.1.11 of the SSAR, Appendix C12 of the PRA submittal, and Appendix B of WCAP-13633 conflict with each other. Provide the correct description of the DAS inputs in these documents.

Response:

The SSAR description is correct. The proposed SSAR revision clarifies the diverse actuation system function for steam generator overfill prevention. Currently in SSAR Subsection 7.7.1.11, steam generator overfill prevention is listed as a separate item in the list of manual actuation functions. The steam generator overfill prevention function provided by the diverse actuation system includes a diverse indication of high steam generator water level and manual actuation of the automatic depressurization system valves.

Appendix C12 of the PRA submittal differs from the SSAR subsection in the following three areas:

- Reactor trip, turbine trip, and passive residual heat removal actuation on feedwater flow / steam flow mismatch instead of low wide range steam generator water level
- High containment actuation of containment isolation and passive containment cooling system instead of high containment temperature
- Low pressurizer water level trip functions do not include reactor trip.

In all three instances the SSAR description is correct. The diverse actuation system functions, as described in SSAR Subsection 7.7.1.11 will be included in the PRA re-quantification as described in the proposed PRA revision.

WCAP 13633, "AP600 Instrumentation and Control Defense-in-Depth and Diversity Report," is consistent with the system described in SSAR Subsection 7.7.1.11.

SSAR Revision:

SSAR Subsection 7.7.1.11 includes proprietary information. The proposed revision to Subsection 7.7.1.11 is included in letter NTD-NRC-94-4041.

PRA Revision: Section C12.2.1 will be modified as follows:

C12.2.1 Diverse Actuation System

C12.2.1.1 Diverse Automatic Actuation

The diverse actuation system provides control rod insertion, turbine trip, passive residual heat removal (PRHR) heat exchanger start, core makeup tank start, selected containment line isolation (see Appendix C21), passive containment cooling system start, and in-containment refueling water storage tank motor operated valve actuation during shutdown.

To accomplish its functions, the diverse actuation system uses the following signals:

- ~~Main feedwater (FW) flow and main steam flow mismatch~~Low wide range steam generator level per steam generator -- To trip rods via the motor-generator set, trip the turbine, and start the passive residual heat removal heat exchanger
- High hot leg temperature -- To start the passive residual heat removal heat exchanger
- Low pressurizer water level -- To trip the reactor, trip the reactor coolant pump, and to start the core makeup tank
- High containment temperature -- To isolate selected containment penetrations and to start passive containment cooling water flow
- Low hot leg level -- To open the motor-operated valves of the in-containment refueling water storage tank injection lines, if isolated during the shutdown condition.

Question 420.114

Figure B-3.1 of WCAP-13633, "Diverse Actuation System Diverse Reactor Trip," indicates that the DAS reactor trip is initiated either by high pressurizer level or low steam generator level. Explain why these two parameters were chosen. The sensors are shared between the safety-related protection system and the DAS. Provide a defense-in-depth analysis for potential common mode failure of these level sensors.

Response:

Actuation of reactor trip, passive residual heat removal, and turbine trip on low wide range steam generator level was chosen because it provides a direct indication of the need to trip during a loss of heat sink anticipated transient without scram (ATWS) condition.

Actuation of reactor trip, core makeup tanks, and reactor coolant pump trip on low pressurizer water level was chosen to address the more probable events that require core makeup tank actuation. Specifically, these functions would provide core makeup tank actuation for events such as steam generator tube rupture, passive residual heat removal tube rupture, and direct vessel injection line rupture.

Sensors utilized by the diverse actuation system are not required to be diverse from those utilized by the safety-related protection and safety monitoring system. Common mode failure of like sensors (such as differential pressure cells) is not coupled with common mode failure of the instrumentation and control processing/actuation hardware and software. The diverse actuation system provides nonsafety-related diverse actuation of protection functions in the low probability instance of a common mode failure of the protection and safety monitoring system hardware or software. Common mode failure of similar sensors is addressed by providing diversity in the sensing of plant parameters. SSAR Table 7.2-6 provides a summary of the diverse protection functions provided by the safety-related protection and safety monitoring system for each of the Chapter 15 design basis events.

In addition, the AP600 PRA evaluated the impact of common sensor failures. The PRA evaluation indicates that for a common mode failure of similar sensors (such as all pressure or differential pressure cells), the AP600 is protected by other sensor types, such as temperature or power.

SSAR Revision: NONE

Question 420.115

Figure B-3.4 of WCAP-13633 indicates that the Diverse ESF-Containment Isolation system is initiated by containment temperature measurements. Describe the actuation system design requirements to meet the functional requirements of containment isolation. How many sensors will be required? Where are the sensors to be located to meet the response time requirement?

Response:

The diverse actuation system (DAS) is a nonsafety-related system that provides diverse backup to the protection and safety monitoring system. It reduces the probability of a severe accident that results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and safety monitoring system and the plant control system. The protection and safety monitoring system is designed to minimize common mode failures. However, in the low probability case where a common mode failure does occur, the DAS provides diverse protection. The specific functions performed by the DAS were selected based on PRA evaluation. The diversity is achieved by the following design criteria:

- The signal conditioning, communication, and processing hardware and software are diverse from the plant safety and monitoring system.

- The interface with the actuated devices is arranged to prevent failures in either the diverse actuation system or the plant safety and monitoring system from blocking the actuation from the other system.

The diverse actuation system is not safety-related, and it is not required to have redundancy. Two out of two voting logic is used to prevent spurious actuation. Diversity from the protection and safety monitoring system is required from the sensor output to, but not including the final actuation device. Details of the functional requirements of the system may be found in SSAR Subsection 7.7.1.11. Additional information may be found in Appendix C12 of the AP600 Probabilistic Risk Assessment.

For the isolation function of the selected containment penetrations, the DAS uses a high containment temperature signal. For high containment temperature, four sensors are employed to provide input signals. Two out of four high temperatures sensed will generate an input to the two out of two voting logic for automatic system actuation. The time response for the temperature sensing and containment isolation function is not a critical parameter since elevated containment temperature would be reached well before fuel damage in a severe accident scenario.

SSAR Revision: NONE

Question 420.117

Westinghouse's April 29, 1993 response to Q420.31 references WCAP-8897, "Bypass Logic for the Westinghouse Integrated Protection System." That report was written in 1977 for the RESAR-414 application, and was not approved by the NRC. Westinghouse should revise that report to make the analysis applicable for the AP600 application. In addition to evaluating the bypass capability with respect to the single failure criterion, Westinghouse should address potential software common mode failures in performing the evaluation. The evaluation should cover all modes of operation (start-up, full power, shutdown, etc.). Provide a software test plan and test results in the ITAAC to demonstrate that the analysis performed for the indefinite bypass can be verified.

Response:

The bypass logic functional design described in WCAP-8897 applies to the AP600, although the implementation hardware has changed. An addendum to WCAP-8897 describing the AP600 hardware implementation will be provided by February 15, 1994.

In the AP600 trip logic design, logic has been added to remove the global bypass permissive (and thereby generate a trip demand if a global bypass request is present) when two of the remaining cabinet sets have a trip demand.

The functions of the trip bus and the reactor trip breaker bypass device described in WCAP-8897 have been implemented by the dynamic trip bus and reactor trip breaker arrangement described in WCAP-13382, Revision 0, "AP600 Instrumentation and Control Hardware Description." The AP600 bypass path and power converter together are equivalent to the reactor trip breaker bypass device described in WCAP-8897. The AP600 reactor trip subsystems are equivalent to the trip logic computers described in WCAP-8897.

The functional design of the AP600 ESF logic is the same as the ESF logic described in WCAP-8897. The AP600 protection logic cabinets implementation uses 2/3 logic for the power interface, as described in WCAP-13382.

The effect of software common mode failures in the AP600 instrumentation and control has been evaluated in the AP600 Probabilistic Risk Assessment. The design features of the AP600 instrumentation and control architecture that address software common mode failures are described in WCAP-13633, Revision 0, "AP600 Instrumentation and Control Defense-in-Depth and Diversity Report."

The reply to RAI 420.107 addresses software ITAAC issues.

SSAR Revision: NONE

AP600

Question 420.118

Describe the digital metal impact monitoring system (DMIMS) that monitors the reactor coolant system for the presence of loose metallic parts.

Response:

The digital metal impact monitoring system is described in Subsection 4.4.6.4 of the AP600 SSAR.

SSAR Revision: NONE

Question 420.119

Describe the program language to be used for the AP600 safety-related I&C systems. Justify why this language was chosen for the safety-critical system application.

Response:

The software language chosen for the AP600 protection and safety monitoring system is PL/M-86. This language was chosen for the application based on a comparison with other languages. The features of PL/M-86 that were considered include:

PL/M-86 is a high level language that supports modern programming approaches.

- Block structuring
- Structured control
- Modularity
- Compound data types
- Identifiers of a readable length

With PL/M-86 there is a minimum need to revert to assembly coding to meet hardware interface or execution speed requirements.

PL/M-86 can be executed with a minimal language support library and does not require an operating system, consequently PL/M-86 code can be written in a highly visible manner that enhances verification.

PL/M-86 is the native language for the microprocessor family selected for the application and is widely used.

Westinghouse has extensive experience with PL/M-86.

SSAR Revision: NONE

Question 420.120

Describe the software system architecture planned for the AP600 (see also Q420.107).

In response to a question raised during the August 11, 1993 meeting between the NRC and Westinghouse, Westinghouse stated that the software system architecture for the AP600 will be basically the same as that used for Sizewell B. Several items of concern regarding the software system architecture for the Sizewell B PPS were raised during the Forum on Safety Related Systems in Nuclear Applications, Royal Academy of Engineering, dated October 28, 1992. Items of concern discussed at the Forum included the use of pointers in dynamic memory management. These pointers are used to link together the three major software blocks of the software architecture; the application software, the common function software, and the configuration and calibration data. At this forum, the points raised by critics centered around their inability to quantify software reliability, not on any specific faults in the system.

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 test(s) performed on the program at run time to verify that it is correct.

As a general principle, the NRC staff believes that acceptable test methods and tools should exist to verify the acceptability of the software system design with consideration given to all the features employed in that design.

Response:

See also the responses to RAIs 420.121 and 420.122

A software architecture description is included as attachment 1 to letter number ET-NRC-94-4036.

The use of pointers, also referred to as indirect addressing, is a well-established, commonly-used, accepted programming practice for microprocessor software. Westinghouse uses pointers to support modularization of the software and to decouple the application portion of the code from the common computer systems support function portion of the code. Memory is allocated to data items at initialization, but is never deallocated or reallocted. Consequently, the values of pointers are established a single time at initialization. This supports the goal of shielding the application software designers from the details of the microprocessor system design, allowing them to concentrate on implementation of the functions.

The discussion as reported in "Proceedings of a Forum on Safety Related Systems in Nuclear Applications;" October 28, 1992, addressed the ability of a software analysis tool used by the customer's independent verifier to deal with pointers, and not with the suitability of the use of pointers for the application. During this discussion it was stated by the customer's independent verifier: "the use of pointers is reasonably limited in this particular system."

The software verification and validation process is described in WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," Rev 0. Further information regarding software test methods and test tools is included as attachment 2 to letter no. ET-NRC-94-4036.

SSAR Revision: NONE

Question 420.121

Describe the AP600 software development process.

At the forum referenced in Q420.120, there was a criticism by a member of the British Computer Society regarding the Westinghouse coding standards being not on a par with the software development process used by NASA, even though the cost per line of code appeared to be equivalent. Discuss this statement and any improvements planned for the Westinghouse software development process for the AP600.

The NRC is in agreement with the statement in Section 6.1.2.22 of Chapter 10 of the ALWR EPRI URD, which states:

> The M-MIS Designer shall use modern software development techniques and practices as appropriate to provide high integrity software. Modern software development techniques and practices include methods in the design process to reduce the chance of errors, techniques in the V&V process to find errors, and software fault tolerant design features to prevent unfound errors from causing unacceptable consequences.

Provide a discussion regarding how Westinghouse maintains its software development standards to ensure that they are consistent with those considered to be modern development standards for the design of safety-critical software systems.

Response:

See also the responses to RAIs 420.120 and 420.122

The software development process is described in WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," Rev 0.

Further information is included as attachment 3 to letter no. ET-NRC-94-4036.

The reply to RAI 420.108 includes software development standards used by Westinghouse. Westinghouse continues to evaluate new software techniques as their maturity, level of industrial acceptance, and applicability to the AP600 implementation warrants.

SSAR Revision: NONE

Question 420.122

Describe the review and confirmatory supporting activities for AP600 software design.

According to information presented at the forum referenced in Q420.120, there was considerable effort spent in fitness-for-purpose review and confirmatory supporting activities for the Sizewell B PPS software. Describe plans for similar activities for the AP600 software and the bases for the planned activities. The plans should include activities planned during the commissioning stages to demonstrate the correctness of the digital I&C systems. Show how these plans are incorporated into the life cycle activities that are proposed by Westinghouse in response to Q420.107.

Response:

See also the responses to RAIs 420.120 and 420.121

The verification and validation process described in WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report," Revision 0, provides software and hardware fitness-for-purpose review and confirmatory activities to demonstrate the correctness of the digital instrumentation and control systems. The functional logic test described in the protection and safety monitoring system ITAAC also demonstrates the correctness of the digital instrumentation and control systems.

The software verification and validation process and the functional logic test are applicable during the entire software life cycle.

SSAR Revision: NONE

Question 480.46

The staff's position is that the igniters must be covered by technical specifications. Provide a justification for not submitting a technical specification for the AP600 igniters.

Response:

The NRC Policy Statement (Federal Register, Vol. 52, No. 25, February 6, 1987) criteria stated below has been used to identify all structures, systems, and parameters for which Limiting Conditions for Operation (LCOs) have been included in the AP600 Technical Specifications.

1. Installed instrumentation that is used to detect, and indicate in the control room, a significant abnormal degradation of the reactor coolant pressure boundary.

2. A process variable that is an initial condition of a Design Basis Accident (DBA) or Transient Analyses that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.

3. A structure, system or component that is part of the primary success path and which functions or actuates to mitigate a Design Basis Accident or Transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.

4. Structures, systems, and components which operating experience and probabilistic risk assessment have generally shown to be important to public health and safety.

The hydrogen recombiner and the hydrogen ignition subsystems of the Containment Hydrogen Control System are both provided to limit the hydrogen concentration in the containment so that containment integrity is not endangered.

The hydrogen recombination subsystem is provided to limit containment hydrogen concentration resulting from a design basis LOCA accident case where there is a limited reaction of fuel cladding zirconium with water to form hydrogen. It, therefore, falls under Criteria 3 and the electric hydrogen recombination portions of this system are included in the Technical Specifications. The hydrogen ignition subsystem is provided only to address the low-probability severe accident case. Based on the very low probability of core damage documented in Chapter 8 of the AP600 PRA and that other plant operating experience has not shown the system to be important to public health and safety, the igniters are not included in the Technical Specifications.

Hydrogen igniters are included in the technical specifications for some plants. In these cases the hydrogen igniters are required to limit design basis accident hydrogen concentration due to small containment volume, (e.g., ice condenser plants). However, this is not the case for the AP600 containment volume and is, therefore, not applicable.

SSAR Revision: None