UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555



# SAFETY EVALUATION

# BY THE OFFICE OF NUCLEAR REACTOR REGULATION

# PLANT SAFETY MONITORING SYSTEM (PSMS)

# DUQUESNE LIGHT COMPANY

# BEAVER VALLEY POWER STATION UNIT 2 (BVPS-2)

# DOCKET NO. 50-412

## 1.0 INTRODUCTION

Revised License condition 2.C.(7) of the BVPS-2 license requires that an approved verification and validation (V&V) plan for the PSMS be implemented before startup after the second refueling outage. By letter dated November 25, 1987 the licensee submitted its proposed V&V plan. The staff reviewed the plan, evaluated the PSMS hardware and performed an audit (assisted by contractors) at the Beaver Valley site from January 31 to February 2, 1989. The purpose of this review and audit was to determine if the license condition had been met.

The licensee has installed and operated a PSMS as a part of its commitment to Regulatory Guide (RG) 1.97. The PSMS is a digital microprocessor-based system and is classified as a safety-related system because of the Category 1 requirements of RG 1.97. Both the hardware and software for this system were provided by Westinghouse. Conformance to RG 1.97 will be reviewed separately. This audit was limited to the hardware and software of the PSMS as it pertained to the license condition.

The PSMS monitors safety-significant variables such as core exit temperature, reactor coolant system pressure, and neutron flux. The system includes graphic plasma displays in the control room and provides data (via data links) to the emergency response facility computer and plant computer. No reactor trip, engineered safety feature, actuation or control functions are performed by the PSMS at BVP2.

## 2.0 Hardware And System Assessment

This portion of the review focused on the areas of potential vulnerability or susceptibility of the PSMS which might prevent its ability to provide accurate information to the operators when required. Issues investigated included single failure, environmental qualification, seismic qualification, surge withstand capability (SWC), electromagnetic compatibility (EMC), failure modes and effects, reliability, error detection, and independence.

During the audit, the licensee made an initial presentation covering the licensing, engineering, testing and training aspects of the PSMS. The presentation included summary block diagrams of the PSMS configuration, a listing of design documentation and a listing of the field design requests and change notices (hardware and software) involving the PSMS. Also included in this presentation was a specific point-by-point hardware comparison between the BVPS-2 PSMS and similar Vogtle and South Texas equipment which had been previously reviewed by the staff. This comparison showed that the hardware is virtually identical for the plants, with some comparatively minor exceptions. The BVPS-2 system is smaller with fewer inputs and fewer cabinets. The specific display format and key pad layout are different due to unique plant requirements.

BVPS-2 is covered by Westinghouse topical reports WCAP-8587 for environmental qualification and WCAP 11340 for noise, fault, surge and RFI testing. WCAP-11340 also addresses maximum credible fault voltage, maximum continuous fault current, maximum surge withstand capability, RFI compatibility for field strength at various frequencies, random noise, crosstalk, chattering relay sources, high voltage transient noise and military specification MIL N 19900 noise testing. No deleterious effects were observed during these vendor-performed tests and no design changes were required as a result of the testing. On the basis of the extensive testing by Westinghouse and the similarity to the previously approved Vogtle and South Texas equipment, the staff finds the hardware design to be acceptable for use in the BVPS-2 PSMS.

The next area reviewed involved the plant installation, testing and operational history.

## 2.1 Temperature And Humidity Environment

The PSMS is installed in the control room and instrumentation room areas of the plant and are therefore considered to be in a mild environment. High cabinet temperature alarms are provided in the control room. The staff has concluded, based on environmental testing performed and the mild environment location, that the PSMS should not be unduly susceptible to temperature and humidity effects.

## 2.2 Electromagnetic Interference (EMI) Environment

The control room and instrumentation room areas have been clearly posted to indicate that the use of radio communications in the area was prohibited. Due to problems with EMI from walkie-talkies at other facilities in the past, the staff considers the radio prohibition to be prudent. The staff reviewed the grounding and shielding configuration for the analog inputs to the PSMS, the found them acceptable.

Westinghouse had stipulated a functional requirement that peak-to-peak noise be limited to 0.5 percent of the output span for any noise occurring in a frequency range which could affect downstream modules or systems (exclusive of process noise). The licensee was unable to demonstrate that this functional requirement had been validated in the site acceptance tests (SAT). The staff requires that this requirement either be demonstrated by testing or shown not to be a valid requirement. The staff would consider the resolution to this item in a functional requirements conformance matrix (which the staff requires for software assessment in Section 3 of this safety evaluation) to be acceptable.

## 2.3 Power Supplies

The staff reviewed the normal and alternate power supplies to the PSMS. The licensee measured and recorded the inverter bus (PSMS normal supply) output voltage waveform to assure that the total harmonic distortion (THD) was less than 5 percent as required. The THD was found by the licensee to be within acceptable limits. Based on the vendor testing (WCAP-11340) and the successful THD test, the staff concludes that there is reasonable assurance that the PSMS as installed should exhibit sufficient surge-withstand capability .

## 2.4 Failure Modes And Effects

The PSMS does not perform any reactor protection, engineered safety feature actuation, or control functions. Additionally, FSAR section 7.4 takes no credit for using any of the PSMS data for alternate shutdown scenarios such as a design basis fire. FSAR section 7.5 describes the qualification and the parameters required for the safety-related instrumentation. The FSAR provides a listing of the RG 1.97 parameters and specifies which of them are provided on the plasma (PSMS) display.

Trouble alarms are provided for the PSMS, including on-screen indication and a watchdog timer which could indicate system stall. The licensee reported that no significant failures have been experienced for the PSMS since installation and operation over the past 18 months. The staff concludes that the failure modes and effects for the PSMS are acceptable.

## 2.5 Independence

The staff reviewed the data link interfaces between the PSMS and the Emergency Response Facility (ERF) and the plant computers. The non-1E computers receive data only and do not communicate (no requests or interrupts) to the PSMS, therefore software independence of the PSMS is maintained. The data links to the ERF computer are by means of fiber optic data links which preclude any electrical fault from the non-safety ERF from propagating to the Class-1E PSMS. The electrical isolation of the RS232 interface between the plant computer and the PSMS was previously reviewed and approved for Vogtle. The staff concluded that the data link interfaces provide the required independence for the PSMS.

## 2.6 Testing And Operating History

Extensive testing of the PSMS has been done by both the vendor and the licensee. The licensee and vendor identified 13 hardware and software modifications for the PSMS. The staff reviewed a sample of the modifications to assess the root cause and basis for the changes. In general, the changes appeared to result from typical system/plant interface problems such as synchronizing the data links and correcting impedance mismatch. In particular the staff reviewed the changes to determine if there were extensive problems that a formal verification and validation program may have prevented. The review did not detect extensive problems. During preparation of surveillance procedures, the licensee appeared to make a conscientious effort to develop engineering memos to resolve any

problem identified. The licensee reported that the system has had good acceptance by the operators, that specific training on the PSMS has been accomplished, and that the system has been unavailable for a total of one minute in 18 months of operation. The one downtime was required to make a minor planned hardware change (internal clock reset). Based on the testing and this operating history, the staff concluded that the PSMS has exhibited reliable operation to date.

One aspect of the testing was not acceptable to the staff. The licensee could not demonstrate that the factory acceptance testing (FAT) and/or the site acceptance testing (SAT) assured completeness of implementation and conformance to the PSMS functional requirements. An example noted in Section 2.2 above involved the functional requirement peak-to-peak noise limit which was not shown by the licensee to have been tested at either the factory or the site. A sample of other functional requirements was shown to have been included in the testing. To assure that all of the functional requirements have been included in the design, the staff requires, as a minimum, the preparation of a functional requirement conformance matrix which can demonstrate that each functional requirement was tested by the FAT, SAT or other testing.

## 3.0 SOFTWARE ASSESSMENT

Revised license condition 2.C.(7) requires that an approved V&V plan for the PSMS be implemented prior to startup following the second refueling outage. To determine the acceptability of the PSMS V&V plan, the NRC reviewed the V&V plan, examined the functional requirements, reviewed the use of independent software verifiers and reviewed the capability for V&V during maintenance of the software.

### 3.1 Criteria

The staff compared the PSMS V&V plan to Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems at Nuclear Power Plants," which endorses ANSI/IEEE 7.4.3.2 - 1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Station." Although the software used at South Texas, Vogtle and Beaver Valley are similar, no direct program-by-program comparison was made to demonstrate the extent of the similarity. The licensee and Westinghouse (software and hardware vendor) also stated that V&V was not part of the PSMS contract and therefore was not performed by the vendor.

### 3.2 V&V Plan

In a letter dated November 25, 1987, the licensee submitted its V&V plan for the PSMS. The staff concluded that the V&V plan did not identify the design and development methodologies and did not show how the V&V process interfaced with the design and development processes. The V&V plan did not identify the procedures for V&V or how those procedures were to be implemented. The V&V plan did not delineate sufficiently the reporting and review requirements that must be met during key stages or phases of the software development process.

The V&V plan did not provide for an independent verifier to execute the verification procedures. The responsibilities between the vendor, the licensee and the independent verifier were not clearly evident. It was not clear to the staff how the V&V plan was to be implemented as the software code was not a deliverable Part of the PSMS contract, and was therefore still in the vendor's sole possession. The conclusion of the staff after the review and audit is that the V&V plan is not acceptable as presented because it is missing the major elements that are necessary to carry out an effective V&V process.

3.3 Design Process

The overall design process was reviewed to determine if it began with a clearly stated set of functional requirements. The functional requirements (DMW-D-5648, September 15, 1986) were the result of a cooperative effort by the licensee, the vendor and the architect/engineer and represented the starting point for the development of the PSMS. The staff reviewed the design iteration of the tradeoffs between analog and digital logic, hardware and software implementation and the inclusion of hybrid devices.

The linkage between the functional requirements for the PSMS and the final product was ambiguous. The licensee was not able to demonstrate to the staff's satisfaction that all of the functional requirements had been included in the final product and unwanted functions had been excluded. There was no evidence of how the software and hardware specifications were developed. There was no evidence of the design process from the software specification to the software architecture, the module definitions, the interfaces, and the resultant software code. The vendor stated that it followed its standard design process and, unless requested to do so by the customer, it would not perform the additional documentation required for a formal V&V plan. The licensee stated that the design process was done entirely by the vendor and the licensee was not involved in specific code development.

The staff concluded that the design process has not been shown to have included all of the relevant requirements. One method which has been acceptable to the staff for other applications is the functional requirements matrix. The matrix identifies each functional requirement as a line item and correlates it to a specific test which demonstrates that the requirement has been satisfied.

3.4 Testing

The staff reviewed the FAT and the SAT. The staff reviewed the test procedures, discrepancy and trouble reports, signoffs and independence of the testers. The testing for the PSMS appeared to be extensive and thorough. The staff could not clearly determine whether all the requirements have been tested because there was no verification of the test plan. The vendor FAT was extensive and used a test jig to simulate the external senor inputs to the PSMS. The test procedures for the FAT were written by a separate group that was not involved in the software development. The staff noted that this provides some level of independence in the process.

The SAT was performed by the licensee startup personnel at the plant. The basis of the SAT was a functional test specification that had been developed by the architect/engineer (AE). There was no correlation demonstrated between the test specification, The SAT and the original functional requirements. In addition to exercising the software, the SAT also covered the installation of the sensors and other hardware.

3.5 Implementation Process

As software implementation started to come together as integrated modules were developed, verification can be performed on parts of the system. The verifier should trace the development of the code to the previous level of specification and determine whether the coder has interpreted and implemented the specification correctly. Discrepancies should be described in trouble reports and reflect the progress of the code development. The implementation of the PSMS was done using the vendor's standard practices.

Most of the design notes on the PSMS were informal and there was no independent verification of the steps as the coding progressed, therefore trouble reports and verification reports were not available. The staff reviewed the Remote Processing Unit (RPU) with one of the RPU implementers to gain an understanding of the development process. In general, the code was well modularized, with adequate comments and documentation. Each module had a preamble which documented the change history for that module. All numbers and key parameters were in well organized tables that could be examined easily by a reviewer. The code reflected a commendable level of design discipline and procedure such that, even though the design derivation and implementation was informally controlled and documented, formal V&V procedures could be effectively applied.

The vendor has a software development methodology that represents good engineering practice. The basis of its software development environment is the Code Maintenance System from Digital Equipment Corporation. This system provides a variety of software engineering tools and procedures that facilitate the development of code, documentation, tracking of changes between versions, testing and configuration management. There was no evidence of verification activities in conjunction with this development methodology.

3.6 Configuration Management (CM)

Installed software must be maintained. V&V procedures must continue to be in force because maintenance (upgrades and other modifications) includes at least the same possibilities for errors that initial coding does. The basis for CM is the baseline, which is the configuration of the current software in terms of the various modules and their current versions. CM must also include a methodology by which trouble reports are translated into new or modified requirements which are then implemented as modifications to the original code. Important elements of this methodology to track baseline changes includes the initiation of change request, change review, development change notice/specification, change approvals, list of changes made and PROM testing.

The staff considers that the importance of V&V grows as the software ages and undergoes numerous revisions. Each modification has the potential to undermine the design integrity of the software and can lead to unanticipated effects in other parts of the code. Verification of each change ensures that the design basis has not been violated and provides further assurances that the resultant software is reliable.

The staff reviewed the change development processes of both the licensee and the vendor. Although somewhat complex, the staff concluded it was adequate. The key deficiency noted by the staff was the difficulty in associating the changes with the functional requirements and the trouble report that initiated the changes. The lack of independent verification for changes was noted, although the process seems to provide sufficient opportunities for V&V insertions.

## 4.0 CONCLUSIONS

The hardware design of the PSMS was found acceptable by the staff. In addition to the review and audit for the Beaver Valley PSMS the staff had previously reviewed and accepted similar hardware at the South Texas and Vogtle plants. Due to the staff's reliance, in part, on the similarity to previous equipment, the staff requires that the licensee formally submit a copy of the comparison of the Beaver Valley PSMS and previous PSMS installations at other facilities. The staff has reviewed an informal copy of the similarity comparison during the audit and found it acceptable.

Regarding the system and software design, the V&V plan submitted by the licensee was found incomplete and therefore unacceptable. The software design process was not adequately documented, and it was not possible to trace the functional requirements to the end product. The design and implementation of the software followed the vendor's standard practices, but with only informal documentation. Although the PSMS code appeared to be well structured and modular, no formal verification was provided. There was no evidence that the FAT/SAT testing demonstrated completeness of implementation and conformance to the PSMS functional requirements.

To fulfill the license condition, the licensee should, as a minimum and in addition to the above similarity documentation, develop a functional requirements matrix. This matrix must be completed prior to restart from the second refueling outage, as stated in the revised licensee condition 2.C(7). An acceptable matrix should provide a listing of each applicable requirement and a corresponding line-by-line listing of the specific test or review which the licensee believes demonstrates that the requirement has been met. Any testing which has been completed or will be completed prior to restart may be used including FAT, SAT, other Beaver Valley tests (calibrations, specific testing of similar equipment at other facilities) and topical reports.

Finally, the licensee should implement an ongoing V&V program for the PSMS software for future modifications in accordance with ANSI/IEEE 7-4.3.2.

Principal Contributor: Jim Stewart, with contractual assistance provided by Jim Leivo and Ray Ets.

Dated: May 10, 1989