HOPE CREEK SAFETY PARAMETER DISPLAY SYSTEM

VERIFICATION AND VALIDATION PROGRAM PLAN

Document: NOV-1000-87-003
(formerly PSE-1210-01)

Revision 3

December 2, 1987

Prepared For:

Hope Creek Generating Station
Public Service Electric and Gas Company
80 Park Plaza
Newark, New Jersey 07101

Prepared By:

Eigen Engineering, Inc.
3150 Almaden Expressway
San Jose, CA 95118

INTRODUCTION

Revision 2 to the HCGS SPDS V&V Plan was issued on October 1, 1985 as a result of the audit findings during the NRC audit of August 27 and 28, 1985. The Eigen Engineering document number was PSE-1210-01.

Subsequent to the NRC audit, PSE&G decided to install a separate SPDS at HCGS and transfer the SPDS functions from the existing CRIDS to the new system.

This document (Revision 3) has been prepared to ensure that the V&V program remains adequate based on the new hardware configuration. In addition, the Eigen Engineering document number has been changed to NOV-1000-87-003.

TABLE OF CONTENTS

HOPE CREEK SAFETY PARAMETER DISPLAY SYSTEM
VERIFICATION AND VALIDATION PROGRAM PLAN

I. OBJECTIVES

The Safety Parameter Display System (SPDS) is one of the elements of the emergency response facilities called for in NUREG 0660 (Reference [1]) and clarified in Supplement 1 to NUREG 0737 (Reference [2]). The Hope Creek SPDS Verification and Validation (V&V) program has been developed in accordance with NSAC-39 (Reference [3]), to ensure that the SPDS is acceptable and meets applicable requirements of NUREG 0737, Supplement 1.

Specifically, the program will provide a basis for ensuring the following:

A. The variables displayed on the SPDS are sufficient to provide the minimum information required to assess the critical safety functions.

B. The SPDS is suitably isolated from electrical and electronic interference with equipment and sensors that are used in safety systems.

C. Means are provided to ensure that the data displayed are valid.

D. Characteristics of the SPDS displays and other operational interfaces are sufficient to allow reasonable assurance that the information provided will be readily perceived and comprehended by the Hope Creek Operations Staff.

Radiation data in the SPDS is supplied by a separate Radiation Monitoring System (RMS). The RMS collects the data, performs engineering unit conversion and supplies the data to the SPDS. Range checking and failed data determination functions performed by SPDS will be verified during testing.

II. METHODOLOGY

The SPDS V&V program will be performed in the following five parts:

A. System Requirements Review

The requirements review will consist of the development of a matrix to identify and track applicable SPDS requirements throughout the validation program. The requirement list will be a compilation of applicable Hope Creek design requirements in addition to any requirements obtained from a search of applicable regulatory and industry standard documents.

B. Design Review

The design review will document in a traceable manner that the identified design requirements are implemented in an unambiguous and consistent manner.

Test results documentation (ie. hardware supplier and site acceptance tests) shall be reviewed to assure that applicable performance characteristics have been demonstrated. Additional tests will be performed as part of the performance validation or field verification testing for performance characteristics not previously demonstrated.

Any deficiencies identified during the design review will be documented along with their resolutions.

C. Performance Validation Test

The performance tests will consist of a series of static and dynamic tests performed at the SPDS vendor facility and/or the HCGS simulator to determine the effectiveness of the SPDS.

D. Field Verification Test

The field tests will be performed on the installed equipment and are intended to verify that the installed system is in accordance with that previously validated.

E. Final Report

A final report will be prepared to provide documentation of the conclusions of the above efforts and to provide traceability for future reference. Included within the report will be any observed deficiencies and associated resolutions.

III. SYSTEM REQUIREMENTS REVIEW

The system requirements are the foundation on which the completed system is designed, built, and accepted. Consistent with the intent of NSAC 39, the requirements review shall include hardware, software, performance, and effectiveness evaluations.

During the SPDS system requirements review a literature search of regulatory documents will be conducted for applicable requirements which are considered to be relevant to the SPDS to assure that the system is adequate to support the safe operations of the plant.

From the following minimum set of documents a list of requirements will be compiled and cross referenced to show which document each requirement was derived from.

1. NUREG 0800, Section 18.2 (Reference [4])
2. NUREG 0737, Supplement 1 (Reference [2])
3. NSAC 39, (Reference [3])

This list will then be incorporated into a design characteristics versus requirements matrix, as described in NSAC 39, to be used during the Design Review phase of this program.

The following topics shown in NSAC 39, Section 2 and expanded by NUREG 0800 will be addressed as a minimum.

A. Completeness and correctness in specifying the performance requirements and operational capabilities and concepts of the system relative to Emergency Operating Procedures (EOP).

1. Display format and content.

(a) Assure that critical plant variables for the SPDS are presented on a single primary display or on a group of displays at a single location.

(b) The display should be responsive to transient and accident sequences including scenarios which assume plant conditions beyond the design basis conditions, such as (i) Primary containment pressure at emergency venting level, (ii) Reactor water level below top of active fuel, and (iii) Reactor building radiation at the reactivity release alert level.

(c) The display should be capable of presenting magnitudes and trends of critical plant variables or derived variables.

(d) The system will continuously display information from which the plant safety status can readily and reliably be assessed by the control room personnel.

(e) SPDS users are made aware of important changes in critical safety-related variables when they occur and that the SPDS users can readily obtain information from SPDS to help them determine the safety status of the plant.

(f) The minimum information to be provided shall be sufficient to provide information to control room operators about (i) reactivity control, (ii) reactor core cooling and heat removal from the primary system, (iii) reactor coolant system integrity, (iv) radioactivity control, and (v) containment conditions.

(g) For each mode of operation, the displays contain the minimum set of indicators and data

needed to assess the plant functions that are used to determine the plant's safety status.

(h) There should be provisions in the display to indicate to the control room operator that a change in the mode of plant operation has occurred.

2. Sensor scan intervals.

(a) The sampling rate for each critical plant variable is such that there is no meaningful loss of information in the data presented to the control room operator.

(b) The time delay from when the sensor signal is sampled to when it is displayed should be consistent with other control room displays and should be responsive to control room operators needs in performing assigned tasks.

(c) Each critical plant variable is displayed with an accuracy sufficient for the control room operator to discriminate between conditions that impact the plant's safety status and normal operating conditions.

(d) The display does not give false indications of plant status.

3. Scale optimization.

Scales for displayed variables allow tracking of variables over a wide range of conditions. The conditions include normal plant modes of operation such as startup, shutdown, and power operation; and abnormal conditions up to and including design limits. These displays may also provide a means of reading values should any variable go off scale during abnormal conditions.

4. Data Validity.

Displayed data is validated on a "real time" basis where practical and redundant sensor readings, where available, are compared before displaying the critical plant variable.

5. SPDS Failure.

Members of the control room operating crew are provided with the information and criteria they need to perform an operability evaluation of the SPDS. In addition, the crew must be able to easily recognize a failed SPDS.

B. Completeness and correctness in system definition and interfaces with other equipment.

SPDS is suitably isolated from electrical or electronic interference with equipment and sensors that are in use for the safety systems.

C. Unambiguous, correct and consistent description of the interfaces and performance characteristics of each major function.

Major SPDS interfaces and performance characteristics (hardware and software) are adequately documented to provide a basis for evaluating the acceptability of future system alterations/modifications.

D. Establishment of a reasonable and achievable set of test requirements.

The Hope Creek SPDS V&V Program shall include the development of acceptance criteria (see Sections IV & V of this plan).

E. Definition of physical characteristics, reliability, and maintainability objectives, operating environment, transportability constraints, and design and

construction standards, including those intended for software.

1. SPDS Location.

   (a) Assure that the SPDS is convenient to the control room operating crew;

   (b) The SPDS is readily distinguished from other displays on the control board;

   (c) The display is readily accessible to the following personnel, but not necessarily simultaneously:

       Shift Supervisor
       Control Room Senior Reactor Operator
       Shift Technical Advisor
       One Reactor Operator

   (d) The control room operating crew, not personnel outside the control room, control images displayed on the control room SPDS.

2. The SPDS reliability analysis shall be reviewed for consistency with the overall requirements objectives defined herein. Included will be the review of any maintainability (ie. repair) assumptions incorporated within that analysis.

F. Definition of the necessary logistics, personnel, and training requirements and considerations.

1. Since operators must be trained to evaluate plant status in response to accident conditions both with and without SPDS, this assumption shall be factored into the "effectiveness" acceptance criteria for the simulator performance test (see Section V of this plan).

2. Procedures and Training.

   (a) Assure that operating procedures and training are provided to the control room operating crew that will allow timely and correct safety status assessment when the SPDS is not operating.

(b) No additional operating staff other than the normal control room operating crew should be needed to operate the SPDS display during normal and abnormal plant operation.

(c) The control room operators training program contains instruction and training in the use of the SPDS in conjunction with operating procedures for normal, abnormal, and emergency operating conditions.

G. Definition of input and output signals, and establishment and management of the database.

1. Critical plant variables.

(a) Assure that the predetermined set of critical plant variables will aid control room operators in rapidly and reliably determining the safety status of the plant.

(b) The variables associated with each critical safety function should also be available for display and operator assessment.

H. Treatment of man/machine interface requirements.

Assure that the SPDS display incorporates accepted human factors engineering principles so that the displayed information can be readily perceived and comprehended by SPDS users.

I. Definition of subsystems and integration requirements.

Subsystem integration characteristics will be validated during the performance test as they are intrinsic to system operation (see Section IV of this plan).

J. Definition of installation, operation, and maintenance requirements.

1. Operation characteristics will be verified during the performance test as they are intrinsic to system operation.

2. Installation Audit.

   Assure that the data displayed reflects the sensor signal which measures the variable displayed.

3. Vendor equipment documentation shall be reviewed to verify implementation of recommended periodic maintenance guidelines in plant procedures.

IV. DESIGN REVIEW

The objective of a design review activity is to ascertain in a planned, controlled, and documented manner that the implementation of system requirements into hardware and software is complete, and there are no ambiguities or deficiencies.

During the design review, a literature search of system documentation which describes the Hope Creek SPDS will be conducted in order to complete the compliance section of the requirements matrix which was developed during the systems requirements review. This includes a review of vendor and site test programs to ensure that appropriate performance characteristics are demonstrated.

Any deficiencies identified during the design review will be documented along with their resolutions and will be included in the final report.

A "walk-through" of the SPDS will also be conducted to supplement the documentation being reviewed.

The design review of the Hope Creek SPDS will be approached in four parts.

A. The first part of the SPDS verification task shall consist of an analytical review of the existing documentation for a random selection of safety-related sensors which require Class 1E isolation between the sensor output and its SPDS input to assure that the required isolation has been included in the system design. The same sensors selected for documentation review will also be included in the "walk-through" of the installed system to assure consistency between the design and installation.

B. The second part of the review shall be an evaluation of the display descriptions, SPDS hardware descriptions, and vendor/site acceptance test reports. This review will address requirements such as:

1. Available Data
   (a) display feature development descriptions
   (b) display functional descriptions
   (c) selection of critical plant variables

2. Data Manipulations
   (a) sensor throughput intervals
   (b) display update timing intervals
   (c) engineering unit conversions

3. Data Validation

   (a) validation and algorithms

   (b) display of invalid data

4. Acceptance Testing

   (a) acceptable results demonstrated

   (b) results applicable to the installed system

A design "walk-through" will be conducted to supplement the review of design documentation. This review will compare actual display format and content with that described in the display description documentation. Any deficiencies identified will be documented along with their resolutions.

C. The third part of the review shall consist of reviewing the SPDS "Human Engineering Discrepancy Reports" resulting from the Control Room Design Review to assure that all applicable discrepancies are resolved and incorporated into the displays as necessary. This will ensure that items such as operator physical capability considerations, system compatibility with human input/output abilities and limitations, along with a review of the display formats, color selections and operator comprehension of display content, were considered.

D. The fourth part consisting of a system performance assessment will be included in the performance validation test defined in Section V of this plan. The scope of the performance validation test will be expanded as necessary to include the demonstration of those appropriate characteristics not documented in Item IV.B.4 above. The remaining items will be addressed during the Field Verification test described in Section VI.

V. PERFORMANCE VALIDATION TEST

A. Validation Philosophy

The principal function of the SPDS is to aid the operator in determining the plant safety status. More precisely, the design objectives of the Hope Creek SPDS are defined in Section I of this Plan. The purpose of the system validation phase of the V&V program is to confirm that the system, as implemented, adequately meets these objectives.

Objectives A and C will be validated via static factory testing. This testing, together with the supporting information derived during the Design Review Phase will ensure that all system features intended to address these objectives perform as intended. Objective B will be verified during the preoperational testing phase.

Objective D deals with how well the integrated system performs its principal function; to aid the operator in determining the plant safety status. The issues in evaluating the degree to which the operator is aided, and the system objectives are met are;

Compatibility -

The nature of the SPDS presentations to the operator and the response expected from the operator should be compatible with human input/output abilities and limitations.

Understandability -

The structure, format, and content of the operator/SPDS dialogue should result in a meaningful communication.

Effectiveness -

The SPDS should support the operator in a manner which leads to improved performance, or results in a difficult task being less difficult, or enables accomplishing a task that could not otherwise be accomplished.

The primary focus of the dynamic validation tests shall be to demonstrate SPDS "effectiveness". It is recognized that "compatibility" and "understandability" are necessary to achieve "effectiveness". Assurance that the SPDS displays can be readily perceived and comprehended by the plant operators (see Objective D Section I of this plan) is an "effectiveness" goal. If sufficient assurance is demonstrated that the system is

"effective", then the system will also have been demonstrated to be "compatible" and "understandable". To establish reasonable assurance that the system is "effective", a series of dynamic tests using time dependent data via the plant simulator will be performed.

B. Acceptance Criteria

To assist in determining the functionality aspect of the static testing, acceptance criteria shall be developed from results of the requirements review. The static test acceptance criteria shall include the following minimum set of items, depending on the applicability of each item to the specific design.

1. Alarm and status changes occur as defined,
2. Range checking occurs as defined,
3. Data validation occurs as defined,
4. Analog input is within prescribed accuracy and appropriate engineering units assigned,
5. Sensor input failure detection,
6. Hardware failover occurs as designed,
7. Storage deadband and data throughput are within prescribed limits,
8. Screen update times are within prescribed limits.

The explicit goals of the dynamic performance test that shall be addressed relative to effectiveness are whether or not the operator can determine the following, via his experience, training, SPDS, and knowledge of prior plant conditions and activities.

1. If plant conditions warrant entry into an EOP.
2. Which is (are) the appropriate EOP(s) to enter.

C. Test Description

1. Static Tests

The factory testing shall be performed at the SPDS vendor facility when possible with the remaining testing being performed at the site. A unique functional compatibility test shall be performed to demonstrate each of the static test acceptance criteria.

(a) Documentation Implementation Test: Test(s) will be performed to verify that;

1. The database defined in the SPDS design documentation is duplicated in the SPDS.

2. Screen displays described in the SPDS design documentation are duplicated in the SPDS with respect to content and arrangement.

(b) Display Features Test: All display features described in the SPDS design documentation will be tested to verify that;

1. Display feature changes (e.g., parameter value, color, status, etc.) occur as described.

2. Display links (e.g., transfer between primary, secondary and tertiary displays) occur as described. Screen refresh shall be within the specified time limit.

(c) System Operational Test: All operational features described in the SPDS design documentation will be tested to verify that;

1. All data points are scanned at the required frequency.

2. Analog values in the SPDS database do not update for changes less than the storage deadband, and do update for changes at, or greater than, the storage deadband.

3. Data throughput occurs within the specified time.

4. Data validation (e.g., analog range checking, redundant sensor comparison, and/or logical validation) occurs as required.

5. Analog accuracies are within the required value. If specific accuracy requirements are not identified, the accuracy shall be within the accuracy of the associated control room benchboard instrumentation.

6. Station keyboard functions occur as described.

7. All composed point algorithms function as required.

8. Sensor Input Failure: A single randomly selected input for each sensor type, excluding digital inputs, shall be subjected to: a simulated hardware failure such as "point selection failure" or "analog to digital overflow"; and both open & short circuited inputs to confirm that an invalid status is displayed.

9. Hardware Failover: One of the redundant CPU's shall be intentionally failed to verify transfer to the alternate processor has occurred and normal SPDS functions resume.

2. Dynamic Test

The simulator dynamic performance test shall subject three randomly selected control room crews to three different transient scenarios. The transients shall be selected so that as many of the SPDS displays as possible are addressed. Each transient shall focus on a different EOP and at least one of the transients shall introduce multiple failures to ensure concurrent execution of at least two EOP's. Two permutations of each

transient, resulting in six separate tests overall, shall be performed.

One of the permutations shall be the baseline for comparison upon test completion. Only control room instrumentation shall be utilized. The second permutation shall require the use of SPDS in addition to normal control room instrumentation. For the purposes of these tests it shall be assumed that the training of each of the three crews is comparable. This will facilitate the effectiveness evaluation by allowing a different crew to perform each transient permutation. Test results evaluation will compare general crew performance to substantiate this assumption.

Sufficient safety parameter data shall be recorded to determine if the operator was able to appropriately follow the correct EOP(s), remain within normal EOP control bands, and recover from the transient.

To assist in making an evaluation on the effectiveness of the SPDS, the following will be considered. Assuming time "zero" is the initiation of the transient:

1. The elapsed time required to enter the appropriate EOP.

2. The elapsed time required to exit the appropriate EOP.

3. The worst case value of the EOP entry parameter.

Evaluation of these results shall be limited to determination of performance trends since no real significance can be associated with any absolute measurements.

Feedback from test participants will be included in the evaluation of performance trends via operator/instructor post test interviews.

VI. FIELD VERIFICATION TESTS

The objective of this activity shall be to verify that the system was properly installed. Construction installation and test specifications shall be reviewed to ensure that sensor inputs to the system and system power supply transfer schemes are physically checked for correctness. Specific items that shall be included are:

A. Point to point continuity checks,

B. Polarity checks, and

C. Calibration

The design review "walk through" discussed in Section IV of this plan will be coordinated with the audit of the installed system. This will include a check to verify that the installation of Class 1E isolation devices, for randomly selected sensors, is consistent with design drawings.

Randomly selected parameters will be tested by varying the sensor output signal to assure that the variable being displayed is being measured by the sensor assigned to that function.

The existing graphic displays will also be reviewed at this time for consistent format and content with those validated during prior testing.

Test items not incorporated into the Performance Validation test will be subject to a field verification test.

VII. FINAL REPORT

A final report will be prepared to provide documentation of the results of the above efforts and to provide traceability for future reference.

The report will contain the design requirements matrix, any deficiencies noted with their associated resolutions, results of the performance validation tests and results of the field verification test.

VIII. REVIEW TEAM QUALIFICATIONS

The Hope Creek SPDS V&V program shall be conducted by qualified individuals from EIGEN Engineering, Inc. who were not involved in the design, development and installation of the SPDS equipment or software.

The team from EIGEN Engineering, Inc. will consist of the following individuals:

Luis E. Flores, P.E.

Principal Engineer

Mr. Flores earned BS degrees in Physics and Mechanical Engineering, has professional engineering licenses in California and Ohio, and holds a Senior Reactor Operator Certification.

Mr. Flores has had extensive experience in the design, operation and testing of nuclear power plant systems, including instrumentation and control system engineering, data acquisition system specification and implementation and design verification testing of process computer systems.

He has been responsible for various projects at the Hope Creek Generating Station, including: Development of the power Ascension Test Program; Design and implementation of the Plant Transient Analysis and Recording System; and

Analysis of Post Accident Monitoring capabilities. He has also directed a group of startup engineers and participated in all phases of several startup programs for nuclear power plants.

Joseph D. Doyel, P.E.

Principal Engineer

Mr. Doyel attended San Jose City College and Northeast Missouri State College. He also graduated from the U.S. Navy Nuclear Power School. He is a Registered Mechanical Engineer in California and is qualified per ANSI N.45.2.6 Inspection, Surveillance and Testing.

He has twenty years experience in commercial and military power plant construction, startup, operations, maintenance and testing.

He has been responsible for several projects for PSE&G including; development of HCGS Power Ascension Test Procedures, identification of discrepancies between HCGS and the HCGS simulator, development of HCGS CRIDS documentation, preliminary design of a Sequence of Events, Transient Analysis, Post Trip Review system for Salem, and development of a Power Supply Failure database for HCGS.

He has also been involved in development of Sequence of Events, Transient Analysis and Post Trip Review systems for other nuclear facilities.

Gregg A. Reimers, P.E.

Senior Consulting Engineer

Mr. Reimers earned a BS degree in Electrical Engineering and has completed courses at the General Electric BWR Simulator and Westinghouse PWR Simulator. He has a professional Engineering license in California.

Mr. Reimers has over ten years experience in the nuclear power industry in the areas of power plant operations, system design, design implementation, design and analysis of electrical power systems, process system instrumentation and control circuits and design reviews of actual plant systems to design criteria.

He has participated in several projects for Hope Creek Generating Station, including: Development of various test, instrumentation and control tuneup procedures for the Power Ascension Test Program; responsible for the preparation and instruction of site engineering on the Emergency Core Cooling System design theory and operation; and responsible for development of relational database software for plant information tracking management. He has also been involved

in several design projects at other plants and was assigned to the technical staff of an operating nuclear power plant for a number of years.

REFERENCES

1. NUREG 0660, Task I.D. TMI Task Action Plan, May, 1980.

2. NUREG 0737, Supplement 1, Requirements for Emergency Response Capability (Generic Letter 82-33) dated December 17, 1982.

3. NSAC 39, Verification and Validation for Safety Parameter Display System, December, 1981.

4. NUREG 0800, 18.2, Rev. 0, Safety Parameter Display System (SPDS), November, 1984.

5. NUREG 0700, Human Factors Acceptance Criteria for the Safety Parameter Display.