[redacted]

WESTINGHOUSE CLASS 3 (Non-Proprietary)

[redacted]

Westinghouse Energy Systems

9311160344 931108
PDR ADOCK 05000390
A PDR

WCAP-13191
Revision 2.0

WESTINGHOUSE PROPRIETARY CLASS 3

WATTS BAR EAGLE 21

PROCESS PROTECTION SYSTEM

REPLACEMENT HARDWARE

VERIFICATION AND VALIDATION

FINAL REPORT

October 1992

Prepared by: _____
T. C. Tuite
Product Support Engineering

Reviewed by: _____
D. M. Rao
Chief Verifier, Product Support Engineering

Approved by: _____
S. J. Breznican
Manager, Product Support Engineering

Westinghouse Electric Corporation
Process Control Division
200 Beta Drive
Pittsburgh, Pennsylvania 15238

(C) 1992 WESTINGHOUSE ELECTRIC CORPORATION
ALL RIGHTS RESERVED

ABSTRACT

This report documents the implementation of the Eagle 21, Replacement Hardware Design, Verification and Validation Plan (DS 408A47, R3), as applied to Tennessee Valley Authority Station.

The report summarizes the Verification and Validation program results which demonstrate that the Watts Bar Eagle 21 Process Protection Upgrade System enhancements have been satisfactorily completed in accordance with all of its functional and design requirements.

Record of Changes

REV/ DATE	DESCRIPTION OF CHANGE	APPROVALS
- /APRIL1992	Initial Issue	
1.0 /15JUL1992	Removed references to Unit 2, made minor corrections and re-issued.	
2.0 /09OCT1992	Revised Figure 3-1 to show only the V&V processes and renamed it to Section 3.3. Incorporated a break down of all items identified in the problem reports.	

TABLE OF CONTENTS

SECTION	TITLE	PAGE
1.0	SUMMARY	1-1
2.0	EAGLE 21 SYSTEM FUNCTION OVERVIEW	2-1
3.0	VERIFICATION AND VALIDATION PROCESS PHILOSOPHY	3-1
4.0	SUMMARY OF VERIFICATION AND VALIDATION ACTIVITIES	4-1

LIST OF FIGURES

FIGURE		PAGE
4-1	Verification Problem Reports	4-3
4-2	Verification Problem Reports Analysis	4-4
4-3	Software Configuration	4-5 & 4-6

1.0 SUMMARY

Tennessee Valley Authority has purchased and will install a microprocessor based system to replace 10 racks of the analog process protection system and 4 racks of the digital process protection system at Watts Bar Unit 1.

The Microprocessor based equipment is the Eagle 21 Process Protection System Replacement Hardware. This equipment performs the following major functions:

1. Reactor Trip Protection (Channel Trip to Voting Logic);
2. Engineered Safeguard Features (ESF) Actuations;
3. Isolated Outputs to Control Systems, Control Panels, and Plant Computers;
4. Isolated Outputs to information displays for Post Accident Monitoring (PAM) indication; and,
5. Automatic Surveillance Testing to verify channel performance.

A brief description of the Eagle 21 System hardware architecture and related functions is given in Section 2.0.

A comprehensive Verification and Validation (V&V) program was conducted in accordance with Regulatory Guide 1.152 and ANSI/IEEE/ANS 7-4.3.2 to verify the functionality of the system to a level commensurate with that described in the system requirements. The Eagle 21 Replacement Hardware Design, Verification and Validation Plan is documented by Design Specification 408A47, Revision 3, dated May 12, 1989. A brief discussion of the V&V program is provided in section 3.0 of this report.

This report presents the results of the V&V program conducted on the Eagle 21 System Upgrade for Watts Bar Unit 1.

To see the results of the previous Verification and Validation projects, reference the following V&V final reports:

- WCAP 12588 — Sequoyah Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, April 1990 (Proprietary Class 3)
- WCAP 12588 Supplement 1 — Sequoyah Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, March 1991 (Proprietary Class 3)
- WCAP 12858 — Turkey Point Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, February 1991 (Proprietary Class 3)

- WCAP 12934 Diablo Canyon Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, April 1991 (Proprietary Class 3)

- WCAP 12889 Zion Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, February 1991 (Proprietary Class 3)

- WCAP 12889 Supplement 1 Zion Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, January 1992 (Proprietary Class 3)

- WCAP 12889 Supplement 2 Zion Eagle 21 Process Protection System Replacement Hardware Verification and Validation Final Report, May 1992 (Proprietary Class 3)

The software verification effort for the Watts Bar Unit 1 Eagle 21 System was completed in November 1991 with the total number of software units involved being 506. For these units, a total of 10 verification problem reports were generated. Verification problem reports generated have been resolved. Changes to the software documentation have been reviewed and/or tested to demonstrate successful resolution of the problems found.

It should be noted that the software verification was performed on generic type Eagle 21 software. This software includes possible Eagle 21 process algorithms, whether they are used in a particular installation or not. Therefore not all of the 1179 software units are actually ever executed in the Watts Bar Unit 1 system. However, as the totality of the software package includes this code, this report covers all findings in the software.

The system validation program for the Eagle 21 System was completed in April 1992, including 4 comprehensive tests and 239 hardware/software /FAT reviews. The hardware/software/FAT reviews and validation tests are complete. The Validation review generated 3 Validation reports. Validation problem reports which were generated are resolved. These reviews and tests are unlike the verification findings, in that they are all directly applicable to the Watts Bar Unit 1 upgrade. The validation was covered by the following; reviews of applicable prior testing such as tests from previous Validation efforts for the Eagle 21 systems, Watts Bar FAT's (Factory Acceptance Tests) and 4 additional Validation tests were conducted for evaluation of Validation concerns.

It should be noted that none of the anomalies identified in the validation problem reports are errors that would be expected to be identified during the verification process. All problem reports generated during the validation process are in areas specific to validation.

The Eagle 21 functional upgrade implemented for Watts Bar Unit 1 has been demonstrated to meet its functional and design requirements.

2.0 EAGLE 21 SYSTEM FUNCTION OVERVIEW

The Westinghouse Eagle 21 microprocessor based Process Protection Upgrade System applicable for those instrument systems which are "safety-related" as defined by IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations". The Eagle 21 portion of process instrumentation includes all necessary devices with the exception of transmitters, indicators, and recorders.

The Westinghouse Eagle 21 microprocessor-based process protection system is a functional replacement for existing analog process protection equipment used to monitor process parameters at nuclear generating stations and initiate actuation of the reactor trip and engineering safeguards systems. Features of the Eagle 21 equipment include the following:

A. Automatic surveillance testing to significantly reduce the time required to perform surveillance tests.

B. Self calibration to eliminate rack drift and time consuming calibration procedures.

C. Self diagnostics to reduce the time required for troubleshooting.

D. Significant expansion capability to easily accommodate functional upgrades and plant improvements.

E. Modular design to allow for a phased installation into existing process racks and use of existing field terminations.

The Eagle 21 System Hardware consists of three basic subsystems per rack: Loop Processor Subsystem, Tester Subsystem and Input/Output Subsystem.

1. Loop Processor Subsystem

   The Loop Processor Subsystem receives a subset of the process signals, performs one or more protection algorithms, and drives the required isolated outputs.

2. Tester Subsystem

   The Tester Subsystem serves as the focal point of the human interaction with the protection rack. When used in conjunction with the Man-Machine-Interface (MMI) test cart, the Tester Subsystem provides a user-friendly interface that permits test personnel to configure (adjust setpoints and tuning constants), test and maintain the system.

3. Input/Output (I/O) Subsystem

   The microprocessor based system interfaces with the field signals through various input/output (I/O) modules. These modules accommodate the plant signals and test inputs from the Tester Subsystem, which regularly monitors the integrity of the Loop Processor Subsystem.

In an Eagle 21 Process Protection Instrument Channel, field sensors are connected to cabinet mounted terminal blocks. The process electronics power the sensors and perform signal conditioning, calculation, and isolation operations on the input signals. However, each element of the process is not an individual electronic module or printed circuit board assembly. A multiple channel Analog Input module is used to power the field sensor(s) and perform signal conditioning. All calculations for the process channel functions are performed by a centralized Loop Calculation Processor (LCP). Typical functions performed by the Loop Calculation Processor are as follows: summation, lead/lag, multiplication, comparator, averaging, and square root conversion. Trip logic is provided through multiple channel Partial Trip Output modules. Multiple channel isolated analog outputs are provided by Analog Output modules. In addition, all Eagle 21 process protection channels are configured to perform automatic surveillance testing via a centralized Test Sequence Processor (TSP).

Protection and Monitoring channels processed with the Eagle 21 process protection system are as follows:

A. Steam Flow/Feed Flow Mismatch

B. Delta Temperature and Temperature Averaging

C. Turbine Impulse Chamber Pressure

D. Steam Pressure

E. Pressurizer Pressure

F. Containment Sump Level

G. Trip Time Delay

H. RCS Wide Range Pressure

I. Containment Pressure

J. Pressurizer Level

K. Narrow Range Steam Generator Level

L. Reactor Coolant Flow

M. Wide Range THot Temperature

N. Wide Range TCold Temperature

O. Pressurizer Vapor Temperature

P. Pressurizer Liquid Temperature

Q. RHR Pump Discharge

R. Boric Acid Tank Level

S. Wide Range Steam Generator Level

T. Refueling Water Storage Tank Level

U. Containment Spray Pump

The Eagle 21 equipment has been designed to fit into existing process racks and to interface with other plant systems in a manner identical to the existing analog equipment. This design maintains the existing field terminals to avoid new cable pulls or splices within the rack. The components for each rack are built into subassemblies which are easily installed into the existing racks. All internal rack cabling is prefabricated. The subassemblies are tested in a factory mock-up to verify proper fit and operation. Detailed installation procedures and drawings are provided with each system.

3.0 VERIFICATION AND VALIDATION PROCESS PHILOSOPHY

3.1 Verification Philosophy

With the application of programmable digital computer systems in safety systems of nuclear power generating stations, in order to ensure the functionality of software to a level commensurate with that described in the system requirements, designers are obligated to conduct independent reviews of the software associated with the computer system.

Section 3.3 specifies the independent verification and validation process. The verification process was divided into two distinct phases: verification of design documentation and verification of software. Section 3.3 identifies where an independent review of design documentation was performed. After completed software was turned over to the verifier by the design team, an independent review and/or test of each software unit was performed to verify the software unit met the associated Software Design Specification (SDS) and Software Design Requirement (SDR). As part of the software unit review, the unit was linked with other interfacing software units where appropriate. Structural testing was performed on the software units. This Structural testing exercised the software program code and its component logic structures. This process required the verifier to inspect the code against its associated documentation and understand how it functions before selecting the test inputs and predicting the test outputs consistent with code documentation. The test inputs were chosen to exercise all executable lines of code within the software entity.

3.2 Validation Philosophy

Whereas the system verification process was performed to verify the software entities, the system validation process was performed to demonstrate the system functionality. The system validation testing results demonstrated that the system design completely satisfied the system functional requirements. Hence, any inconsistencies that may have occurred during the system development in this area that were not discovered during the software verification activities were identified through the validation process. Validation compliments the verification process by ensuring that the system meets its functional requirements by conducting testing from a total systems perspective. The major phases of the validation process included the following:

A. Functional Requirements/Abnormal-Mode Testing Phase

B. Prudency Review and/or Testing of the Design and Implementation Phase.

The functional requirements/abnormal-mode testing process treated the system as a black box, while prudency review and/or testing required that the internal structure of the integrated software/hardware system be understood and analyzed in detail. This dual approach to the validation process provided a level of thoroughness and testing accuracy which ensured the functionality of the system commensurate with that described in the system requirements.

The Validation Plan defines the methodology utilized to perform a series of reviews and tests which compliment the verification process. Four independent types of reviews and/or tests were conducted to ensure overall system integrity:

1. Functional requirements based testing -- ensured that the final system satisfied the functional requirements. A functional decomposition was prepared from the system functional requirements and used as a basis for the validation test procedures. The functional requirements documents reviewed were

   a) Watts Bar, Revision 7, Document 3, "Functional Requirements for Thermal Overpower and Overtemperature Protection".

   b) Watts Bar, Revision 4, Document 4, "Functional Requirements for Reactor Coolant System Water Level Protection".

   c) Watts Bar, Revision 4, Document 5, "Functional Requirements for Reactor Coolant System Low Flow Protection System".

   d) Watts Bar, Revision 4, Document 6, "Functional Requirements for Safety Systems Actuated by Containment Pressure Signals".

   e) Watts Bar, Revision 4, Document 7, "Functional Requirements for Steam Generator Protection System".

   f) Watts Bar, Revision 4, Document 8, "Functional Requirements for Secondary High Energy Line Break Protection Systems".

   g) Watts Bar, Revision 4, Document 9, "Functional Requirements for Miscellaneous Protection System".

   h) Watts Bar Eagle 21 Supplemental Functional Requirements, Revision 0

2. Abnormal-mode testing -- ensured that the design operated properly under abnormal-mode conditions.

3. System Prudency Review/Testing -- ensured that good design practice was utilized in the design and implementation of critical design areas of the system. These tests required that the internals of the system design and implementation be analyzed in detail.

4. Configuration Data Review -- ensure the Eagle-21 System is configured with the appropriate Plant Specific Data.

3.3 Independent Verification & Validation Process

Validation of the Eagle-21 System Design

INPUTS:
- Functional Requirements and Functional Decompositions are used as the bases for the Validation Process

PROCESS:
- Validate that the System Design completely satisfies the System Functional Requirements.

OUTPUTS:
- System Design Matrix Document which provides traceability from the Functional Requirements through the supporting System Design Specification, Software Design Requirements, and the Actual Software Code.
- All findings, if any, are transmitted to design in the form of Problem Reports. Formal resolution by Design Team is documented.
- Verification and Validation Final Report

Verification of the Eagle-21 Configuration Data

INPUTS:
- Functional Requirements, Block Diagrams, I/O Board Location Drawings, and the Configuration Specification are all used to verify the Eagle-21 Plant Specific Configuration Files.

PROCESS:
- The Configuration Data Verification is broken up into two processes, Inspection and Testing:
  * The Inspection Process is made up of the following reviews:
    - Functional Requirements Versus Configuration Documentation.
    - Block Diagrams and I/O Board Location Drawings versus Configuration Documentation.
    - Configuration Documentation versus Configuration Files.
  * The Testing Process is made up the following:
    - Input/Output testing of the Eagle-21 System using plant specific configuration data. This testing is accomplished during the Validation Testing phase and Factory Acceptance Testing phase.
    - System on-line review to verify proper configuration of the Eagle-21 System. For example, confirming certain tuning constants by accessing the Tuning Constant Information on the MMI Screen.

OUTPUTS:
- Documented results of the Configuration review activities.
- All findings, if any, are transmitted to design in the form of Problem Reports. Formal resolution by Design Team is documented.
- Verification and Validation Final Report

Verification of the Eagle-21 System Design Documentation

INPUTS:
- Functional Requirements and Generic Eagle-21 Design Requirements are the Bases for this review.

PROCESS:
- Verified the System Design Specification against the System Design Requirements and the Functional Requirements for specific Eagle-21 Process Protection Requirements.

OUTPUTS:
- Signed off document identifying formal concurrence. Records of comments and their resolutions.
- System Design Matrix Document which provides traceability from the Functional Requirements through the supporting System Design Specification, Software Design Requirements, and the Actual Software Code.

Verification of the Eagle-21 Software Design

INPUTS:
- Software Design Requirement (SDR), Software Design Specification (SDS), the Eagle-21 Software Coding Standards and the Source Code makeup the verification package.

Note: Verification may find it necessary to refer to higher level documentation when testing certain Eagle-21 design elements.

PROCESS:
- The Verification of the Eagle Software is broken up into two processes, Review and Testing:
  * The Review Process is made up of the following:
    - Is the Source Code in compliance with the Eagle-21 Coding Standards.
    - Verify the Source Code against it's reference documentation SDS and the SDR.
  * The Testing Process is made up of the following:
    - After the verifier has reviewed the code against its associated documentation and has gained a functional understanding of the source code, test cases can be generated by selecting test inputs and predicting the test outputs.

OUTPUTS:
- Documented results of the verification activities.
- All findings, if any, are transmitted to design in the form of Problem Reports. Formal resolution by Design Team is documented.
- Verification and Validation Final Report

4.0 SUMMARY OF VERIFICATION AND VALIDATION ACTIVITIES

The verification process was performed in accordance with the Eagle 21 Replacement Hardware Design, Verification and Validation Plan. Eagle 21 system software was verified using Level 1 (safety related) type of testing and review. The overall scope of the verification effort on the Eagle 21 System consisted of 1179 units of software whose configuration is documented in Figure 4-3.

The validation process was performed in accordance with the Eagle 21 Replacement Hardware Design, Verification and Validation Plan, by a team of individuals independent from the design team. The overall scope of the validation effort on the Eagle 21 System consisted of performing 4 comprehensive tests and 239 hardware/software/FAT reviews.

The verification and validation efforts were focused mainly on new, modified, and impacted code. Credit was taken for previously verified and validated code.

Related software units were grouped together into software modules. Each software module consisted of a single source code file. When any anomaly was discovered during the source code review or during testing, a verification problem report was issued from the verification team to the design team for resolution. These problem reports consisted of three types, depending upon the scope of the discovered anomaly: 1) unit level problem reports; 2) module level problem reports; and, 3) generic problem reports. The unit level problem reports addressed anomalies specific to a single unit of code. The module level problem reports addressed anomalies covering entire modules (typically due to formatting standards concerns). Generic problem reports covered issues which spanned multiple modules (again typically due to formatting standards concerns). When any validation test result failed the applicable acceptance criteria, a problem report was issued from the validation team to the design group for resolution. It should be noted that the validation problem reports were in areas specific to validation. None of the errors precipitating a validation problem report were of a type that should have been found during the verification process. A total of 13 problem reports were generated consisting of 6 unit level problem reports, 2 module level reports, 2 generic level reports, and 3 validation level report. Verification and validation problem reports were satisfactorily resolved.

For the 13 problem reports generated during the Verification and Validation activities, an itemized break down of what phase the items were addressed is as follows:

Verification of the Eagle-21 Software	- 64%
Configuration Data review of the Eagle-21 System	- 28%
Validation of the Eagle-21 System	- 8%

It should be noted that the vast majority of items reported were addressed in the Verification and Configuration Data Review Phases and only a few items were addressed during the Validation Phase.

The verification and validation problem reports were assigned error codes as the reports were generated. Working from a list of 12 possible error codes, error types were assigned to each problem report. A problem report may contain more than one error type.

All problem reports were made up of the following 6 error types:

A. Design Requirements not implemented (Type A)	7.8%
B. Design Requirements implemented incorrectly (Type B)	35.9%
C. Implementation includes items not in design requirements (Type C)	4.7%
D. Computation Defects (Type D)	7.8%
E. Logic Defects (Type E)	1.6%
F. Header/ Comment Defects (Type J)	42.2%

Note that a single problem report may be counted several times in the above percentages as it may have multiple categories.

A categorized breakdown of software verification/validation problem reports is provided in Figure 4-1.

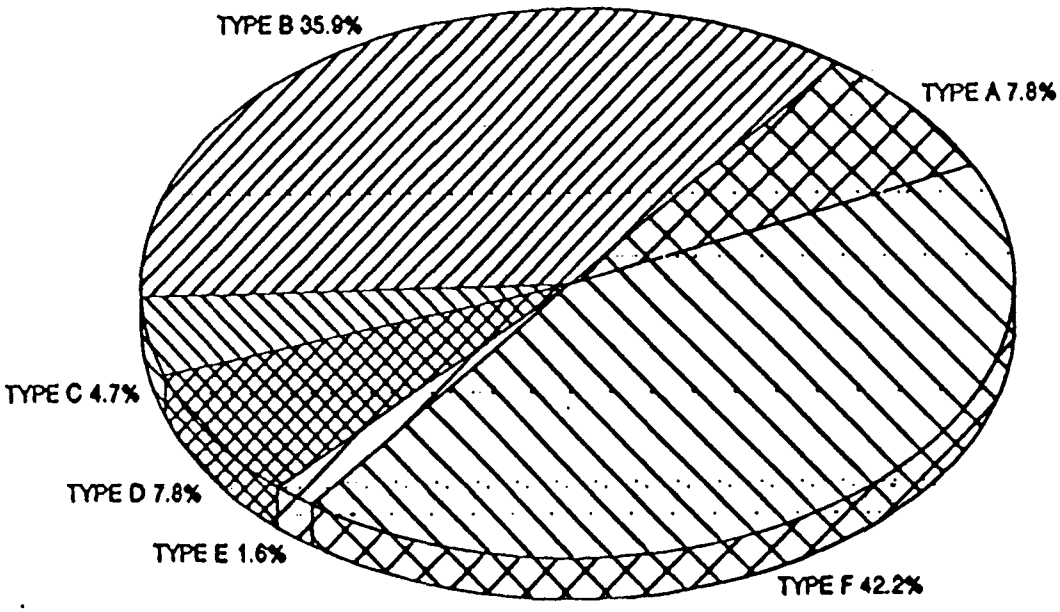
An Analysis of the verification and validation problem reports was done to determine the results of the action taken by the design team to resolve the reports. Working from a list of 5 possible resolutions, code types were assigned to problem reports. A problem report may contain more than one code item type.

EC- Designer Revised Code due to item reported.	28.1%
ED- Designer Revised Design Documentation due to item, contents of code not changed.	54.7%
CL- Verifier asked for clarification on item, designer replied.	0%
CS- Designer changed code due to comment on programming style or coding standard violation.	1.6%
NA- No action taken, design provided clarification and verification concurred.	15.6%

Note that a single problem report may be counted several times in the above percentages as it may have multiple categories.

A categorized breakdown of software verification/validation problem report Anaylsis is provided in Figure 4-2.

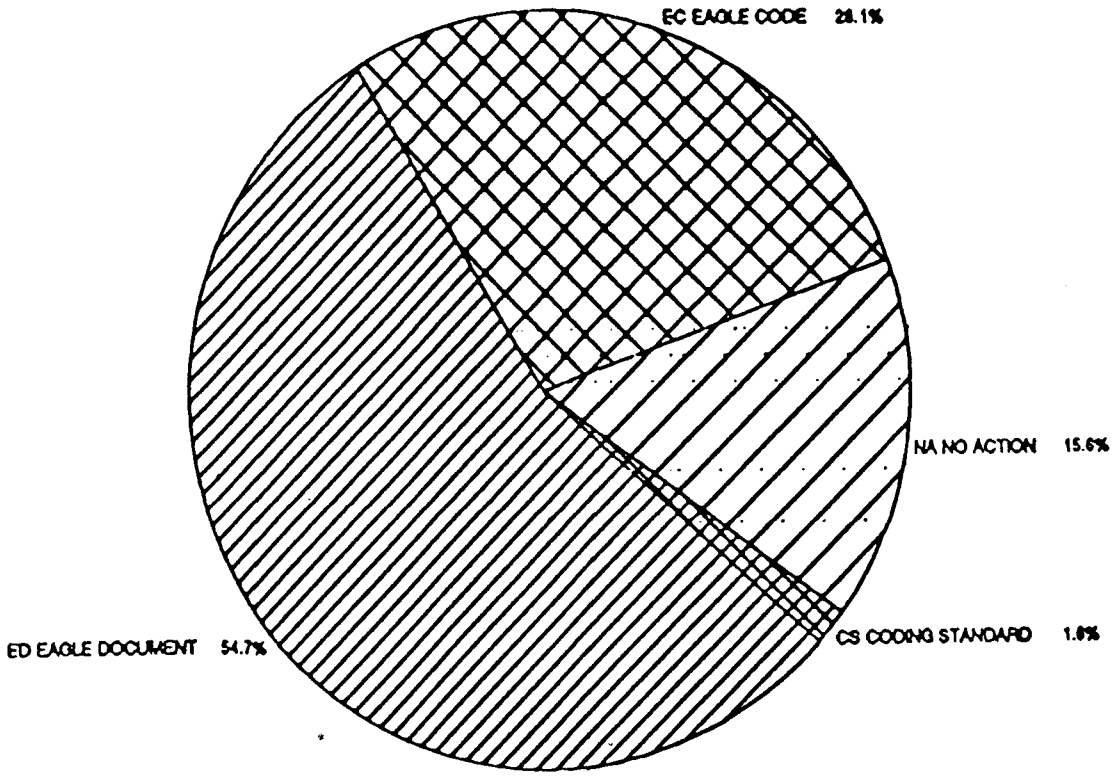
WATTS BAR UPGRADE EAGLE-21 VERIFICATION AND VALIDATION PROBLEM REPORTS



Note: Total of 13 problem reports consisting of 64 items. Configuration files were also part of the Verification and Validation effort.

Figure 4-1

WATTS BAR UPGRADE EAGLE-21 VERIFICATION AND VALIDATION PROBLEM REPORT ANALYSIS



EC - DESIGNER REVISED CODE DUE TO ITEM
ED - DESIGNER REVISED DESIGN DOCUMENTATION DUE TO ITEM, CONTENTS OF CODE NOT CHANGED
CL - VERIFIER ASKED FOR CLARIFICATION ON ITEM, DESIGNER REPLIED.
CS - DESIGNER CHANGED CODE DUE TO COMMENT ON PROGRAMMING STYLE OR CODING STANDARD VIOLATION.
NA - NO ACTION TAKEN, DESIGNER CLARIFIED AND VERIFICATION CONCURRED.

Note: Total of 13 problem reports consisting of 64 items. Configuration files were also part of the Verification and Validation effort.

Figure 4-2

SOFTWARE CONFIGURATION
(Continued on next page)

Firmware Part #	Drawing Rev.	Description	Software Version - Revision
3D22128G01	4	Watts Bar Unit 1 Rack 1 LCP Firmware Configuration	V01 - 01
3D22128G02	4	Watts Bar Unit 1 Rack 2 LCP Firmware Configuration	V01 - 02
3D22128G03	4	Watts Bar Unit 1 Rack 3 LCP Firmware Configuration	V01 - 01
3D22128G04	4	Watts Bar Unit 1 Rack 4 LCP Firmware Configuration	V01 - 01
3D22128G05	4	Watts Bar Unit 1 Rack 5 LCP Firmware Configuration	V01 - 01
3D22128G06	4	Watts Bar Unit 1 Rack 6 LCP Firmware Configuration	V01 - 02
3D22128G07	4	Watts Bar Unit 1 Rack 7 LCP Firmware Configuration	V01 - 01
3D22128G08	4	Watts Bar Unit 1 Rack 8 LCP Firmware Configuration	V01 - 01
3D22128G09	4	Watts Bar Unit 1 Rack 9 LCP Firmware Configuration	V01 - 01
3D22128G10	4	Watts Bar Unit 1 Rack 10 LCP Firmware Configuration	V01 - 02
3D22128G11	4	Watts Bar Unit 1 Rack 11 LCP Firmware Configuration	V01 - 01

Figure 4-3

SOFTWARE CONFIGURATION
(Continued from previous Page)

3D22128G12	4	Watts Bar Unit 1 Rack 12 LCP Firmware Configuration	V01 - 01
3D22128G13	4	Watts Bar Unit 1 Rack 13 LCP Firmware Configuration	V01 - 02
3D22128G14	4	Watts Bar Unit 1 Rack 28 LCP Firmware Configuration	V01 - 01
8250C08G04	13	E21 STD TSP Firmware Configuration	V04 - 03
8250C07G01	3	E21 STD DFP Firmware Configuration	V01 - 01
8250C06G01	3	E21 STD DLH Firmware Configuration	V01 - 00
8250C05G04	8	E21 STD MMI Firmware Configuration	V04 - 01
8250C20	3	E21 STD Microcontroller Firmware Config.	V01 - 03 (G01) -FTP V01 - 02 (G02) -I/O

Figure 4-3 (continued)

WCAP-13869

ENCLOSURE

WCAP-13869
REVISION 1

FUNCTIONAL DIVERSITY ASSESSMENT FOR THE REACTOR PROTECTION SYSTEM/ENGINEERED SAFETY FEATURES ACTUATION SYSTEM AT WATTS BAR UNITS 1 AND 2