REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR: 8606060050 DOC. DATE: 86/06/02 NOTARIZED: NO DOCKET #
FACIL: 50-400 Shearon Harris Nuclear Power Plant, Unit 1, Carolina 05000400
AUTH. NAME AUTHOR AFFILIATION
ZIMMERMAN, S. R. Carolina Power & Light Co.
RECIP. NAME RECIPIENT AFFILIATION
DENTON, H. R. Office of Nuclear Reactor Regulation, Director (post 851125

SUBJECT: Forwards responses to 851025 request for addl info re SPDS. Review & issuance of SSER requested. Display design modified such that Class 1E multiplexer cards powered from Class 1E power within div.

DISTRIBUTION CODE: B001D COPIES RECEIVED: LTR 1 ENCL 1 SIZE: 22
TITLE: Licensing Submittal: PSAR/FSAR Amdts & Related Correspondence

NOTES: Application for permit renewal filed. 05000400

	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL
	PWR-A ADTS	1	1	PWR-A EB	1	1
	PWR-A EICSB	2	2	PWR-A FOB	1	1
	PWR-A PD2 LA	1	1	PWR-A PD2 PD	1	1
	BUCKLEY, B 01	2	2	PWR-A PSB	1	1
	PWR-A RSB	1	1			
INTERNAL:	ADM/LFMB	1	0	ELD/HDS1	1	0
	IE FILE	1	1	IE/DEPER/EPB 36	1	1
	IE/DQAVT/QAB 21	1	1	NRR BWR ADTS	1	0
	NRR PWR-A ADTS	1	0	NRR PWR-B ADTS	1	0
	NRR ROE, M. L	1	1	NRR/DHFT/HFIB	1	1
	NRR/DHFT/MTB	1	1	REG FILE 04	1	1
	RGN2	3	3	RM/DDAMI/MIB	1	0
EXTERNAL:	24X	1	1	BNL(AMDTS ONLY)	1	1
	DMB/DSS (AMDTS)	1	1	LPDR 03	1	1
	NRC PDR 02	1	1	NSIC 05	1	1
	PNL GRUEL, R	1	1			

TOTAL NUMBER OF COPIES REQUIRED: LTTR 34 ENCL 28

[illegible]

[illegible]

[illegible]

[illegible]

CP&L
Carolina Power & Light Company

JUN 2 1986

SERIAL: NLS-86-067

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
United States Nuclear Regulatory Commission
Washington, DC 20555

SHEARON HARRIS NUCLEAR POWER PLANT
UNIT NO. 1 - DOCKET NO. 50-400
SAFETY PARAMETER DISPLAY SYSTEM

REFERENCE: 1) NRC Safety Evaluation Report from Mr. G. W. Knighton (NRC) to Mr. E. E. Utley (CP&L), Dated October 25, 1985

Dear Mr. Denton:

Carolina Power & Light Company submits responses to your staff's request for additional information identified in the NRC's Safety Evaluation Report (SER) for the Shearon Harris Nuclear Power Plant Safety Parameter Display System (Reference 1). Please review these attached responses and issue a supplemental SER.

If you have any questions, please contact Mr. Gregg A. Sinders at (919) 836-8168.

Yours very truly,

for S. R. Zimmerman
Manager
Nuclear Licensing Section

SRZ/GAS/pgp (3450GAS)

Attachments

cc: Mr. B. C. Buckley (NRC)
Mr. G. F. Maxwell (NRC-SHNPP)
Dr. J. Nelson Grace (NRC-RII)
Mr. Travis Payne (KUDZU)
Mr. Daniel F. Read (CHANGE/ELP)
Mr. L. Beltracci (NRC)
Mr. R. J. Eckenrode (NRC)
Mr. T. S. Moore (ASLAB)
Wake County Public Library
Mr. Wells Eddleman
Mr. John D. Runkle
Dr. Richard D. Wilson
Mr. G. O. Bright (ASLB)
Dr. J. H. Carpenter (ASLB)
Mr. J. L. Kelley (ASLB)
Mr. S. H. Weiss (NRC)
Dr. R. L. Gotchy (ASLAB)
Mr. H. A. Wilber (ASLAB)

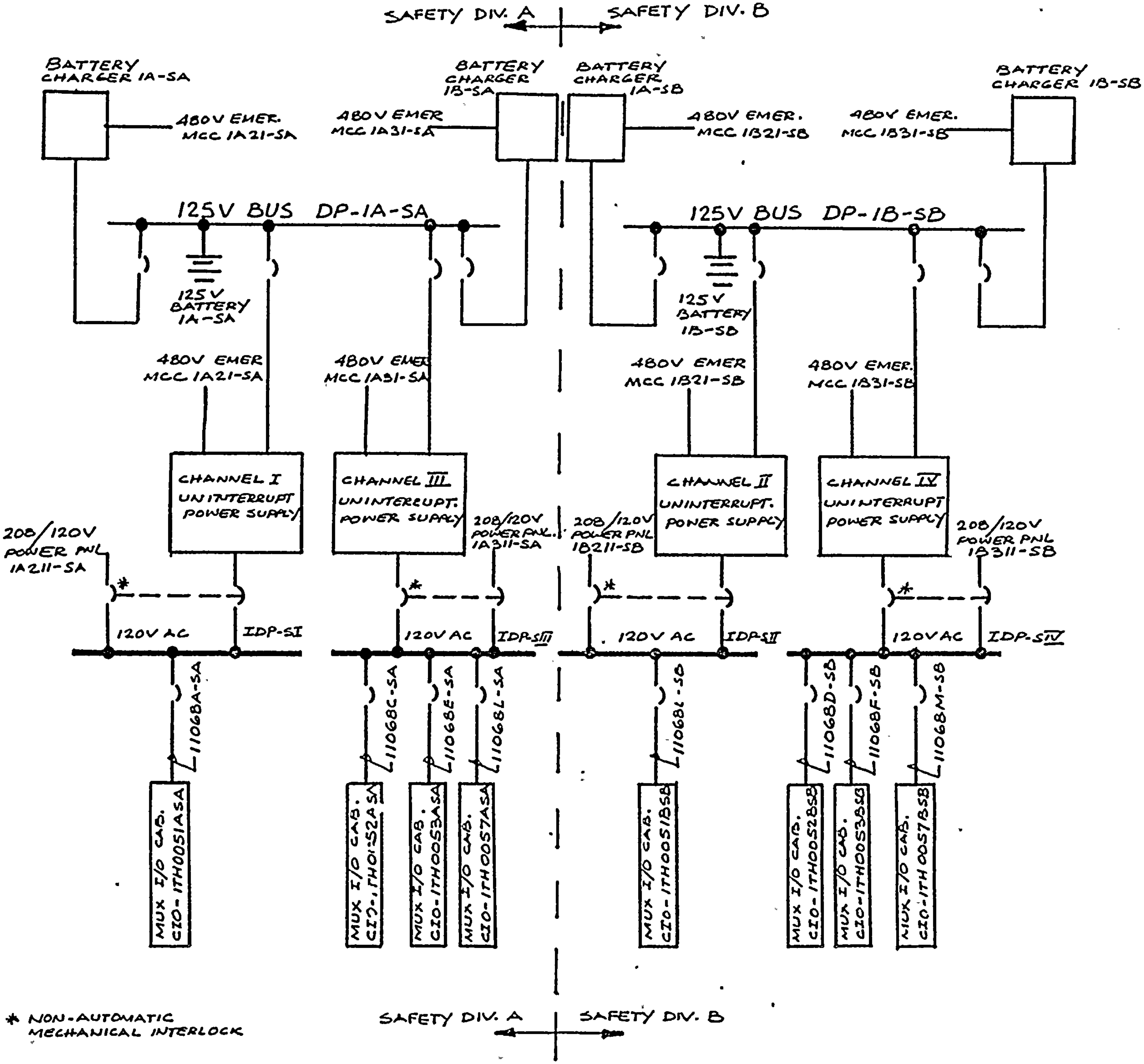
B001 1/1

Question 1

Modify the display's design such that the Class 1E multiplexer cards be powered from Class 1E power within their division. This modification shall be completed prior to declaring the safety systems operational for the plant. Documentation to support this modification should be submitted to the NRC for confirmatory review.

Response

The display's design has been modified such that the Class 1E multiplexer cards are powered from Class 1E power within their division. Documentation to support this modification is attached. The modification will be completed prior to fuel load.


SAFETY DIV. A
SAFETY DIV. B
BATTERY CHARGER 1A-SA
BATTERY CHARGER 1B-SA
BATTERY CHARGER 1A-SB
BATTERY CHARGER 1B-SB
480V EMER. MCC 1A21-SA
480V EMER MCC 1A31-SA
480V EMER. MCC 1B21-SB
480V EMER. MCC 1B31-SB
125V BUS DP-1A-SA
125V BUS DP-1B-SB
125V BATTERY 1A-SA
125V BATTERY 1B-SB
480V EMER MCC 1A21-SA
480V EMER MCC 1A31-SA
480V EMER MCC 1B21-SB
480V EMER. MCC 1B31-SB
CHANNEL I UNINTERRUPT POWER SUPPLY
CHANNEL III UNINTERRUPT. POWER SUPPLY
CHANNEL II UNINTERRUPT. POWER SUPPLY
CHANNEL IV UNINTERRUPT POWER SUPPLY
208/120V POWER PNL 1A211-SA
208/120V POWER PNL. 1A311-SA
208/120V POWER PNL 1B211-SB
208/120V POWER PNL 1B311-SB
120V AC
IDP-SI
IDP-SIII
IDP-SII
IDP-SIV
11068A-SA
11068C-SA
11068E-SA
11068L-SA
11068I-SB
11068D-SB
11068F-SB
11068M-SB
MUX I/O CAB. CIO-1TH0051ASA
MUX I/O CAB. CIO-1TH0052ASA
MUX I/O CAB. CIO-1TH0053ASA
MUX I/O CAB. CIO-1TH0057ASA
MUX I/O CAB. CIO-1TH0051BSB
MUX I/O CAB. CIO-1TH0052BSB
MUX I/O CAB. CIO-1TH0053BSB
MUX I/O CAB. CIO-1TH0057BSB
* NON-AUTOMATIC MECHANICAL INTERLOCK

Question 2.a

A report on the Safety Parameter Display System's (SPDS) design availability analysis for confirmatory staff review.

Response

The availability analysis is completed and the calculated availability of the SPDS is 99.87 percent.

The availability (A_i) is calculated by the following equation:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Where MTBF = Mean Time Between Failure
MTTR = Mean Time to Repair

The MTBF is calculated by the following equation:

$$MTBF = \frac{1}{\Sigma(\lambda_i)}$$

Where λ_i = Failure Rate of Any Component

Availability is the probability that a system or equipment, when used under specified operational conditions and support environment, will operate satisfactorily at any time. The inherent availability, as quantified in this analysis, assumes an ideal support environment (i.e., available tools, spares, trained personnel, etc.) and excludes preventive maintenance actions, logistics supply time, and administrative downtime.

The MTTR is defined as the average time to perform corrective maintenance action. This time period begins with equipment failure and ends when the equipment is returned to operational status. It includes time for fault detection, fault isolation, access/secure, maintenance operations (repair and/or replace), and function testing. It is also assumed that adequate spares are available at the site. A MTTR of 4 hours was used throughout as specified by most of the vendors.

For the purpose of this analysis, system success means that the status information (analog value or digital status) of each of the specified SPDS points is available to the operator in the Control Room.

An apparent single point of failure is the peripheral switch controller system. However, there are two features that provide additional reliability for the system. One is that should the CPU control circuitry fail, the switches may be switched manually. The other feature is that since the switch modules are mechanical, magnetically-latched relays they remain in the last commanded position and permit signal continuity even without power.

The calculated availability of 99.87 percent exceeds the high availability goal of 99 percent requested by the NRC. Carolina Power & Light Company (CP&L) considers this matter closed.

Question 2.b

A commitment that procedures which describe the timely and correct safety status assessment when the SPDS is and is not available will be developed and that operators be training to respond to accident conditions both with and without the SPDS available.

Response

The Critical Safety Function Status Trees (CSFST) developed as part of the Westinghouse Owners' Group Emergency Response guidelines form the basis of the SPDS displays. The Shearon Harris Nuclear Power Plant (SHNPP) Emergency Operating Procedures (EOPs) and EOPs network currently specify when the CSFST are to be monitored and when the Functional Restoration Procedures required by the respective states of the CSFST are to be implemented.

The value of the input parameters for the CSFST and the resulting states of the CSFST are available directly from the SPDS. The current information is available through the CRTs in the Control Room. The SPDS has a calculated availability of 99.87 percent, however, if the SPDS is not available, a hard copy of the CSFST will be available for manual assessment of the CSFST. The EOPs do not distinguish between the manual or the computerized acquisition of the CSFST information since they produce identical results.

The training of the Shift Technical Advisors (STAs) (the primary individual responsible for evaluating the CSFST) and the licensed operators has covered the use of the EOPs, the purpose and use of the CSFST, and the implementation of the manual method. The STAs and licensed operators will be trained on how the SPDS displays are accessed from the Control Room CRTs.

CP&L considers this matter closed.

Question 2.c

Information on how new displays created by users from the keyboard will not be confused with the standard set of displays within the SPDS.

Response

Users cannot create new displays from consoles located in the Control Room, Technical Support Center, or Emergency Operations Facility. The console in the plant computer room is the only console from which new displays can be created. This console is a locked console and the key is controlled by Control Room personnel in accordance with administrative procedures. These administrative procedures, along with other plant access security controls to the computer room, comprise the security measures in place for the SPDS. Additionally, top level, second level, and third level displays are called by labeled, dedicated function keys, or operator functions from top or second level displays. P&IDs or one-lines cannot be inadvertently called by SPDS function keys or from a second level SPDS. The display structures are completely separate and distinctively labeled. CP&L considers this matter closed.

Question 2.d

A list which coordinates the SPDS variables with the critical safety functions specified in NUREG-0737, Supplement 1. In addition, the list could contain information which identifies the display format (or page) where the variable is presented to the user.

Response

For a response to this question, please refer to our December 2, 1983 letter (from M. A. McDuffie to H. R. Denton) which transmitted the safety analysis of the SPDS.

CP&L considers this matter closed.

Question 2.e

Data which demonstrates that the SPDS adequately monitors the Radioactivity Control Function under plant conditions with isolated steam generators.

Response

See response to Item 4 below.

Question 2.f

A description of how the design validation of the SPDS variables will be achieved as part of the Validation Test Plan.

Response

The Critical Safety Function Status Trees originating from the Westinghouse Owners' Group (WOG) Emergency Response Guidelines (ERGs) form the basis of the SHNPP SPDS top two levels of display. These status trees provide an explicit, systematic mechanism for evaluating the plant safety status. For multiple event/multiple failure scenarios that go beyond the design basis of the Engineered Safeguards System and the scope of the Emergency Operating Procedures (EOPs), the operator is provided with the means of directly monitoring the Critical Safety Functions and taking the prescribed action based on the Critical Safety Function display. The WOG selected the "appropriate set of plant parameters" for the Critical Safety Functions. For each parameter selected to be read, evaluated, and displayed on the SPDS, the WOG has provided a basis/background document. Based on Regulatory Guide 1.97 instruments and plant instrumentation for the values requiring plant specific input, explicit evaluation guidelines have been provided. For SHNPP, a complete setpoint study has been completed and included in the Procedures Generation Package (PGP) transmitted to the NRC in 1984. The draft Technical Specification values have also been evaluated with the EOP values for consistency.

The status trees require no operator action other than monitoring a limited set of plant parameters. The SPDS status trees are a part of the integrated plant computer system and display a subset of the plant parameters the operators use for routine operations terminating an event or in mitigating the consequences of an event. Once a change of status is acknowledged and the EOP network has been entered, the operator should begin monitoring the appropriate branch of the tree. The top level SPDS is defined as the six-critical safety function boxes which are displayed constantly. When the operator is not displaying a second level status tree, an overview of key plant parameters will be displayed in the general display area. The third level displays consist of sets of pre-defined variables for trending.

In addition to the WOG analysis for the type of variable for the "standard plant," CP&L has performed scenarios on two different simulators, licensed a class of operators, walked through the procedures in table top emergency planning reviews, and utilized the experiences of the H. B. Robinson Plant whose procedures were written in parallel by the same author. With the large amount of operator input, review, and the setpoint study combined with the results from simulator exercises, CP&L feels that the variables in the SPDS as well as the EOPs have been proven to be acceptable. The variables have been verified, tested, validated, and analyzed and the results show that the actual result matches the expected results.

Finally, CP&L must also note that both plants, H. B. Robinson and SHNPP, have been using the SPDS function for well over a year in the hard copy mode (w/o the computer). CP&L has found that not only does the concept function better than expected, but that the operators use SPDS functions during EOP situations. The operators also trust the SPDS function and the EOP function especially after the extensive amount of EOP/SPDS background information and analysis that support these functions and the simulator exercises.

As the WOG/Westinghouse utilized human factors principles in the evaluation of the transition from procedure to procedure in the layout/format of the EOPs (which include the CP&L EOPs and the Critical Function Status Trees) and in the area of simulator V & V, CP&L believes that these procedures have a sound engineering, analytical, and human factors basis.

CP&L has also provided sound engineering in the transition from generic to plant specific, sound analysis in the development of the setpoint study and the other evaluations required in the transition from generic to plant specific. Sound human factors have also been utilized in the many hours of evaluation on simulators, procedures walkthroughs during the Control Room Design Review (CRDR) effort, operator interviews, and the total CRDR effort. This includes receiving operator comments, evaluating the comments, and making modifications where necessary.

Question 2.g

A Validation Test Plan which includes human factors acceptance criteria for evaluating the use of the SPDS.

Response

See Response to Question 5

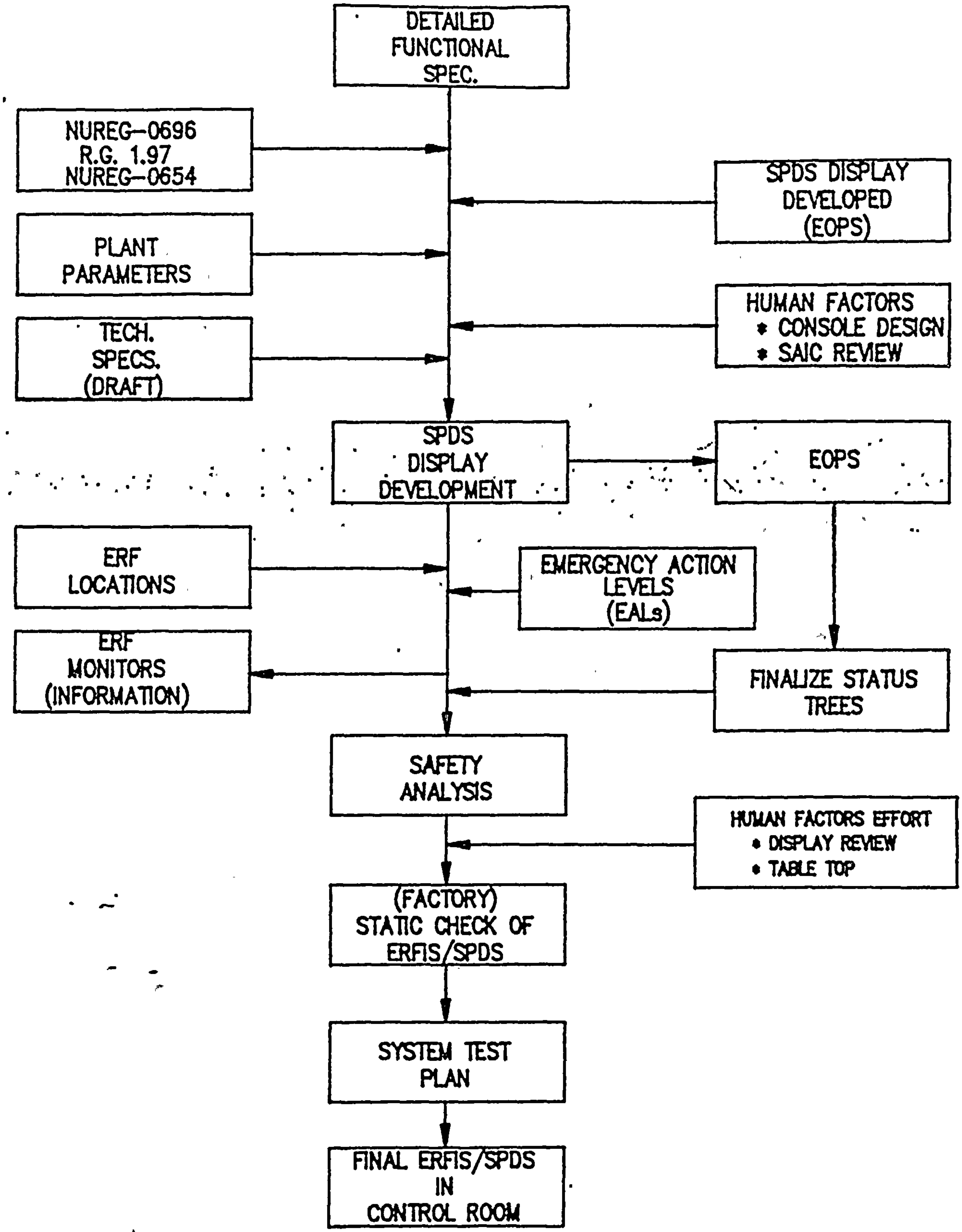
Question 2.h

A Validation Test Report which describes test results and plans for resolution of problems identified during the test program.

Response

CP&L has a high degree of confidence that the Final Validation Test Report will demonstrate that the SHNPP SPDS is an extremely well designed computer system. The SPDS has been developed from the top down as shown in the attached figure. Additionally, hardcopy outputs of the as-designed SPDS have been used on the Harris simulator with great success and acknowledged by the NRC staff in a Trip Report dated May 22, 1984. The Final Validation Test Report will be available prior to startup following the first refueling outage.

FIGURE 1-1
ERFIS/SPDS EFFORT



Question 3

Conduct a review of all SPDS display formats for human engineering discrepancies (HEDs). All identified HEDs from the review should be assessed and resolved within the DCRDR effort and the results of the assessment reported in the DCRDR Summary Report which is submitted for staff review.

Response

A preliminary review of SPDS display formats for HEDs has been completed. HEDs identified from this review have been assessed within the DCRDR effort. The disposition of the HEDs were reported to the staff in the DCRDR Final Summary Report submitted to the NRC on September 13, 1985 (A. B. Cutter to H. R. Denton, NLS-85-235). Additional HEDs identified on the SPDS will be resolved prior to startup following the first refueling outage.

Question 4

Address the following variables which are not included in the SPDS by:

1) adding these variables to the SHNPP SPDS,

2) providing alternate added variables along with justifications that these alternates accomplish the same safety function for all scenarios,

3) providing justification that variables currently on the SHNPP SPDS do in fact accomplish the same safety functions for all scenarios, or

4) identifying that these variables are in fact available from the SPDS console:

   a. source range neutron flux,

   b. intermediate range neutron flux,

   c. RHR flow,

   d. steam generator (or steamline) radiation,

   e. stack radiation,

   f. containment isolation status,

   g. containment hydrogen concentration.

Response

Variables a-c are in fact available from the SPDS consoles. Based on discussions with the NRC staff, CP&L will add variables d-g to the SPDS top level display to resolve this item. CP&L considers this matter closed.

Question 5

Submit the Verification and Validation Program Plan for docketing.

Response

A Summary of Verification and Validation Plan is attached.

SUMMARY OF THE

VERIFICATION AND VALIDATION PLAN

1. INTRODUCTION

1.1 Objective

The objective of the Verification and Validation (V&V) Program for the Carolina Power & Light Company (CP&L) Shearon Harris Nuclear Power Plant (SHNPP) Unit 1 Safety Parameter Display System (SPDS) Emergency Response Facility Information System (ERFIS) is to provide a quality system through independent technical review and evaluation. The V&V effort described meets the basic objective that an adequate independent technical evaluation has been made on the SPDS functions provided by the ERFIS computer.

The ERFIS will be evaluated to determine that SPDS functions provide continuous and reliable display of SPDS plant parameters to control room operators. The SPDS function is required in order to keep the control room operator informed of the status of critical safety functions and alert to abnormal operating conditions. The SPDS computer functions have been incorporated with other plant computer functions such as the NSSS functions. These other plant computer functions provided by ERFIS will also be subject to limited V&V. An evaluation of the interactions and interfaces between these functions and the SPDS functions will be performed by the V&V Team.

1.2 Background

To ensure that a separate technical evaluation of the SPDS will be performed without programmatic bias, the V&V Team staff is independent of the Development Team and Quality Assurance Program.

2. ERFIS V&V SCOPE

2.1 V&V Approach

The V&V Program activities described in this V&V Plan are based on the NSAC-39 Report. Our approach is a practical balance with the size and complexity of the SPDS/ERFIS. The five V&V activities described in NSAC-39 and being applied for SPDS/ERFIS include Systems Requirements Verification (System Requirements Review), Design Verification (Design Review), System Validation (Validation Test and Report), Field Installation Verification (Field Verification Test), and preparation of the Final V&V Report.* The Final V&V Report will summarized the results of the four V&V activities listed above and will summarize all discrepancies found during the V&V evaluation. The balanced approach provides assurance that the system has been constructed in accordance with system requirement specifications.

Figure 2-1 shows the V&V activities in relation to generic system development activities.

2.2 V&V Activity Overview

Figure 2-2 shows an overview of the V&V activities to be applied in evaluating the ERFIS and the following paragraphs describe each of these activities.

2.2.1 System Requirements Verification

System Requirements Verification is a technical evaluation of the SPDS/ERFIS requirements documentation against NRC standards and regulations relating to the upgrade of Emergency Response Facilities. It also involves an evaluation to ensure the SPDS/ERFIS design specification is a proper translation of the SPDS/ERFIS requirements documentation.

Evaluation of the design specification documentation is normally a System Design Verification step. Exception to this normal V&V procedure is being taken to consider the design specification documentation as the requirements baseline document once the System Requirement Verification is complete.

2.2.2 System Design Verification

System Design Verification is an evaluation of SPDS/ERFIS detailed hardware and software design documentation against the verified SPDS/ERFIS requirements documentation. Design Verification provides assurance that the system complies with the system requirements. Hardware design utilizing off-the-shelf items will not undergo independent design verification.

2.2.3 System Validation

System Validation provides assurance that the final system complies with the system requirements. Demonstration of acceptable operation of implemented functions is accomplished through a planned testing and evaluation process.

---

* The activity names shown in parentheses are the names used in NSAC-39.

The objective of validation testing and evaluation is to provide an end-to-end check to determine that the system implements the required functions in compliance with the specified system criteria. System Validation comprises two primary phases: 1) preparation of the Validation Test Plan, and 2) validation testing and evaluation.

2.2.4 Field Installation Verification

Field Installation Verification is an evaluation of the validated system after it has been installed. It is a verification that the installed system is the one validated during validation testing. Verification that the information displayed is directly correlated with the sensor data input is an objective of Field Verification Installation.

2.2.5 Final V&V Report

The purpose of the Final V&V Report is to summarize the V&V activities performed throughout the project and to summarize the results of those evaluation activities. The report provides a summary of results of the V&V effort; it will be organized to aid in reviewing the adequacy of the validation effort and providing confidence in the validated system. Traceability of the V&V activities throughout the project, identification and resolution of discrepancies, and reference to more detailed documentation will be provided in the Final V&V Report.

2.3 V&V Documentation

The contents of the documentation will be consistent with the typical report contents which are described in NSAC-39.

2.4 Configuration Management of V&V Documentation

An important activity in the V&V Program is the management and control of project documentation and correspondence received by and V&V reports issued by the V&V Team. An individual within the V&V organization is assigned the responsibility of controlling the project documentation. This individual will be referred to as the V&V Configuration Manager. The V&V Configuration Manager is responsible for logging and filing all project documentation, controlling changes to V&V deliverable documentation, and maintaining the status of the documentation changes.

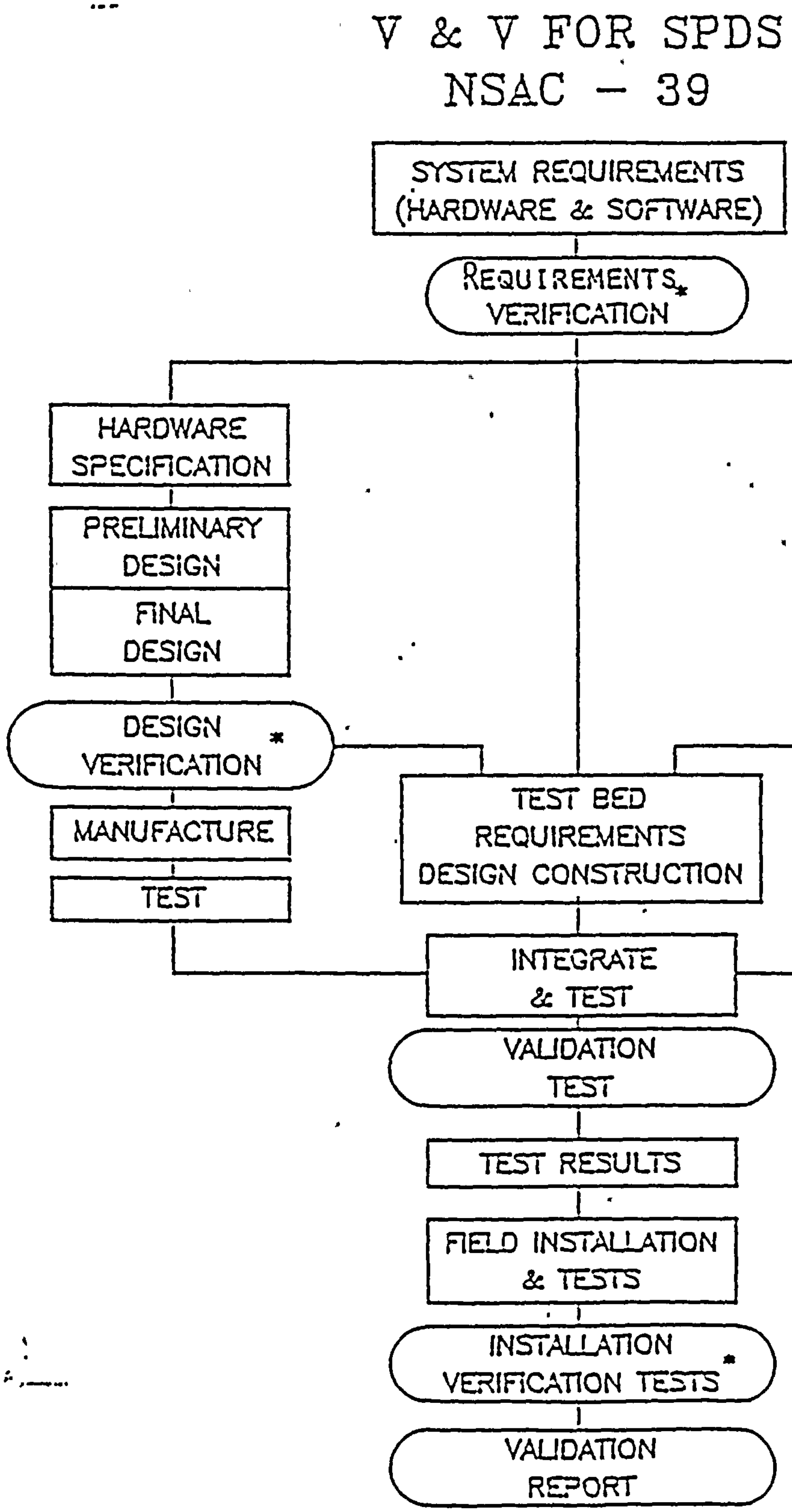
Project documentation and correspondence received by the V&V Team must be acknowledged and made available to each team member. When documentation items are received, the V&V Configuration Manager records the item received on a project log which is available to all V&V Team members. The documentation item is then filed in a central file location designated specifically for this project.

Formal V&V reports are subject to change control by the V&V Team. A change control system has been designed to provide identification and traceability of documentation changes throughout the V&V activities.

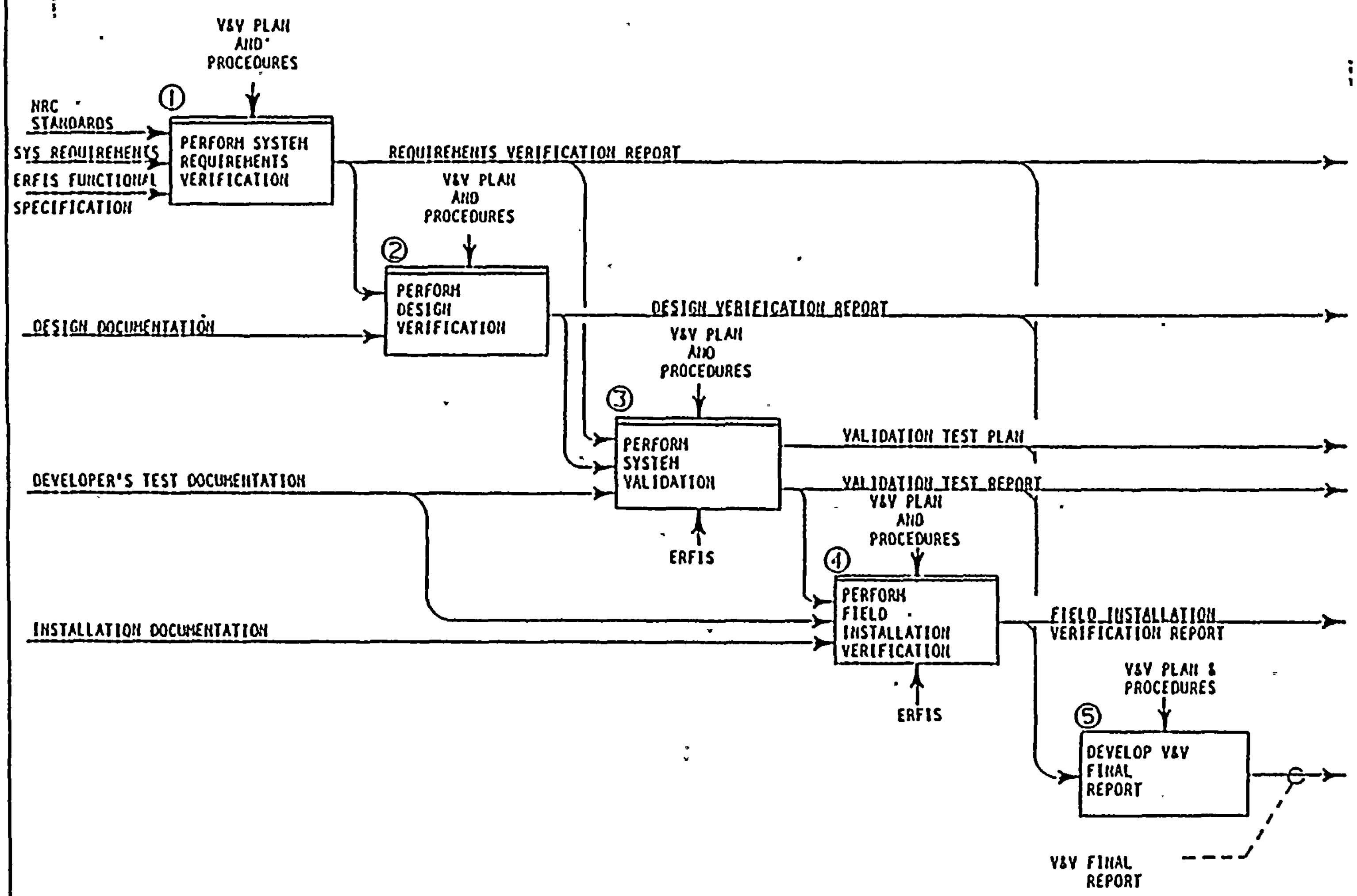
Once a document has been released as a final document (is no longer a draft) changes are controlled under this procedure. Each formal document released by the V&V Team is assigned a unique identification number and a revision level. Each document contains a revision page in the front which indicates the date on which the document was revised, the document section, and page numbers of the text affected by the change.

Figure 2-1

Relationship of V&V to Generic System Development Activities



* NAMES CHANGED



OVERVIEW OF V&V ACTIVITY PERFORMANCE

FIGURE 2-2

Question 6

Provide revised Implementation Plan to reflect currently planned activities and schedules for the design completion, control room installation, and operation of the SPDS.

Response

The design of the SPDS is complete. The SPDS will be operational and the other related activities discussed in this letter will be completed prior to fuel load, except as discussed in response to Questions 2.h and 3.

CP&L believes that these responses will allow the NRC to issue a supplemental SER and that a post-implementation audit will not be necessary.