WCAP-12272

WATTS BAR
EAGLE 21
PROCESS PROTECTION SYSTEM
REPLACEMENT HARDWARE
VERIFICATION AND
VALIDATION REPORT

by

C. W. Vernon

and

J. R. Rindfuss

Approved by

D. G. Theriault
Manager, Software Reliability
April, 1989

ABSTRACT

This report documents the implementation of the Eagle 21, Replacement Hardware Design, Verification and Validation Plan for Watts Bar.

The report summarizes the results that demonstrate the Eagle 21 functional upgrade to be implemented for Watts Bar Unit 1 meets its functional and design requirements.

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SUMMARY

The Tennessee Valley Authority has purchased and will install a microprocessor based system to replace 4 racks of the 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.

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 ANSI/IEEE/ANS 7-4.3.2 to ensure 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. A brief discussion of the V&V program is provided in section 3.0 of this report.

This final report presents the results of the V&V program conducted on the Eagle 21 System.

The software verification for the Eagle 21 System was completed in February, 1989 with the total number of software units involved being 1180. [ ]^{a,c} All verification trouble reports generated were resolved. All changes to the documentation and code were reviewed and/or tested to demonstrate successful resolution of the problems found.

The system validation program for the Eagle 21 System, was also completed in February, 1989, including [ ]^{a,c} tests and [ ]^{a,c} hardware/software reviews. The hardware/software reviews and validation tests have been satisfactorily completed. All validation problem reports generated were successfully resolved.

It should be noted that none of the errors identified in the validation problem reports were 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 to be implemented for Watts Bar Unit 1 is demonstrated to meet its functional and design requirements.

2.0 EAGLE 21 SYSTEM FUNCTION OVERVIEW

The Eagle 21 System is a microprocessor based system which performs several safety related functions.

The Watts Bar Eagle 21 System performs the following functions:

1. Data acquisition and digital processing of primary coolant narrow range hot leg and cold leg temperature signals, pressurizer pressure signals, and upper and lower ion chamber neutron flux signals for:

    a. Transmission of channel trip signals to voting logic in the Reactor Trip Protection System/Engineered Safeguards Features Actuation System and

    b. Isolation of Class 1E signals for input to non-Class 1E display and control systems.

1.1 Hot Leg (T_{hot}) Temperature Averaging is used to calculate the narrow range hot leg RTD average temperature in each loop. Additionally, the three narrow range hot leg RTD signals per loop are subjected to a sensor quality check that automatically rejects any failed sensor and incorporates a bias to compensate for its loss. Should the sensor quality check detect more than one failed hot leg sensor per loop, a signal is output to an alarm and annunciator.

1.2 Cold Leg (T_{cold}) Temperature Averaging is used to calculate the narrow range cold leg RTD average temperature in each loop. Additionally, the two narrow range cold leg RTD's per loop are subject to a sensor quality check. Should both sensors fail the quality check, a signal is output to an alarm and annunciator.

1.3 Delta T, TAVG, Overtemperature Delta T Setpoint, and Thermal Overpower Delta T Setpoint per loop are calculated using the narrow range T_{hot} average per loop, narrow range T_{cold} average per loop, pressurizer pressure, and upper and lower ion chamber neutron flux (current) signals. These calculated values are then compared to a setpoint which can output a partial trip signal for the subject loop to the Reactor Protection System/Engineered Safeguards Features Actuation System.

2. Data acquisition for Post Accident Monitoring. This function implements qualified monitoring channels to comply with post accident monitoring equipment design and qualification criteria. This function also isolates Class 1E and associated signals for input to non-Class 1E display equipment.

3. Data acquisition and digital processing of primary coolant wide range pressure signals for transmission of RHR isolation valve autoclosure interlock signals.

The Eagle 21 System Hardware consists of three basic subsystems per cabinet: 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 appropriate channel trip (or partial engineered safeguards actuation) signals. It also drives the required isolated outputs.

2. Tester Subsystem

   The Tester Subsystem serves as the focal point of the human interaction with the channel set. It 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.

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.

Figure 3-1 illustrates the integration of the system verification and validation with the system design process. The verification process was divided into two distinct phases: verification of design documentation and verification of software. Figure 3-1 illustrates where an independent review and signoff 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 applicable Software Design Specifications. 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. Structural testing is intended to comprehensively exercise the software program code and its component logic structures. This process required the verifier to inspect the code against it associated documentation and understand how it functions before selecting the test inputs and predicting the test outputs that are consistent with its 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 is performed to verify the software entities, the system validation process is performed to demonstrate the system functionality. The system validation testing results demonstrate that the system design meets the system functional requirements. Hence, any inconsistencies that may have occurred during the system development in this area that would not be discovered during the software verification activities are identified through the validation process.

During the verification process each software entity within the system was thoroughly and individually reviewed and/or tested. 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 include the following:

a. Functional Requirements/Abnormal-Mode Testing Phase
b. Prudency Review and/or Testing of the Design and Implementation Phase
c. Specific Man-Machine (MMI) Testing Phase

The functional requirements/abnormal-mode testing process treats the system as a black box, while prudency review and/or testing requires that the internal structure of the integrated software/hardware system be understood and analyzed in detail. This dual approach to the validation process provides a level of thoroughness and testing accuracy which ensures 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 testing -- ensures that the final system meets the functional requirements. A comprehensive functional decomposition was conducted on system functional requirements from which the validation test requirements originated.

2. Abnormal-mode testing -- ensures that the design operates properly under abnormal-mode conditions.

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

4. Specific Man-Machine Interface testing -- ensures that the operator interface utilized to modify the systems data-base performs properly under normal-mode and abnormal-mode data entry sequences. This is an important area due to the impact on that portion of the system level information which can be modified via this interface.

4.0 SUMMARY OF VERIFICATION ACTIVITIES

The verification process was performed in accordance with the Eagle-21 Replacement Hardware Design, Verification and Validation Plan. All Eagle System software was verified using the Level 1 (safety related) type of testing and reviews. The overall scope of the verification effort on the Eagle 21 System consisted of evaluating 1180 units of software.

When any software unit failed the verification activity, a trouble report was issued from the verification team to the design group for resolution. [ ]^{a,c} All verification trouble reports were satisfactorily resolved.

In addition to trouble reports, clarification reports were issued when the verifier found something of a minor nature which was not significant enough to fail a unit. These were typically typographical or other minor documentation errors. Clarification reports also provide a mechanism for identifying to the designer something minor which occurred during testing. [ ]^{a,c} All clarification reports were satisfactorily resolved.

The verification trouble reports have been assigned an error code as each report was generated. Working from a list of [ ]^{a,c} possible error codes used to classify previous software efforts, [ ]^{a,c} error types were assigned to trouble reports. A trouble report may contain more than one error type. A significant portion of the total (67%) was made up of five error types. [

]^{a,c}

Based on Westinghouse and industry experience, these were expected to be the dominant error types.
[ ]^{a,c}

5.0 SUMMARY OF VALIDATION ACTIVITIES

The validation process was performed in accordance with the Eagle-21 Replacement Hardware Design, Verification and Validation Plan, by a team independent of the design team. The overall scope of the validation effort on the Eagle 21 System consisted of conducting [ ]^{a,c} tests and [ ]^{a,c} hardware/software reviews.

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. [ ]^{a,c}
All validation problem reports were satisfactorily resolved. It should be noted that none of the errors precipitating a validation problem report would have been found during the verification process. All problem reports were in areas specific to validation.

[

]^{a,c}

The validation and design teams identified five avenues for resolving the problem reports: software changes; hardware changes; functional requirement changes; validation test procedure changes; and no problem identified.
[

]^{a,c}

ENCLOSURE 6

Westinghouse Electric Corporation -
Application for Withholding Proprietary Information
from Public Disclosure