



Tennessee Valley Authority, Post Office Box 2000, Spring City, Tennessee 37381

William J. Museler
Site Vice President
Watts Bar Nuclear Plant

DEC 27 1993

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Gentlemen:

In the Matter of the Application of)
Tennessee Valley Authority) Docket No. 50-390

WATTS BAR NUCLEAR PLANT (WBN) UNIT 1 - EAGLE-21 PROCESS PROTECTION SYSTEM
(TAC M81063)

This letter provides TVA's response to the NRC request for additional information (RAI) dated June 14, 1993. The RAI contained 19 questions concerning the recent design change to WBN's reactor protection system to replace its original analog electronics with microprocessor-based, digital electronics. This upgrade consisted primarily of installing a Westinghouse-supplied Eagle-21 process protection system in place of the older Foxboro process control system.

Enclosure 1 restates these 19 questions and gives TVA's answer to each one. Enclosure 2 is a list of the commitments made in Enclosure 1.

If you have any questions about the information provided in this letter, please telephone John Vorees at (615) 365-8819.

Very truly yours,

William J. Museler

Enclosures
cc: See Page 2

9401060429 931227
PDR ADOCK 05000390
A PDR

U.S. Nuclear Regulatory Commission
Page 2

DEC 27 1993

cc (Enclosures):

NRC Resident Inspector
Watts Bar Nuclear Plant
Rt. 2, Box 700
Spring City, Tennessee 37381

Mr. P. S. Tam, Senior Project Manager
U.S. Nuclear Regulatory Commission
One White Flint, North
11555 Rockville Pike
Rockville, Maryland 20852

U.S. Nuclear Regulatory Commission
Region II
101 Marietta Street, NW, Suite 2900
Atlanta, Georgia 30323

ENCLOSURE 1

REQUEST FOR ADDITIONAL INFORMATION
WATTS BAR UNIT 1
USE OF EAGLE-21 DIGITAL PROTECTION SYSTEM

1. Electromagnetic Interference/Radio Frequency Interference (EMI/RFI)

Question 1:

Provide the methodologies and the results of the EMI/RFI site survey for the preinstalled and installed environment. If a preinstalled site survey is not performed, provide justification for not performing the preinstalled survey.

Response:

No EMI/RFI site survey was performed prior to installation of the Eagle-21 process protection system because WBN is not an operating plant. TVA saw no benefit to such a survey since the construction environment that currently exists at WBN is not representative of an operating plant. TVA believes that operating experience with the Eagle-21 systems at both units of Sequoyah Nuclear Plant (SQN) is more relevant to any concern about EMI/RFI susceptibility. SQN's experience to date clearly indicates that EMI/RFI in a normal operating environment is not a significant problem for the Eagle-21 system.

In spite of this, TVA has contracted with Westinghouse to perform an EMI/RFI site survey of WBN's Eagle-21 system during hot functional testing. TVA chose Westinghouse to perform this survey primarily due to their familiarity with similar EMI/RFI surveys that were performed at other plants which have recently installed Eagle-21 systems (e.g., Zion and Diablo Canyon). TVA will submit the results of this survey to the NRC. The submittal will include a description of the methodologies and test equipment that were used to perform the survey, a comparison between on-site and factory EMI/RFI test results, and an assessment of the margin between the measured EMI/RFI spectrum and a conservative threshold above which EMI/RFI problems could occur.

Note that the above commitment supersedes previous commitments concerning EMI/RFI testing of the Eagle-21 system. In particular, the commitment from TVA's letter dated May 22, 1989, for in-situ testing of Eagle-21 equipment and evaluating the need for additional RFI precautions is superseded.

Question 2:

Provide a summary of TVA's comparison between the on-site and factory EMI/RFI test results. Does Eagle-21 equipment have a sufficient margin? Explain.

Response:

Refer to the response to Question 1 and the commitment stated therein. TVA expects that the results of the planned EMI/RFI survey for WBN will demonstrate that the intensity and frequency range of measured EMI/RFI is within factory allowable limits. This expectation is based on successful operating experience at SQN, which has an Eagle-21 equipment configuration and plant environment very similar to WBN, and the results of extensive EMI/RFI surveys at Zion and Diablo Canyon during the installation of their Eagle-21 systems.

Question 3:

Provide the list of equipment used to perform the site survey. Are they adequate for performing an EMI/RFI test and survey required by the Eagle-21 system? Explain in detail.

Response:

Refer to the response to Question 1 and the commitment stated therein. TVA expects to perform WBN's EMI/RFI survey using test equipment with capabilities that are at least equivalent to the test equipment which was used for the EMI/RFI surveys at Zion and Diablo Canyon during the installation of their Eagle-21 systems.

Question 4:

Explain how the WBN Eagle-21 system prevents a ground loop. Is the Eagle-21 system to be tested for ground loops after installation? If so, by what procedures?

Response:

Each electronic equipment rack in the Eagle-21 system uses the same grounding scheme. A nickel-plated bus bar, which is mounted across the rear bottom of the rack, serves as a common ground point for the rack. This single-point grounding method is commonly used in instrumentation of this type to prevent potential ground loops. It is endorsed by the National Electric Code.

Five separate leads are bolted to the bus bar and terminate at the following points in each of the racks:

- 5Vdc common from the left backplane of the microprocessor card cage,
- 5Vdc common from the right backplane of the microprocessor card cage,
- Chassis ground from the microprocessor card cage,
- 15Vdc common from the bottom of the rail in the power bus, and
- Chassis ground from the power distribution box.

Also, all instrumentation cable shield wires are grounded to this bus. Each protection set rack ground is connected to the main station ground grid as an additional means of minimizing the potential for ground loops. This installation was performed in accordance with plant procedures for grounding.

The Eagle-21 system is designed to maintain all of the analog inputs and outputs floating with respect to ground. This design approach is a further safeguard against the occurrence of ground loops. It establishes a differential input/output voltage between each of the inputs/outputs. The differential voltage reduces the possibility of a ground loop caused by the input sensor power supply or the output current loop device (i.e., indicator, recorder, plant computer(s)).

2. Electrostatic Discharge (ESD)

Question 5:

Explain how WBN is planning to reduce ESD occurrence.

Response:

Standard practices to minimize ESD are followed when performing work on the Eagle-21 system. Any person working on the Eagle-21 system wears a wrist ground strap. An Eagle-21 circuit board that is removed from its rack is placed on an anti-static mat. Additionally, an Eagle-21 board that is out-of-service is stored and transported in an anti-static bag. All personnel who work with the Eagle-21 system receive training on these methods to reduce the potential for ESD.

3. Class 1E/Non-Class 1E Isolation

Question 6:

Explain how the Class 1E equipment communicates with the non-Class 1E equipment at WBN. Also, describe how the non-Class 1E system will not prohibit the Class 1E equipment from performing its intended safety functions. In addition, explain how the Class 1E equipment is isolated and how isolation devices meet the requirements of Regulatory Guide 1.75 and other applicable IEEE standards.

Response:

WCAP-11733 ("Noise, Fault, Surge, and Radio Frequency Interference Test Report for Westinghouse Eagle-21 Process Protection Upgrade System") demonstrates the operability of Eagle-21 equipment under adverse conditions such as noise interference, fault isolation, power surges, and RFI. This test report was prepared to support the design of the original four Eagle-21 cabinets that were part of WBN's design change for resistance temperature detector (RTD) bypass elimination. However, the report is also applicable to all fourteen of the Eagle-21 cabinets that now comprise WBN's process protection system (including the four cabinets associated with RTD bypass elimination, which have recently been upgraded to the latest electronic design of the ten new cabinets).

WCAP-11733 was submitted for NRC staff review by a letter dated March 24, 1989. The NRC's review determined that the testing of Eagle-21's design features for redundancy, electrical isolation, physical separation, fault tolerance, and surge withstand capability was acceptable. This determination is documented in the NRC staff's safety evaluation report (SER) dated June 13, 1989, for the Eagle-21 equipment that was used for RTD bypass elimination. The SER concluded, in part, that: "All of the isolators passed the pass/fail criteria for all of the tests noted above. Therefore, the requirement that the isolators protect the Class 1E side of the isolator is satisfied and the requirements of General Design Criterion (GDC) 25 and IEEE-STD-279-1971 regarding isolation are met. The staff concludes that the isolation devices are acceptable."

Although this topic has been reviewed and found acceptable by the NRC staff, the following key points are offered to confirm that the same test methods that were reviewed by the staff in the SER are still applicable:

- Communication between Class 1E and non-Class 1E equipment is provided through qualified isolation devices that have been tested commensurate with the requirements of IEEE-279-1971, IEEE-384-1981, and Regulatory Guide 1.75 Revision 2.
- The following noise and fault tests were performed to demonstrate that the Class 1E circuits and protective actions of the Eagle-21 system are not degraded when subject to environmental conditions which are less than desired:
 - Random noise test (antenna coupled),
 - Crosstalk noise - chattering relay test (antenna and direct coupled),

- Military Specification MIL-N-19900B noise test (antenna coupled),
- High voltage transient noise test (antenna coupled),
- Static noise test (antenna and direct coupled),
- Maximum credible fault tests (ac and dc fault voltages), and
- Surge withstand capability (SWC) test (in accordance with IEEE-472-1974).

The results from these tests are presented in Section 8 of WCAP-11733. Section 9 of WCAP-11733 reaches the following general conclusions based on the test results: 1) the Eagle-21 isolation devices prevent degraded operation of Eagle-21 Class 1E circuits and protective functions when subjected to maximum credible fault conditions, 2) the protective actions of Eagle-21 are not affected by surges applied to the isolation devices, 3) no component failures occurred as a result of the SWC tests, and 4) channel calibrations were not affected by surges.

The following summaries paraphrase the specific conclusions reached in Section 9 of WCAP-11733.

NOISE TESTS

The protective action of the Eagle-21 system was not affected by noise injected into or adjacent to non-Class 1E wiring. Analog output signal noise that was recorded during testing was coupled wire-to-wire or through the analog output channel. Two possible effects of analog output noise on plant non-Class 1E systems and the post-accident monitoring system were noted.

- Sources of ac noise generated noise spikes on the analog output signal. No change in the nominal dc value of the analog output signal was recorded. These noise spikes will not affect slow-responding monitoring equipment.
- Sources of dc and high-voltage transient noise generated a shift in the nominal dc value of the analog output signal of 0.5% or less. These effects are of minimal concern since the accuracy tolerances of the plant monitoring/control systems exceed the observed effects.

FAULT TESTS

The protective action of the Eagle-21 system was not affected by the injection of maximum credible faults of 250Vdc and 580Vac into the designated non-Class-1E-to-Class-1E isolators. The analog output signal noise that was recorded was coupled wire-to-wire and consisted of a noise spike of 0.88% or less upon fault application. No change in the nominal dc value of the analog output signal was recorded. These noise spikes will not affect monitoring equipment.

SWC TESTS

The protective action of the Eagle-21 system was not affected by the injection of the surge withstand test wave to the designated non-Class-1E-to-Class-1E isolators. In addition, no component damage

4. Software

Question 7:

How long can the WBN Eagle-21 resistance temperature detectors (RTDs) that are associated with reactor coolant system (RCS) overpower (OPAT) and overtemperature (OTAT) protection be removed from scan and entered into the newly added disabled "D" state, and how many RTDs can be removed from scan and entered into this state? Can failed RTDs be removed from scan and entered into the "D" state? If so, explain why this would not reduce the reliability of the system.

Response:

Eagle-21's redundant sensor algorithm (part of the RTD bypass elimination functional upgrade) permits one T_{Hot} RTD and one T_{Cold} RTD which have either failed or become inoperable to be removed from scan and entered into the disabled "D" state indefinitely. Such action is taken only after streaming factors have been determined based on temperature fluctuations measured by the RTDs during the RCS flow calorimetric. Disabling one T_{Hot} RTD and one T_{Cold} RTD does not reduce the reliability of the Eagle-21 system because the setpoints for OPAT and OTAT are conservatively calculated allowing for the failure of one T_{Hot} RTD and one T_{Cold} RTD. Additionally, redundant RCS temperature measurements are still available from two T_{Hot} RTDs and one T_{Cold} RTD in the event of a single failure in the hot or cold leg. This design feature is consistent with Section 4.2 of IEEE-279-1971.

Question 8:

Explain how the threshold settings for the steam flow and feed flow are added to the WBN Eagle-21 system. This should include the threshold setting analysis report if there is any.

Response:

The steam flow and feed flow threshold settings are features that were present in the Foxboro process control system which was originally installed at WBN. Although these are new features for the Eagle-21 process protection system, their implementation and use are similar to the equivalent features that were previously installed in the Foxboro system. Note that, as a result of design changes developed in conjunction with the Eagle-21 functional upgrade, the steam flow and feed flow loops no longer perform a reactor protection function.

Steam flow and feed flow threshold settings are initially calculated using scaling procedures which take into account steam flow and feedwater flow ranges, equivalent ranges of differential pressure, and the steam flow and feedwater flow rates that are equivalent to full flow. The threshold setting values are calculated manually for initial startup conditions using the above variables. Once the initial settings are established, the tuning constants associated with steam flow and feed flow are entered into the Eagle-21 system via the man-machine interface (MMI) using the parameter update mode. Additional information about this process is contained in Section 2.3.9 of WCAP-12374 Revision 1 ("Eagle-21 Microprocessor-Based Process Protection System"). WCAP-12374 Revision 1 was submitted for NRC staff review by a letter dated February 26, 1992.

The purpose of adding threshold settings to the steam flow and feed flow calculations for WBN is to set the associated flow output to zero if the differential pressure input signal is less than the minimum value established by the threshold setting. In effect, the threshold settings are used to suppress noise-induced fluctuations (flutter) in the flow output signals for low-flow conditions (i.e., flow less than the threshold setting). If required, the feature can be turned off by setting the thresholds to zero.

Question 9:

Are all the hardware and software modifications for WBN complete? If not, provide: (1) the descriptions of the modifications that have not been finalized and (2) the completion schedule.

Response:

Installation of the Eagle-21 process protection system is essentially complete. One planned Eagle-21 hardware modification has not yet been implemented. This modification consists of routing 15-volt relay power directly to the power bus bar, rather than routing it through the front test panel keyswitch. Direct routing eliminates switching noise to the Eagle-21 analog input and RTD input boards. The modification is required for each Eagle-21 equipment rack. It is currently scheduled for completion by the end of 1993.

Although not specifically a part of the Eagle-21 system, many of the electrical cables to and from peripheral components (i.e., process sensors, main control room indicators and alarms, computer inputs, etc.) are not yet connected to the Eagle-21 racks. TVA plans to connect these cables a few at a time whenever they are needed to support preoperational testing of the associated components.

Question 10:

Provide scaling and setpoint documents (SSDs) for WBN.

Response:

The SSDs that were prepared for WBN consist of 95 individual documents. An SSD was prepared for each channel associated with the 21 functions processed by the Eagle-21 system. The following general approach was used to prepare an SSD. First, plant-specific data was collected to describe the functional configuration and physical installation of the instrumentation channel at WBN. This data was reviewed and translated to the appropriate format for scaling and setpoint calculations. Then, the test methods that would be used for the Eagle-21 system and its input/output peripheral components were defined. This included measurement and test equipment requirements. Next, any differences in calculational methodology with respect to standard Westinghouse methodology for instrument scaling and setpoints (as defined in WCAP-12096) were identified. Finally, engineering calculations were prepared to determine the uncertainties associated with the operating limits, calibration values, and scaling limits for the instrumentation channel. Note that the above process for preparing an SSD is controlled by WBN plant procedures.

After the SSDs are prepared and issued as controlled documents, they become design-basis input for use in writing WBN's surveillance instructions (SIs). SIs are first used during final checkout and preoperational calibration of the Eagle-21 process protection system and associated interfaces (i.e., sensors, indicators, recorders, plant computer(s)). After Eagle-21 preoperational testing is completed and WBN is licensed, the SIs are used as the principal procedures for periodic testing of Eagle-21 and its interfaces in accordance with the applicable surveillance requirements from WBN's Technical Specifications.

Formal submittal of the SSDs for NRC staff review is not practical because of the number and size of the documents. However, the SSDs are available on site for detailed review at any time. Based on a telephone discussion between TVA and the NRC staff reviewer for Eagle-21 on August 3, 1993, this arrangement is acceptable and formal submittal of the SSDs is not required.

Question 11:

Explain how the WBN Eagle-21 main program and supporting software are tested. Is the entire Eagle-21 software retested to ensure that the modified software section would not cause any problems elsewhere? If all the Eagle-21 software is not retested, provide the justifications for not retesting the entire Eagle-21 software.

Response:

Software testing is part of the verification and validation (V&V) process that is used for Eagle-21 design and development work. Appendix A of WCAP-12374 Revision 1 is the "Eagle 21 Replacement Hardware Design, Verification and Validation Plan." This plan has been used consistently throughout the system and software design and testing phases of Westinghouse's Eagle-21 program. It was previously used for WBN's original four Eagle-21 cabinets, which were part of the modification for RTD bypass elimination. It continues in use today for the additional Eagle-21 cabinets that upgrade the remainder of the process protection system. Note that the NRC's review of the original four Eagle-21 cabinets concluded that the software testing process and the overall V&V process were adequate. Specifically, the NRC staff's SER dated June 13, 1989, stated: "... the staff concludes that the Design, Verification and Validation Plan and resulting processes are acceptable."

The following discussion addresses the question of how the Eagle-21 main program and supporting software are tested. Two types of software testing are performed during system verification--structural testing and functional testing.

- Structural testing is a comprehensive method of exercising the software program code and its component logic structures at the unit level. Structural testing uses computer emulation to verify the proper functioning of both the complete program and the specific internal structure within the program that responds to the test input. This type of testing requires that the verifier inspect the code and understand how it functions before selecting test inputs. The test inputs are chosen to exercise all the possible control paths within the software component. If this is not possible, the test inputs are chosen to exercise every executable statement within the component.
- Functional testing is a method of evaluating the properties of the program in comparison to those that are required by the design specification. During functional testing, the internal structure of the program (i.e., unit level) is ignored. The module or subsystem level is tested instead. Examples of this type of testing include random testing and testing special cases by function.

Random testing is used in the following circumstances:

- To simulate real time events that are clearly random,
- To provide added confidence that a very complex module is correct,
- To test a subsystem or a system where it is not necessary to test all of the possible paths,

- To obtain a quantitative measurement of the accuracy of a numeric calculation, and
- To measure the average time required for a calculation.

Testing special cases by function is used in the following circumstances:

- To test a subroutine for matrix inversion by using almost-singular and ill-conditioned matrices,
- To test subroutines that accept arguments from a specified range by using arguments at the extreme limits of the range,
- To test an arithmetic package by using variables that have the largest and smallest mantissae, the largest and smallest components, all zeroes, and all ones and negative variables.

Two further types of testing are performed during system validation--top-down functional requirements testing and prudency review/testing of the design and its implementation. Top-down functional requirements testing treats the system as a black box, while prudency review/testing requires that the internal structure of the integrated software/hardware system be analyzed and tested in detail.

- Top-down functional requirements testing involves dividing the highest-level system functional requirements into subrequirements such as accuracy, range, time response, comparator type, etc. The integrated system is then tested for each of these subrequirements to verify that the system performs as required.
- Prudency review/testing provides assurance that the system operates properly under abnormal-mode conditions such as below or above range, etc. Prudency review/testing also demonstrates that the system accepts only designated inputs and rejects inputs which are not permitted. Finally, prudency review/testing ensures that good engineering judgment and standard industry practices were used in the design and implementation of the critical areas of the system. In order to evaluate the above items during prudency review/testing, the technical details of system design and implementation must be identified and compared to the "system prudency checklist." This checklist addresses the following critical design areas:
 - Firmware program storage,
 - Database information storage,
 - System architecture supporting shared memory among multiple processors,
 - System architecture oriented to available data links,
 - Diagnostics, and
 - System time synchronization.

In answer to the question concerning the extent of retesting associated with modification of a section of the software, only the affected elements of the main program and supporting software are tested. An impact analysis is done to identify the software elements (i.e., system, subsystem, module, or unit) that need to be tested and to determine if existing (unchanged), new, or functionally modified code must be tested. This technique determines which functionally modified code structures must be retested. It also determines

if the modified code functionally impacts existing code (i.e., an impact analysis determines how much retesting of existing code must be done to reverify and revalidate the existing code).

Question 12:

Is each of the WBN Eagle-21 software modification requirements covered by at least one test case? Explain how the modified Eagle-21 software meets the: (1) performance requirements, (2) external interface requirements, and (3) man-machine and system control requirements. In addition, describe the acceptance criteria and provide the summary of the test results.

Response:

Each of WBN's Eagle-21 software upgrades (modifications) is covered by at least one test case. The test results for the original and modified (upgraded) code are documented in WCAP-13191 ("Watts Bar Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report"). The latest version of this report (Revision 2) was submitted for NRC staff review by a letter dated November 8, 1993. Software testing was done in accordance with the V&V plan, which is discussed in the response to Question 11. The testing demonstrated that the software modifications satisfy appropriate design specifications and top-level functional requirements. The acceptance criteria for these functional modifications were based on applicable instrument uncertainties and the loop cycle times that are required to process the functions that were affected. More specific information about the acceptance criteria can be found in Westinghouse design documents that are available on site for detailed review at any time.

Question 13:

Provide a summary of the: (1) verification and validation (V&V) process and (2) software configuration management for the modified WBN Eagle-21 system. The summary should also include the revised V&V report (WCAP-13191, Revision 2) and TVA's evaluation of Westinghouse's V&V process and problem reports.

Response:

The Eagle-21 V&V plan and the NRC staff's prior acceptance of this plan for WBN's original four Eagle-21 cabinets are discussed in the response to Question 11. The same V&V plan was also used by Westinghouse during the design and development of the Eagle-21 systems for both units at Sequoyah Nuclear Plant (SQN). SERs issued by the NRC staff for SQN's Eagle-21 systems evaluated the V&V process and found it to be acceptable. For SQN, the NRC staff's evaluation included a special audit at Westinghouse on April 18-20, 1990, to examine Eagle-21 software design and the associated V&V process in detail. Based on this audit and other supporting information, the NRC staff concluded that the V&V plan meets the intent of Standard ANSI/IEEE-ANS-7-4.3.2-1982 and is therefore acceptable.

(1) Verification and Validation Process

The following is a summary of the Eagle-21 V&V process. WCAP-13191 Revision 2, which is the V&V report for WBN's Eagle-21 system, was submitted for NRC staff review by a letter dated November 8, 1993. This submittal also included TVA's evaluation of Westinghouse's V&V process and associated problem reports.

DEVELOPMENT ORGANIZATION AND VERIFICATION AND VALIDATION ORGANIZATION

Two independent organizations are used during the system design process--one for development and one for V&V. The software development organization prepares the software design specifications based on the system design specification. Then, this organization designs, develops, tests, and documents the code. The verification organization performs the required reviews and tests to produce a V&V report after receiving the released code and its documentation.

This organizational structure has several advantages. The involvement of two independent entities adds diversity into the process of software generation and reduces the probability of an error remaining undetected. Also, the designer of the code must prepare extensive and clear documentation of the code before the V&V effort can begin.

Since functional independence is essential to achieve these goals, the two organizations have separate lead engineers. Note that the development organization submits the code for V&V only after the various designers in the development team agree that the code is satisfactory. Errors that are discovered and corrected (debugging) during development phase testing are not required to be documented by the verification organization.

VERIFICATION AND VALIDATION BASIS

The V&V process was modeled after the guidance provided in the following programs and processes:

- The 414 Integrated Protection System Prototype Verification Program, which was presented to NRC in 1977 as part of the Westinghouse RESAR 414 system,
- Standard ANSI/IEEE-ANS-7-4.3.2-1982,
- Regulatory Guide 1.152, and
- The Design, Verification, and Validation Plan that was used for the Qualified Display Processing System (QDPS) at South Texas Nuclear Plant.

SYSTEM VERIFICATION

Designers are obligated to conduct independent reviews of the software that is associated with a programmable digital computer which is used as part of a safety system at a nuclear power station. Such reviews ensure the functionality of the software to a level of detail that is consistent with the system requirements.

As discussed in the response to Question 11, both structural testing and functional testing are performed to verify the software. This testing is done by an organization that is independent from the organization which designed the software.

SYSTEM CODE VERIFICATION AND DOCUMENT REVIEWS

There are three types of reviews used in the verification of system software--design document reviews, source code reviews, and functional test reviews.

- Design document reviews ensure that the lower level of code (i.e., unit) meets all of the performance requirements which are stated at a higher level in the code design document (i.e., module).
- Source code reviews visually examine the software program to confirm that it agrees with specifications. Source code reviews are used to verify that the provisions of a design specification are adequately transformed into high-level code.
- Functional test reviews confirm that the documentation associated with functional tests of the software provides a high degree of assurance that the software will perform the functions which are specified in the design requirements. The functional tests were performed by the software designer as part of system integration testing.

SYSTEM VALIDATION

The system validation process demonstrates that the system design satisfies the system functional requirements. System validation testing ensures that the the system requirement documents were correctly interpreted and captured during the definition and design stage of

software development. This testing also ensures that each of the software entities (i.e., unit, module, and subsystem) functions properly beginning from the smallest software entity and progressing to the program level. System validation testing is performed on an integrated system package that includes both hardware and software.

Any inconsistencies that are identified during system validation are recorded and tracked until resolution by the design team. However, only verified code is used during validation testing, so the likelihood of finding software/algorithm errors is minimal.

As discussed in the response to Question 11, system validation testing includes both top-down functional requirements testing and prudency review/testing of the design and its implementation. Like system verification testing, system validation testing is performed by an organization that is independent from the organization which designed the software.

SYSTEM REVIEWS

System validation reviews of the software and hardware ensure that any plant-specific features or configuration differences have been addressed. These reviews also ensure that a consistent design approach was used to implement the top-level requirements in the functioning of the system. The pertinent top-level requirements are those that are specified by the system functional requirements and translated to the process protection/control block diagrams.

The software configuration review confirms that the system configuration file which is uniquely associated with each Eagle-21 equipment rack contains the correct information for each type of channel in the rack. For example, WBN's Rack 1 contains information relative to reactor coolant flow, pressurizer pressure, and pressurizer level. Its configuration file contains specific information associated with each of these functions. The following items are representative of this configuration information.

- There is one partial trip output for each input to the reactor coolant flow channel.
- A de-energize-to-actuate low (decreasing) comparator is the tripping function for the low-flow reactor trip.
- An analog-output 4-20mA current loop is provided to interface with peripheral equipment.
- A 10-50mA input is provided via a TAPS power supply for the sensor signal.
- The range for the reactor coolant flow channel is 0-110% flow. All other inputs for range above or below the specified range are considered abnormal.
- Etc.

HARDWARE REVIEWS

The hardware review determines that there was consistency in the system design. For example, this review confirms that:

- Eagle RTD input (ERI) boards have been used for all RTD inputs,
- Eagle partial trip (EPT) boards have been used for all comparator outputs,
- The front test panel is capable of measuring the analog inputs, analog test points, and analog output points that are associated with a channel,
- Etc.

Most of the hardware review is performed as part of prudency review/testing during system validation. Additional information concerning the hardware review is contained in the Eagle-21 V&V plan, which is Appendix A of WCAP-12374 Revision 1, as previously noted in the response to Question 11.

MAN-MACHINE INTERFACE VERIFICATION AND VALIDATION PROCESS

The man-machine interface (MMI) test cart is a moveable electronics rack that can be connected to the various Eagle-21 process protection system racks to perform surveillance testing, calibrations, and diagnostic checks. The same V&V process that was used to confirm the adequacy of the overall design of the Eagle-21 system was also used to evaluate the MMI subsystem and its associated software. V&V activities to demonstrate the adequacy of MMI functions were completed at the same time as the V&V activities for the remainder of the Eagle-21 system. WCAP-13191 describes how V&V was performed for the MMI subsystem.

(2) Software Configuration Management

Westinghouse has established the Code Management System (CMS) as the part of its software management process that develops procedures and standards to control an evolving software system. The same CMS process was used for both the WBN and SQN Eagle-21 codes. In essence, the application of CMS to Eagle-21 software involves identification of changes, controlling these changes, managing the portions of the system that are subject to the changes, and releasing the changes to users of the system. Applying CMS to the Eagle-21 software is a post-development activity during design implementation of the software system. It provides a means to control specific "versions" of the developed software.

The need for CMS arises because software systems, particularly large ones, have a long lifetime and are expected to change during that lifetime. Furthermore, the anticipated changes are "team" activities and not the responsibility of an individual software developer (programmer). Through CMS, a configuration manager (an assigned person in the design/developing organization) becomes responsible for keeping track of the differences between various versions of the software. The configuration manager is also responsible for ensuring that new versions are derived in a controlled manner. The CMS process ensures that the proper revisions of the software are released to the correct users at the appropriate time.

In addition to the Westinghouse CMS process, future Eagle-21 configuration changes are also governed by WBN plant procedures. WBN maintains Eagle-21 configuration control drawings that specify jumper

and switch configurations, board and software revision levels, and rack configurations. These drawings are used by instrument technicians to ensure that Eagle-21 boards and racks are restored to their approved design configurations after testing or maintenance.

Question 14:

Explain the software error reporting procedures. Explain how software errors are reported to the NRC.

Response:

During the V&V process at Westinghouse, problem reports are prepared to document anomalies (typically software errors) that are found during testing and review activities. These problem reports are not provided directly to affected Westinghouse-client utilities or NRC unless they are determined to affect Eagle-21 systems that are currently in operation or to affect plant safety. Instead, the problem reports are used as an internal (Westinghouse) means to track system-related anomalies. Such an anomaly (i.e., software error) is not typically reported to NRC unless it is determined to affect the safety of a utility operating an Eagle-21 process protection system. The response to Question 17 describes the error reporting process that would be used to notify NRC, if required.

Problem reports are generated during the V&V process when any of the following concerns arise.

- When any anomaly is discovered during source code review or during testing, a verification problem report is issued from the verification team to the design team for resolution. The three types of these problem reports depend on the scope of the discovered anomaly: 1) unit-level problem reports that address anomalies specific to a single unit of code, 2) module-level problem reports that address anomalies covering entire modules (typically due to formatting standards concerns), and 3) generic problem reports covering issues that span multiple modules.
- When any validation test fails the applicable acceptance criteria, a problem report is issued from the validation team to the design team for resolution. These problem reports are typically associated with four types of anomalies: 1) software changes that require additional verification once resolved, 2) test setup changes, 3) test procedure changes, and 4) external influence corrections.

As stated earlier, problem reports provide a formal tracking mechanism within the V&V process. They ensure that anomalies which are found in the software system during testing and reviews are resolved satisfactorily and do not prevent the system from satisfying its functional and software design requirements.

5. Defense Against Failures

Question 15:

Explain how the WBN Eagle-21 system defends against common-mode failures. The explanation should include the applicant's evaluation on defense-in-depth analysis and functional diversity. Does WBN use Westinghouse's Eagle-21 family product line in the anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC)?

Response:

The design of the Eagle-21 process protection system provides either three or four instrumentation channels for each reactor trip or engineered safety features actuation system (ESFAS) function. The outputs from these instrumentation channels feed into two trip logic trains that initiate appropriate reactor protective actions. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent a required protective action. The aforementioned design provisions of the digital Eagle-21 system are identical to the design provisions of the analog Foxboro process control system that it replaces.

Neither TVA nor Westinghouse believes that a common-mode failure of the Eagle-21 system due to an undetected software error or hardware failure is a credible event. However, a detailed evaluation of such an event has been performed to demonstrate how it could be mitigated by other plant systems that provide appropriate functional diversity and defense-in-depth. The evaluation is contained in WCAP-13869 Revision 1 ("Functional Diversity Assessment for the Reactor Protection System/Engineered Safety Features Actuation System at Watts Bar Units 1 and 2"). This report identifies various alternate means of accident mitigation for the accident transients that are analyzed in Final Safety Analysis Report (FSAR) Chapter 15. It emphasizes alternate means of mitigation for the accident analyses that rely on both primary and backup protective functions (i.e., functions that are taken credit for in the accident analysis) from the Eagle-21 system. WCAP-13869 Revision 1 was submitted for NRC staff review by a letter dated November 18, 1993.

WBN does not use a Westinghouse-supplied AMSAC system. WBN's AMSAC system was supplied by Atomic Energy of Canada Limited (AECL). The AECL system design uses redundant programmable logic controllers supplied by Gould-Modicon. The microchips in these controllers are manufactured by Sharp Electronics.

6. Hardware

Question 16:

Discuss the hardware changes incorporated in the Eagle-21 hardware for WBN to increase its capabilities as compared to Sequoyah's Eagle-21 system to process an additional type of sensor that uses gain and offset adjustment coefficients. The discussion should also explain: (1) what hardware is changed and (2) what tests are performed. Finally, provide the results of the tests.

Response:

In response to a previous question from the NRC staff, TVA provided a detailed comparison of WBN's Eagle-21 system design to SQN's Eagle-21 system design in a letter dated October 26, 1992. This comparison discussed the design provisions in WBN's Eagle-21 system to process an additional type of sensor that uses gain and offset adjustment coefficients.

WBN's Eagle-21 system has software provisions that allow an operator to adjust gain and offset for the process instrument loops associated with reactor coolant flow. The gain and offset adjustment coefficients (i.e., tuning constants) that the operator enters are based on flow calorimetric data. The adjustments are made via Eagle-21's man-machine interface parameter update mode. Additional information is contained in Section 2.3.9 of WCAP-12374 Revision 1.

This new design provision in WBN's Eagle-21 system (as compared to SQN's Eagle-21 system) is a human factors improvement that resulted from a review of the periodic readjustments which are required upon completion of a flow calorimetric. It eliminates the need to adjust or rescale the reactor coolant flow sensors in a "hot" environment. The addition of gain and offset adjustment coefficients to the Eagle-21 system did not require any hardware changes. The software changes that were involved have been through the V&V process which is described in the response to Question 13.

Question 17:

How is information on Eagle-21 system failures (chip problems or failures specific to the Eagle-21 system) and their corrective actions communicated between Westinghouse and WBN?

Response:

Westinghouse communicates information regarding Eagle-21 failures (either hardware or software) to affected utilities as required by the applicable provisions of 10 CFR 21, 10 CFR 50.55(e)(1), and 10 CFR 50.59. The specific notifications that Westinghouse makes for each known defect or nonconformance related to the Eagle-21 system are procedurally determined by its "potential issue" reporting process with management oversight provided by the Westinghouse Safety Review Committee. Affected utilities and the NRC are informed of a defect or nonconformance if it is determined to create a substantial safety hazard or if a failure to comply with the Atomic Energy Act is associated with a substantial safety hazard as defined in 10 CFR 21. However, if a deviation from or failure to comply with the Atomic Energy Act associated with a substantial safety hazard is identified or if a defect in a component that was supplied by Westinghouse is identified, then 10 CFR 50.55(e)(1)(i) requires only that Westinghouse notify its corporation partnerships (i.e., affected utilities such as TVA). Westinghouse states that all past nonconformances and failures that were identified during Eagle-21 use or testing have been communicated to affected utilities using the above process.

In addition to this formal notification and reporting mechanism, an Eagle-21 users group has been formed to help identify, prioritize, and expedite the resolution of Eagle-21 issues. This users group is a voluntary organization that currently has members from Zion, Diablo Canyon, Turkey Point, SQN, WBN, and Westinghouse. The group held its first formal meeting in September 1991 in conjunction with the annual Westinghouse instrumentation and control seminar in Pittsburgh. There were twelve attendees representing four utilities and Westinghouse at the meeting. The Eagle-21 users group allows an active exchange of information, ideas, and concerns related to Eagle-21 equipment and procedures. It provides a forum to discuss design enhancements proposed by Westinghouse and user feedback from the utilities. In addition, working relationships between key individuals at the various member utilities are developed. These relationships help disseminate information about emerging Eagle-21 issues quickly.

There are also communication pathways within TVA for personnel at WBN and SQN to discuss Eagle-21 experience and issues. Furthermore, TVA procedures for design review, problem evaluation, and corrective action ensure coordination of the Eagle-21 systems at WBN and SQN. These procedures require that any concern, problem, testing anomaly, system failure, procedural discrepancy, or potential safety issue which is identified at either plant must be addressed and resolved, if applicable, by the other plant. TVA's organizational structure provides another means to ensure consistency in the configuration, operation, maintenance, and testing of the Eagle-21 systems at WBN and SQN. Specifically, TVA has corporate-level organizations for engineering, maintenance, and operations support. These corporate organizations are responsible for reviewing generic issues that are common to both plants.

7. System

Question 18:

Do the Eagle-21 design changes impact WBN's commitments to meet Regulatory Guide (RG) 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident?"

Response:

No, all of WBN's previous commitments to RG 1.97 remain in effect.

Note that a recent NRC audit of SQN Units 1 and 2 determined that their degree of compliance with RG 1.97 was acceptable. This audit was documented in NRC Inspection Report Nos. 50-327/92-16 and 50-328/92-16 dated July 28, 1992. The report concluded that: "The licensee either conformed to or was justified in deviating from the guidance with RG 1.97. Within the conditions of the Safety Evaluation Report and this report, the licensee was in compliance with the design and qualification criteria for instrumentation in RG 1.97, Revision 2." Since the design of WBN's Eagle-21 system is very similar to SQN's Eagle-21 system, TVA expects that a review of WBN's Eagle-21 system would reach the same conclusion with respect to compliance with RG 1.97 Revision 2.

8. Power

Question 19:

Describe the power source for the WBN Eagle-21 racks. Does this power system have sufficient capability to power all the Eagle-21 racks? How much margin does the power source have?

Response:

Each of the four protection channels is powered by an inverter and distribution panel. The vital inverters for the four protection channels are physically independent and meet appropriate electrical separation criteria. The distribution panels facilitate load grouping and provide circuit protection. The output of each vital inverter is 120Vac (nominal) for load factors from 0.8 to 1.0. Within the output current range, the ac output voltage does not vary more than 2.0% for normal 480Vac supply voltage amplitude variations of 10% and frequency variations of 2.0% and an emergency supply voltage variation from 102Vdc to 140Vdc. The output frequency regulation is 60Hz \pm 0.5Hz with a maximum harmonic distortion of 5% and a maximum rate of change of 1.0Hz per second. The maximum total loading on each vital inverter board is less than 20KVA.

There is no design requirement for the Eagle-21 power source to have a specific reserve margin. However, TVA has performed an inverter loading calculation to ensure that the total connected load does not exceed the full-load rating of each vital inverter. The calculation is updated as necessary to incorporate load changes due to Eagle-21 system modifications. Based on experience at SQN, which has similar Eagle-21 power supplies and equipment, a net load diversity factor of approximately 60% is anticipated.

ENCLOSURE 2

List of Commitments

- TVA has contracted with Westinghouse to perform an electromagnetic interference/radio frequency interference (EMI/RFI) site survey of WBN's Eagle-21 system during hot functional testing. TVA will submit the results of this survey to NRC. The submittal will include a description of the methodologies and test equipment that were used to perform the survey, a comparison between on-site and factory EMI/RFI test results, and an assessment of the margin between the measured EMI/RFI spectrum and a conservative threshold above which EMI/RFI problems could occur.