

ENCLOSURE 2

EAGLE 21 PROCESS PROTECTION SYSTEM
VERIFICATION AND VALIDATION AUDIT REPORT
WATTS BAR NUCLEAR PLANT UNIT 1

9311160345 931108
PDR ADDCK 05000390
A PDR

T41 931025 897

QA Record

EAGLE 21 PROCESS PROTECTION SYSTEM

VERIFICATION AND VALIDATION AUDIT REPORT

WATTS BAR NUCLEAR PLANT UNIT 1

OCTOBER 1993

Don F Faulkner for
Prepared by Ron Reeves / 10/20/93
Ron Reeves
by telex approval.
John S. Craig / 10/25/93
John Craig

WATTS BAR EAGLE 21 PROCESS PROTECTION SYSTEM

VERIFICATION AND VALIDATION AUDIT

ATTENDEES:

Westinghouse

Jim Doyle, Eagle 21 Engineer
Terry Tuitt, V & V Manager
Larry Erin, I&C Licensing

TVA

Ron Reeves, Corporate Engineering, Computer Systems Specialist
Tim Jenks, Information Systems Consultant
John Craig, Eagle 21 Instrument Engineer

PURPOSE

The purpose of this audit was to ensure that the Eagle 21 Process Protection System supplied to Watts Bar was produced under an acceptable software development process. The Westinghouse Verification and Validation (V & V) process has been reviewed by the NRC for the Eagle 21 systems installed at Sequoyah, Turkey Point, Zion, and the original four racks installed at Watts Bar with the RTD Bypass Elimination modification.

SCOPE

The focus of this audit was to verify that the Watts Bar software changes were implemented acceptably; however, this required a broad look at the total Westinghouse software development process. Topics of the investigation included the items listed below.

- 1). Confirm adequate resolution of 13 problem reports from the V & V of the Watts Bar software changes.
- 2). Confirm that the Westinghouse software development process satisfies ANSI/IEEE-ANS-7-4.3.2-1982.
- 3). Confirm Westinghouse resolution of open items from the Zion SER.
- 4). Ensure that software errors identified at Sequoyah or other Eagle 21 installations have been resolved in the Watts Bar software.
- 5). Identify differences between the latest Watts Bar version of the Eagle 21 software and earlier revisions installed at Zion and Sequoyah.

SCOPE (Continued)

- 6). Evaluate the Westinghouse software development process according to the NRC Software Audit Plan. (See attached Figure 2.)
- 7). Determine the extent to which Westinghouse identified and resolved "Hazards", i.e. abnormal conditions, to which the Eagle 21 system might be subjected.
- 8). Determine the applicability of Zion's Defense-in-Depth Analysis to Watts Bar.

Results of the audit are summarized according to the order of the major topics listed above.

1). VERIFICATION AND VALIDATION PROBLEM REPORTS

A total of 13 problem reports were generated during the process of verification and validation (V & V) of Watts Bar Eagle 21 software changes. These reports were reviewed individually to verify that the resolution of each problem was acceptable and collectively to verify that there were no programmatic deficiencies in the Westinghouse V & V process. Problems were classified according to the types listed below:

Type A: Design requirements not implemented

Type B: Design requirements implemented incorrectly

Type C: Implementation includes items not in design requirements

Type D: Computational defects

Type E: Logic defects

Type F: Header / comment defects

The review of each problem report is summarized in the following discussion.

Report No. ET02802.PRB

Problem code: 1. Type D 2. Type B

Problem 1

This problem involving an incorrect Input Quality Status Flag was discovered as a result of the D-Code change to the RSA algorithm. The Software Design Requirement (SDR) for this function is clear. This is a random error and the software was changed to correct it.

Problem 2

This problem describes a terminology error in the SDR for the Test Sequence Processor (TSP). The SDR will be revised to correct the error. This item is being tracked on a V & V open items list. Administrative controls in the V & V program require a revision to the SDR before changes are made to the affected software modules.

Westinghouse will confirm that this administrative procedure is in place and close all open items related to SDRs.

Report No. ET02803.PRB

Problem code: 1. Type D 2. Type B

Problem 1

This problem involves the same type of Input Quality Status Flag error identified in Problem Report ET02802 above for a similar software variable. The software was corrected to agree with the SDR.

Problem 2

This problem identifies the same terminology error in the SDR for the TSP as discussed in Problem Report ET02802 above. The SDR will be revised to correct the error. Resolution of this item is also being tracked on an open items list as discussed in Problem Report ET02802.PRB above.

Report No. EL28400.PRB

Problem Code: 1-6 Type B

Problems 1-5

Rack 11 EPROM output codes did not correctly implement the design configuration for the channels identified in this report. These problems were found during the verification process by using independently derived configuration data. These problems would have been caught during validation or the Factory Acceptance Test (FAT) if not found during verification. These errors were corrected in both the configuration spec. and configuration file to reflect the correct output codes. No open items were generated as a result of these problems. However, an observation was made that this process could be improved by using a more user-friendly tool to implement configuration design requirements.

Problem 6

Incorrect analog output gain values were given in the configuration file for the loops identified in this report. These errors were corrected in the configuration file. These corrections completed the resolution of this problem and no open items were generated.

Report No. ES13105.PRB

Problem Code: Type C

This problem identifies a change in the analog output gains and offsets calculation code that was not reflected in the SDR. This problem, which was found during the verification process, represents a code refinement that was not in the SDR. This refinement did not implement an unintended function in the code. The Surveillance Test (SRVT) SDR will be changed to correct this problem. Resolution of this item is being tracked on the V & V open items list as discussed in Problem Report ET02802.PRB above.

Report No. ES21940.PRB

Problem Code: Type C

This problem identifies a change in the time response test code not reflected in the SDR. This problem is similar in nature to the problem described in Report No. ES13105.PRB above. It represents a refinement in the code not reflected in the design requirements and will be resolved by changing the SRVT SDR. The code refinement did not implement an unintended function. Resolution of this item is also being tracked on the V & V open items list.

Report No. ES22035.PRB

Problem Code: C

This problem identifies a change in the trip actuation test code not reflected in the SDR. This problem is also similar to Report No. ES13105.PRB in that it represents a code refinement, but no unintended functions were implemented. The SDR change required to resolve this problem is also being tracked on the V & V open items list.

Report No. EL28100.PRB

Problem Code: B

The verification process identified an error in the configuration file for LB-921A HI LEVEL. The configuration file code was changed to agree with the design requirements. No open items were generated and no further action is required to resolve this problem.

Report No. EL08101.PR8

Problem Code: 1. Type A 2,4,5. Type D
 3. Type B 6. Type E

This report combines several problems identified during the verification of the Redundant Sensor Algorithm (RSA) software change.

Problem 1

The condition of three disabled sensors is not defined in the RSA code. This condition has no impact on the Watts Bar RSA functions since parameter update does not allow the three disabled sensor condition to be entered. However, the RSA code was revised to define this condition to make it more universal. The code revision resolves this problem and no open items were generated.

Problem 2

The RSA code should insert a "Done = True" statement when a three good sensor condition exists to prevent the execution of unnecessary steps. The code was revised to make it more efficient; however, the basic function of the algorithm is not affected. The code revision resolves this problem; no open items were generated.

Problem 3

The RSA had a group quality code of "bad" for the two-disabled, one-good sensor condition. The design requirements specify a group quality of "good" for this condition. The code was revised to agree with the design requirements. This problem would have been found in the validation process or the FAT if it had not been identified in the verification of the code. The code revision resolves this problem and no open items were generated.

Problem 4

When the local quality is set to "bad", the corresponding parameter value in the code should also be set to "bad" when exiting the software module. The RSA had set only the local quality to "bad" for the condition of any quality set to "poor". The code was corrected to set the pass parameter to "bad" when the local quality is set to "bad". This error would have been caught in validation testing if it had not been corrected during the verification process. The code revision resolves this problem and no open items were generated.

Problem 5

The RSA code structure had incorrectly implemented the required IF/THEN/ELSE statements when the condition of one disabled sensor and two bad sensors exists. The error was corrected by inserting IF/ELSE statements in the code. This type of error would also have been caught during validation testing if it had not been corrected by the verification process. The code revision resolves this problem and no open items were generated.

Report No. EL08101.PRB (Continued)

Problem 6

This problem identified an IF statement error in the RSA code. The incorrect IF statement was corrected in the code. The code revision resolves this problem and no open items were generated.

Report No. GEL0001.PRB

Problem Code: 1,6. Type B 2-5. Type A

Problem 1

Some tag names in the Man Machine Interface (MMI) software data files were found to be inconsistent with the configuration spec. Minor errors in software tags such as

PQY-456Q PZR Press (Spec.)
vs.
PQY-456Q Pzr Press (File)

were resolved by changing the spec. to agree with the files. The configuration file for the PQY-456Q PZR Press channel was changed to PQY-456Q Pzr Press to be consistent with the revised configuration spec.

Problem 2

The analog inputs identified in this problem were not found in the Functional Requirements. The limits assigned are default values for the ranges of these channels which were determined from the code. The default values were determined to be acceptable without updating the Functional Requirements. Actual ranges used for processing these channels are stored in NVRAM. These NVRAM values will be verified by preparation of Watts Bar scaling and setpoint documents (SSDs) and controlled by TVA design output documents. No further action is required.

Problem 3

The steam flow, feedwater flow, and containment spray flow analog output ranges listed in this problem description were determined from the code since they were not found in the Functional Requirements. The steam and feedwater flow range problem was resolved by a clarification of the range units specified in the Functional Requirements. The containment spray flow output ranges were determined to be acceptable and the problem was considered resolved by the same rationale used in Problem 2 for the corresponding input range. No Functional Requirements or code changes were required.

Report No. GEL0001.PRB (Continued)

Problem 4

The ranges for the tuning constants listed in this problem description were not found in the Functional Requirements. The steam flow and feed flow values identified were included in the Functional Requirements submitted to TVA for review and approval by Westinghouse letter WAT-D-8900. Streaming factor ranges were determined to be acceptable without updating the Functional Requirements. These are all default values and this problem is resolved for the same reason discussed in Problem 2 above.

Problem 5

The ranges for the comparator channels listed in this problem description were not found in the Functional Requirements. These are internal calculation ranges used only to establish the comparator lockup ranges. The ranges were determined to be acceptable without updating the Functional Requirements. No further action is required to resolve this problem.

Problem 6

This problem identified an apparent discrepancy between the Functional Requirements and the code for Trip Time Delay (TTD) polynomial coefficients A, C, E, and G. The ranges in the code appeared to be the negative of the range specified in the Functional Requirements. This problem was resolved with a clarification of the Functional Requirements. No changes were required to either the code or the Functional Requirements.

Corrective actions for this report were tracked on the V & V open items list, but the open item was subsequently closed as the required corrections were completed. No open items remain, and no further action is required to resolve these problems.

Report No. GEM0001.PRB

Problem Code: 1-11. Type F

This report consolidates eleven problems involving header and comment defects between the code and the software design spec. The problems were resolved by correcting the header or comment errors in the code or the software design spec. None of these problems affected the code itself. No open items remain and no further action is required to resolve these problems.

Report No. WAT.001-VAL

Problem Code: 1-3. Type B

Problem 1

When testing the RSA, an input sensor was disabled, but the rack trouble alarm did not clear. The trouble condition should be set only for a bad sensor input, not for a disabled input. This problem involves a discrepancy between the Loop Calculation Processor (LCP) subsystem and the TSP subsystem software. This problem was identified during V & V and resolved by correcting the RSA code in the LCP subsystem.

Problem 2

Validation testing of the 5 to 7 significant digit change for the MMI static information display found that the MMI printer was still printing in the 5 significant digit format. The problem was identified during V & V and resolved by correcting the MMI print code.

Problem 3

When calibrating test points for the Delta T/T Average (DTTA) Surveillance Test a test point on the front test panel was used twice. Only one test point per channel should be used during this surveillance test. The code was corrected to resolve this problem.

The problems summarized in this report were random errors. No open items remain and no further action is required.

Report No. WAT.002-VAL

Problem Code: 1-5,8. Type B 6,7. Type F

The problems combined in this report include various documentation problems identified during the preparation for validation tests. They are not actual verification test deficiencies. The problems originated from the review of the design requirements specified in three sources: Functional Requirement and Functional Decomposition Documents, Configuration Specs., and Process Control Block Diagrams.

Problems 1-4 originated from the review of Functional Requirement documents.

Report No. WAT.002-VAL (Continued)

Problem 1

A functional decomposition document referred to sections of a Functional Requirements Document which could not be found. This apparent problem was resolved with a response identifying the document section and revision level which contained the referenced requirement. No changes were required to the Functional Requirement Document. This was an administrative problem, not a V & V problem, because the latest revision of the decomposition document must be verified before start of the validation tests. The validation tests consider both documents, but verification of the latest decomposition document starts with the Functional Requirements Document.

Problem 2

This problem identified an apparent discrepancy between the units specified in the Functional Requirements Document for Reactor Coolant Flow range and the corresponding section of the Configuration Specification Document. The problem was resolved with an explanation of the relationship between the units of flow specified in the Functional Requirements Document and the units of differential pressure (dp) specified in the Configuration Specification Document. No changes were required to either document.

Problem 3

This problem concerned the lack of functional requirements for the feedflow algorithm and the newly implemented steamflow/feedflow square root conversion low threshold values. These changes were in the process of being implemented at the time this problem was identified. It was resolved by providing the updated Functional Requirement Document. The updated Functional Requirement Document was submitted to TVA for review and approval by Westinghouse letter WAT-D-8900. This action was tracked on the V & V open items list.

Problem 4

This problem identified a typographical error in Configuration Document 411A38, Rev. 1. The error was corrected in Rev. 2.

Problem 5

The Configuration Spec. review found two typographical errors in Configuration Document 411A38, Rev. 1. These errors were corrected in Rev. 2.

Problems 6-10 identify minor drawing errors found during the review of Process Control Block Diagram 108D408.

Report No. WAT.002-VAL (Continued)

Problem 6

The title sheet was not in agreement with sheet 17 concerning the number of protection sets represented. Sheet 17, which shows Protection Set II, is correct. The title sheet was corrected on Rev. 34, which was submitted to TVA for approval by Westinghouse letter WAT-D-8789.

Problem 7

The revision level for sheet 43 shown on the title sheet was not in agreement with the revision level shown on the actual drawing. This discrepancy was eliminated by correcting the title sheet on the next revision submitted to TVA for approval by Westinghouse letter WAT-D-8789.

Problem 8

The inside containment boundary on sheet 14 was shown incorrectly for the steam pressure channel. This error was corrected on the next revision of the drawing submitted to TVA for approval by Westinghouse letter WAT-D-8789.

The code was not affected by these minor block diagram errors. No open items remain for any of the problems included in this report.

Report No. WAT.003-VAL

Problem Code: 1,2. Type B

Problem 1

The Trip Time Delay (TTD) algorithm for calculating the delay time as a function of power in the Functional Requirements Document uses a normalized power term, P_b , where the source code and SDR for the LCP use ΔT . This problem was resolved by revising the Functional Requirements Document to clarify that the power index is determined from a dedicated ΔT signal. The Functional Requirement Document revision was tracked on the V & V open items list. This change in Document 7, Rev. 5, was submitted to TVA for review and approval by Westinghouse letter WAT-D-8900.

Problem 2

The variable P_b does not appear in the Calculate Thot Estimate function on the Block Diagrams for TTD channels. However, it is used in the calculation of Estimated Thot Values in the SDR. This problem was resolved by confirming that the calculation should use P_b as reflected in the SDR. Since showing this variable on the block diagram would be difficult and confusing, it was determined that the Block Diagram would not be revised to show this variable. No changes were required to the code.

No open items remain, and no further action is required to resolve this report.

PROBLEM REPORT SUMMARY

All the Watts Bar V & V problem reports were resolved in an acceptable manner. No programmatic deficiencies were found in the problems reviewed. However, Westinghouse committed to the following action items as a result of this review:

1. Close all open items related to Software Design Requirements revisions.
2. Verify administrative controls are in place which require that revisions to Software Design Requirements be completed before any changes are issued to the affected software code.

2). ANSI/IEEE-ANS-7-4.3.2-1982 PROCESS REVIEW

ANSI/IEEE-ANS-7-4.3.2-1982 defines an acceptable process for development of computer systems including the application of software verification and validation (V & V). The process that has been applied by Westinghouse for Eagle 21 meets the intent of ANSI/IEEE-ANS-7-4.3.2-1982 (See Figure 1). The process is procedurally controlled and contains documentation of critical steps in the hardware and software design. V & V is performed by an independent organization as a integral part of the development process. Requirements are documented at each hierarchical level and V & V ensures satisfaction of the requirements. Efforts are made at several levels to identify software hazards and verify that the software can accommodate them. The System Design Specification defines interfaces between hardware and software and lower-tier documents address interfaces where they exist.

The V & V Final Report, WCAP-13191, summarizes the Westinghouse V & V process used to develop the Watts Bar Eagle 21 software. This report was reviewed by TVA and discussed with regard to ANSI/IEEE-ANS-7-4.3.2-1982 requirements. The report was found to be acceptable with some minor corrections. However, TVA requested that the sections describing the V & V process be revised to clarify how the Westinghouse program implements ANSI/IEEE-ANS-7-4.3.2 requirements. Westinghouse agreed to revise WCAP-13191 and resubmit it for TVA approval.

3). ZION SER OPEN ITEMS

The NRC conducted a "thread audit" of new Eagle 21 software routines written for the Zion application. As noted in the Safety Evaluation Report (SER) for the Zion Eagle 21 system, three errors were discovered which had no corresponding problem reports and did not appear to be identified by the V & V program. These problems were found to have no operational significance and were characterized as a problem in the implementation of the V & V plan rather than a problem with the plan itself. However, Westinghouse committed to revise procedures governing V & V to clarify the reporting process for documentation anomalies and train design, verification, and validation personnel on these requirements.

Westinghouse confirmed that this commitment had been implemented in PSE - Nuclear Software V & V - Guidance and Instruction Manual, PSE IVV G&I, Revision 1.0, June 30, 1992. This commitment will be documented by project letter.

4). SEQUOYAH AND ZION SOFTWARE ERRORS

Westinghouse confirmed that software errors discovered during operation of Eagle 21 equipment at Sequoyah and Zion have been corrected in the Watts Bar code. The software errors listed below were identified for consideration.

Sequoyah

1. Surveillance test comparator uncertainty calculation
2. Containment spray contact configuration
3. MMI diagnostic printout vs. screen mismatch

Zion

LCP cycle sequencing: EPT board refresh

Westinghouse will document that all the software errors have been corrected in the Watts Bar software by identifying the code version and revision level which implemented the change.

A scaling factor error involving the axial flux difference tuning constant was discovered during startup of the Eagle 21 system installed at Turkey Point. This error did not involve a programming error, however, and no software code revisions were required.

5). CODE DIFFERENCES: WATTS BAR - SEQUOYAH/ZION

Westinghouse provided a summary of the differences between Sequoyah and Watts Bar software as input for TVA's response to NRC's request for additional information. The differences are summarized in the following list.

- a. Addition of a new quality code, "D", to the RSA code for a disabled sensor.
- b. Addition of a new sensor type for the reactor coolant flow channels which provides gain and offset adjustment capability.
- c. Addition of a threshold setting for the steam flow and feed flow channel square root calculation.
- d. Additional instrument channels including boric acid tank level, containment spray flow, pressurizer liquid and vapor temperature, and RHR pump discharge temperature.
- e. Loop Calculation Processor (LCP) execution cycle was rearranged to correct the Zion EPT refresh problem.
- f. Addition of a diagnostic to the LCP software which evaluates high and low counts read by the automatic input calibration routine and initiates a trouble alarm condition for a failed reference signal.

5). CODE DIFFERENCES: WATTS BAR - SEQUOYAH/ZION (Continued)

- g. Addition of a diagnostic to the Test Sequence Processor (TSP) analog output calibration software to evaluate gain and offset coefficients. An error message will be displayed on the MMI to indicate coefficients which fail the diagnostic.
- h. Modification of the MMI software to display static information to seven significant digits rather than five.

These changes involved a total of 506 software units which were developed and reviewed according to the V & V program described in Westinghouse WCAP-13191, Rev. 2. This audit concluded that the V & V program which developed these software changes meets the requirements of ANSI/IEEE-ANS-7-4.3.2 (See Item 2 above), and the 13 problem reports generated during the V & V process were resolved in an acceptable manner (See Item 1 above).

6). NRC SOFTWARE AUDIT PLAN

Figure 2, NRC Software Audit, was used as a guide to determine if the Eagle 21 software development process was properly documented. This audit plan is not a requirement, but documentation to support this plan is indicative of a comprehensive, well-documented program. Although the names of the documents did not always match, Westinghouse has documents that address most of the topics identified on Figure 2. Two discrepancies were identified:

- a. Westinghouse does not have an Interface Design Specification. However, as stated in Item 2 above, Westinghouse has a System Design Specification that defines high-level hardware/software interfaces. Lower level hardware and software specifications also contain interface requirements. This is acceptable.
- b. Westinghouse does not formally define a software "safety" plan or other lower-tier "safety" documents identified in Figure 2. Westinghouse does perform several types of "safety" activities as discussed under Item 7 below. The Westinghouse documentation could be better, but since "safety analyses" are not specifically required in ANSI/IEEE-ANS-7-4.3.2, this discrepancy is not considered a deficiency.

7). HAZARDS ANALYSIS

"Safety" or "Hazards" analyses should be performed to identify the credible abnormal conditions which a system may encounter so that the code can be designed to accommodate them. Westinghouse does not have a formally documented set of "safety" documents as identified in Figure 2, but several analysis steps were performed to identify hazards including:

- a. The Eagle 21 system specification lists potential failures/faults that the system might see.
- b. Prudency testing is done to confirm the ability to handle a set of identified conditions including potential human errors.
- c. Functional specifications cover full range and out-of-range input conditions.
- d. Validation testing covers extreme range conditions.
- e. Diagnostics perform extensive on-line testing to identify system failures.

Westinghouse has done extensive work in the area of hazards analysis going beyond the requirements of ANSI/IEEE-ANS-7-4.3.2. The analyses are not as extensive or well-documented as suggested in MIL-STD-882B or IEEE-P-1228. TVA asked Westinghouse to explore with the Eagle 21 users group whether additional work in this area is warranted.

8). DEFENSE-IN-DEPTH ANALYSIS

Westinghouse developed Eagle 21 using a "robust" development and V & V process. Westinghouse does not consider software common-mode failures to be credible. However, a Defense-in-Depth Analysis was performed for Zion to identify plant features that could be used to accomplish the safety functions in the unlikely event of a software common-mode failure. The Zion analysis relied on both 1E and non-1E equipment to provide diversity. This is acceptable based on the low probability of a software common-mode failure.

Westinghouse has proposed to do a functional diversity analysis for Watts Bar following the basic approach used for Zion and currently being used for Diablo Canyon. Westinghouse will require input from TVA concerning procedures, timing, and simulator verification. The Westinghouse analysis approach focuses on identifying functional diversity rather than performing a step-by-step defense-in-depth analysis as described in NUREG-0493. This approach appears to be adequate.

WESTINGHOUSE ACTION ITEMS

1. Close all V & V open items related to Software Design Requirements.
(See Report Nos. ET02802.PRB Problem 2, ET02803.PRB Problem 2, ES13105.PRB, ES21940.PRB, and ES22035.PRB.)
2. Confirm Westinghouse administrative controls are in place to require that Software Design Requirement revisions be completed prior to issuing changes to affected software modules.
3. Confirm that administrative controls are in place to ensure that all open items are tracked and closed in a timely manner.
4. Revise the V & V final report, WCAP-13191, to better describe the Westinghouse V & V process for the Eagle 21 system.
5. Identify version and revision level of the Watts Bar code which corrects software errors identified at Sequoyah and Zion.
6. Confirm that V & V procedure improvement commitments discussed in the SER for the Zion Eagle 21 system have been implemented.
7. Evaluate the need for additional work in the area of hazards identification with input from other Eagle 21 users.

CONCLUSIONS

All problem reports were reviewed, and the resolution was found to be acceptable for each report. Some problem reports were resolved by determining corrective actions which were tracked on the V & V open items list, and some of these items remain open. Westinghouse will close all open items related to software design requirements and describe the administrative controls in place to ensure that all open items are tracked and closed in a timely manner.

The reports were also reviewed collectively according to the categorization of problem types. WCAP-13191 categorizes the problems according to six error types and analyzes the resolution of the problems by grouping them according to five types of corrective actions. The largest percentage of problems involved header or comment defects. Most problems were resolved by revising design documentation.

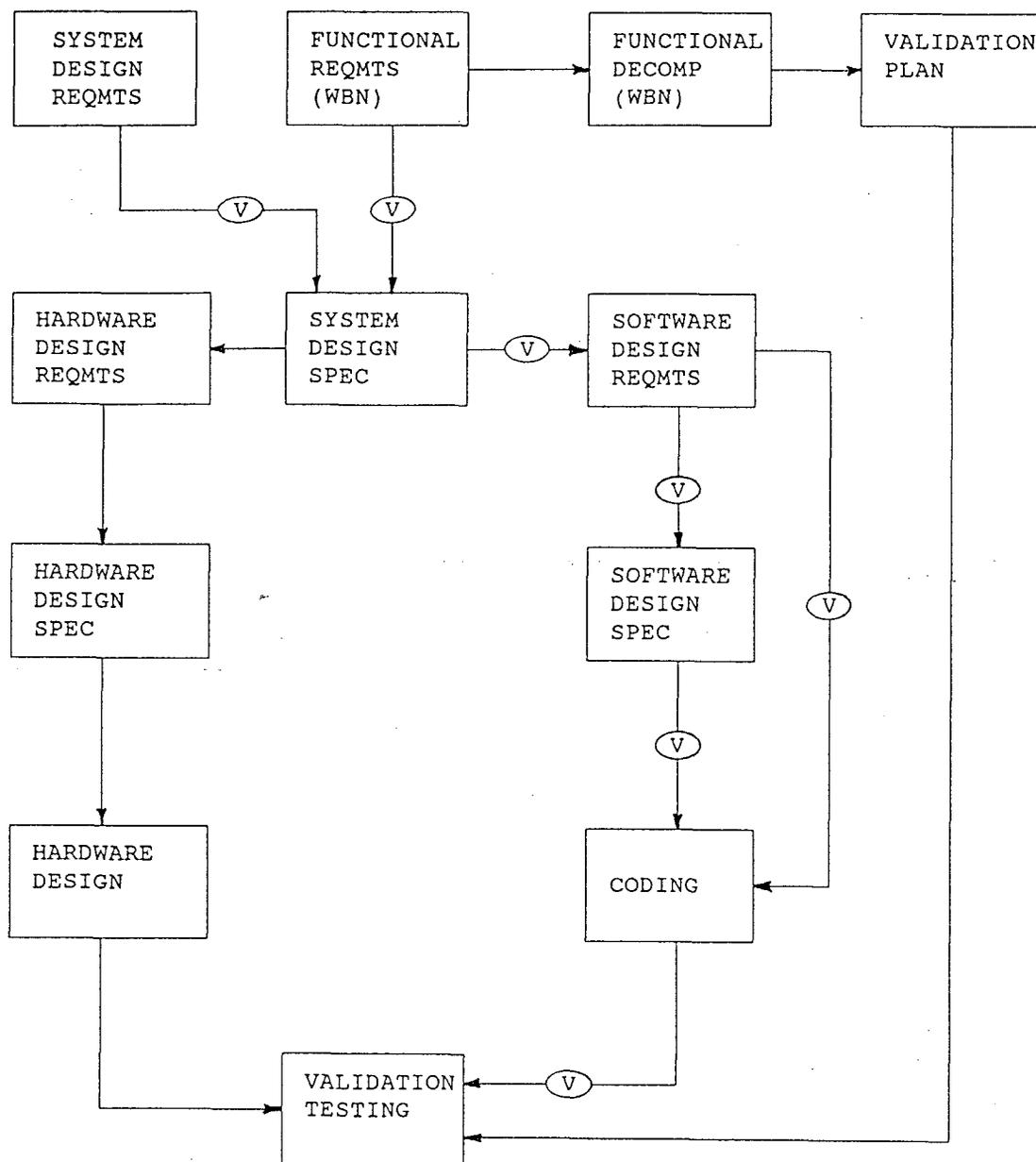
WCAP-13191 also provides a breakdown of the phases of the V & V process in which the problems were addressed. This analysis shows that most problems were addressed in the Verification and Configuration Data Review phases. Relatively few were addressed during the Validation phase. This distribution is characteristic of an effective V & V program. No adverse trends were found in the distribution of problem types or actions required for resolution.

The Eagle 21 development process for hardware and software meets the requirements of ANSI/IEEE-ANS-7-4.3.2 and was found to be acceptable. TVA suggested that Westinghouse revise the V & V report, WCAP-13191, to better describe the development process used for Watts Bar's Eagle 21 equipment.

All areas on the NRC audit plan (Figure 2) were covered by the Westinghouse program. Topics which were not formalized in separate documents were found to be adequately covered within the V & V process. TVA recommended that Westinghouse explore the need for further work on hazards identification with the Eagle 21 users group.

Features unique to Watts Bar have been properly developed and corrective actions for previously identified problems at Sequoyah and Zion have been implemented.

The Westinghouse response to the action items listed in the previous section was provided in letter WAT-D-9511 dated October 20, 1993 (Attachment 1). The resolution described for each item was determined to be acceptable and no further actions are required. Issue of this report documents final approval of the Watts Bar Verification and Validation program for the Eagle 21 Process Protection System upgrade.



(V) = Software Verification Step

FIGURE 1 - EAGLE 21 DEVELOPMENT PROCESS

Table 3.5-1

Flow of Documents through the Software Life Cycle

Software Developer Activities

Life Cycle Stage	Planning Stage	Requirements Stage	Design Stage	Implementation Stage	Integration Stage	Validation Stage	Installation Stage	Operation & Maintenance Stage
Software Management Plan			Unit Test Plan	Integration Plan	Validation Plan	Installation Plan	Maintenance Plan	Regression Test Plan
Software Development Plan				Integration Test Plan	Validation Test Plan	Installation Test Plan	Operations Manuals	
Software QA Plan		Requirements Specification	Hardware & Software Architecture	Code Listings	System Build Documents	Training Plan	Installation Configuration Tables	
		Interface Specifications	Design Specification			Operations Plan	Training Manuals	
			Interface Design Specification				Maintenance Manuals	
Software Safety Plan	Conformance Review	Requirements Safety Analysis	Conformance Review	Code Safety Analysis	Conformance Review	Validation Test Safety Analysis	Conformance Review	Change Safety Analysis
Software V&V Plan		V&V Requirements Analysis Report	V&V Design Analysis Report	V&V Unit Test Report	V&V Integration Test Report	V&V Test & Analysis Report	V&V Installation Test Report	V&V Change Report
		V&V Anomaly Report	V&V Anomaly Report	V&V Test Anomaly Report	V&V Test Anomaly Report	V&V Test Anomaly Report	V&V Test Anomaly Report	
Software CM Plan		CM Requirements Report	CM Design Report	CM Implementation Report	CM Integration Report	CM Validation Report	CM Installation Report	CM Change Report
		Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents
	Planning Audit	Requirements Audit	Design Audit	Implementation Audit	Integration Audit	Validation Audit	Installation Audit	

FIGURE 2 - NRC Software Audit

20



Westinghouse
Electric Corporation

Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

WAT-D-9511
October 20, 1993

Mr. W. L. Elliott
Manager of Engineering
Tennessee Valley Authority
Watts Bar Nuclear Power Plant
IOB-1A, P.O. Box 2000
Spring City, TN 37381

Attention: Steve Robertson

MR:	DRAFT REPLY	COM. COPY	INFO COPY	DATE	WAT-D-9467
EEB					
CEB					
MEB					
NEB					
Steve Robertson, Job 1H			1		
WD Witt, Job 1K			1		

Tennessee Valley Authority
Watts Bar Nuclear Plant Units 1 & 2
Eagle-21 V&V Open Items

cc'd by Ltr # NAR

Dear Mr. Elliott:

In response to TVA's Verification and Validation Audit, the following responses and confirmations are provided to closeout Westinghouse actions resulting from the audit. Please note that this letter supersedes that provided via reference 1.

- 1) Numerous changes have been implemented in the Software Design Requirements (SDR) for the Test Sequence Processor (TSP), Surveillance Test (SRVT) functions, and Loop Calculation Processor (LCP). As a result of these changes, all Watts Bar related V & V open items have been closed. A summary of these changes may be found below:

ET02802.PRB/2 - The TSP SDR has been revised to correct the terminology errors.

ET20803.PRB/2 - The TSP SDR has been revised to correct the terminology error.

ES13105.PRB - The SRVT SDR has been revised to document the refinement made to the analog output gains and offsets calculation code.

ES21940.PRB - The SRVT SDR has been revised to document the time response test code refinement.

ES22035.PRB - The SRVT SDR has been revised to document the refinement made to the trip actuation test code.

WAT-D-9511
Mr. W. L. Elliott

- 2 -

October 20, 1993

- 2) Westinghouse confirms that administrative controls are in place and exercised which require the revision of SDRs prior to the issuance of changes to affected software modules. These controls are documented in guidance entitled "Acceptance Criteria for Code and Documentation Releases to V&V", revision 1, dated October 3, 1989.
- 3) Westinghouse confirms that administrative controls are in place to ensure that all V&V open items are tracked and closed in a timely manner. This is accomplished through the maintenance and periodic review of a V&V open items tracking list. This list is periodically reviewed by the design and V&V groups at Westinghouse.
- 4) The Watts Bar Eagle 21 V & V report, WCAP-13191, has been revised to better describe how Westinghouse implements ANSI/IEEE-ANS-7.4.3.2 requirements. This report has been transmitted to TVA via letter WAT-D-9185, dated February 2, 1993.
- 5) The Watts Bar Eagle 21 system software is comprised of the following software subsystems and revision levels:

Test Sequence Processor Software	V04-03
Data Link Handler Software	V01-00
Digital Filter Processor Software	V01-01
Man-machine Interface Software	V04-01
Front Test Panel Bit Bus Software	V01-03
Input/Output Bit Bus Software	V01-02
Loop Calculation Processor Software	V01-01 (Racks 1,3-5,7-9,11-12, & 28) V01-02 (Racks 2,6,10 & 13)

The software revision levels noted above include corrections to software errors identified during operation of Eagle 21 equipment at Sequoyah, and Zion. The code version and revision levels which first implemented these changes are noted below:

- The SRVT code was revised to properly calculate the comparator uncertainties in TSP software V02-13.
- The proper configuration of the Containment spray contacts is accomplished in Watts Bar's LCP configuration files found in the LCP software versions and revisions noted above.
- A MMI diagnostic printout and screen mismatch was corrected in V02-09 of the MMI subsystem software.
- The LCP main program loop was rearranged to eliminate variability in the Eagle Partial Trip (EPT) board refresh pulse frequency and is included in the LCP software versions and revisions noted above.

There was a scaling factor error involving the axial flux difference tuning constant discovered during the startup of the Eagle 21 system installed at Florida Power & Light's Turkey Point Units 3 & 4. This error did not involve a programming error and as a result, no software code revisions were required to address this for Watts Bar.

WAT-D-9511
Mr. W. L. Elliott

- 3 -

October 20, 1993

- 6) In response to the documentation anomalies identified by the NRC during a thread path inspection of software written for the Zion application, Westinghouse has prepared a guideline which better defines the reporting process and requirements for documentation anomalies. This guideline is entitled "PSE-Nuclear Software V&V-Guidance and Instruction Manual, PSE IVV G&I" and was issued as revision 1.0 on June 30, 1992. This guideline and associated checklists are being implemented to improve the reporting of documentation anomalies.

- 7) At the request of TVA, Westinghouse polled members of the Eagle 21 users group and other users as to whether additional work in the area of hazards analysis is deemed necessary. It was the group's opinion that additional work in this area is not warranted. Westinghouse believes that the present system requirements, coupled with extensive verification, validation, and prudency testing adequately address this issue and exceed the requirements of ANSI/IEEE-ANS-7.4.3.2.

If you have any questions on this matter, please contact this office.

Very truly yours,

Kuth Forst
J. W. Irons, Manager
TVA Watts Bar Project
Domestic Customer Projects

cc: W. L. Elliott, 1L
S. L. Robertson, 1L