PRE-IMPLEMENTATION AUDIT REPORT
FOR
PUBLIC SERVICE ELECTRIC & GAS COMPANY'S
SAFETY PARAMETER DISPLAY SYSTEM AT
SALEM NUCLEAR GENERATION STATION 1 AND 2

SAIC

Science Applications International Corporation

May 5, 1986

Prepared for

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Contract No. NRC-03-82-096

8606020280 XA

Post Office Box 1303, 1710 Goodridge Drive, McLean, Virginia 22102, (703) 821-4300

PRE-IMPLEMENTATION AUDIT REPORT
FOR
PUBLIC SERVICE ELECTRIC & GAS COMPANY'S
SAFETY PARAMETER DISPLAY SYSTEM AT
SALEM NUCLEAR GENERATION STATION 1 AND 2

May 5, 1986

Prepared for

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Prepared by

Science Applications International Corporation
1710 Goodridge Drive
McLean, Virginia 22102

Contract No. NRC-03-82-096

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SAFETY PARAMETER DISPLAY SYSTEM

SALEM NUCLEAR GENERATION STATION 1 & 2

Pre-implementation Audit Report

SECTION 1. BACKGROUND

All holders of operating licenses issueu by the Nuclear regulatory Commission (licensee) and applicants for an operating license (OL) must provide a Safety Parameter Display System (SPDS) in the control room for their plant. The Commission-approved requirements for the SPDS are defined in Supplement 1 to NUREG-0737 (1). PSE&G is completing the design phase of their SPDS and requested a pre-implementation NRC audit of their SPDS design as it currently exists.

The purpose of the SPDS is to provide a concise display of critical plant variables to control room operators to aid them in rapidly and reliably determining the safety status of the plant. NUREG-0737, Supplement 1 (1), requires licensees and applicants to prepare a written Safety Analysis Report (SAR) describing the basis on which the selected parameters are sufficient to assess the safety status of each identified function for a wide range of events, which include symptoms of severe accidents. Licensees and applicants are also required to prepare an implementation plan for the SPDS which contains schedules for design, development, installation, and full operation of the SPDS as well as a design verification and validation plan. The safety analysis and the implementation plan are to be submitted to the NRC for staff review. The results of the staff's review are to be published in a Safety Evaluation Report (SER).

The Public Service Electric & Gas Co. of New Jersey (PSE&G) submitted a SPDS SAR for Salem Nuclear generating Station Units 1 and 2 on January 30, 1984 (2). The NRC reviewed the SPDS SAR and sent a request for additional information to PSE&G (3). In response to this, PSE&G requested that the NRC conduct an in-progress SPDS audit (4). The audit was conducted by the NRC, supported by consultants from SAIC and Comex, from December 4 to December 6, 1985. This report discusses the results of that audit. The SPDS system was still under development, with less than half of the proposed displays having been designed. Because of this, the findings of this audit are limited to general comments and recommendations, rather than specific conclusions and evaluations.

There are both considerable strengths and potential problem areas in the proposed system and the way it is being developed. The computer system architecture should provide a powerful, flexible base for the SPDS and other applications, and the proposed implementation of Emergency Response decision trees should provide plant operators with a useful aid. However, the audit team identified a number of potential problems in the design and development process. The audit team's suggestions for dealing with these problems focused on defining overall system requirements, increasing Verification & Validation (V&V) and Human Factors Engineering (HFE) input in the design process, and improving the configuration management program. The remainder of this report will describe the proposed SPDS, review the specific findings of the audit, and summarize the recommendations of the audit team.

The next section provides a description of the SPDS system being developed by PSE&G and describes the general status of the project. Section 3 discusses system reliability and reviews the Verification and Validation (V&V) and configuration control programs. Section 4 covers Human Factors (HF) considerations in the SPDS system and the Human Factors Review program. The final section presents the major recommendations resulting from the audit. In addition, Appendix A presents an evaluation of the SPDS relative to NUREG 0737 Supplement 1 requirements. Appendix B is the PSE&G briefing package which was distributed for the audit. Appendix C is the list of audit attendees.

SECTION 2. SYSTEM DESCRIPTION

2.1 Principal Functions and Users

The SPDS system is primarily intended to aid Shift Technical Advisors (STAs) during abnormal and emergency conditions. Other operators may occasionally use the SPDS during normal operations and the Senior Reactor Operator (SRO) may use the system during both normal and abnormal operations. However, the STA is the primary user. During emergency operations the SPDS will monitor critical safety parameters and help guide the STA through the Westinghouse Emergency Procedure decision trees.

2.2 SPDS Displays

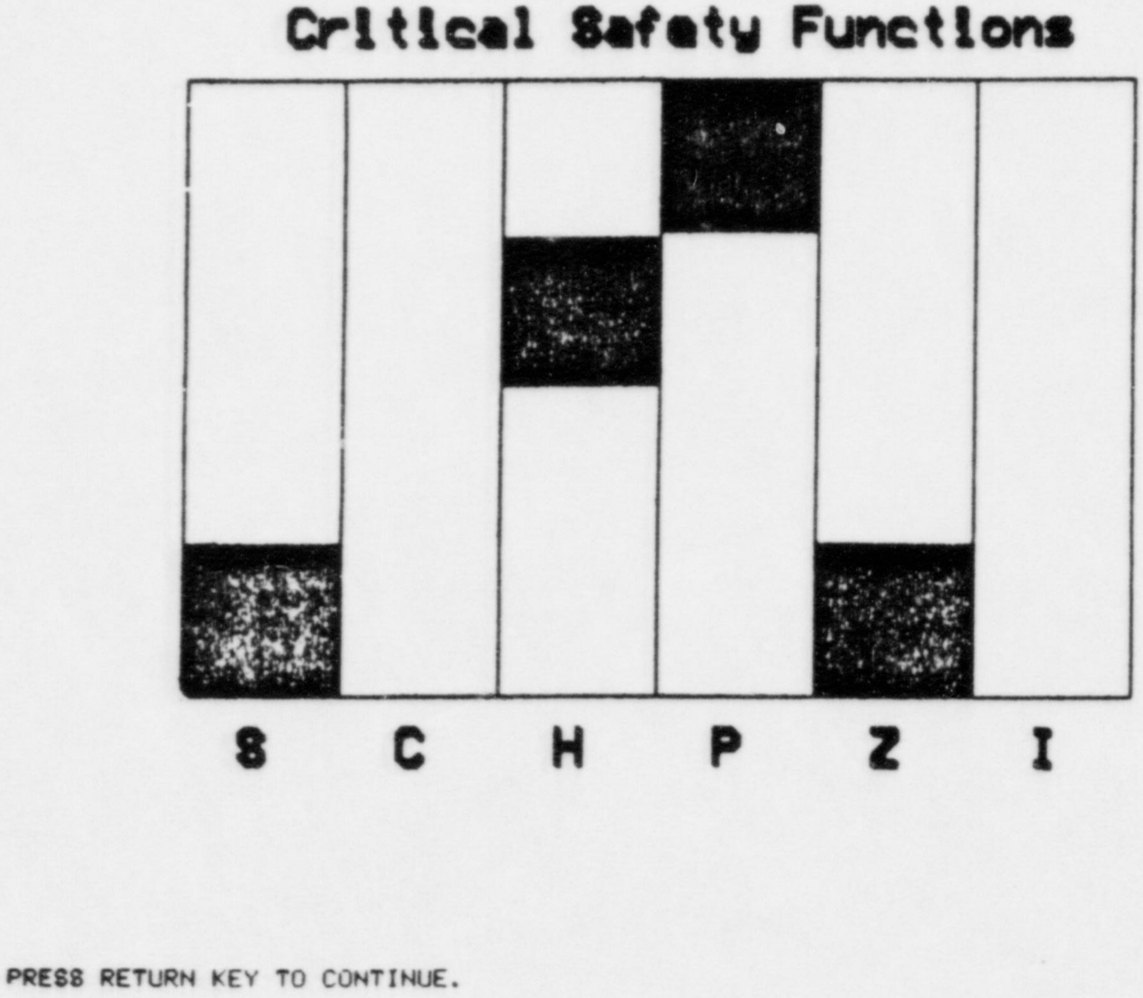
Current plans for the SPDS system will include two CRTs in each control room. The proposed SPDS will consist of four levels of displays. The top level display shows the critical safety functions in the form of color coded bar graphs for the six functions as defined by PSE&G. These functions are described more fully in Section 2.3. The top level display shows a large colored box for each function (Figure 2-1). Each box can appear at one of four vertical positions in the column reserved for the safety function. The color (and vertical position) of the box indicates whether the safety function parameters are normal (green), or at one of three alarm levels (yellow, orange, or red).

The format for the second level displays is taken directly from the Emergency Operating Procedures (EOPs) as developed by PSE&G from the Westinghouse EPGs (Figure 2-2). The SPDS system automatically highlights the appropriate path through these decision trees. These displays (and all others that form a part of the SPDS) contain an insert which shows color coded targets similar to the top level display, without the vertical displacement. This insert would show any changes in other critical safety functions which might occur while the STA is using a status tree second level display for a given critical safety function.

Third and fourth level displays have not been finalized. However, the third level will show the parameter values and condition in a tabular format for those parameters which define the second level status trees. PSE&G should evaluate the appropriate display level which shows parameter values. The NRC feels that the second level may be more appropriate. The fourth level will present trend information for parameters listed in the third level displays. No formats for these displays have been developed.

2.3 Parameter Selection

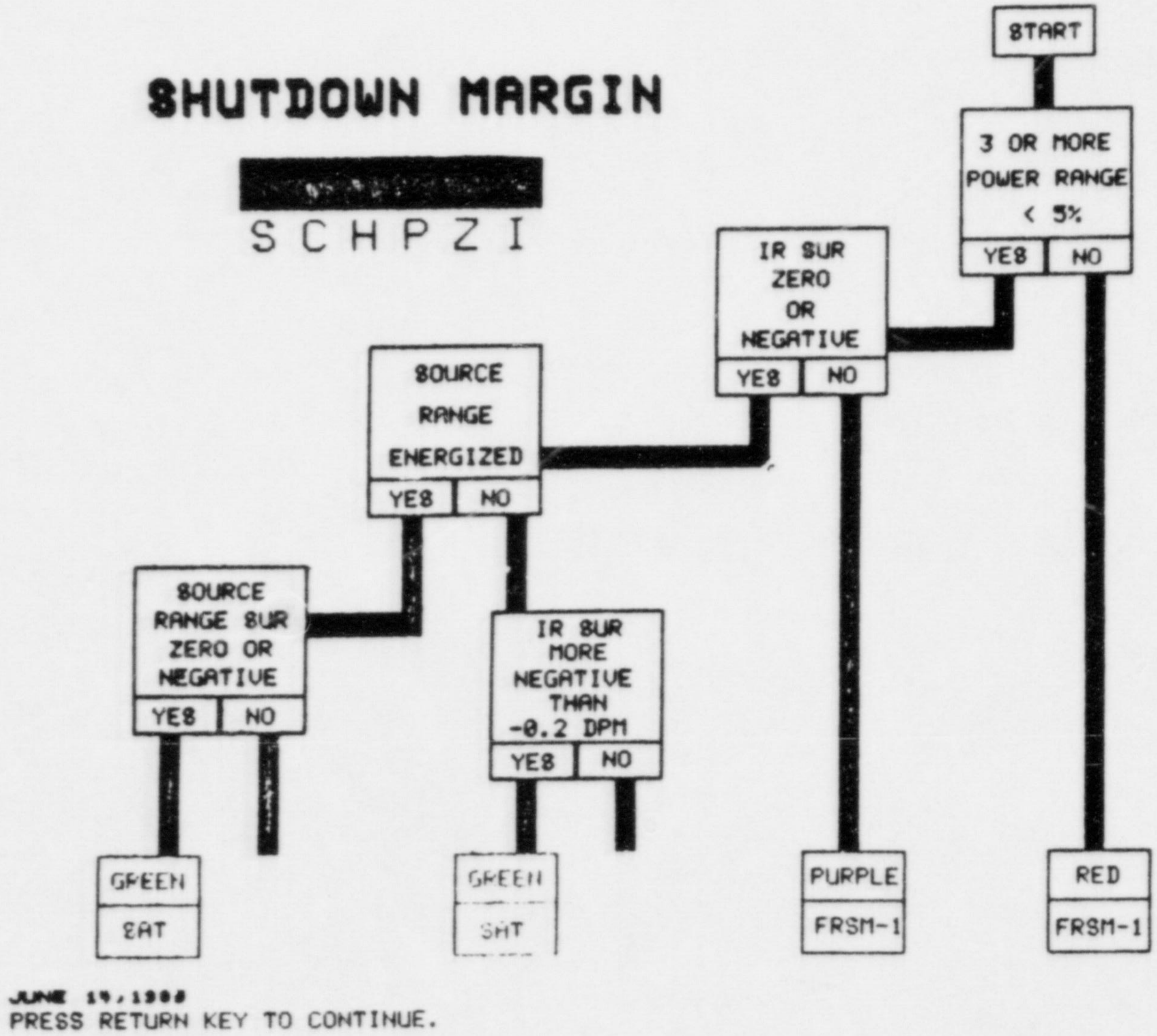
The Salem SPDS parameters are developed from the Westinghouse Emergency Response Guidelines status tree and use Regulatory Guide 1.97 sensors (5).



Critical Safety Functions

PRESS RETURN KEY TO CONTINUE.

Figure 2-1. SPDS Primary Display.



JUNE 19,1988
PRESS RETURN KEY TO CONTINUE.

Figure 2-2. Example SPDS Secondary Display.

The five critical safety functions of NUREG-0737 Supplement 1 (1) are currently displayed by the Salem SPDS through six function blocks (Figure 2-1). The function blocks are:

1. Shutdown Margin
2. Core Cooling
3. Heat Sink
4. Thermal Shock
5. Containment Environment
6. Coolant Inventory

These six function blocks currently utilize fifteen system parameters. These parameters are: neutron flux, RCS cold leg water temperature, RCS pressure, core exit temperature, reactor vessel level, degrees of subcooling, containment sump water level, containment pressure, containment area radiation, reactor coolant pump status, pressurizer level, steam generator level, steam generator pressure, auxiliary feedwater flow, and RCS loop average temperature. However, the licensee stated during the audit that a seventh function block (radioactivity at release points) would be added and four more system parameters would be used for the SPDS. The four added parameters will be: reactor trip, plant vent flow, containment and plant effluent radioactivity release, and main steam radiation. Table 2-1 shows the correspondence of the seven SPDS safety functions and the critical safety functions defined by NUREG-0737 Supplement 1 (1).

The audit team compared the Salem parameter selection with the NRC Procedures and Systems Review Branch guidance on SPDS parameter selection. In general they found good agreement with the NRC staff interpretation of the NUREG-0737 Supplement 1 parameter selection. However, the following items are not identical to the NRC staff interpretation:

(a) Containment isolation status is not on the SPDS. The valve status will be shown on a panel close to the proposed SPDS location in the control room.

(b) RHR/ECCS flow is not displayed.

(c) Hydrogen concentration is not shown.

Table 2-1

CRITICAL SAFETY FUNCTION (NUREG-0737, SUPPLEMENT 1)	CRITICAL SAFETY FUNCTION STATUS TREE (SALEM)	PARAMETERS
Reactivity Contro.	Shut Down Margin	1. Neutron Flux 2. Reactor Trip
Reactor Core Cooling and Heat Removal From the Primary System	Core Cooling	1. Core Exit Temperature 2. Degrees of Subcooling 3. Reactor Coolant Pump Status 4. Reactor Vessel Level
Reactor Coolant System Integrity	Heat Sink	1. Steam Generator Level 2. Steam Generator Pressure 3. Aux. Feedwater Flow
	Thermal Shock	4. RCS Loop Average Temperature 5. RCS Pressure 6. RCS Cold Leg Water Temperature
	Coolant Inventory	7. Pressurizer Level 8. Reactor Vessel Level
Radioactivity Control	Radioactivity at Release Points	1. Plant Vent Flow 2. Containment Effluent Radioactivity 3. Plant Vent Effluent Radioactivity 4. Containment Area Radiation 5. Main Steam Radiation
Containment Conditions	Containment Environment	1. Containment Sump Level 2. Containment Pressure 3. Containment Area Radiation

Parameter acceptability is being reviewed by the NRC and will be determined by the Electrical Instrumentation and Control System Branch. The SPDS display should prove to be a useful tool to the STA and others in assessing abnormal plant conditions and in assisting the STA in planning recovery actions.

2.4 Data Validation

The licensee uses gross checks of data validity. These checks look for zero or off-scale indications and reject these sensors from SPDS display. The checks include thermocouple-open-circuit or out-of-range, multiplexer-unable-to-scan, and RTD-bridge-out-of-range. Similarly, the 4 to 20 milliamp signal conditioners are checked for off-scale operation by checking for less than 4 ma or greater than 20 ma output. Signal conditioners found to be off-scale are rejected from SPDS display. Currently, no other data validation technique is used. The licensee stated that EPRI was studying data validation and the licensee is hoping for some useful guidance from the EPRI effort. Algorithm validation efforts have recently been started by Singer-Link.

2.5 Isolation Devices

The licensee presented a description of an electrical/electronic isolation scheme, which if documented, installed and tested as described, should fulfill the requirements for isolation. A description of the isolation devices was submitted to the NRC in the June 27, 1985 response to the NRC Request for Additional Information. The audit team checked for isolation device testing dates and test results. The licensee stated that the results existed and would be sent to the NRC. The audit team was particularly interested in verifying the isolation test data for the multiplexers where 1E and non-1E signals are processed.

2.6 Computer Architecture

The computer system supporting the SPDS is based on redundant components functioning in a Local Area Network (LAN). Data from existing sensors is input to redundant intelligent multiplexers (MUX). Multiplexed data is transmitted to duplicate host computers (A and B) by means of a high-speed data link. Computer B constantly monitors computer A for failure, and takes over processing if necessary. Communications between the host computer and intelligent terminals is via a LAN data highway. All lines to and from the data highway are duplicated, and the total system will have an uninterruptable power supply. All display formats are contained in bubble memory in the intelligent terminals, so that only parameter values need to be requested by the terminals and transmitted by the host computer across the data highway. This dramatically reduces the load on the host computer and data highway and dramatically speeds the time required to switch from one display to another (one to two seconds).

The system architecture and selection of Gould SEL 32/8750 computers with 384 megabyte hard disks will provide an extremely powerful and flexible computer system. Only a small fraction of this system's capabilities (less than 10%) are expected to be required by the SPDS. It is anticipated that this system will eventually be used to replace the existing plant process computer.

2.7 State of Development

2.7.1 Project Milestones

The SPDS system is currently in the design phase. System development was originally contracted to Electronic Associates Inc. (EAI). In July 1984, EAI went out of business and PSE&G decided to complete development itself. PSE&G is currently using Singer - Link to conduct V&V activities, and General Physics for human factors review.

The computer system has been installed at the PSE&G development site (called the BEST facility) in northern New Jersey. Using the PACE process control-oriented operating system, the system architecture has proven quite reliable. Software development, however, is still in progress, with significantly less than half of the proposed SPDS displays having been developed. In spite of this PSE&G was expecting to begin development testing within a few weeks. The audit team expressed doubts that this was a realistic goal.

Installation of the SPDS is scheduled to begin with cable pulling during the Unit 1 outage in March 1986. Installation in Unit 2 will begin during its next outage, scheduled for late Summer 1986. The SPDS is expected to be fully operational in both units by the end of December 1986. Final validation testing, however, may not be completed for up to 18 months later (Summer, 1988). Given the current state of SPDS software development, the audit team was concerned that the December 1986 deadline may be difficult to obtain. The audit team was also concerned that PSE&G is planning to declare the system operational long before it has been validated. Based on recent information, the licensee has indicated that the SPDS operational date has been delayed and a revised implementation schedule will be submitted later in the summer (1986).

2.7.2 System Strengths

The PSE&G SPDS has the potential to become a powerful system that will be highly useful in both normal and abnormal operations. The computer system being developed will provide a powerful and flexible base for both the SPDS system and future applications. The hardware system is capable of doing much more than handling the minimum SPDS requirements. The parameters being input to the system include not only those required for the EOPs, but basically all the parameters suggested in Regulatory Guideline 1.97. This gives the system the potential to rapidly provide a great deal of useful information.

The SPDS system should prove useful in operations. This appears to be largely due to PSE&G's involving plant operations personnel in the design process and the use of Westinghouse Emergency Operation Guidelines as a basis for the second level displays. Including operations in the design process not only helps insure that the system will be of practical value, but also should help increase user acceptance of the finished system. By helping the STA quickly assess the emergency response procedures, the SPDS should significantly reduce the time required to respond to abnormal conditions.

SECTION 3.0 SYSTEM RELIABILITY

There are several factors that determine the ultimate reliability of a computer system. These include the reliability of the hardware being used, the amount of load on the system, system security, and the reliability of the software. In addition to comprehensive quality assurance (QA) procedures, which were not reviewed by the audit team, there are two major sets of activities that influence how reliable software will be. The Verification and Validation (V & V) program not only tests the system for errors, but also checks to insure that the system design also actually does what the system was intended to do. Finally, a configuration management program insures that system modifications do not introduce undetected problems, and that clear documentation of the system and any major modifications to it are clearly documented to facilitate future software maintenance. Since the Salem SPDS was still under development, there was no way to actually measure how reliable the system actually was. All that could be done was to evaluate the approaches that PSE&G was taking to assure system reliability and to comment on their apparent adequacy.

3.1 Hardware Reliability

The relatively simple and yet sophisticated system architecture should provide high system reliability. There is complete redundancy for all major components of the system and for all dedicated serial data communications lines. For example, the primary computer (A) is constantly being monitored by the back up computer (B) via two redundant serial data links. If computer A malfunctions, computer B will automatically stop what it is doing (program development) and take over. No single failure should be able to interrupt system availability.

The entire system will also be provided with an uninterruptable power supply. In the event of loss of external power, this system will provide power until auxiliary generators can take over. This power system will be used not only for the main processors, but for the MUXs and CRTs as well.

These features should make this a highly reliable system. Verbal reports from the PSE&G computing staff indicated that since a few initial bugs were worked out of the main data highway for the LAN, there have been virtually no serious hardware problems in their development system. Software failures may be a much more significant source of system failures, but since the software is still under development, it is impossible to predict their impact.

3.2 Software Security

The primary storage media for software is magnetic disk, with magnetic tape back-up. Software security depends primarily upon the ability of the PACE operating system to limit which terminals can make modifications to software and databases. All terminals other than the programmer's console will be limited to accessing information. This applies not only to terminals hard wired to the LAN, but also to access to the system over telephone lines via a modem (as in the EOF). Any software changes or changes in terminal access status must be made at the programmer's console. The audit team did not ascertain whether or not this access was also limited by requiring passwords to perform any activities that might impact system functioning. A redundant system, requiring both physical access to a single terminal and knowledge of a series of passwords is strongly recommended.

PACE can also limit which data can be accessed by a specific terminal. This will be used to prevent SPDS terminals for one unit from displaying data from the other unit, preventing a major potential for confusion. In addition, the primary SPDS display terminal for each unit will be limited to presenting only SPDS displays. Care should be taken to insure that these features are properly implemented.

3.3 System Loading

The computer system will not be solely devoted to SPDS. PSE&G eventually plans to transfer the plant process computer's functions to this system, which will compete with SPDS for system resources. Currently the SPDS is only using about two or three percent of the CPU's capacity, providing excellent response times. Procedures will need to be established to insure that future additions and modifications do not overload system capacity or reduce SPDS response times.

3.4 Verification and Validation

PSE&G has employed Singer-Link to plan and conduct their Verification and Validation (V&V) program. The audit team reviewed the V&V plan and found that it appeared to provide a reasonable program for the areas it covered. V&V activities to date have found miscellaneous missing sections, missing format descriptions, missing functions, inconsistent point counts, and missing introductory texts. However, the system is still undergoing development, and little of the V&V program has been implemented, so it is impossible to tell if the program will be adequate in actual practice. In addition, two problems were identified with the V&V effort: there was no assessment of the basic design requirements for the SPDS, and there appear to be problems with the procedures for control and verification of system documentation.

The validation efforts were incomplete at the time of the audit. The only portion of the program that was underway was an examination of the SPDS documentation for consistency. However, the display formats are based on the Westinghouse Emergency Response status trees and the audit team found that the Westinghouse Electric Corporation has validated the status trees themselves. The PSE&G validation of the bar displays and lower level displays is in progress. In fact, most of the lower level display formats have not yet been developed. Algorithm validation efforts are not yet completed. Sensor validation has not yet been addressed by PSE&G. However, they expect to initiate a sensor validation program based on an upcoming EPRI program. Given this, it was inappropriate for the audit team to make any judgment about the eventual quality of the V&V program.

The V&V plan, as proposed, begins with the assumption that the top (or "A") level system design specification validly addresses the actual user requirements of the system. There is no plan to validate whether or not these specifications describe a system that actually will do what an SPDS should do. Since no real front end user-needs and task analysis was performed, the overall goals and objectives for the system were never clearly defined. It is impossible to judge whether the proposed system will do what it is supposed to do, since no one has clearly stated what it really should be doing. It is strongly recommended that some time and effort be spent reviewing what PSE&G feels the SPDS should be able to do for them, and clearly and concisely defining the overall system requirements. The level A system design specifications should then be evaluated to see how well they meet those system requirements.

The other problem may have more to do with configuration control than the V&V program, per se. There are four levels of documentation for the Salem SPDS. Level A is the original design specification, and is the most abstract. Level B describes the SPDS system in greater detail, while levels C and D are the actual pseudo-code software descriptions and program listings, respectively. Every time a significant change is made in one of these documents, the configuration control program is supposed to insure that all the other level documents reflect the change. At the time of the audit, V&V personnel were reviewing the documentation for such consistency, and were finding a number of fairly minor discrepancies. However, when the audit team reviewed the documentation, they found many inconsistencies, particularly between levels A and B, versus B and C. While the level C and D documentation appeared to be relatively consistent and up-to-date, levels A and B were repeatedly found to be long out-of-date with the current system. The V&V program should have uncovered these discrepancies.

3.5 Configuration Control

The audit team found that Singer-Link has been verifying algorithm descriptions, SPDS display formats, status trees, and has established configuration control procedures. The audit team could not find top-level system requirements or descriptions, current SAR descriptions, training documents, maintenance procedures and related system integration documents. Since these system integration documents could not be found, the audit team feels that configuration control methods may not be effective. A comprehensive configuration control program should include these elements, which insure that changes to the SPDS system do not adversely effect training, maintenance or operations, and vice versa. Additionally, as discussed in section 3.4 above, the audit team found many inconsistencies between the use of Level A and B versus level C and D documentation. While these inconsistencies should have been detected by the V&V program, a properly executed configuration control program should have prevented them in the first place.

SECTION 4.0 HUMAN FACTORS ENGINEERING

4.1 PSE&G Human Factors Program

General Physics Corporation has recently been employed by PSE&G to provide human factors guidance. General Physics prepared and submitted (August 8, 1985) a guideline to be used for the upcoming human factors review of the Salem SPDS. The exact date of the human factors review of the Salem SPDS is yet to be determined but is expected to begin in the Spring of 1986. Since the system design is expected to be completed before then, the PSE&G human factors program will be limited to a post hoc evaluation of existing design, with only minor human factors input during the design stages.

4.2 Display Formats

The audit team observed the existing SPDS displays on the development system at the BEST facility. In general, they displayed the key information clearly and were not overcrowded. However, there were some problems with the existing displays.

The top of each screen contained an "alarm box" which contained information about all inoperative sensors, or out-of-range values. These alarms, which are written in fairly small type, are difficult to read, add clutter to the screen, and do not seem to be necessary on every SPDS display. When asked why the alarm boxes were included (even though they were not mentioned in the system design specifications) the response was simply because "it is on all PSE&G displays." The PACE operating system makes such displays easy to implement, so it appears that little thought was given about whether or not they should be included. This type of decision may reflect the lack of a clear analysis of what the SPDS should do and exactly what information it needs to display.

There were a number of deficiencies in the use of color. Some of the colors being used were very hard to discriminate, particularly green and yellow, which were hard to distinguish at any distance from the CRT. Also, red and purple were hard to see against a black background. Red and yellow, which are used to indicate different alarm levels, should not be used in any other way, such as for axis labels. On some graphs, red was used to indicate limits. This should only be done when the limit indicated on the graph is the same as the limit that turns the SPDS alarm box red.

The use of abbreviations was inconsistent in several places. For example, ^{o}F and DEG are both used at different places in the SPDS displays. Care should be taken to ensure that all nomenclature and abbreviations are consistent within the SPDS, and with the control room as a whole.

4.3 Position in the Control Room

No SPDS hardware has been installed at either of the Salem plants. Current plans are to have two CRT displays in each of the two Salem plant control rooms. One display will be a 21" CRT and will be positioned on the panel, in view of the operators, but outside of the control "U." A 19" display will be located at the operator's desk within the envelope of the control "U." Four CRTs are planned for the TSC, and two for the EOF.

As the Salem control rooms are small by comparison to most large nuclear power stations, the large CRT should be visible from within the "U." The plant STA said that he will roam and should spend some of his time in the vicinity of the large CRT. He anticipated no problems because of location. The NUREG-0700 survey of SPDS and control room glare have not yet been evaluated. The glare portion of the DCRDR has yet to be completed. It is possible that glare will make viewing the large CRT difficult. Since the audit team could not see installed displays, it is impossible to judge whether there are any problems with their location.

4.4 Human Factors Engineering Review

The lack of ongoing human factors input in the SPDS design process appears to be a potential problem. Most of the problems discussed above could have been avoided with appropriate human factors input. It is generally much easier, less expensive, and more productive to involve personnel with human factors expertise before the design is firmly established than to wait until the system is finished and then have to modify the system to solve human factors deficiencies.

5.0 TRAINING PROGRAM

The training plan has not yet been developed for the Salem SPDS. The audit team could not find any interfacing between the SPDS design group and the licensee's training personnel.

6.0 AUDIT FINDINGS

The Salem SPDS is currently being designed, the third and fourth level displays are incomplete, a seventh safety function is anticipated, and only limited laboratory testing has been performed; therefore the audit findings are presented as comments and recommendations rather than conclusions.

6.1 Major Comments

Even though the state of the software development for the SPDS is too premature to allow the evaluation of many specific details, the audit team did identify some general concerns about the program. These deal with the way PSE&G is approaching the development of the SPDS more than with specifics of their chosen design. Like many other utilities engaged in a major computer hardware/software system development project, PSE&G seems to be concentrating resources on developing hardware and software, and providing only minimal efforts to insure that the system be integrated into plant operations, maintenance and training.

6.1.1 Insufficient Front-End Analysis

It was not clear to the audit team exactly how and why PSE&G decided on the basic design for the SPDS. There was no clear statement of the overall system requirements and goals for the SPDS. Developing such a design concept will provide direction, focus, and a set of design priorities for the project. Without such a guideline, it is difficult to perform effective system reviews and system verification.

Developing an overall design concept requires a thorough user needs analysis and extensive operator input. The decision to base the second level displays on the Emergency Response trees appears to have been directly due to an operator's suggestion. Such operator involvement will help insure the system will actually be useful and accepted by the operators. However, soliciting operator suggestions alone can not replace a thorough user-needs analysis.

The V&V plan begins with the assumption that the top (or "A") level system design specification validly addresses the actual user requirements of the system. There is no plan to validate whether or not these specifications describe a system that actually will do what an SPDS should do. Since no real front-end user needs and task analysis was performed, the overall goals and objectives for the system were never clearly defined. It is impossible to judge whether the proposed system will do what it is supposed to do, since no one has clearly stated what it really should be doing. It is strongly recommended that some time and effort be spent reviewing what PSE&G feels the SPDS should be able to do for them, and clearly and concisely writing this down in the form of a brief (a few pages) statement of goals for the SPDS. The level A system design specifications should then be evaluated to see how well they meet those objectives. The task analysis performed as a part of DCRDR if revisited could assist in reviewing and documenting user needs.

6.1.2 V&V and Human Factors Review

It is generally inefficient to conduct V&V and Human Factors reviews after the design has been decided upon and developed. These reviews will almost always reveal some problems that need to be addressed (costing additional time and effort) which could have been avoided if they were identified early in the design cycle. In addition, V&V and Human Factors reviewers are often reluctant to question any fundamental design decisions of a system presented to them as a <u>fate accompli</u>, realizing the cost of major changes to a system.

6.1.3 Inadequate Configuration Management

Given the complexity of the system, maintaining high-quality documentation and insuring that the system will be properly integrated with plant operations, maintenance and training is a big job. As mentioned earlier, a number of inconsistencies were found in the level A and B system documentation. While the programming staff were keeping the detailed level C and D documentation accurate, other documentation was not being updated. While some records (non-conformance reports) were being kept on system modifications, they were not sufficiently detailed to permit some future programmer to reconstruct the changes that were made. This may not be a major problem now, while the original programmers are available, but will be critical five or ten years from now. Finally, there did not appear to be any real program established for integrating the SPDS with the rest of the plant. The SPDS, and any future changes made to it, will effect plant operations, maintenance, and training. Conversely, changes in these areas may also effect the SPDS. A plan needs to be developed to provide proper configuration management and integration with other plant activities.

6.2 Recommendations

In order to assure that the Salem SPDS fulfills its purpose, the audit team recommends that the following items be considered, revisited, or conducted.

- Perform an SPDS systems integration review and define the overall system requirements. Include plant engineering, headquarters engineering, licensing, human factors representatives, training, maintenance, configuration control, QA, procedures and testing personnel, and operations personnel. Verify that the input and needs of each discipline have been addressed.

- Complete the SPDS design activities before installation. This will require either increased design efforts or a postponement of installation.

- Ensure that the Validation and Verification activities are consistent with the systems integration review and address all system requirements.

- Resolve the inconsistencies between the levels A, B, C, and D documentation.

- Develop and execute a comprehensive installation and testing plan for the SPDS.

- Improve Salem configuration control requirements to address the SPDS.

- Revise SAR submittals on the SPDS to reflect the additional function block, including parameters and the most recent design changes and provide the electrical isolation test results.

- Develop SPDS security procedures to prevent unauthorized access.

- Develop a process which will insure SPDS priority in the plant process computer.

- Examine the use of color, discriminability and consistency in coding in the SPDS displays. Check for consistency in SPDS abbreviations.

- Perform complete system validation including validation testing prior to declaring the system operational.

- Develop a comprehensive SPDS training program during the current design phase.

- The SPDS implementation schedule should be carefully reviewed.

- Evaluate the appropriate display level for presenting actual tabular parameter data.

- At least one more NRC SPDS audit should be performed.

APPENDIX A

COMPLIANCE WITH REQUIREMENTS OF NUREG-0737, SUPPLEMENT 1

APPENDIX A

Compliance Requirements of NUREG-0737, Supplement 1

Requirement 1: Concise, Continuous Display

The Salem SPDS is developed from the Westinghouse Emergency Response Guidelines status trees and is designed to assist the STA and, secondarily, the Shift Supervisor, during the recovery from an emergency condition. There will be two CRT displays in each control room which administratively are capable of showing the SPDS top level display at all times. The top level display shows the critical safety functions in the form of color coded bar graphs for the 6 functions as defined by PSE&G. The functions are shutdown margin, core cooling, heat sink, thermal shock, containment environment and coolant inventory. The correspondence between these functions and the critical safety functions as defined by NUREG-0737 Supplement 1 are shown in Table 2-1, which also shows the parameters selected to portray the functions.

The format for the second level displays is taken directly from the Emergency Operating Procedures as developed by PSE&G from the Westinghouse EPGs. This was a "given" in the design and not a format developed through human factors analysis. The second level also contains an insert which shows the color coded bar graphs from the top level display (without the displacement in the vertical direction). This would show any changes in other critical safety functions which might occur while the STA is using a status tree second level display within a given critical safety function. The third and fourth level displays have not been finalized. However, the third level will show the parameter values and condition in a tabular format for those parameters which define the second level status tree in use. The fourth level will present trend information. PSE&G should evaluate the appropriate level to present tabular parameter information.

It appears that the SPDS will provide the operators with a concise display of critical plant variables to aid them in rapidly and reliably determining the safety status of the plant. As the operators had a say in the selection of the format, it will probably be accepted and used by them when it is implemented.

Requirement 2: Convenient Location

Two CRT displays will be located in each of the Salem plant control rooms. One display will be a 21" CRT and will be positioned on the vertical panel; the other is a 19" display and will be located at the operators desk within the envelope of the control "U." As the Salem control rooms are small by comparison to most large nuclear power stations, the large CRT should be visible from within the "U." The plant STA said that he will roam and should spend some of his time in the vicinity of the large CRT. He anticipated no problems because of location. The NUREG-0700 survey of control room glare has not been evaluated for the SPDS. The glare portion of the DCRDR has yet to be accomplished, and it is possible that this will turn out to make viewing the large CRT difficult. If so, this will be addressed as a part of that effort. Four CRTs are planned for the TSC, and two for the EOF.

If the glare and lighting studies conducted in the DCRDR show that there is no problem with the SPDS displays as presently planned, their location should provide the operators with a convenient location from which to observe the critical safety functions.

Requirement 3: Incorporation of Human Factors Principles

In its original procurement specification, PSE&G invoked the then current Human Factors design guidance. However, the original system's contractor defaulted and Salem took over design control. By this time, the basic hardware and design approaches had been selected. There has been no meaningful Human Factors analysis incorporated in the design to date other than some attention being paid to the location of the CRTs in the control room.

PSE&G has contracted with General Physics to do the Human Factors review of the system. General Physics has produced a criteria document to quantify the guidance in NUREG-0700 and NUREG-0835, but their present intent is to review the design after-the-fact rather than to work with the design staff to prevent problems before they occur.

The overall lack of an integrated Human Factors engineering effort to date was illustrated by the inclusion of an "alarm box" on the top level display because it "is on all PSE&G CRT displays" and taking the second level displays exactly as formatted in the EOPs without any analysis. Other Human Engineering Deficiencies noted by other members of the team included poor color contrast between green and yellow on the top level display and some cluttered presentations.

Requirement 4: Procedures

The Salem SPDS provides an excellent method of integrating the use of the display with the implementation of the EOPs. During an abnormal event or an emergency, the plant operators proceed to carry out the EOPs which are entered by "any Trip." The prime function of the STA, who is the principal user of the SPDS, is to follow the status trees which lead to the implementation of functional restoration procedures if the operator actions are not accomplishing the job. As the SPDS secondary displays are the status trees, this effectively automates this operation for the STA, giving him instant information with some indication of parameter validity and other displays to further analyze the condition of the plant.

Requirement 5: Training for Accident Response With and Without SPDS

A training plan is yet to be developed for the Salem SPDS. While design of the system is not yet complete, the lack of an overall program plan for the SPDS was indicated by the concentration on the design aspects of the SPDS requirement rather than the "big picture" requirements analyses and planning phases which should have identified the requirements for training as well as design V&V, security.

Requirement 6: Parameter Selection

The basis for the selection of parameters for the Salem SPDS is the EOP status trees. Table 2-1, mentioned above, indicates those parameters selected and their relation to both the Salem-defined critical safety functions and the NUREG-0737, Supplement 1 critical safety functions. At the present time this comprises 19 parameters with about 140 values. The table reflects the proposed seven function blocks.

The audit team made the following comments with regard to Salem parameter selection:

1. Containment isolation closures are not included in the display. Containment closure status is, however, shown on a lighted back panel display which is close to the 25" CRT and easily visible to the operators and the STA. This is probably a satisfactory method of presenting containment isolation status. However, if the lighted back panel is ever relocated such that it is not easily visible to the operator, then the containment isolation closure status will be required in the SPDS.

2. RHR/ECCS flow is not included. This is valuable to give an indication of core cooling when steam generators are isolated.

3. Hydrogen concentration is not included. The reason for this was the standard "not required by the status trees" plus the argument that it is a parameter required late in the game when things happen more slowly, and because it is available on the boards.

The audit team recommends that these parameters be added.

Requirement 7: Electrical/Electronic Isolation

The licensee presented a description of an electrical/electronic isolation scheme which, if documented and tested as described, should fulfill the requirements for isolation. However, no test or design data was presented to the audit team by PSE&G. The licensee indicated that this information would be forwarded to the NRC.

Class 1E and non-class 1E signals are separated and processed by different multiplexers. Cards in the multiplexers provide optical and transformer isolation. Fiber optic signal transmission provides isolation between the multiplexers and the data concentrators.

Verification and Validation

The licensee has initiated a verification and validation program for the SPDS. The validation efforts were incomplete at the time of the audit. The NRC audit had some difficulty locating the top level system design specifications. The display formats are based on Westinghouse Emergency Response status trees and were validated by Westinghouse. SPDS algorithm validation efforts are currently under way and therefore were not evaluated by the NRC audit team. Sensor validation has not yet been addressed.

APPENDIX B

INTRODUCTION

* SPDS OVERVIEW

* SYSTEM TECHNICAL OVERVIEW

* DISPLAYS

* PARAMETER SELECTION

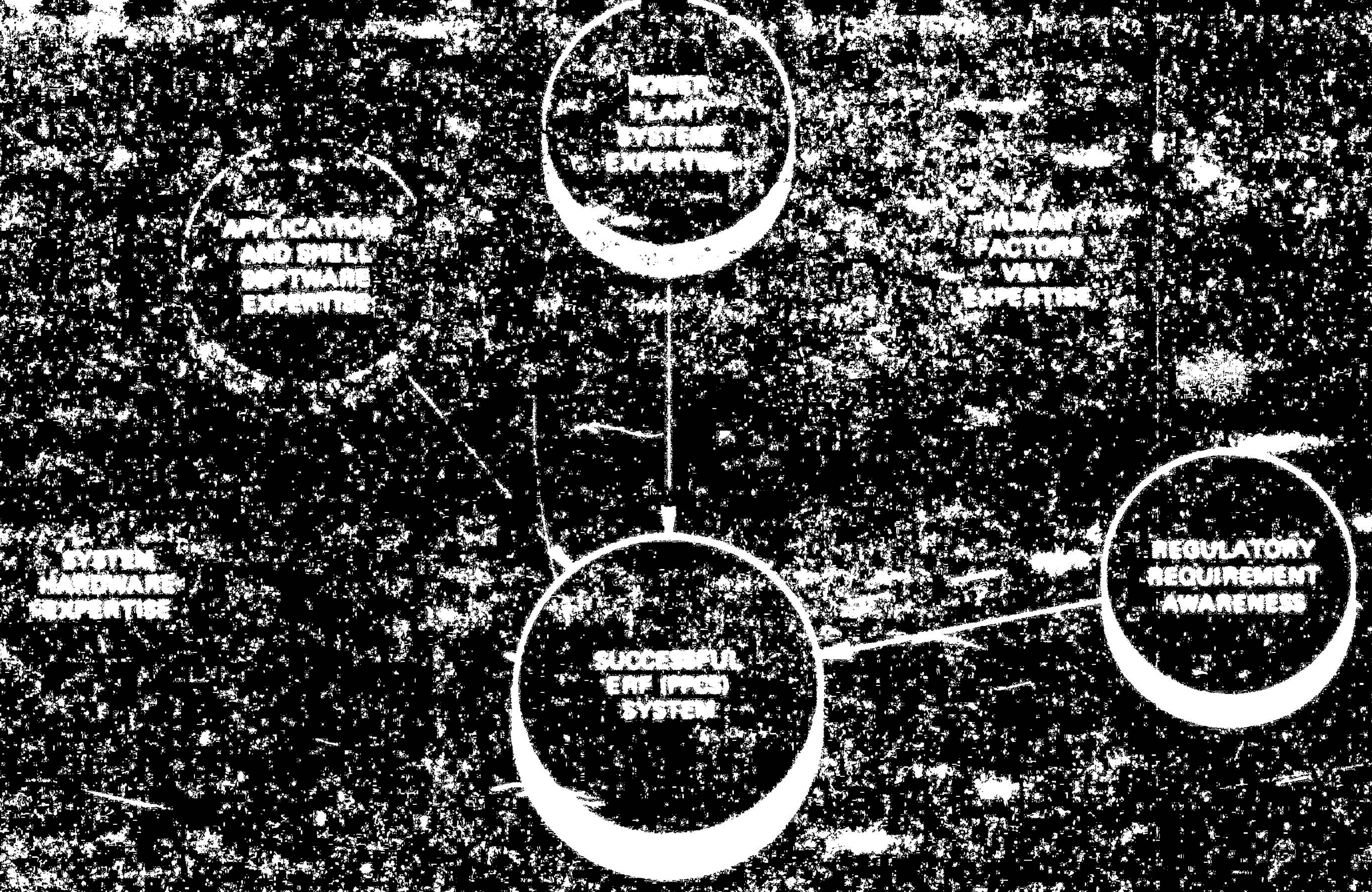
* DATA VALIDATION

* HUMAN FACTORS

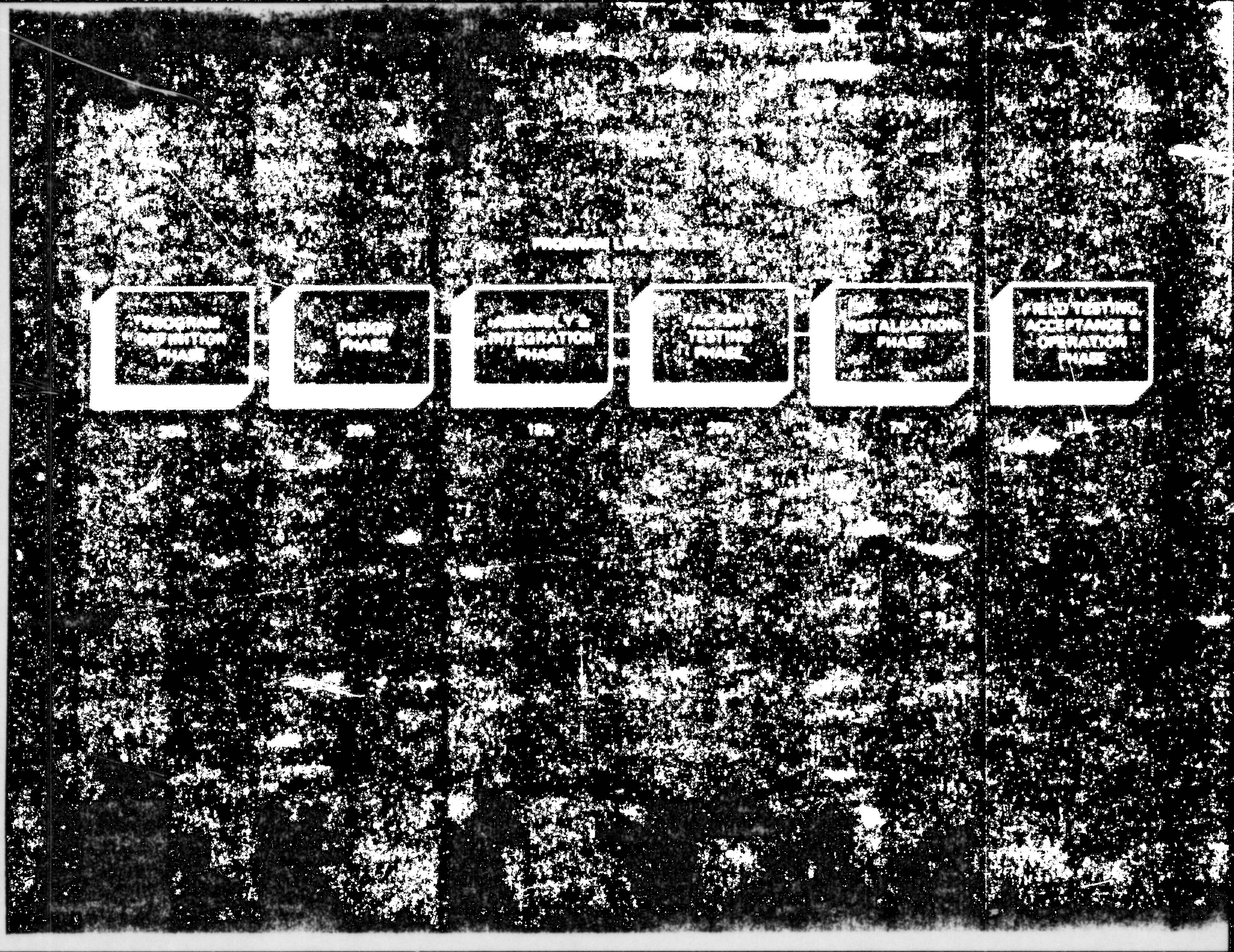
* VERIFICATION & VALIDATION

* OPERATIONAL TESTING

PRESS RETURN KEY TO CONTINUE.


POWER PLANT SYSTEMS EXPERTISE
APPLICATIONS AND SHELL SOFTWARE EXPERTISE
HUMAN FACTORS V&V EXPERTISE
SYSTEM HARDWARE EXPERTISE
SUCCESSFUL EMF (PPCS) SYSTEM
REGULATORY REQUIREMENT AWARENESS

EMF (PPCS) Design Requirements



PROGRAM LIFE CYCLE

PROGRAM DEFINITION PHASE

20%

DESIGN PHASE

30%

ASSEMBLY & INTEGRATION PHASE

15%

FACTORY TESTING PHASE

20%

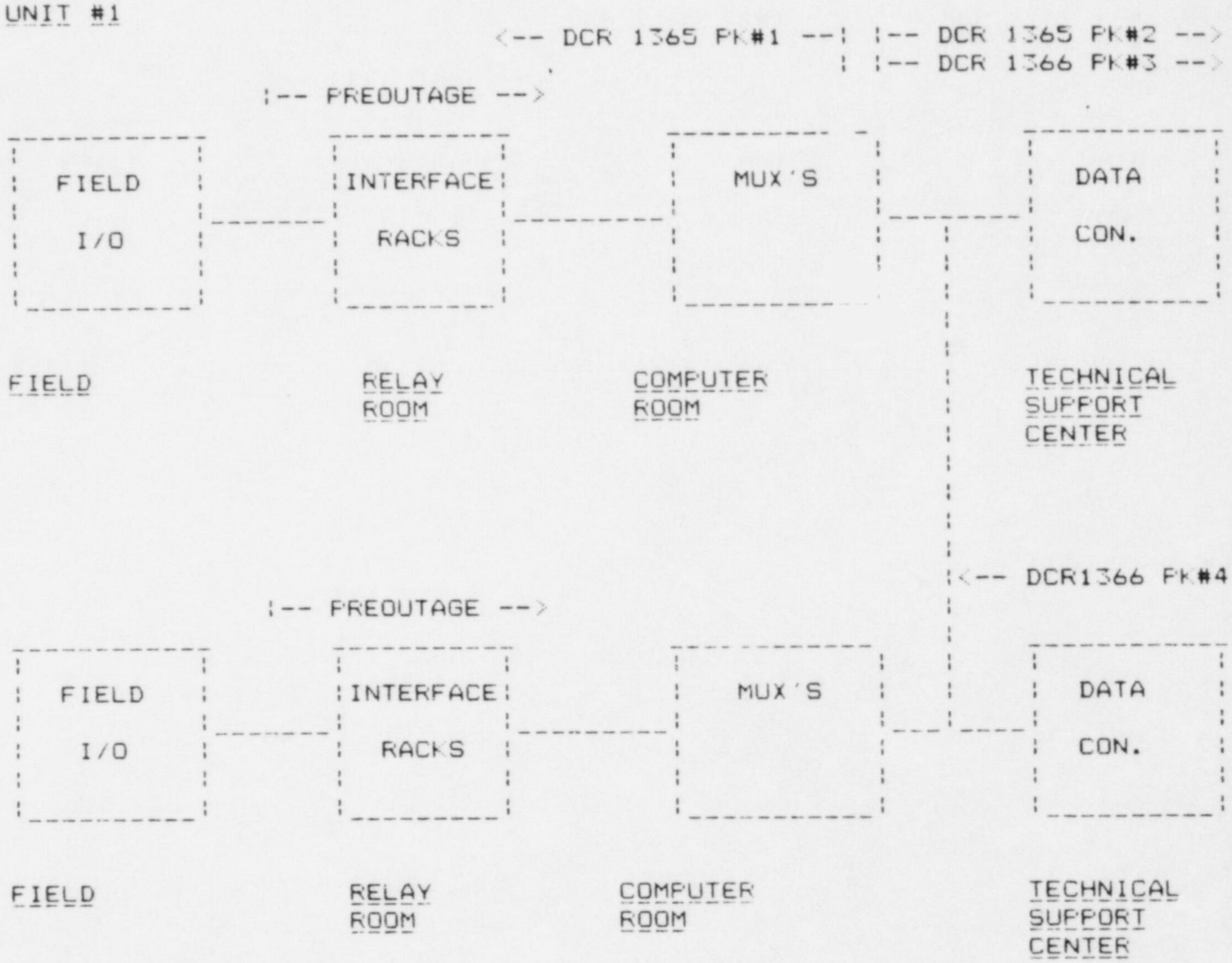
INSTALLATION PHASE

7%

FIELD TESTING, ACCEPTANCE & OPERATION PHASE

[illegible]

DCR PACKAGE PHASING



UNIT #1

<-- DCR 1365 PK#1 --| |-- DCR 1365 PK#2 -->

| |-- DCR 1366 PK#3 -->

|-- PREOUTAGE -->

FIELD I/O

INTERFACE RACKS

MUX'S

DATA CON.

FIELD

RELAY ROOM

COMPUTER ROOM

TECHNICAL SUPPORT CENTER

|<-- DCR1366 PK#4

|-- PREOUTAGE -->

FIELD I/O

INTERFACE RACKS

MUX'S

DATA CON.

FIELD

RELAY ROOM

COMPUTER ROOM

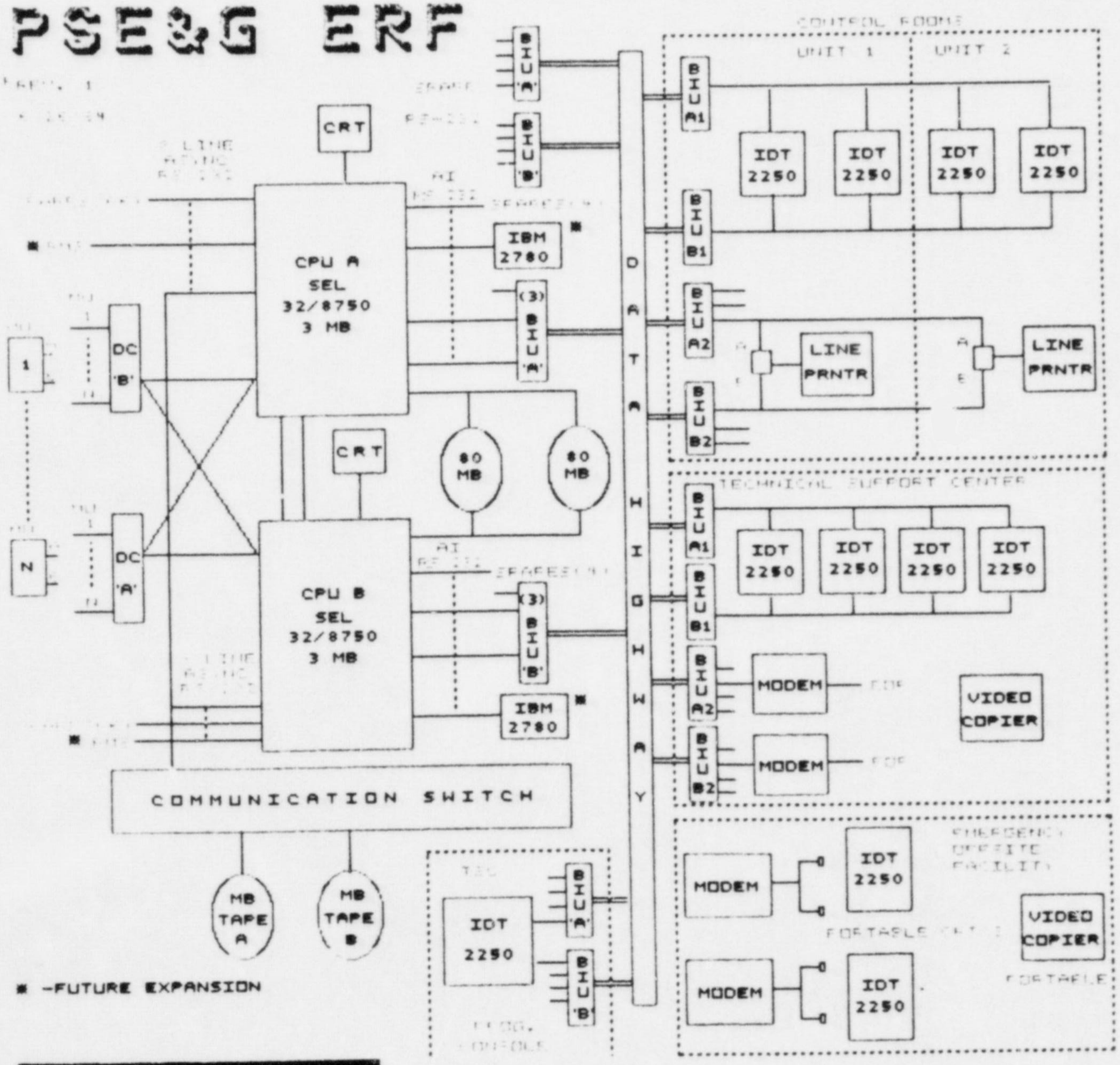
TECHNICAL SUPPORT CENTER

NOTE:

THE FOLLOWING ITEMS ARE FOR OUTAGE WORK ONLY
FIELD TERMINATIONS
TESTING
CONTROL ROOM

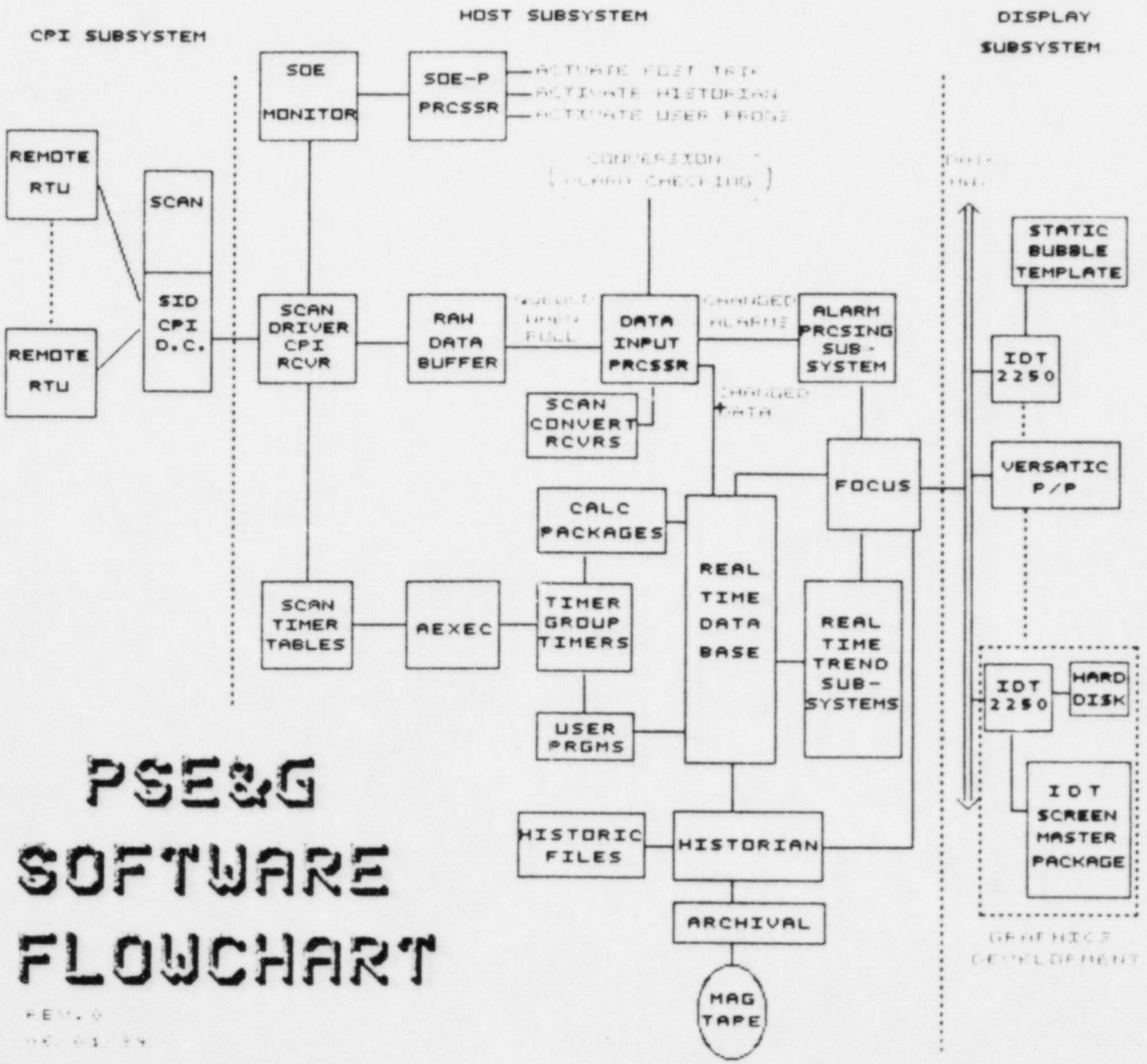
PSE&G ERF

REV. 1



■ -FUTURE EXPANSION

[redacted]

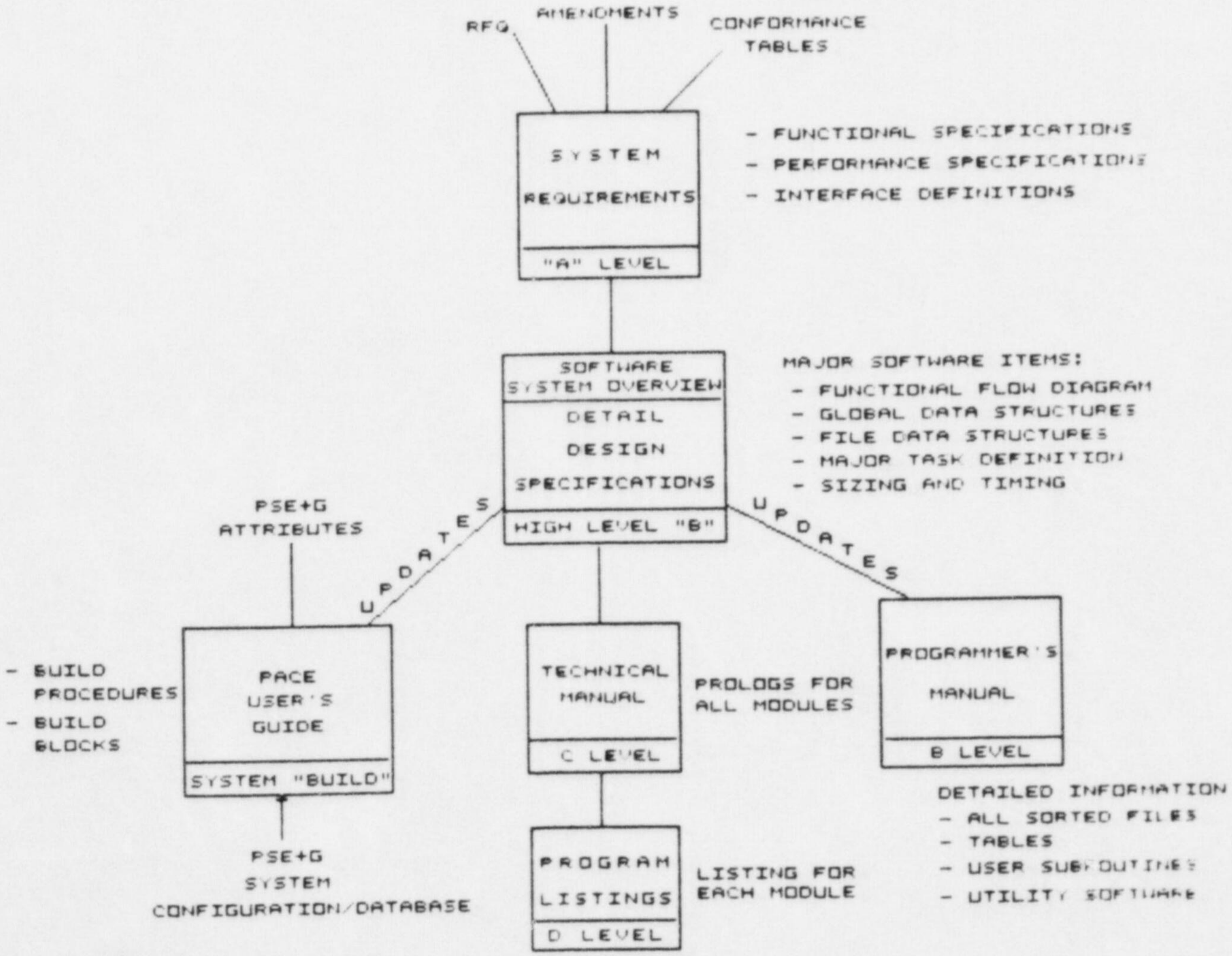


PSE&G SOFTWARE FLOWCHART

REV. 0
[illegible]

PSE&G SOFTWARE DOCUMENTATION TREE

06-21/89
REV. 0



RFQ

AMENDMENTS

CONFORMANCE TABLES

SYSTEM REQUIREMENTS

"A" LEVEL

- FUNCTIONAL SPECIFICATIONS
- PERFORMANCE SPECIFICATIONS
- INTERFACE DEFINITIONS

SOFTWARE SYSTEM OVERVIEW

DETAIL DESIGN SPECIFICATIONS

HIGH LEVEL "B"

MAJOR SOFTWARE ITEMS:

- FUNCTIONAL FLOW DIAGRAM
- GLOBAL DATA STRUCTURES
- FILE DATA STRUCTURES
- MAJOR TASK DEFINITION
- SIZING AND TIMING

UPDATES

UPDATES

PSE+G ATTRIBUTES

- BUILD PROCEDURES
- BUILD BLOCKS

PACE USER'S GUIDE

SYSTEM "BUILD"

PSE+G SYSTEM CONFIGURATION/DATABASE

TECHNICAL MANUAL

C LEVEL

PROLOGS FOR ALL MODULES

PROGRAM LISTINGS

D LEVEL

LISTING FOR EACH MODULE

PROGRAMMER'S MANUAL

B LEVEL

DETAILED INFORMATION

- ALL SORTED FILES
- TABLES
- USER SUBROUTINES
- UTILITY SOFTWARE

[redacted]

PSE&G ERS

OPERATOR INTERFACE SYSTEM

DESIGN CRITERIA

- o HIERARCHICAL DISPLAY ORIENTATION
- o MINIMAL USE OF TEXTUAL DISPLAYS
- o MINIMAL OPERATOR ENTRY REQUIREMENTS (KEYSTROKES)
- o MAXIMUM USE OF COLOR, FLASH TO INDICATE PLANT CONDITIONS
- o MAXIMUM USE OF PROMPTING
- o MULTIPLE METHODS OF MOVEMENT FROM DISPLAY TO DISPLAY
- o DISPLAY CONTENT FLEXIBILITY
- o USER CAPABILITY OF DISPLAY EDITING

SUMMARY

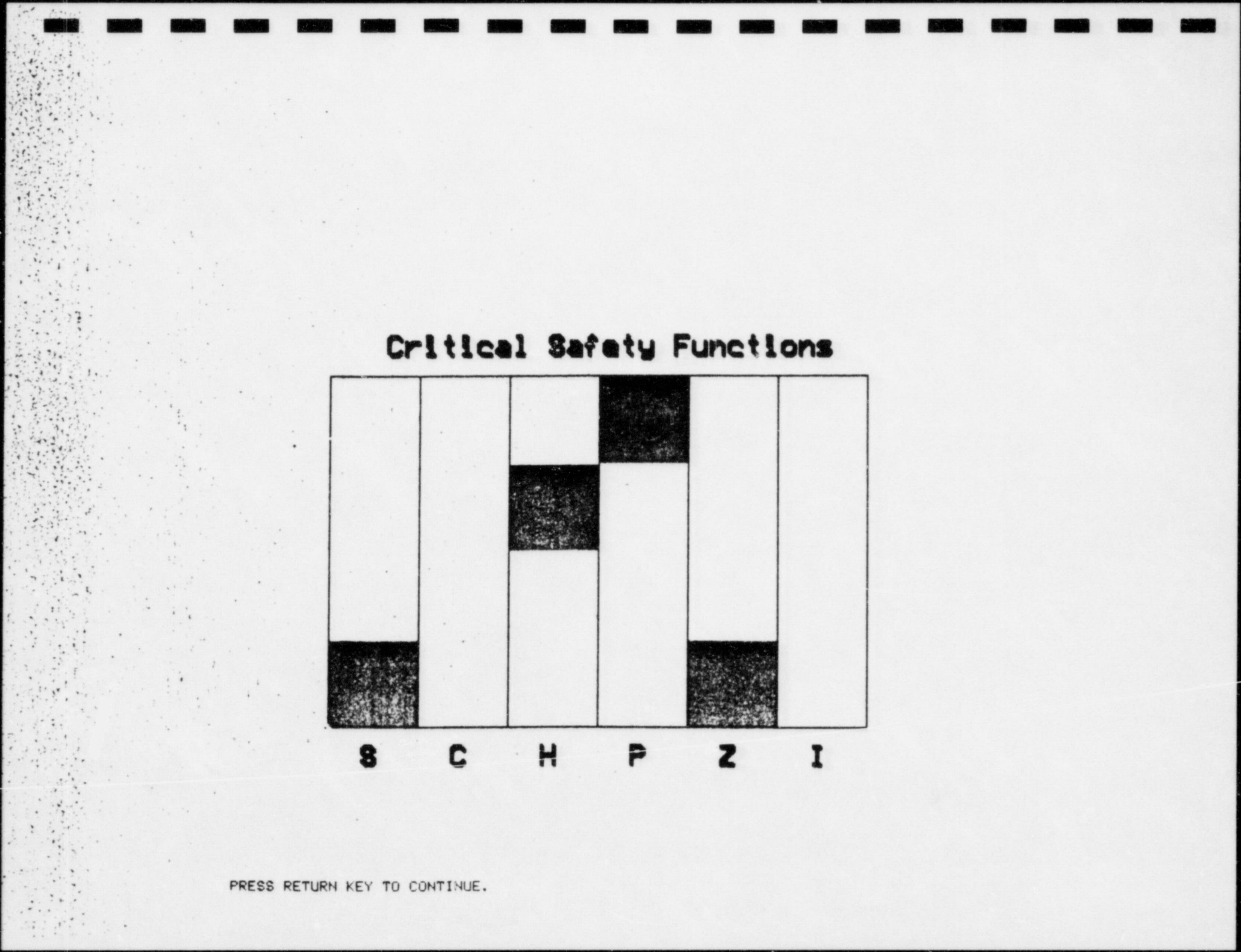
OIS IS DESIGNED TO PROVIDE THE OPERATOR WITH <u>ACCURATE</u> AND TIMELY INFORMATION ON THE CONDITION OF THE PLANT IN A FORM ALLOWING <u>RAPID PERCEPTION OF CHANGES</u> IN PLANT CONDITIONS.

PSE&G ERS

OPERATOR INTERFACE SYSTEM

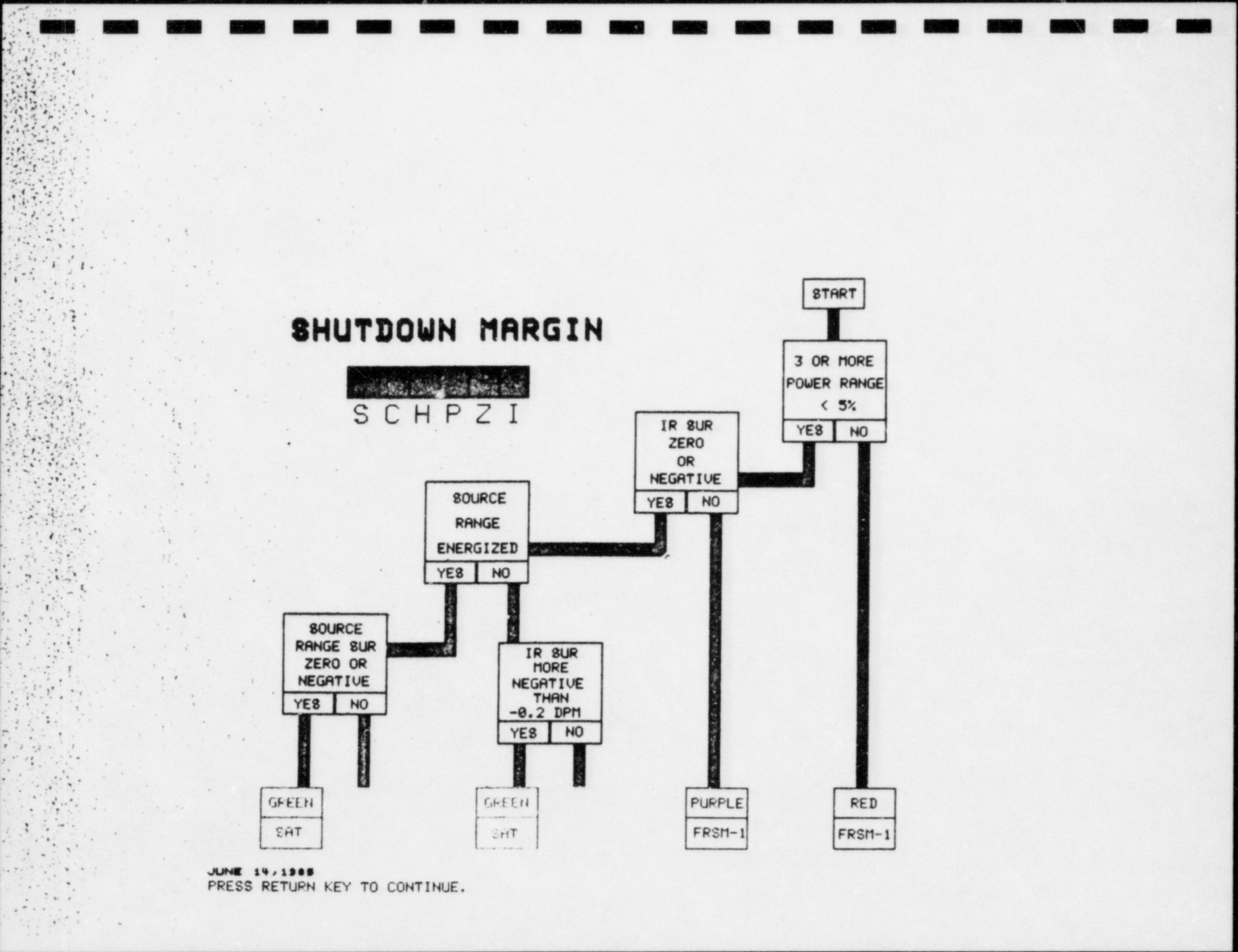
SYSTEM S/W ARCHITECTURE

- o Shell Architecture Supports Full Host Driven OIS as well as Host/Intelligent Terminal OIS
- o Host Functions in PSE&G Configuration Include:
  - Distribution of Dynamic Data to Intelligent Terminals on Scheduled Basis
  - Support of Asynchronous Intelligent Terminal Requests for Data
  - Maintenance of Master Copies (on Disk) of Static Templates
  - Linking and Distribution of New Displays/Edited Displays to Intelligent Terminals
- o Intelligent Terminal Functions Include:
  - Keyboard Service Functions;
  - Storage (local) of Static Portions of Displays;
  - Interactive Display Editing (Special Terminal);
  - Screen Generation Utilizing Terminal Capabilities.



Critical Safety Functions

PRESS RETURN KEY TO CONTINUE.



SHUTDOWN MARGIN

[redacted]

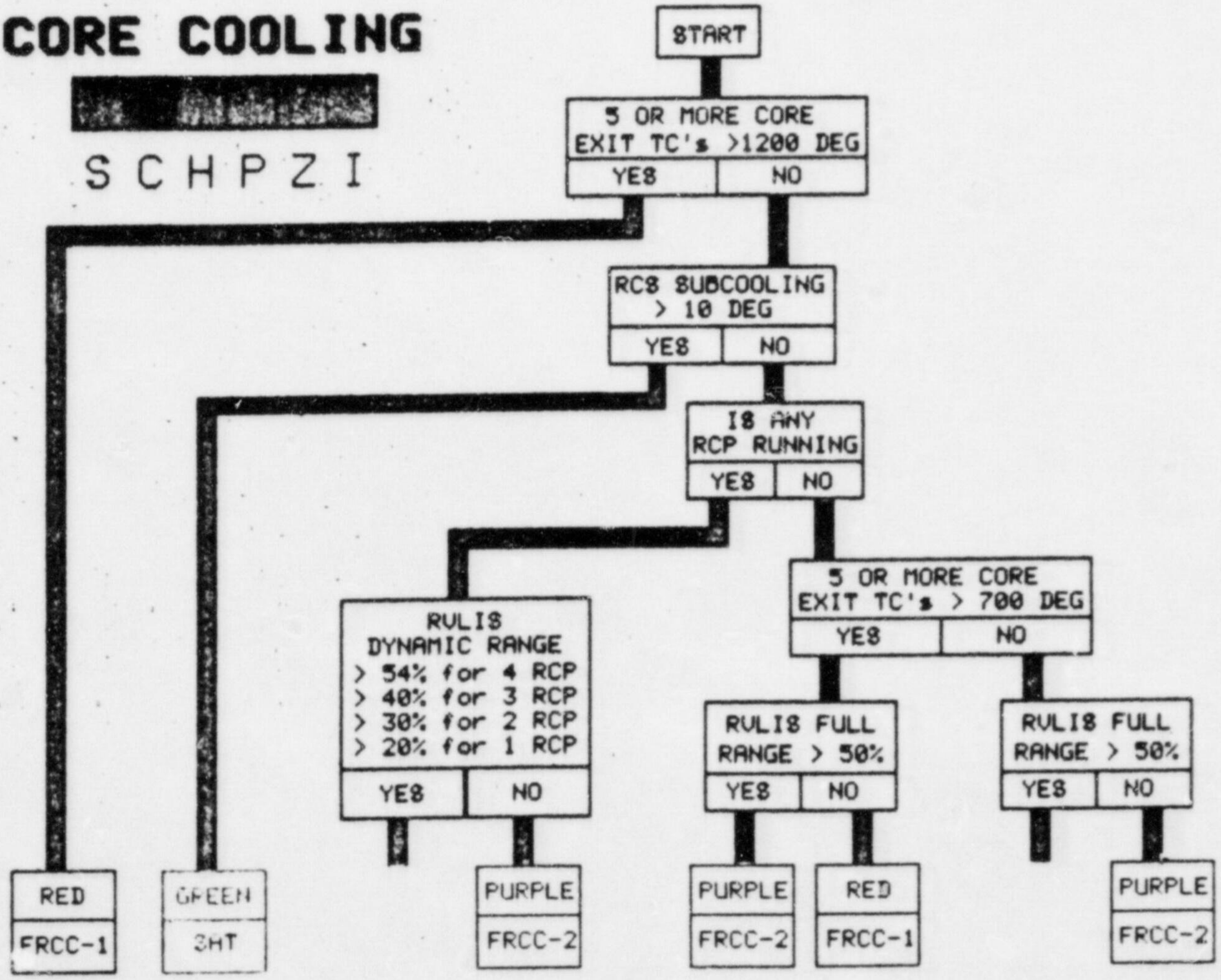
SCHPZI

JUNE 14,1985

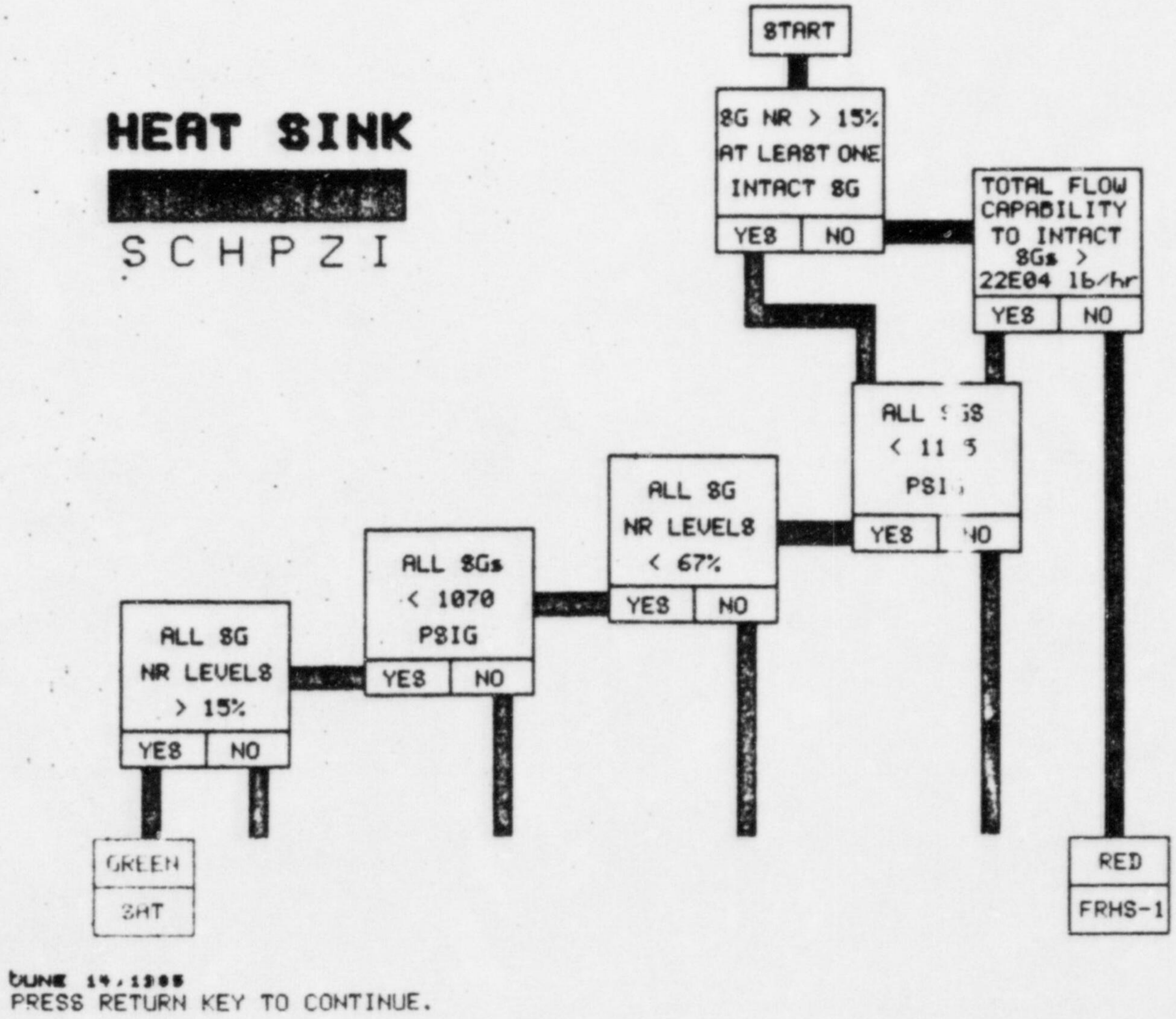
PRESS RETURN KEY TO CONTINUE.

CORE COOLING

S C H P Z I



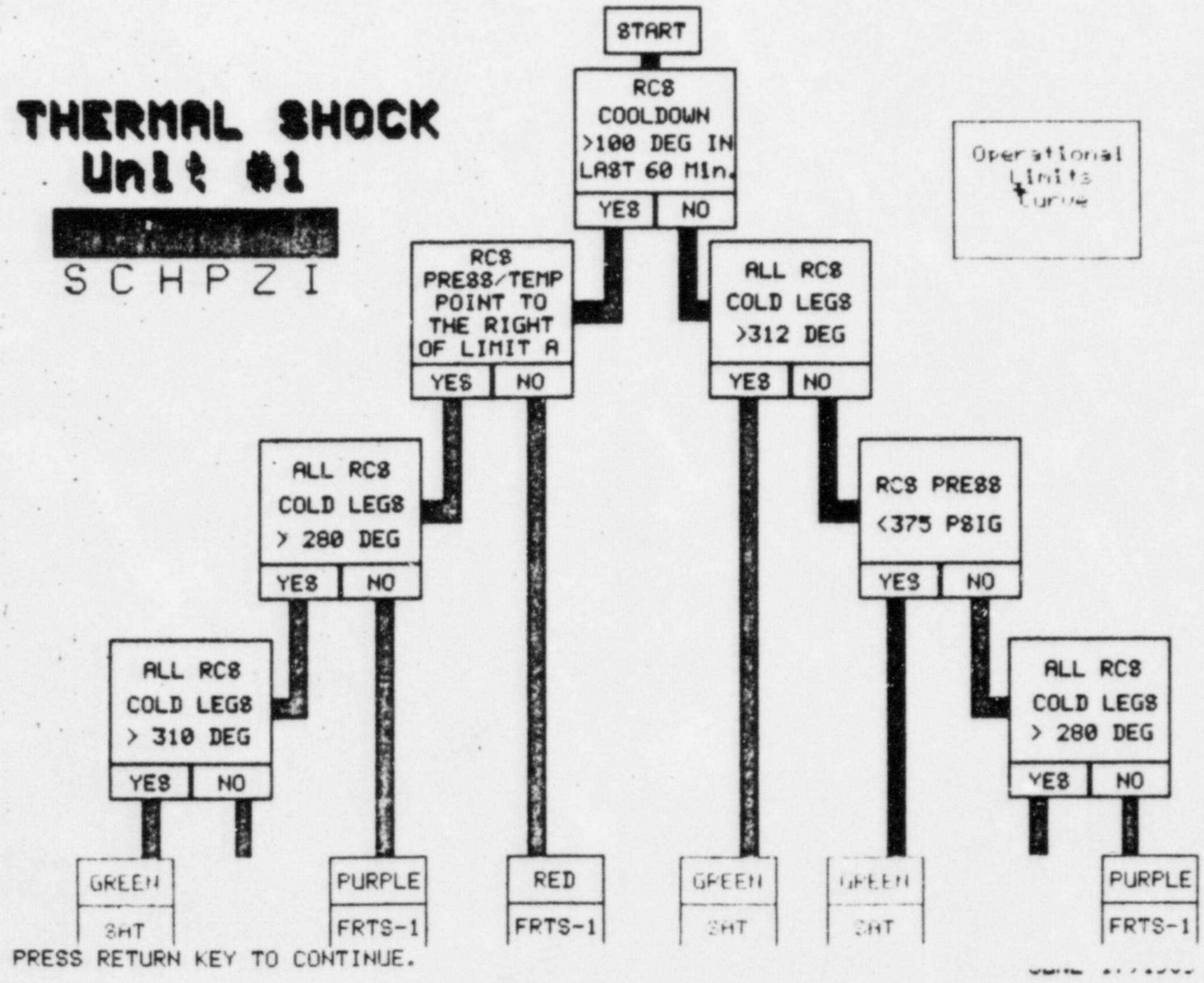
JUNE 18,1985



HEAT SINK

SCHPZI

JUNE 19,1985
PRESS RETURN KEY TO CONTINUE.



THERMAL SHOCK
Unit #1

[redacted]

S C H P Z I

START

RCS COOLDOWN >100 DEG IN LAST 60 Min.
YES NO

RCS PRESS/TEMP POINT TO THE RIGHT OF LIMIT A
YES NO

ALL RCS COLD LEGS >312 DEG
YES NO

Operational Limits Curve

ALL RCS COLD LEGS > 280 DEG
YES NO

RCS PRESS <375 PSIG
YES NO

ALL RCS COLD LEGS > 310 DEG
YES NO

ALL RCS COLD LEGS > 280 DEG
YES NO

GREEN
SAT

PURPLE
FRTS-1

RED
FRTS-1

GREEN
SAT

GREEN
SAT

PURPLE
FRTS-1

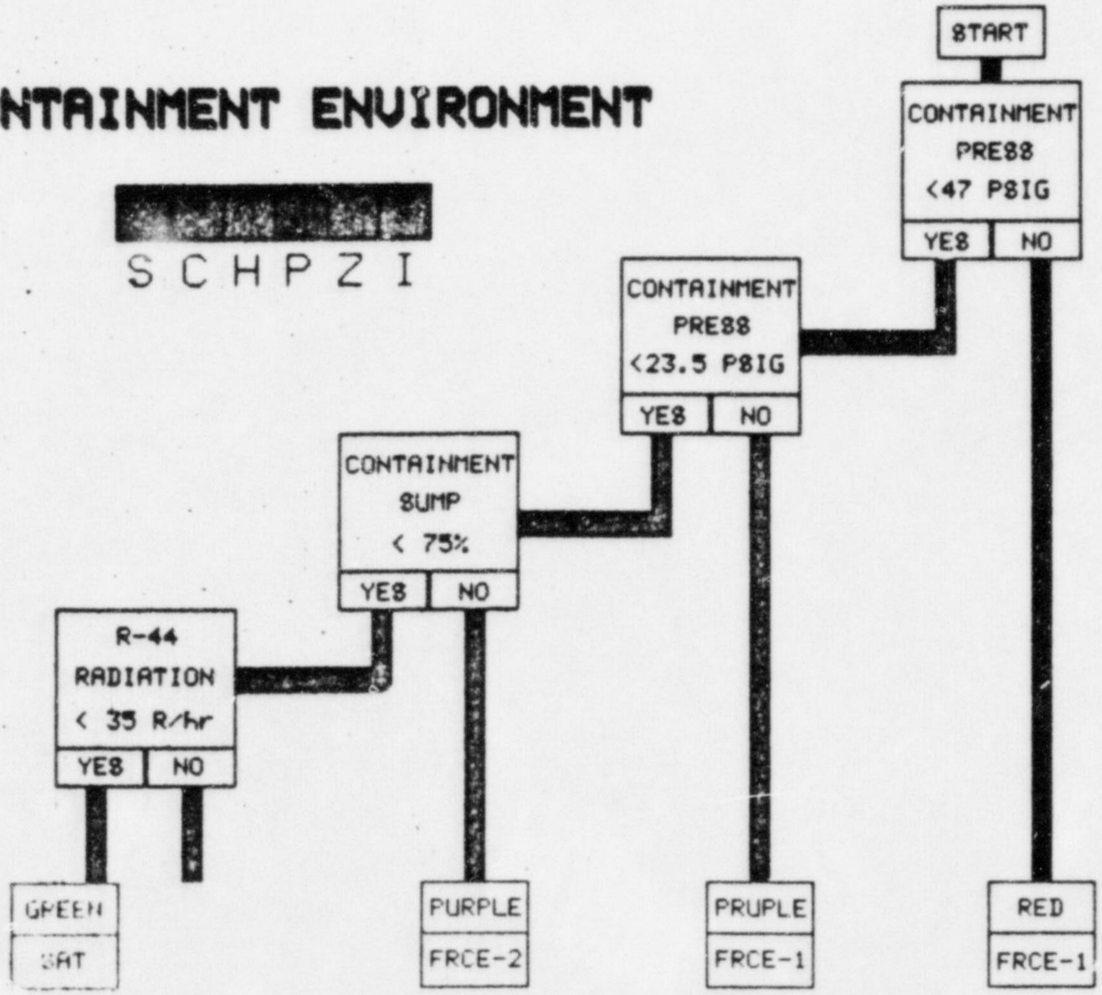
PRESS RETURN KEY TO CONTINUE.

[illegible]

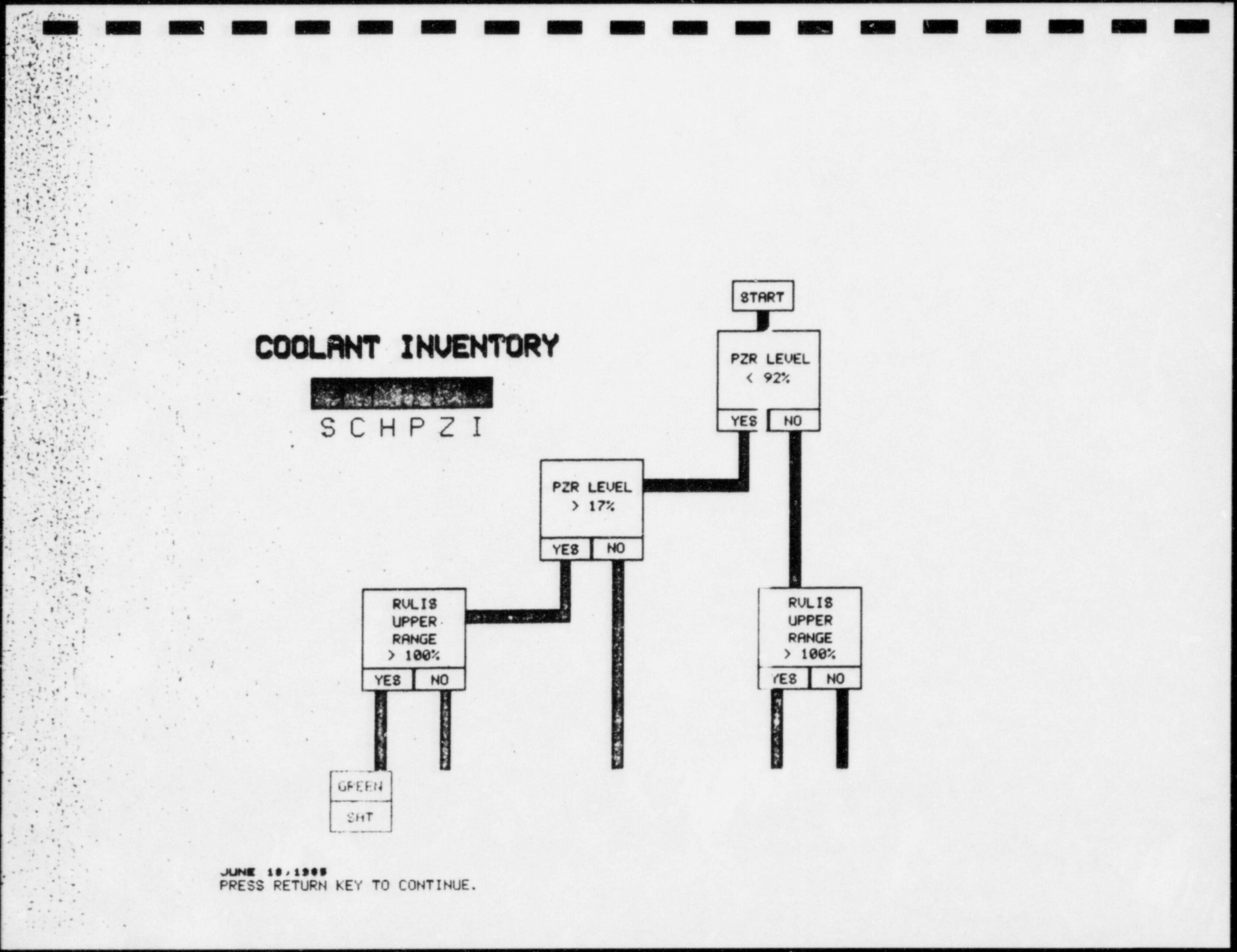
CONTAINMENT ENVIRONMENT

[redacted]

S C H P Z I



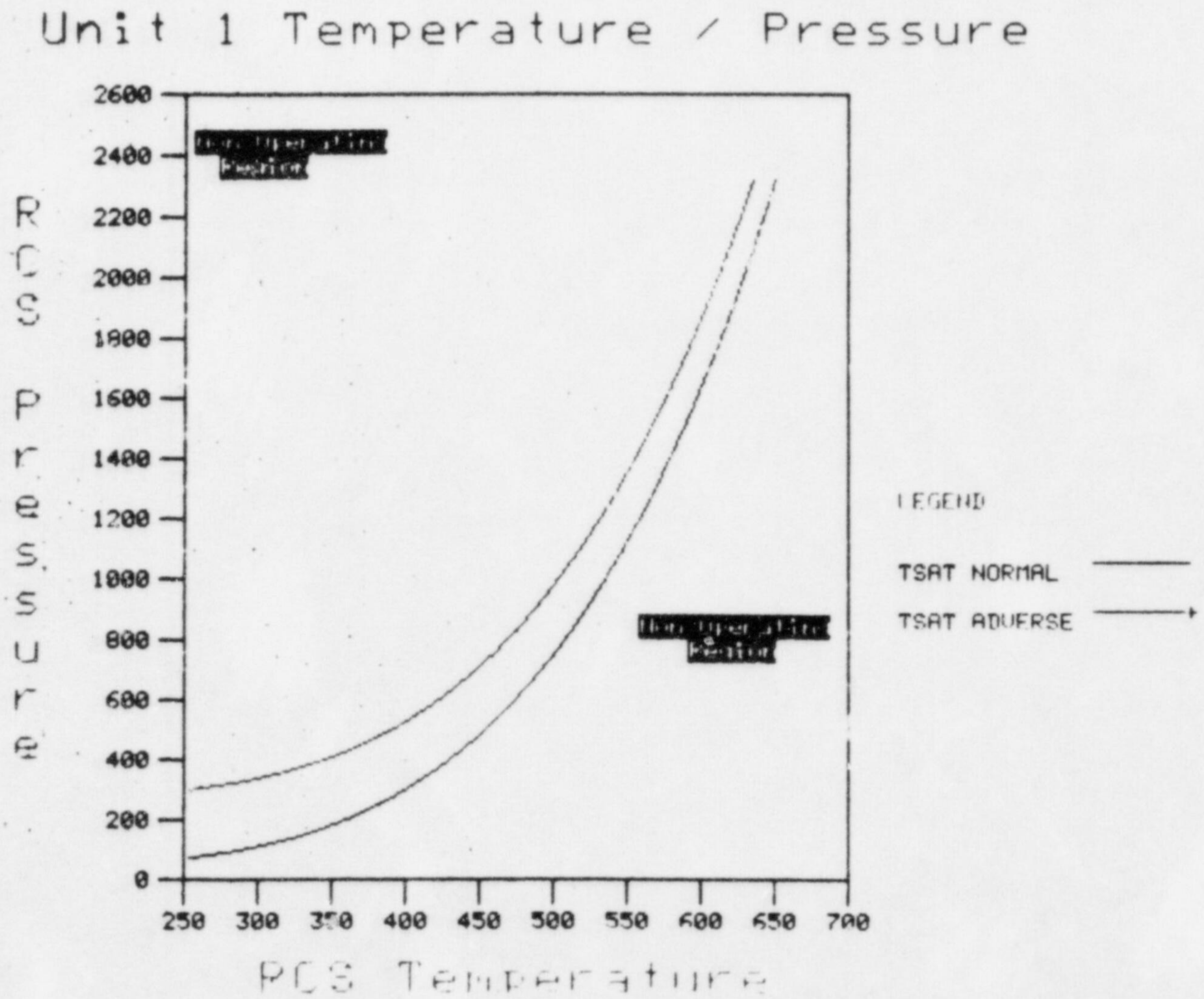
JUNE 17,1985
PRESS RETURN KEY TO CONTINUE.



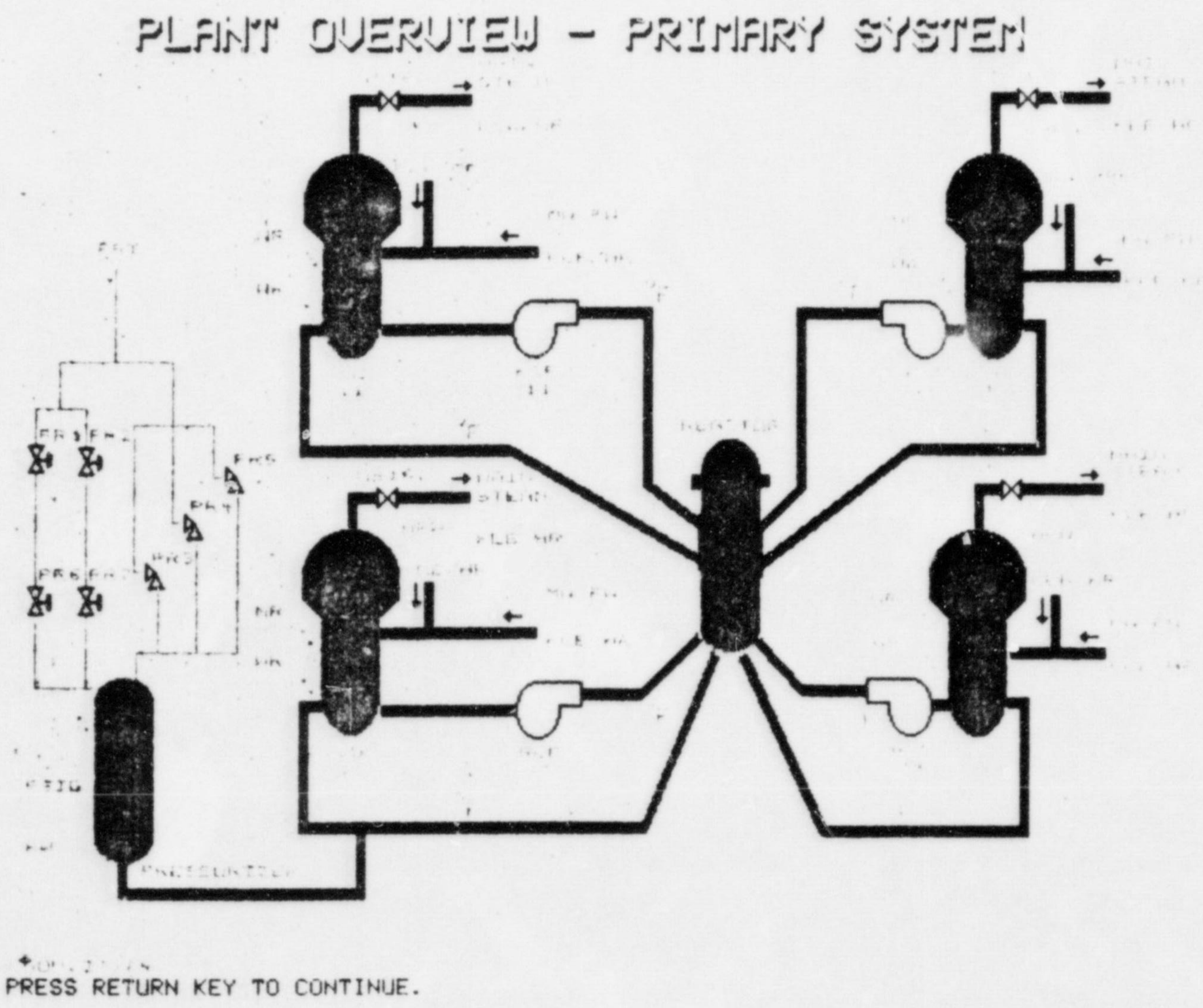
COOLANT INVENTORY

SCHPZI

JUNE 18,1985
PRESS RETURN KEY TO CONTINUE.



PRESS RETURN KEY TO CONTINUE.



PLANT OVERVIEW - PRIMARY SYSTEM

PRESS RETURN KEY TO CONTINUE.

SAFETY PARAMETER DISPLAY SYSTEM
NRC AUDIT

- ERF/SPDS PARAMETERS
- BASIS FOR SPDS
- SELECTION OF SPDS DISPLAYS

ERF COMPUTER SYSTEM/SAFETY PARAMETER DISPLAY SYSTEM

PSE&G has selected a total of sixty-two parameters which will make up the data base for the Emergency Response Facilities (ERF) Computer System. Regulatory Guide 1.97 was used as a guideline. These parameters are listed in Attachment 1.

The basis for the SPDS is the critical safety functions (CSFs) which were identified in the Westinghouse Emergency Response Guidelines (ERGs). The status trees for the CSFs were developed for critical safety function evaluation.

The CSFs were selected to monitor three barriers to the release of radioactivity. The CSFs are associated with the barriers in the following manner:

Barrier	Critical Safety Function
Fuel Matrix and Fuel Clad	Maintenance of SUBCRITICALITY (minimize energy production in the fuel)
	Maintenance of CORE COOLING (provide adequate reactor coolant for heat removal from the fuel)
	Maintenance of a HEAT SINK (provide adequate secondary coolant for heat removal from the fuel)
	Control of Reactor Coolant INVENTORY (maintain enough reactor coolant for effective heat removal and pressure control)
Reactor Coolant System Pressure Boundary	Maintenance of a HEAT SINK (provide adequate heat removal from the RCS)
	Maintenance of Reactor Coolant System INTEGRITY (prevent failure of RCS)
	Control of Reactor Coolant INVENTORY (prevent flooding and loss of pressure control)
Containment Vessel	Maintenance of CONTAINMENT Integrity (prevent failure of containment vessel)

The SPDS parameters were selected based on the CSFs status trees. The parameters are used to satisfy the status trees and their association with the CSFs are as follows:

CRITICAL SAFETY FUNCTION		PARAMETER
1. SHUT DOWN MARGIN		a. Reactor Trip
	Neutron Flux	b. Power Range
		c. Start up Rate
		d. Source Range
		e. Intermediate Range
2. CORE COOLING		a. Core Exit Temperature
		b. RCS Subcooling
		c. RCP Status
		d. Reactor Vessel Level
3. HEAT SINK		a. Steam Generator Level
		b. Total Feedwater Flow
		c. Steam Generator Pressure
4. THERMAL SHOCK		a. RCS Loop Average Temperature
		b. RCS Pressure
		c. RCS Temperature (CIT)
		d. RCS Cold Legs Temperature
5. CONTAINMENT ENVIRONMENT		a. Containment Pressure
		b. Containment Sump Level
		c. Containment Area Radiation
6. COOLANT INVENTORY		a. Pressurizer Level
		b. Reactor Vessel Level

The following are the displays selected for the SPDS:

1. Critical Safety Function Overview
2. Shutdown Margin Status Tree
3. Core Cooling Status Tree
4. Heat Sink Status Tree
5. Thermal Shock Status Tree
6. Thermal Shock Limit A Curve
7. Containment Environment Status Tree
8. Coolant Inventory Status Tree
9. Pressure/Temperature Saturation Curve
10. A display showing the values of the following variables which are associated with Radioactivity Control:

a. Plant vent flow.
b. Containment or Plant Vent gas effluent fixed filter iodine radiation monitor (R12B).
c. Containment or plant vent gas effluent radiation monitor (R12A).
d. Containment or plant vent air particulate monitor (11A).
e. Plant vent radiation monitor, noble gas (R45).
f. Plant vent effluent radiation monitor (R16).
g. Auxiliary Building Plant Ventilation Process Radiation Monitors (R41) (particulate, iodine, noble gas).
h. Main Steam Radiation Monitoring (R46).

Attachment 2 provides in table format a comparison of che Critical Safety Functions in Salem with those listed in Supplement 1 to NUREG 737.

ATTACHMENT 2

CRITICAL SAFETY FUNCTION NUREG 0737, SUPPLEMENT 1)	CRITICAL SAFETY FUNCTION STATUS TREE (SALEM)	PARAMETERS
Reactivity Control	Shut Down Margin	1. Neutron Flux 2. Neactor Trip
Reactor Core Cooling and Heat Removal From the Primary System	Core Cooling	1. Core Exit Temperature 2. Degrees of Subcooling 3. Reactor Coolant Pump Status 4. Reactor Vessel Level
Reactor Coolant System Integrity	Heat Sink	1. Steam Generator Level 2. Steam Generator Pressure 3. Aux. Feedwater Flow
	Thermal Shock	4. RCS Loop Average Temperature 5. RCS Pressure 6. RCS Cold Leg Water Temperature
	Coolant Inventory	7. Pressurizer Level 8. Reactor Vessel Level
Radioactivity Control	Radioactivity at Release Points	1. Plant Vent flow 2. Containment Effluent Radioactivity 3. Plant Vent Effluent Radioactivity 4. Containment Area Radiation 5. Main Stear Radiation
Containment Conditions	Containment Environment	1. Containment Sump Level 2. Containment Pressure 3. Containment Area Radiation

ATTACHMENT 1.

ERF COMPUTER SYSTEM PARAMETERS

CODE#	PARAMETER	INSTRUMENT #	QUALIFICATION
1	Neutron Flux: Source Range	NI-31B, XA5699	NON-IE
		NI-32B, XA5700	
	Intermediate Range	NI-35B, XA5705	
		NI-36B, XA5706	
	Power Range	NI-41B, XA5711	
		NI-42B, XA5712	
		NI-43B, XA5713	
		NI-44B, XA5714	
	Start Up Rate	NI-31D, XA5701	
		NI-32D, XA5702	
		NI-35D, XA5703	
		NI-36D, XA5704	
2	Control Rod Position	See Attachment 1	NON-IE
3	Plant Vent Flow	FA-8602	NON-IE
4	RCS Cold Leg Water Temperature	TA-2757, TA-2758 TA-2759, TA-2760	IE
5	RCS Hot Leg Water Temperature	TA-0043, TA-0053 TA-0063, TA-0073	IE
6	Reactor Coolant System Pressure	PA-8088, PA-0039	IE
7	Core Exit Temperature	See Attachment 2	NON-IE
8	Coolant Level in Reactor	LA-3617, LA-3619	IE
		LA-3620 (Train "A")	NOTE: Sensors are IE but the signal to MUX is NON-IE
		LA--3638, LA-3639	
		LA-3666 (Train "B")	

CODE #	PARAMETER	INSTRUMENT	QUALIFICATION
9	Degrees of Subcooling	Inputs are from thermocouples and RCS pressure	
10	Containment Sump Level	LA-0223, LA-0224	IE
11	Containment Pressure	PA-2386, PA-2405 PA-2344, PA-2345 PA-2346, PA-2568	IE
12	Containment Isolation Valves	See Attachment 3	IE
15	Containment Area Radiation	RA-2584, RA-2586 (R44 A & B)	IE
16	Delete		
17	Containment Hydrogen Concentration	XA-3361, XA-3362	IE
18	Containment AND PLANT VENT Effluent Radioactivity Noble Gases From Identified Release points	RA-4313 (R12B) RA-4330 (R12A) RA-10153, RA-10154 RA-10155 (R41A,B & C) RA-4303 (R11A) RA-4057 (R45,B & C)	IE
		RA-8346 (R16)	NON-IE
19	Deleted		
20	Delete		
21	RHR System Flow	FA-1416, FA-1422 FA-1423, FA-1419	IE
22	RHR Heat Exchanger Outlet Temperature	TA-1425, TA-6486	NON-IE
23	Accumulator Tank Levels	LA-0241, LA-0237 LA-0233, LA-0228 LA-0242, LA-0238 LA-0234, LA-0229	IE
	Accumulator Tank Pressures	PA-0243, PA-0239 PA-0235, PA-0230 PA-0244, PA-0240 PA-0236, PA-0231	IE

CODE #	PARAMETER	INSTRUMENT #	QUALIFICATION
24	Accumulator Isolation Valve Position	SJ54, (4 valves, one per tank)	IE
25	Boric Acid Changing Flow	FA-135, FA-2174	IE
26	Flow in HPI System	FA-7462	IE
27	Flow in LPI System	FA-7464, FA-0226	IE
28	Refueling Water Storage Tank Level	LA-209, LA-210 UNIT #1 ~~LA-3144, LA-3146~~ LA-4183, LA-4182 Unit #2	IE
29	Reactor Coolant Pump Status (amps)	IA-6832, IA-6834 IA-6837, IA-6839	NON-IE
30	Primary System Safety Relief Valve Positions	PR1, PR2 PR6, PR7	IE
31	Pressurizer Level	LA-0086, LA-0087 LA-0088, LA-0089	IE
32	Pressurizer Heater Status (amps)	IA-5266, IA-5267 IA-5268	NON-IE
33	Pressurizer Relief Tank Level	LA-0094	NON-IE
34	Pressurizer Relief Tank Temperature	TA-0095	NON-IE
35	Pressurizer Relief Tank Pressure	PA-0096	NON-IE
36	Steam Generator Level	LA-0009, LA-0015 LA-021, LA-0027 LA-0005, LA-0013 LA-0017, LA-0025	IE
37	Steam Generator Pressure	PA-0671, PA-0672 PA-0673, PA-0674 PA-0734, PA-0736 PA-0738, PA-0740	IE
38	Main Steam Flow	FA-0687, FA-688 FA-689, FA-690 FA-101, FA-102 FA-103, FA-104	IE

CODE #	PARAMETER	INSTRUMENT #	QUALIFICATION
39	Main Feedwater Flow	FA-0656, FA-0658 FA-0660, FA-0662 FA-1901, FA-1902 FA-1903, FA-1904	IE
40	Auxiliary Feedwater Flow	FA-1087, FA-1091 FA-1095, FA-1097	IE
41	Auxiliary Feedwater Storage Tank Level	LA-1688	IE
42	Containment Spray Flow	No instrument at this time	
43	Containment Spray Additive flow	FA-0218	IE
44	Containment Fan Cooler Outlet flow	FA-3539, FA-3540 FA-3541, FA-3542 FA-3543	IE
	Containment Fan Cooler Unit Running (High/Low Speed)	XD-5486, XD-5487 XD-5491, XD-5492 XD-5496, XD-5497 XD-5501, XD-5502 XD- 5506,XD-5507	
45	Containment Atmosphere Temperature	TA-4306, TA-4307 TA-4308, TA-4309 TA-4310, TA-4311 TA-4312, TA-4313 TA-4314, TA-4315 TA-4316, TA-4318 TA-4319, TA-4320 TA-4321, TA-4348	NON-IE
46	Letdcwn Flow	FA-141	IE
47	Volume Control Tank Level	LA-0119	IE
48	Component Cooling Water Temperature	TA-1564, TA-1576	NON-IE
49	Component Cooling Water Flow	FA-1565, FA-1577	NON-IE
50	High Level Radioactive Liquid Tank Level	LA-0165, LA-0166 LA-0167, LA-1526 LA-1523, LA-1535 LA-1536, LA-1537	NON-IE

CODE #	PARAMETERS	INSTRUMENTS	QUALIFICATION
51	Radioactive gas Hold up Tank Pressure	PA-4030, PA-4029 PA-4032, PA-4031	NON-IE
52	Control Room Emergency Ventilation Damper Position	CAA1, CAA2, CAA3 CAA4, CAA5, CAA14 CAA17, CAA18, CAA19 CAA20, CAA31 CAA32, CAA33	IE
53	Auxiliary Building Emergency Dampers	ABV1, ABV3, ABV7 ABV8, ABV9, ABV10 ABV21	IE
54	Fuel Handling Building Emergency Dampers	FHV1, FHV2 FHV3, FHV4	IE
55	Status of Standby Power and Other Emergency Energy Sources Important to Safety	See Attachment 4	IE
56	Control Air	PA-3825, PA-2140	NON-IE
57	Main Steam Radiation Monitors	RA-4072 (R46A) RA-4073 (R46B) RA-4074 (R46C) RA-4075 (R46D) RA-4076 (R46E)	IE
58	Wind Direction	XA-8499 (30 FT. ELEV.) XA-8500 (150 FT. ELEV.) XA-8501 (300 FT. ELEV.)	NON-IE
59	Wind Speed	XA-8496 (30 FT. ELEV.) XA-8497 (150 FT. ELEV.) XA-8498 (300 FT. ELEV.)	NON-IE
60	Atmospheric Stability (Temperature)	*TA-8502 (30 FT. ELEV.) TA-8505 (30-300 FT.) TA-8506 (30-150 FT.)	NON-IE
61	Deleted		

Two signals were deleted.

ODE #	PARAMETER	INSTRUMENT #	QUALIFICATION
62	Condenser Availability (Condenser Vacuum)	PA-2396, PA-2397 PA-2398, PA-2399	NON-IE
	(Circulator motor amperes)	IA-6833, IA-6838 IA-6835, IA-6840 IA-6836, IA-6841	
63	Reactor Coolant System Loop Average temperature	TA-5360, TA-5361 TA-5362- TA-5363	NON-IE
64	Main Steam Isolation valve position open/close	MS-167 (4 valves, one per steam generator)	IE
65	Reactor trip demand signal for train "A"	1ASTR-A	IE
66	Reactor trip demand signal for train "B"	1ASTR-B	IE

ATTACHMENT 1

*CODE # 2 LIST OF INSTRUMENTS

INSTRUMENT #

NA - 4301

NA - 4302

NA - 4303

NA - 4304

NA - 4305

NA - 4306

NA - 4307

NA - 4308

NA - 4309

NA - 4310

NA - 4311

NA - 4312

NA - 4313

NA - 4314

NA - 4315

NA - 4316

NA - 4317

NA - 4318

NA - 4319

NA - 4320

NA - 4321

NA - 4322

NA - 4323

INSTRUMENT #

NA - 4324

NA - 4325

NA - 4326

NA - 4327

NA - 4328

NA - 4329

NA - 4330

NA - 4331

NA - 4332

NA - 4333

NA - 4334

NA - 4335

NA - 4336

NA - 4337

NA - 4338

NA - 4339

NA - 4340

NA - 4341

NA - 4342

NA - 4343

NA - 4344

NA - 4345

CODE #2 LIST OF INSTRUMENTS

INSTRUMENT
NA - 4370
NA - 4371
NA - 4372
NA - 4373
NA - 4374
NA - 4375
NA - 4376
NA - 4377

*Eight signals were deleted

ATTACHMENT 2

CODE #7 LIST OF INSTRUMENTS

INSTRUMENT #

TA - 4112

TA - 4328

TA - 4329

TA - 4330

TA - 4331

TA - 4332

TA - 4333

TA - 4334

TA - 4335

TA - 4336

TA - 4337

TA - 4338

TA - 4339

TA - 4340

TA - 4341

TA - 4342

TA - 4343

TA - 4344

TA - 4345

TA - 4346

INSTRUMENT #

TA - 4347

TA - 4116

TA - 4415

TA - 4416

TA - 4417

TA - 4418

TA - 4419

TA - 4488

TA - 4489

TA - 4490

TA - 4491

TA - 4492

TA - 4493

TA - 4494

TA - 4495

TA - 4496

TA - 4497

TA - 4498

TA - 4499

TA - 4500

CODE #7 LIST OF INSTRUMENTS

INSTRUMENT

TA - 4501

TA - 4502

TA - 4503

TA - 4504

TA - 4505

TA - 4506

TA - 4507

TA - 4508

TA - 4509

TA - 4510

TA - 4511

TA - 4536

TA - 4537

TA - 4538

TA - 4539

TA - 4540

TA - 4541

TA - 4542

TA - 4543

TA - 4544

TA - 4545

TA - 4546

TA - 4547

TA - 4548

TA - 4549

TA - 4550 (RTD)

TA - 4551 (RTD)

TA - 4552 (RTD)

TA - 4553 (RTD)

ATTACHMENT 3

CODE #12 LIST OF ISOLATION VALVES

VALVE I.D.#

SS94 (4)

VC11

VC12

VC13

VC14

VC7

VC8

VC9

VC10

VC1

VC2

VC3

VC4

VC5

VC6

DR29

CA330 (2)

SW58 (5)

SW72 (5)

WL16

WL17

VALVE I.D. #

FP147

CC215

CC113

CC117

CC118

CC187

CC136

CC190

CC131

WL96

WL97

WL98

WL108

WL99

WL12

WL13

NT32

SJ123

SJ53

SJ60

ATTACHMENT 4

CODE #55 LIST OF INSTRUMENTS

INSTRUMENT #	IDENTIFICATION
VA - 5417	A Diesel Generator
QA - 5418	A Diesel Generator
WA - 5415	A Diesel Generator
IA - 5416	A Diesel Generator
VA - 5843	B Diesel Generator
QA - 5844	B Diesel Generator
WA - 5841	B Diesel Generator
IA - 5842	B Diesel Generator
VA - 5851	C Diesel Generator
QA - 5852	C Diesel Generator
WA - 5849	C Diesel Generator
IA - 5850	C Diesel Generator
VA-5288	A 28VDC
IA-5295	A 28VDC
VA-5355	A 125VDC
IA-5367	A 125VDC
VA-5333	B 28VDC
IA-5340	B 28VDC
VA-5394	B 125VDC
IA-5406	B 125VDC
VA-5427	C 125VDC
IA-5428	C 125VDC

June 27, 1985

Director of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, MD 20014

Attention: Mr. Steven Varga, Chief
Operating Reactors Branch 1
Division of Licensing

Dear Mr. Varga:

REQUEST FOR ADDITIONAL INFORMATION CONCERNING
THE SAFETY PARAMETER DISPLAY SYSTEM
SALEM GENERATING STATION
DOCKET NOS. 50-272 AND 50-311

PSE&G hereby submits, in the attachment to this letter, its response to your request of December 7, 1984 for additional information concerning the Safety Parameter Display System (SPDS).

Inasmuch as we had also been requested to respond to questions concerning our Detailed Control Room Design Review, we had requested an extension in providing the information on SPDS. Your Mr. D. C. Fischer, in a telephone conversation with our Mr. R. S. Patwell on February 27, 1985, granted that extension until July 1, 1985.

Should you have any questions, do not hesitate to contact us.

Sincerely,

Corbin A. McNeill, Jr.
Vice President - Nuclear

AJG:nvm
Attachment

C Mr. Donald C. Fischer
Licensing Project Manager

Mr. Thomas J. Kenny
Senior Resident Inspector

BC Vice President - Nuclear
Assistant Vice President - Nuclear Operations Support
General Manager - Nuclear Quality Assurance
General Manager - Nuclear Services
General Manager - Salem Operations
General Manager - Hope Creek Operations
General Manager - Nuclear Engineering
General Manager - Nuclear Assurance and Regulation
General Manager - Nuclear Safety Review
Assistant General Manager - Engineering
Assistant General Manager - Nuclear Joint Owners and Regulatory Actvities
Assistant to General Manager - Nuclear Engineering
Manager - Nuclear Licensing and Reliability
Manager - Nuclear Engineering Design
Manager - Nuclear Systems Engineering
Manager - Nuclear Plant Engineering
Manager - Nuclear Engineering Control
Manager - Nuclear Training
Manager - Licensing and Analysis
Manager - Nuclear Safety Assurance
Manager - Onsite Safety Review
Public Affairs Manager - Nuclear
Operations Assessment Engineer
Station Quality Assurance Engineer
Salem Operations Technical Dept,Technical Staff, B. Leap
Associate General Solicitor
Nuclear Review Board Manager
LIS (R. Buckles)
D. Dodson (FSAR Update)
PE (W. T. Ullrich)
R. S. Patwell (Commitment Tracking)
PL&G (T. R. Robbins)
A. J. Greenfeld
File 13.3.2

atl4 1-2

SALEM GENERATING STATION UNITS NO. 1 AND 2

SAFETY PARAMETER DISPLAY SYSTEM

RESPONSE TO NRC LETTER DATED DECEMBER 7, 1984

REFERENCE: PSE&G'S REPORT "SAFETY ANALYSIS FOR SPDS
PARAMETERS" DATED JANUARY 30, 1984

Response to NRC concerns are in the order indicated in the enclosure to the letter dated December 7, 1984.

ISOLATION DEVICES

The data acquisition system consists of five multiplexer cabinets and one data concentrator per unit and is configured to meet redundancy requirements. Four of the cabinets are 1E which are physically separated and the one dual cabinet is Non-1E. The data concentrator is Non-1E. There are 323 class 1E field signals per unit which go to the 1E cabinets and 220 Non-1E field signals per unit which go to the Non-1E cabinets. The foregoing indicates that no isolation devices are required prior to the multiplexer cabinets. The signals from these cabinets however are transmitted to the data concentrator by means of fiber optic cables. These cables isolate the multiplexer cabinets from data concentrator and the rest of the system. Fiber optic cables were used for the Non-1E cabinets because of their noise immunity capability. Attachment 1 is a one-line block diagram showing the system configuration. The fiber optic cable specification is as follows:

Fiber Manufacturer: Corning Corporation or Corning
Corporation Licensee
Core Diameter: 50 Micron
Core and Cladding Diameter: 125 Micron
Numerical Aperature (NA): 0.2
Attenuation: 4dB/km or better
Bandwidth/length: 200MHZ/km
Fiber Type: Glass core and cladding

HUMAN FACTORS PROGRAM

Display System

The display system provides the primary means of information presentation to the operator. Man-Machine Interface (MMI) consideration will be addressed by utilizing a CRT/keyboard configuration. Included in this system are CRT copiers for color hard copy of CRT displays and high-speed printers for hard copy of logs, reports and nongraphic CRT displays.

All console CRTs are provided with interactive keyboards. The primary CRT utilizes a special purpose function keyboard for presentation of SPDS primary displays. The secondary CRT utilizes a full ASCII keyboard with 60 functional keys for interactive system dialog as well as presentations of both primary and secondary system displays.

Graphics CRT

The graphics CRTs in the system are IDT #2250 graphics computer systems. These devices utilize four (4) microprocessors for graphics processing and I/O handling. The display is a 19-inch color CRT with 512x512 dot resolution.

Included with each CRT system are:

- Standard keyboard with minimum of 60 functional keys;
- Eight color (plus blink) display capability;
- Two serial ports for host computer communication;
- 2MBIT of Bubble Memory for program storage;
- Real-time clock and CMOS RAM for system functions;
- Hardware vector generator for fast display processing;
- Extended plot and complex fill routines for fast display processing.

High-Speed Printer

The high-speed printers which will be located in the Control Rooms (CR) are Versatec V-80 Printer Plotter.

CRT Copier

A color copier will be located in each control room, TSC and EOF.

Subsystem Operation

Static picture information for displays is initially created in an off-line environment using the Interactive Display Editor. Display information is data compressed utilizing an encoding technique and stored on the system data disks.

Static picture information is kept within each graphic CRT and stored in bubble memory. When a primary display is requested (either by a primary function key or secondary keyboard keystrokes) the static information is obtained from the local CRT memory and written to the screen. The current dynamic data for the display is assembled at the host computer and transmitted to the CRT for screen display. The total display call-up time for primary displays (time from keyboard entry to complete static and dynamic screen display) is typically one second.

Once a display has been called up on a CRT, only the dynamic portions need to be periodically updated. This is done by the primary host computer every two seconds for all displays that are dynamic. Note that since only dynamic data is regularly assembled and distributed by the host computer, system loading is dependent only on the number of display CRTs and is not a function (except for static picture storage) of the total number of displays in the data base. Communication between the host and the CRTs is accomplished via 19.2KB RS-232 serial links to the data highway.

Future addition of secondary displays can be readily accommodated. Based on an average compressed size of 5000 bytes per static display, bubble memory capacity exceeds 70 mimic type displays and additional bubble memory can be added as an option.

Hard copy of a screen image is initiated directly by the operator at the CRT keyboard. Upon initiation of the copy command, the screen image is transferred through a high-speed parallel interface to the video copier. Printing takes between one and a half and three minutes, depending on display complexity. Upon completion, the hard copy may be used immediately because no drying time is required. During the print cycle, the copier input buffer is disabled. If a new copy command is issued, the copier will issue a "busy" to the requesting CRT. Hard copy of logs, reports and nongraphic screen images are initiated at the secondary display keyboards for printing on the line printers in the control room.

The display system is presently being designed. A contract was awarded to General Physics Corporation to conduct a human factors review. The results of the review will be evaluated and incorporated into the design as appropriate. This review is expected to be completed by October 30, 1985. At that time the report will be available for your review.

DATA VALIDATION

The ERF Computer System addresses sensor validation at two distinct modes, the Computer Products Inc. (CPI) data concentrator and the PACE alarm processor. PACE is the name of the software package which will be used for the system. The data concentrator will detect the following hardware channel failures as the first mode of sensor validation:

o Current loop less than 4ma and greater than 20ma.

o Thermocouple open circuit.

o Thermocouple out of range.

o RTD out of defined bridge range.

o Multiplexer unable to scan sensor.

PACE produces several sensor qualities or flags that will be used to validate a sensor's value, e.g. alarm, offscan, and hardware channel failure. PACE supports four levels of alarms: Hi, Hi-Hi, Lo, and Lo-Lo. Except as discussed below, the Hi and Lo alarms will be used in the conventional sense to warn of approach to operating limits while Hi-Hi and Lo-Lo will be used to indicate nonsense readings such as a negative tank level.

Offscan is a validation indicator because it means that at the second consecutive instrument limit violation, the point is taken offscan. This means that the sensor's value is invalid. Instrument violation can also be set at nonsense instrument process readings.

Invalid data being displayed can be detected by the operator using the following techniques:

- A foreground color blink of the value when it is Hi-Hi or Lo-Lo with the symbol 'NV' placed on the right of the value. For those parameters which have an actual Lo-Lo or Hi-Hi alarm (e.g. containment pressure and steam generator level) the offscan technique will be used.

- A foreground color blink of the value when the point is offscan with the symbol 'OS' placed on the right of the value. If the value disappears off the screen when the point is offscan, then there will be an 'OS' in place of the value.

- Graphic represented data, e.g. a pump or valve, will have its color and blink changed based on the above flags.

PARAMETER SELECTION

Please refer to PSE&G's submittal dated January 30, 1984 for the rationale which justifies parameter selection. This is under the section entitled "Parameter Selection" and Attachment No. 3. Attachment No. 4 "Critical Safety Function Status Trees" shows the relationship between the parameters selected for display on the Safety Parameter Display System and the Critical Safety Functions.

Radioactivity Control and Containment Conditions indicated on page 8 of Supplement 1 to NUREG 0737 is addressed by the Critical Safety Function "Containment Environment." Radioactivity Control is monitored by Containment Area Radiation, Containment Effluent Radioactivity and Main Steam Radiation monitors and these parameters are available on the Safety Parameter Display System.

Other parameters not used for the Critical Safety Functions can be accessed at the terminal by using a track ball and one or two keystrokes.

UNREVIEWED SAFETY QUESTIONS

The signals for all parameters used for the Safety Parameter Display System will be acquired from existing instrument loops. During the design of the data acquisition system interface with the plant instruments, the possibility of failure or malfunction due to circuit overload and the effects on existing systems were addressed. The function of the existing systems will not be altered and the safe shut down of the reactor will not be affected. The SPDS interfaces wer^ also designed taking into consideration electrical separation and isolation. This will ensure that failure of the SPDS or any associated equipment will not increase the probability or consequences of accidents analyzed in the FSAR. The margin of safety has not been diminished due to the addition of the SPDS. Because of the foregoing, an unreviewed safety question is not involved.

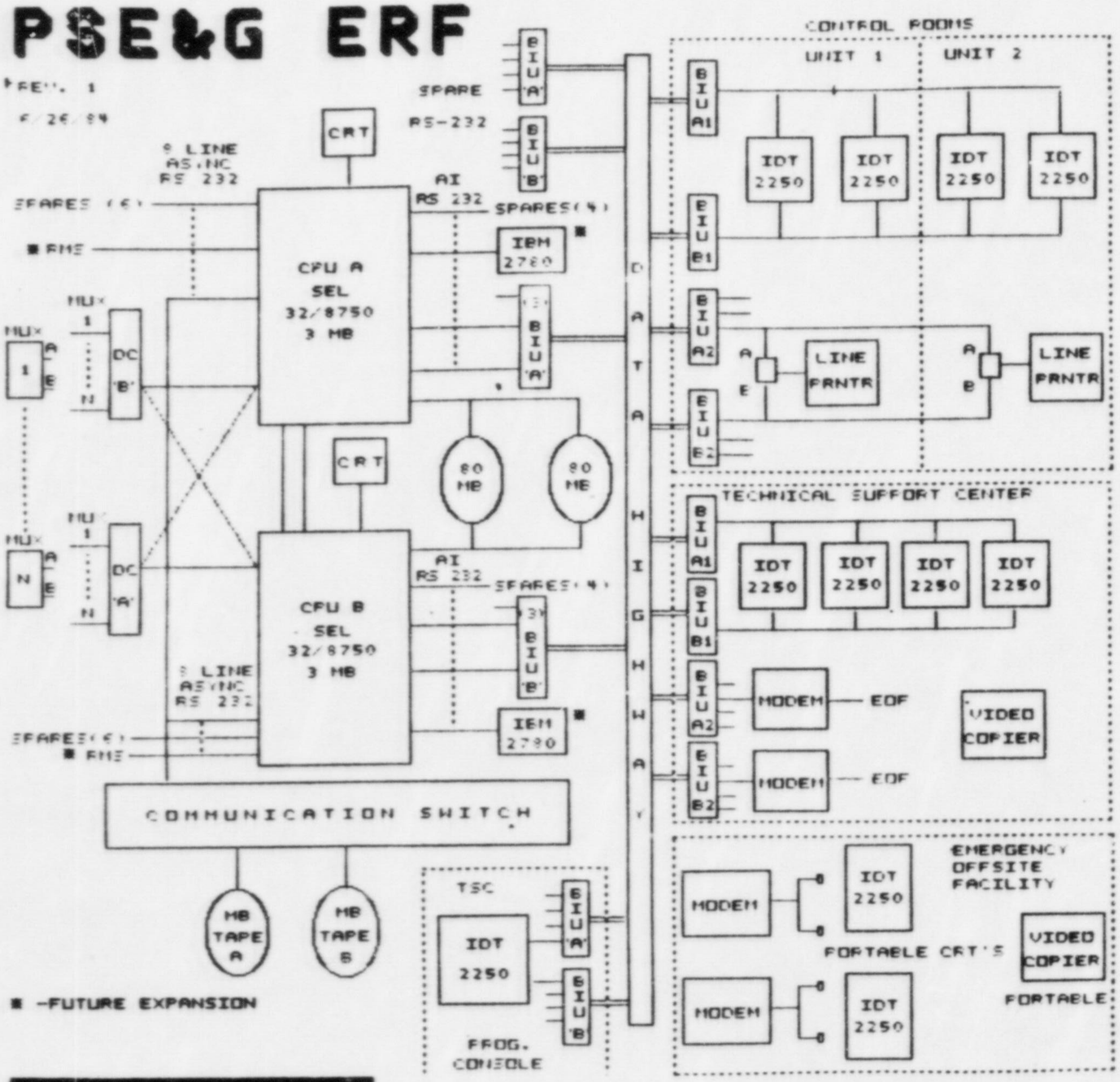
There will be no new systems or instruments added as a result of the installation of the data acquisition system. Since the functions of the existng systems will not be changed, the technical specifications associated with any system or instrument in that system will not be affected.

MHA:ljs
6/24/85

PSE&G ERF

REV. 1

6/26/84



■ -FUTURE EXPANSION

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

03

December 7, 1984

Docket Nos. 50-272
and 50-311

Mr. Richard A. Uderitz, Vice President -
Nuclear
Public Service Electric and Gas Company
Post Office Box 236
Hancocks Bridge, New Jersey 08038

Dear Mr. Uderitz:

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION CONCERNING THE SAFETY PARAMETER DISPLAY SYSTEM FOR SALEM UNITS 1 AND 2

The staff has reviewed your January 30, 1984 submittal "Safety Parameter Display System, Safety Analysis and Implementation Plan" and concluded that insufficient information was provided for us to complete our evaluation. The additional information required is discussed in the enclosure. Please respond to this request for information within 60 days from receipt of this letter.

The reporting and/or recordkeeping requirements of this letter affect fewer than ten respondents; therefore, OMB clearance is not required Under P.L. 96-511.

Sincerely,

Steven A. Varga

Steven A. Varga, Chief
Operating Reactors Branch #1
Division of Licensing

REQUEST FOR ADDITIONAL INFORMATION

CONCERNING THE

SALEM UNITS 1 AND 2

SAFETY PARAMETER DISPLAY SYSTEM

Each operating reactor shall be provided with a Safety Parameter Display System (SPDS). The Commission approved requirements for an SPDS are defined in NUREG-0737, Supplement 1. In the Regional Workshops on Generic Letter 82-33 held during March 1983, the NRC discussed these requirements and the staff's review of the SPDS.

Prompt implementation of the SPDS in operating reactors is a design goal of prime importance. The staff's review of SPDS documentation for operating reactors called for in NUREG-0737, Supplement 1, is designed to avoid delays resulting from the time required for NRC staff review. The NRC staff will not review operating reactor SPDS designs for compliance with the requirements of Supplement 1 of NUREG-0737 prior to implementation unless a preimplementation review has been specifically requested by licensees. The licensee's Safety Analysis and SPDS Implementation Plan will be reviewed by the NRC staff only to determine if a serious safety question is posed or if the analysis is seriously inadequate. The NRC staff review to accomplish this will be directed at: (a) confirming the adequacy of the parameters selected to be displayed to detect critical safety functions, (b) confirming that means are provided to assure that the data displayed are valid, (c) confirming that the licensee has committed to a human factors program to ensure that the displayed information can be readily perceived and comprehended so as not to mislead the operator, and (d) confirming that SPDS will be suitably isolated from electrical and electronic interference with equipment and sensors that are used in safety systems. If based on this review the staff identifies a serious safety question or seriously inadequate analysis, the Director of IE or the Director of NRR may require or direct the licensee to cease implementation.

The staff has reviewed the SPDS safety analysis and implementation plan provided in your submittal dated January 30, 1984. In order to complete our evaluation the following additional information is requried:

1. ISOLATION DEVICES

a. For each type of device used to accomplish electrical isolation, describe the specific testing performed to demonstrate that the device is acceptable for its application(s). This description should include elementary diagrams when necessary to indicate the test configuration and how the maximum credible faults were applied to the devices.

b. Data to verify that the maximum credible faults applied during the test were the maximum voltage/current to which the device could be exposed, and define how the maximum voltage/current was determined.

c. Data to verify that the maximum credible fault was applied to the output of the device in the transverse mode (between signal and return) and other faults were considered (i.e., open and short circuits).

d. Define the pass/fail acceptance criteria for each type of device.

e. Provide a commitment that the isolation devices comply with the environmental qualifications (10 CFR 50.49) and with the seismic qualifications which were the basis for plant licensing.

f. Provide a description of the measures taken to protect the safety systems from electrical interference (i.e., Electrostatic Coupling, EMI, Common Mode and Crosstalk) that may be generated by the SPDS.

HUMAN FACTORS PROGRAM

Provide a description of the display system, its human factored design, and the methods used and results from a human factors program to ensure that the displayed information can be readily perceived and comprehended so as not to mislead the operator.

DATA VALIDATION

Describe the method used to validate data displayed in the SPDS. Also, describe how invalid data is defined to the operator.

PARAMETER SELECTION

Provide the rational which justifies parameter selection and relates the parameters selected for display on the SPDS to the critical safety functions stated in NUREG-0737, Supplement 1.

UNREVIEWED SAFETY QUESTIONS

Provide conclusions regarding unreviewed safety questions and changes to technical specifications.

PSE&G

Public Service Electric and Gas Company P.O. Box 236 Hancocks Bridge New Jersey 08038

Nuclear Department

January 30, 1984

Director of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, MD 20014

Attention: Mr. Steven Varga, Chief
Operating Reactors Branch 1
Division of Licensing

Dear Mr. Varga:

SAFETY PARAMETER DISPLAY SYSTEM
SAFETY ANALYSIS AND IMPLEMENTATION PLAN
REQUIREMENTS FOR EMERGENCY RESPONSE CAPABILITY
SALEM GENERATING STATION
NO. 1 AND 2 UNITS
DOCKET NOS. 50-272 AND 50-311

PSE&G hereby submits its Safety Analysis and implementation plan for the Safety Parameter Display System in accordance with the requirements of Generic Letter 82-33, Requirements for Emergency Response Capability.

Should you have any questions, please do not hesitate to contact us.

Sincerely,

E. A. Liden
Manager - Nuclear
Licensing and Regulation

A057/1/1

RSP:jab

cc: Mr. Donald C. Fischer
Licensing Project Manager

Mr. James Linville
Senior Resident Inspector

bcc: Vice President - Nuclear
General Manager - Nuclear Services
General Manager - Nuclear Support
General Manager - Salem Operations
General Manager - Hope Creek Operations
General Manager - Nuclear Assurance and Regulation
Assistant General Manager - Nuclear Engineering
Assistant General Manager - Engineering
Manager - Nuclear Systems Engineering
Manager - Nuclear Plant Engineering
Manager - Nuclear Engineering Control
Manager - Nuclear Operations Quality Assurance
Manager - Nuclear Training
Manager - Licensing and Analysis
Public Affairs Manager - Nuclear
Safety Review Group
Operations Assessment Engineer
Station Quality Assurance Engineer
Associate General Solicitor
Nuclear Review Board Manager
LIS (J. C. Plunkett, Jr.)
OPS (D. C. Aabye)
PE (W. T. Ullrich)
PL&G (T. R. Robbins)
R. S. Patwell (Commitment Tracking)

H28 1/2

Submitted to NRC on 1.30.84

PUBLIC SERVICE ELECTRIC AND GAS COMPANY
NUCLEAR DEPARTMENT

DATE: January 25, 1984
RESPONSE DUE:

TO: E. A. Liden
Manager - Nuclear Licensing And Regulation

FROM: R. L. Gura
Manager - Nuclear Plant Engineering

SUBJECT: SAFETY PARAMETER DISPLAY SYSTEM

Attached please find copies of the Safety Analysis for the SPDS parameters and the SPDS Implementation Plan which have to be submitted to the NRC. It should be noted that the commitment date for submittal is January 31, 1984.

MHA:ljs

Attachment

CC: J. Bailey
L. Leitz
R. MacWatters
CARMS - X500

DO4 1/01

SAFETY ANALYSIS FOR SPDS PARAMETERS

Functional Description

The Safety Parameter Display System will serve as an aid to the control room personnel during abnormal and emergency conditions in determining the safety status of the plant. It will also function as an operator aid during normal operation by monitoring other parameters or graphic displays that are determined to be important to the operator for maintaining safe operation of the plant. The displays will serve to concentrate a set of plant parameters to aid in assessing plant safety status without surveying the entire control room. The primary display will provide an overview of plant conditions and the secondary displays will provide more detailed information on specific plant systems and equipment.

System Description

General

The Safety Parameter Display System will be a redundant computer system with CRTs located in the TSC, EOF and Units 1 and 2 Control Room. This system is independent of the Plant Computer. The major components are as follows:

- three 1E multiplexer cabinets per unit
- two NON-1E multiplexer cabinets per unit
- two data concentrators
- two SEL 32/8705 Central Processing Units
- two color CRT/keyboards per unit control room
- one line printer per unit
- four color CRT/keyboards for TSC
- one video copier for TSC
- two color CRT/keyboards for EOF
- one video copier for EOF

The data concentrators and the two Central Processing Units will be shared by both Units. The CRT/keyboard assemblies and video copiers in the TSC and EOF will not be dedicated to any one unit. Attachment 1 gives a general layout of the above mentioned components and other peripheral equipment.

Data Acquisition Subsystem

Each multiplexer in the subsystem functions as an independent unit utilizing a 16 bit microprocessor. Complete isolation of field inputs is maintained by use of fiber optic communication links to the rest of the system. Signal conditioning and buffers necessary to isolate the P-250 process computer is included.

Computer Subsystem

The computer subsystem utilizes two SEL 32/8705 processors in a fully redundant configuration. Each CPU acquires and processes the data from all multiplexers and maintains its own data base. One CPU is designated as the primary unit and handles all display subsystem interfacing. This allows the other CPU to be utilized for development work while maintaining a hot standby condition for smooth fail-over. A full duplex RS-232 "watchdog" communication channel is provided so that the CPUs can monitor each other. All communication with equipment outside the computer environs is via fiber optic links or standard RS-232 modems.

Display Subsystem

The display subsystem comprises high resolution color graphics CRTs, color video hard copy units and printers for data output. The IDT #2200 color graphics CRTs are used and full graphics editing capabilities are provided for building and modifying color displays.

Isolation of Class 1E Signals

At the output of the multiplexer cabinets, the communication link to the computer will be by fiber optic cables which will perform an isolation function. All class 1E signals will be isolated prior to entering the multiplexer cabinets. These isolators will be qualified based on their function.

Availability

The Host processor/display system will be designed to achieve an availability of 99.0% under the following conditions:

- All of the ERF on-line functions are executing without degradation and the following minimum complement of hardware is operational.

    1. One of the two CPUs with all of its main memory and its programmer's I/O device, and with sufficient hardware in the CPU interfaces to communicate with all of the field multiplexers communication circuits at the specified scan rates.
    2. One of the two auxiliary memories.
    3. One printer in either unit control room.
    4. One of the two unit CRTs in the control room, one of the two unit CRTs in the TSC and one of the two CRTs in the EOF excluding the modems and phone lines.

- Each multiplexer will be designed to achieve the availability under the following conditions:

    1. The multiplexer is considered available unless:

a. Any function is lost for all points of a single type, or
b. More than one input card of the same type fails, or
c. One input card of each type fails.

Human Factors

The Safety Parameter Display System display will be designed to incorporate accepted Human Factor Principles. The following Human Factors Principles references will be used:

- NUREG 0700, Section 6.
- NUREG 0835, Section 6.
- "Human Engineering Principles for Control Room Design Review", Section 3.7, published by the Nuclear Utility Task Action Committee.

Parameter Selection

PSE&G has selected a total of sixty-one parameters to be displayed on the SPDS using the parameters listed in Regulatory Guide 1.97 as a guideline. These parameters are listed in Attachment 2.

The basis of this safety analysis is the Critical Safety Function Status Trees. The Critical Safety Functions were identified and Status Trees developed by PSE&G based on the Westinghouse Emergency Response Guidelines, Revision 1. The Status Trees and the procedures associated with them are contained within the Emergency Operating Procedure Set, which was also developed based on the Westinghouse Owners Group Emergency Response Guidelines. For any transient or accident condition, the Emergency Operating Procedures will direct the operator to monitor the Status Trees. Operator training also addresses the use of the Status Trees during transient or accident conditions. The following is a list of the six Critical Safety Functions for Salem Generating Station:

1. Shutdown Margin
2. Core Cooling
3. Heat Sink
4. Thermal Shock
5. Containment Environment
6. Coolant Inventory

Attachment 3 is "The Critical Safety Function Status Trees Basis Document", and Attachment 4 is "The Emergency Operating Procedure EOP-CFST-1 and Status Trees". These documents are in draft form. They will be made final when the Emergency Operating Procedures are implemented.

The "Critical Safety Function Status Trees Basis Document" basically lists the Critical Safety Functions and describes the use and organization of the Status Trees. It also explains how the Status Trees are used in evaluating the Critical Safety Functions. The "Emergency Operating Procedure EOP-CFST-1 and Status Trees" document shows graphically the Status Tree for each Critical Safety Function and explains the significance of the colors used.

Of the total parameters that were selected for the Safety Parameter Display System, fifteen are utilized in satisfying the Critical Safety Functions. The parameters are as follows:

1. Neutron Flux
2. RCS Cold Leg Water Temperature
3. RCS Pressure
4. Core Exit Temperature
5. Reactor Vessel Level
6. Degrees of Subcooling
7. Containment Sump Water Level
8. Containment Pressure
9. Containment Area Radiation
10. Reactor Coolant Pump Status
11. Pressurizer Level
12. Steam Generator Level
13. Steam Generator Pressure
14. Auxiliary Feedwater Flow
15. RCS Loop Average Temperature.
16. REACTOR TRIP

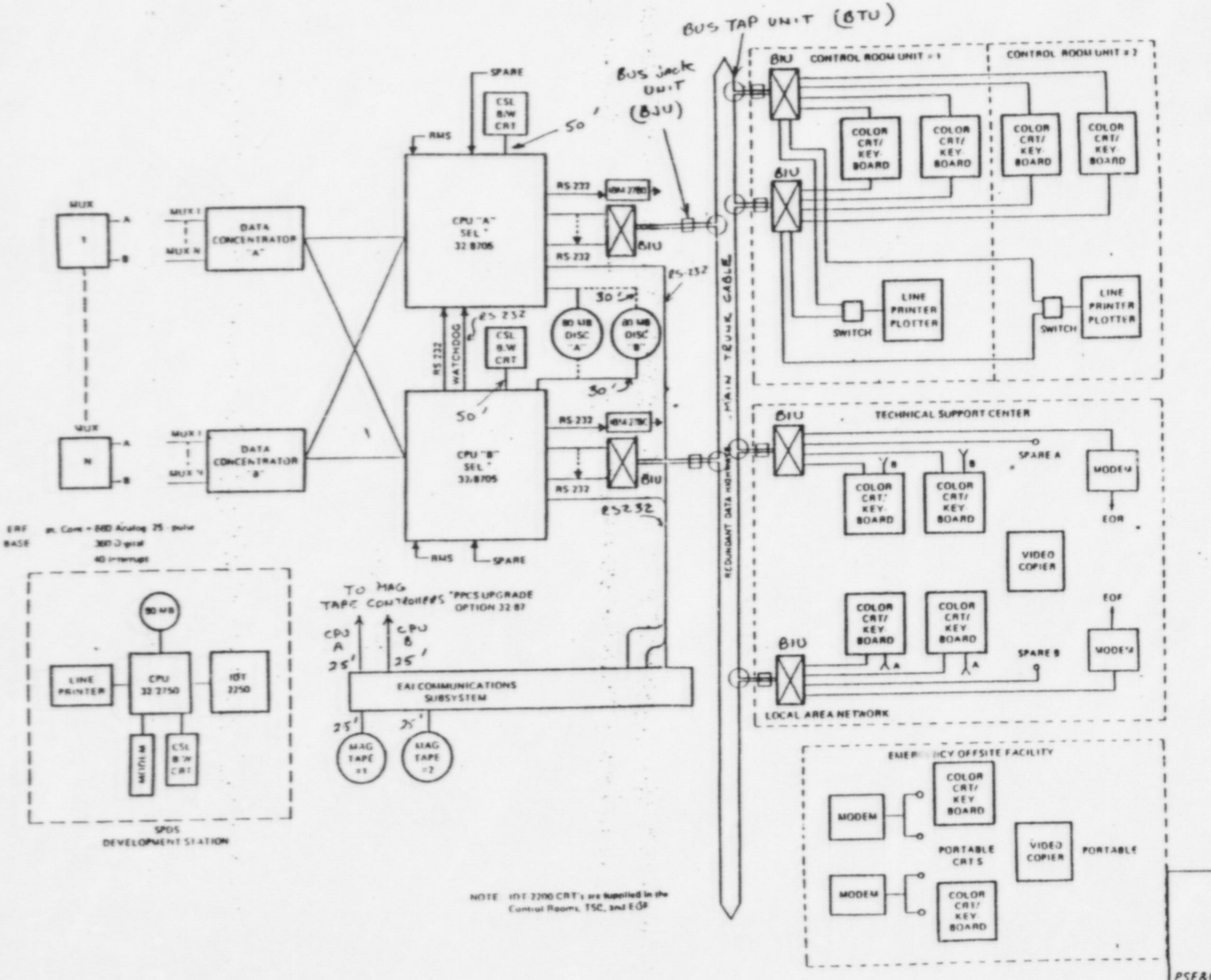
The other forty-six parameters will be included in the SPDS data base because they have been determined to be important in aiding the operator in determining the status of the plant. Most of these parameters will be used in developing graphic displays which will be used as an operator aid.

17 PLANT VENT FLOW

18 CONTAINMENT AND PLANT VENT EFFLUENT RADIOACTIVITY FROM IDENTIFIED RELEASE POINTS.

19 MAIN STEAM RADIATION

Attachment 1



NOTE IDT 2200 CRT's are supplied in the Control Rooms, TSC, and EOF

MAXIMUM Lengths

- ALL RS232 CABLES - 5
- MAX DISTANCE Between FARTHEST TWO BIU's - 4
- TAP TO BIU -50'
  AS Follows
  BTU TO BJU - 30' or 4
  BJU TO BIU - 20' or 1

NOTE: All CABLES shown IN CONTROL ROOM UNITS 1 & 2 AND Tech Support center ARE RS-232 UNLESS otherwise specified

MAIN TRUNK CABLE IS 75Ω COAX

BTU TO BJU, BJU TO B CABLES ARE specially d TWIN COAXIAL CABLES

Preliminary
MAXIMUM CABLE Length
SPECIFICATION
FOR
PSE&G Emergency Response Facilities.

11/22/8

ATTACHMENT 2

SALEM GENERATING STATION UNITS 1 AND 2
SAFETY PARAMETER DISPLAY SYSTEM PARAMETERS

1. Neutron Flux - Source, Power, and Intermediate Ranges, Start-up Rate.

2. Rod Control Positions

3. RCS Soluble Boron Concentration

4. RCS Cold Leg Water Temperature

5. RCS Hot Leg Water Temperature

6. RCS Pressure

7. Core Exit Temperature

8. Coolant Level in Reactor

9. Degrees of Subcooling (calculated)

10. Containment Sump Water Level

11. Containment Pressure (Wide and Narrow Range)

12. Containment Isolation Valve Position (excluding check valves)

13. Containment Area Radiation

14. Noble Gas Effluent Radioactivity from Condenser Air Removal System.

15. Containment Hydrogen Concentration

16. Containment Effluent Radioactivity (Plant Vent)

17. Radiation Exposure Rate (Fuel Storage Room, Charging Pump Room, Fuel Handling Building, and Mechanical Penetration Area) [illegible]

18. Radiation Exposure Rate (Electrical Penetration Area)

19. RHR System Flow

20. RHR Heat Exchanger Outlet Temperature

21. Accumulator Tank Level and Pressure
22. Accumulator Isolation Valve Position
23. Boric Acid Charging Flow
24. Flow in HPI System (Charging Pumps Discharge)
25. Flow in LPI System (Safety Inspection Pumps Discharge)
26. Refueling Water Storage Tank Level
27. Reactor Coolant Pump Status
28. Primary System Safety Relief Valve Position
29. Pressurizer Level
30. Pressurizer Heater Status
31. Pressurizer Relief Tank Level
32. Pressurizer Relief Tank Temperature
33. Pressurizer Relief Tank Pressure
34. Steam Generator Level
35. Steam Generator Pressure
36. Main Steam Flow
37. Main Feedwater Flow
38. Auxiliary Feedwater Flow
39. Auxiliary Feedwater Storage Tank Level
40. Containment Spray Flow Additive Rate
41. Heat Removal by the Containment Fan Heat Removal System
42. Containment Atmosphere Temperature
43. Letdown Flow
44. Volume Control Tank Level
45. Component Cooling Water Temperature to ESF System

ATTACHMENT 2 (Continued)

46. Component Cooling Water Flow to ESF System

47. High Level Radioactive Liquid Tank Level

48. Radioactive Gas Hold Up Tank Pressure

49. Control Room Emergency Ventilation Damper Position

50. Auxiliary Building Emergency Damper Position

51. Fuel Handling Building Emergency Damper Position

52. Status of Stanby Power and Other Emergency Energy Sources Important to safety.

53. Control Air

54. Main Steam Radiation

55. Wind Direction

56. Wind Speed

57. Estimation of Atmospheric Stability

58. Steam Generator Blowdown Radiation — [illegible]

59. Condenser Availability (Condenser Vacuum and Circulator Amperes)

60. RCS heat up/cool down rate (Average Loop Temperature)

61. Main Steam Isolation Valve Position

CRITICAL SAFETY FUNCTION STATUS TREES (CFST) BASIS DOCUMENT

1.0 INTRODUCTION

The Critical Safety Function Status Trees ares used to monitor specific plant conditions while the Emergency Operating Procedures are in use. The conditions that are monitored relate directly to the barriers to release of fission products to the environment. These barriers are the fuel matrix and cladding, RCS pressure boundary and Containment.

Protection and Control Systems, augmented by trained operator response to annunciator alarms and backed by Technical Specifications, serve to ensure that small departures from preferred operating conditions are rectified before any challenge to the Critical Safety Functions develops. Failures in system components and the Protection System can create conditions which threaten the integrity of one or more barriers.

The Status Trees determine when these challenges are present and designate Functional Restoration Procedures to use to correct the condition.

2.0 ORGANIZATION

The six Critical Safety Functions evaluated by the Status Trees are necessary to maintain the integrity of the three barriers to fission product release.

The first barrier is the fuel matrix and clad. Three conditions are necessary to maintain fuel integrity during accident conditions:

1. Maintenance of subcriticality to prevent power generation and excessive fuel temperatures.

2. Maintenance of adequate Reactor Coolant inventory to allow Core Cooling.

3. Maintenance of Core Cooling to remove core decay heat.

The second barrier is the RCS pressure boundary. Three conditions necessary to maintain RCS integrity are:

1. Maintenance of the secondary Heat Sink to provide heat removal from the RCS.

2. Prevention of Thermal Shock to the Reactor Vessel which could lead to vessel brittle fracture.

3. Control of Reactor Coolant inventory to prevent filling the pressurizer and loss of RCS pressure control.

The third barrier is the Containment. The Containment Environment (pressure) is controlled to prevent overpressurization of the Containment structure.

The six Status Trees relate to the above conditions as shown in the table below.

Critical Safety Function	Status Tree		Functional Restoration
Subcriticality	3.1	Shutdown Margin	FRSM
Core Cooling	3.2	Core Cooling	FRCC
Secondary Heat Sink	3.3	Heat Sink	FRHS
Thermal Shock	3.4	Thermal Shock	FRTS
Containment	3.5	Containment Environment	FRCE
Reactor Coolant Inventory	3.6	Coolant Inventory	FRCI

Also shown is the Functional Restoration block used by each Status Tree to restore threatened Critical Safety Functions.

3.0 CFST USE

3.1 Status Tree Scanning

The Status Trees are used by an SRO licensed individual in the Control Room to monitor Critical Safety Functions while the Desk Operator and Control Operator respond to a unit trip or Safety Injection with the Emergency Operating Procedures.

Status Tree scanning begins when EOP-TRIP-1, "Reactor Trip or Safety Injection" is departed. EOP-TRIP-1 also directs Status Tree use if the SI cannot be terminated but the problem has not been diagnosed. The Status Trees are evaluated in order while the fault specific EOP is conducted. The Status Trees are scanned continuously until all Critical Safety Functions are satisfied. The Status Trees are then scanned periodically until the event is terminated.

3.2 Functional Restoration Priorities

Priority of a Status Tree designated Functional Restoration is determined by the color of the condition and the order of the Status Trees. Red is the highest priority condition, followed by orange and yellow. Green is used to signify that a Critical Safety Function is satisfied. The Status Trees are arranged in descending order of priority.

Color is considered first, then order. Thus a Red condition on Status Tree 3.1 would have priority over all other challenges to Critical Safety Functions. Likewise an Orange condition on Status Tree 3.5 would have priority over a Yellow condition on any Status Tree.

3.3 Response to an Unsatisfied CSF

When a CSF is evaluated as unsatisfied a Functional Restoration is identified. Performing the Function Restoration removes the challenge to the CSF. A Red condition requires immediate suspension of the EOP in use. The current step is noted and the page marked for later reference. The Functional Restoration is initiated and continues until the challenge is removed. The EOP in effect is then resumed unless an additional Red condition is present. Note that if a Red condition is identified while a Functional Restoration is in progress for a lower priority Red condition, the lower priority procedure is suspended and the higher priority Functional Restoration initiated.

When an Orange condition is encountered, note the associated Functional Restoration and continue tree evaluation. When the current pass through the Status Trees is complete, initiate the Orange related Functional Restorations in order of importance.

A Yellow condition is a slight challenge to a CSF and could lead to a serious challenge if not corrected. Initiate Yellow condition Functional Restorations when practical.

4.0 <u>REFERENCES</u>

4.1 WOG Guideline F-0 "Critical Safety Function Status Trees" Rev HP-Basic.

END OF PROCEDURE
FINAL PAGE

EMERGENCY OPERATING PROCEDURE
EOP-CFST-1
CRITICAL SAFETY FUNCTION STATUS TREES

1.0 ENTRY CONDITIONS

1.1 EOP-TRIP-1.

2.0 STATUS TREE USAGE

2.1 Initiate CRT tests 23 and 41 to facilitate monitoring CORE EXIT TC's. If PRODAC 250 not available, then direct Performance Department to perform Emergency Surveillance Procedure PD-14.3.010, "Extended Range Reading of Incore Thermocouples" and establish contact with operator monitoring CSFT.

2.2 START Status Tree evaluation after departing EOP-TRIP-1, "Reactor Trip or Safety Injection."

2.3 IF a Red is encountered, immediately go to the designated functional restoration procedure. The EOP in effect is resumed when the Function Restoration is completed unless otherwise directed.

2.4 IF an Orange is encountered, note the designated functional restoration procedure and continue status tree evaluation. When the current pass through the trees is complete, initiate the designated procedures in order of importance unless otherwise directed.

2.5 IF a Yellow is encountered, note the nature of the deficiency and continue status tree evaluation. When practical, initiate the designated procedures unless otherwise directed.

2.6 The Status Trees are arranged in descending order of importance. Consider the condition color and then the procedure order to determine the priority among a group of Functional Restorations.

2.7 Red conditions require suspension of the procedure in effect. Orange and Yellow condition Functional Restorations take precedence over any conflicting procedure steps in the EOP in effect.

3.0 Critical Safety Function Status Trees

3.1 Shutdown Margin.

3.2 Core Cooling.

3.3 Heat Sink.

3.4 Thermal Shock.

3.5 Containment Environment.

3.6 Coolant Inventory.

END OF PROCEDURE

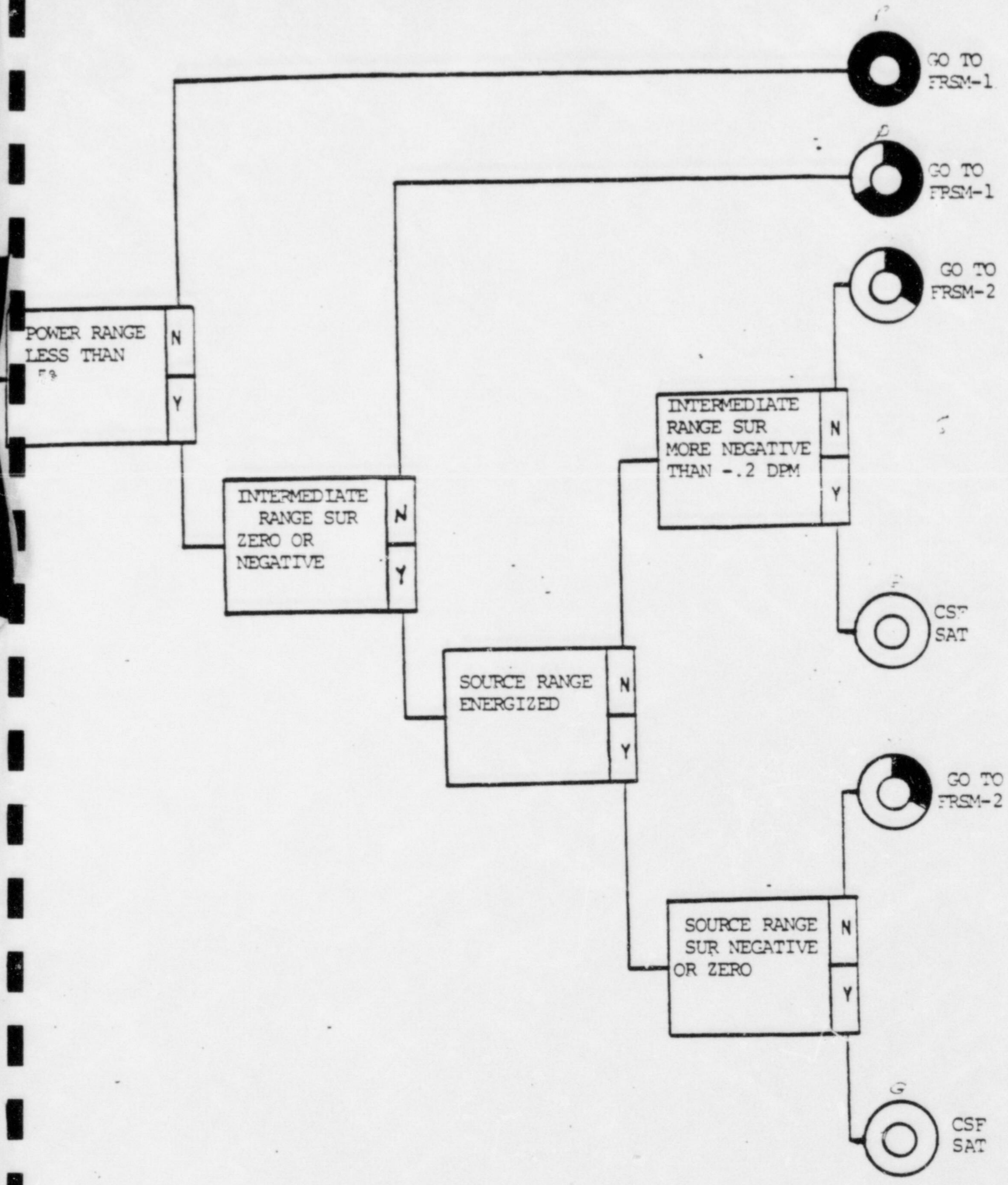
FINAL PAGE

Attachment 4

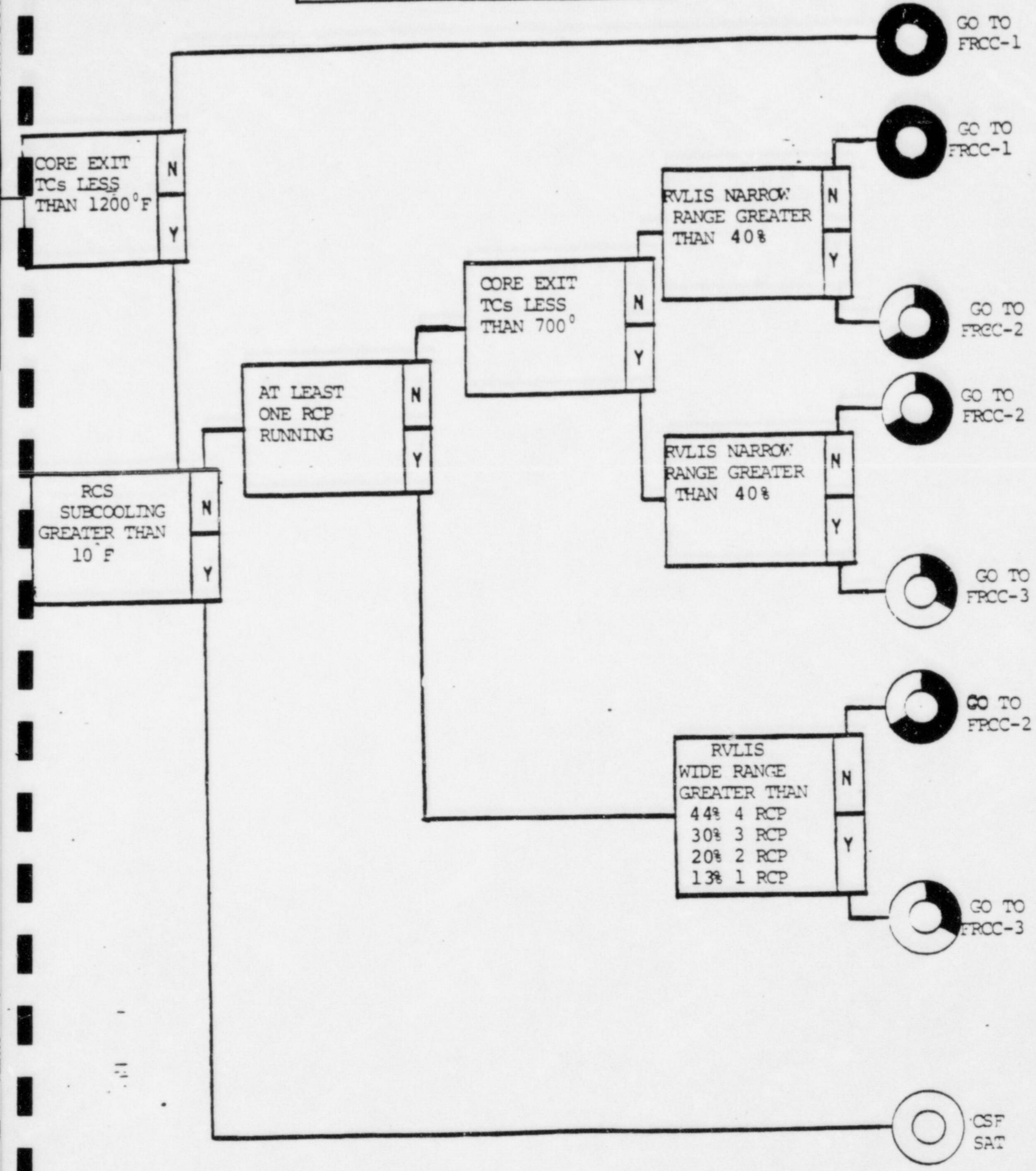
CRITICAL SAFETY FUNCTION

STATUS TREES

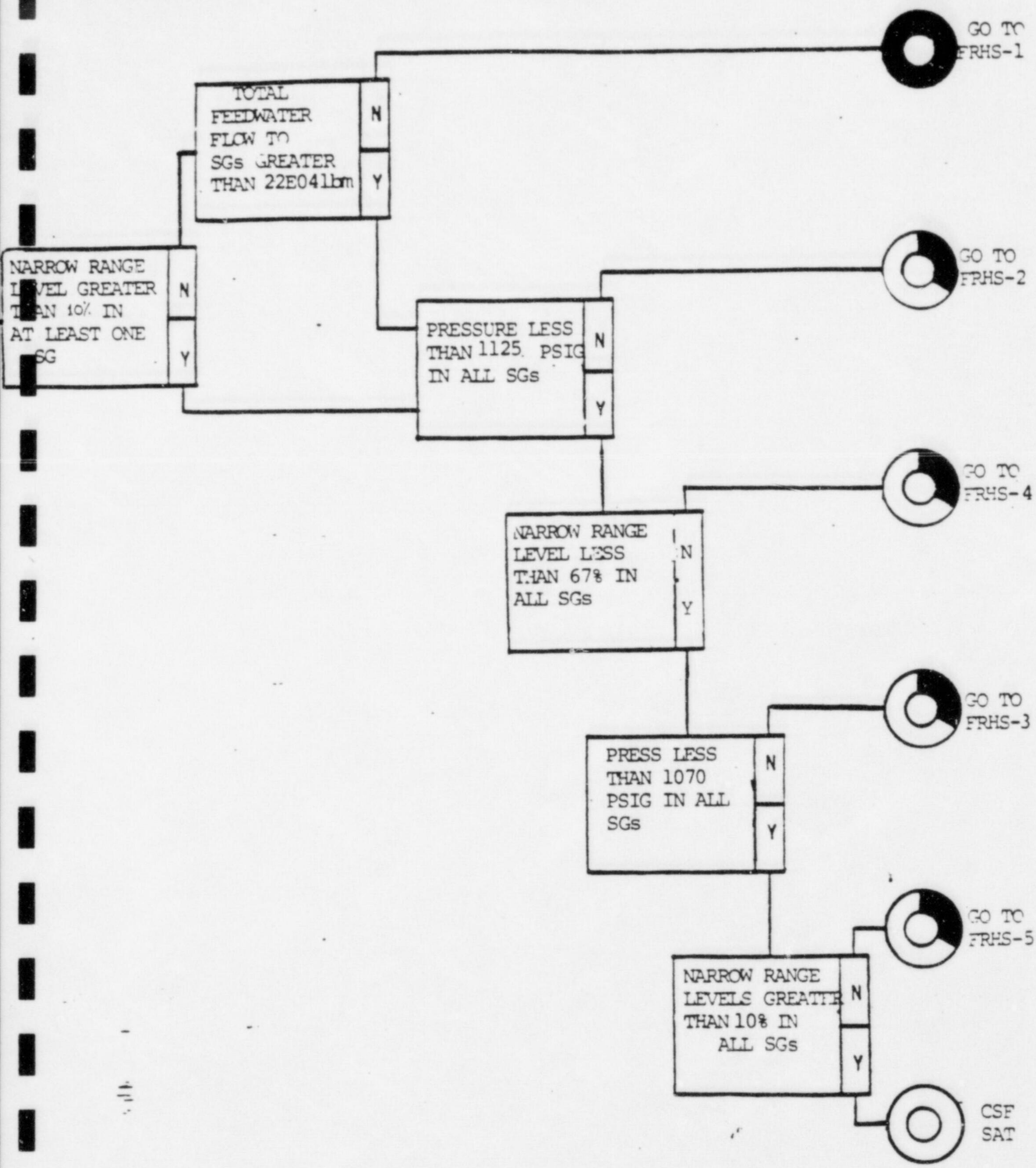
3.1 SHUTDOWN MARGIN



3.2 CORE COOLING

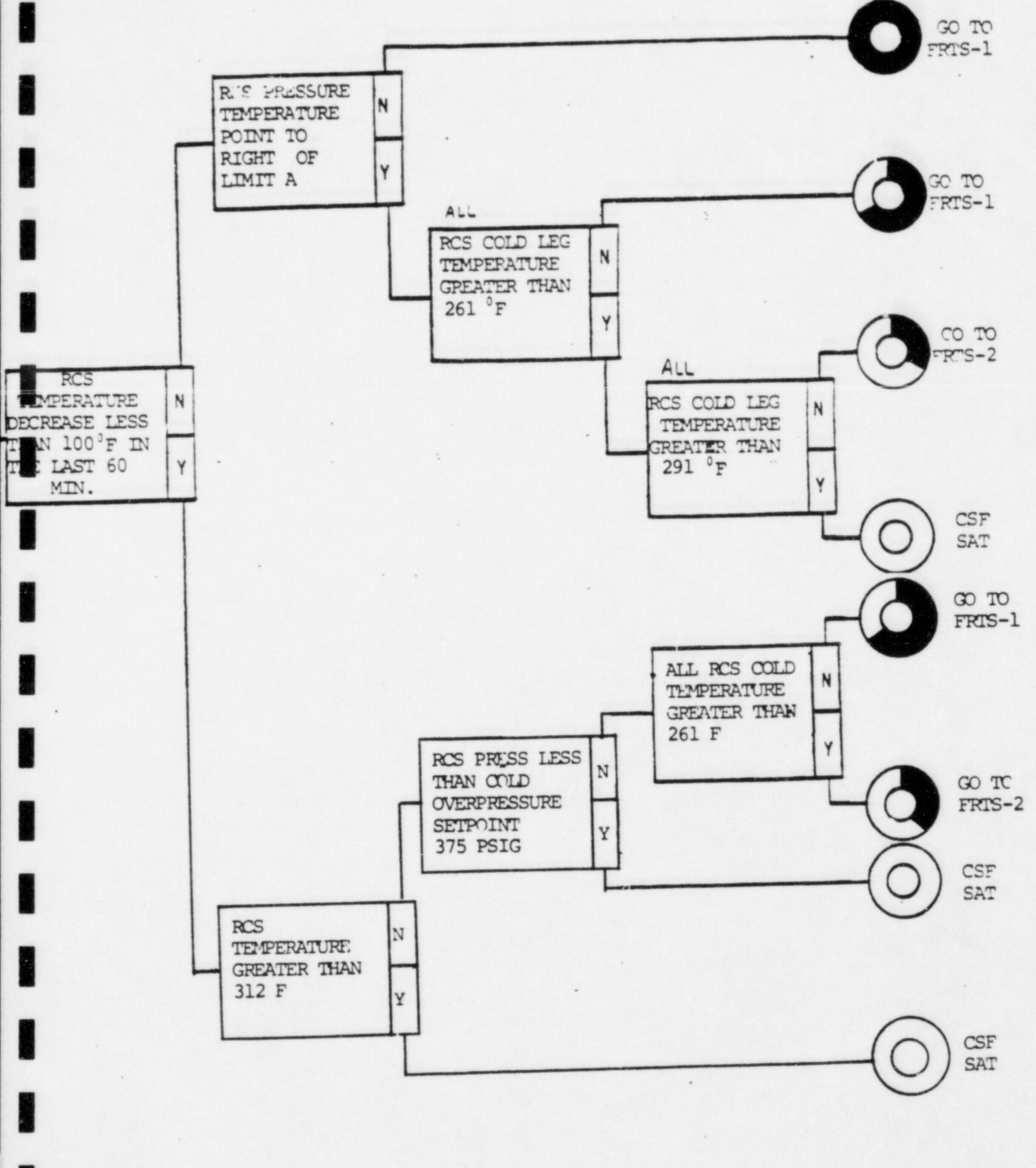

CORE EXIT TCs LESS THAN 1200°F
N
Y
GO TO FRCC-1
RCS SUBCOOLING GREATER THAN 10°F
N
Y
AT LEAST ONE RCP RUNNING
N
Y
CORE EXIT TCs LESS THAN 700°
N
Y
RVLIS NARROW RANGE GREATER THAN 40%
N
Y
GO TO FRCC-1
GO TO FRCC-2
RVLIS NARROW RANGE GREATER THAN 40%
N
Y
GO TO FRCC-2
GO TO FRCC-3
RVLIS WIDE RANGE GREATER THAN
44% 4 RCP
30% 3 RCP
20% 2 RCP
13% 1 RCP
N
Y
GO TO FRCC-2
GO TO FRCC-3
CSF SAT

3.3 HEAT SINK

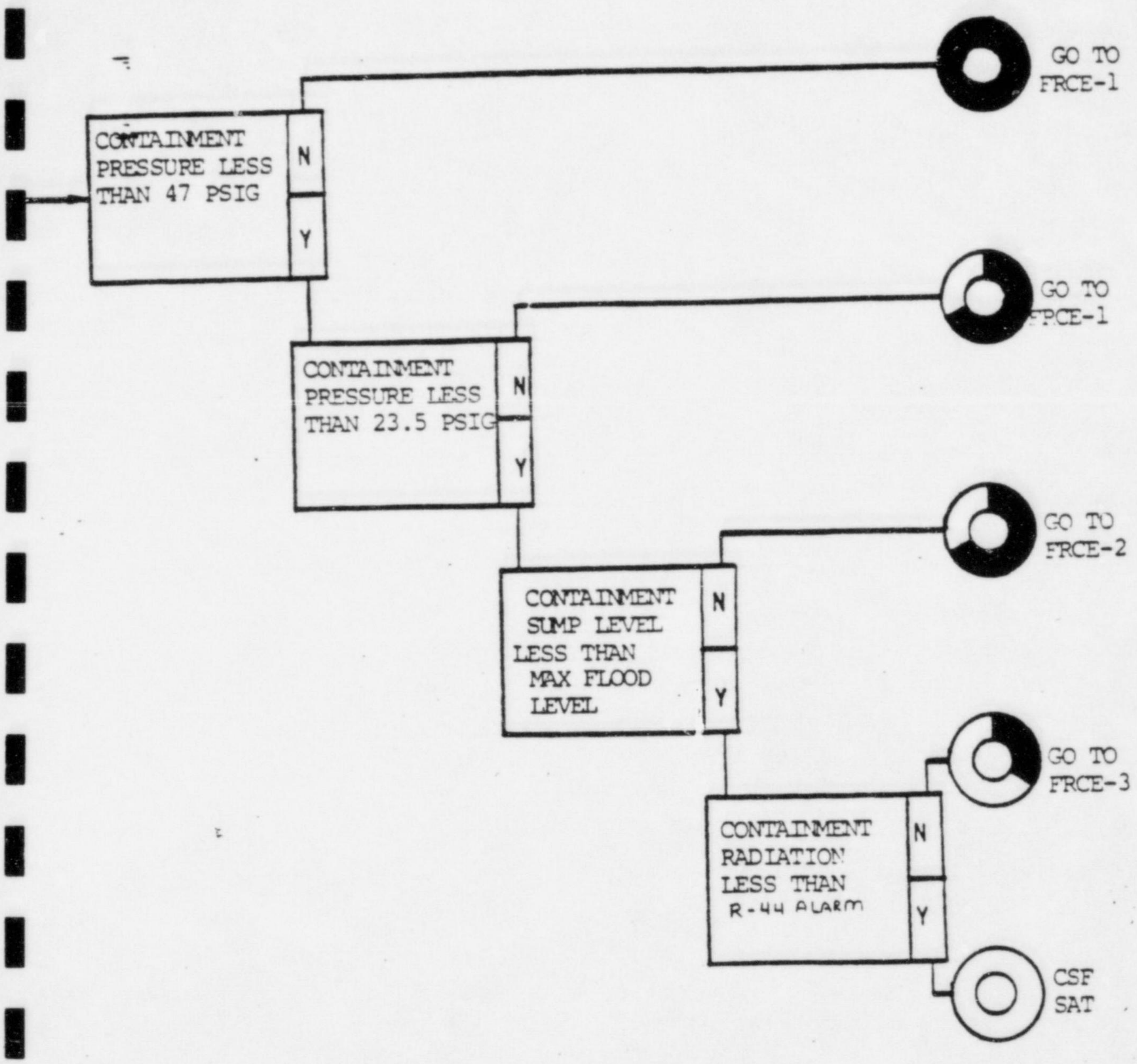


NARROW RANGE LEVEL GREATER THAN 10% IN AT LEAST ONE SG
N
Y
TOTAL FEEDWATER FLOW TO SGs GREATER THAN 22E04lbm
N
Y
GO TO FRHS-1
PRESSURE LESS THAN 1125 PSIG IN ALL SGs
N
Y
GO TO FRHS-2
NARROW RANGE LEVEL LESS THAN 67% IN ALL SGs
N
Y
GO TO FRHS-4
PRESS LESS THAN 1070 PSIG IN ALL SGs
N
Y
GO TO FRHS-3
NARROW RANGE LEVELS GREATER THAN 10% IN ALL SGs
N
Y
GO TO FRHS-5
CSF SAT

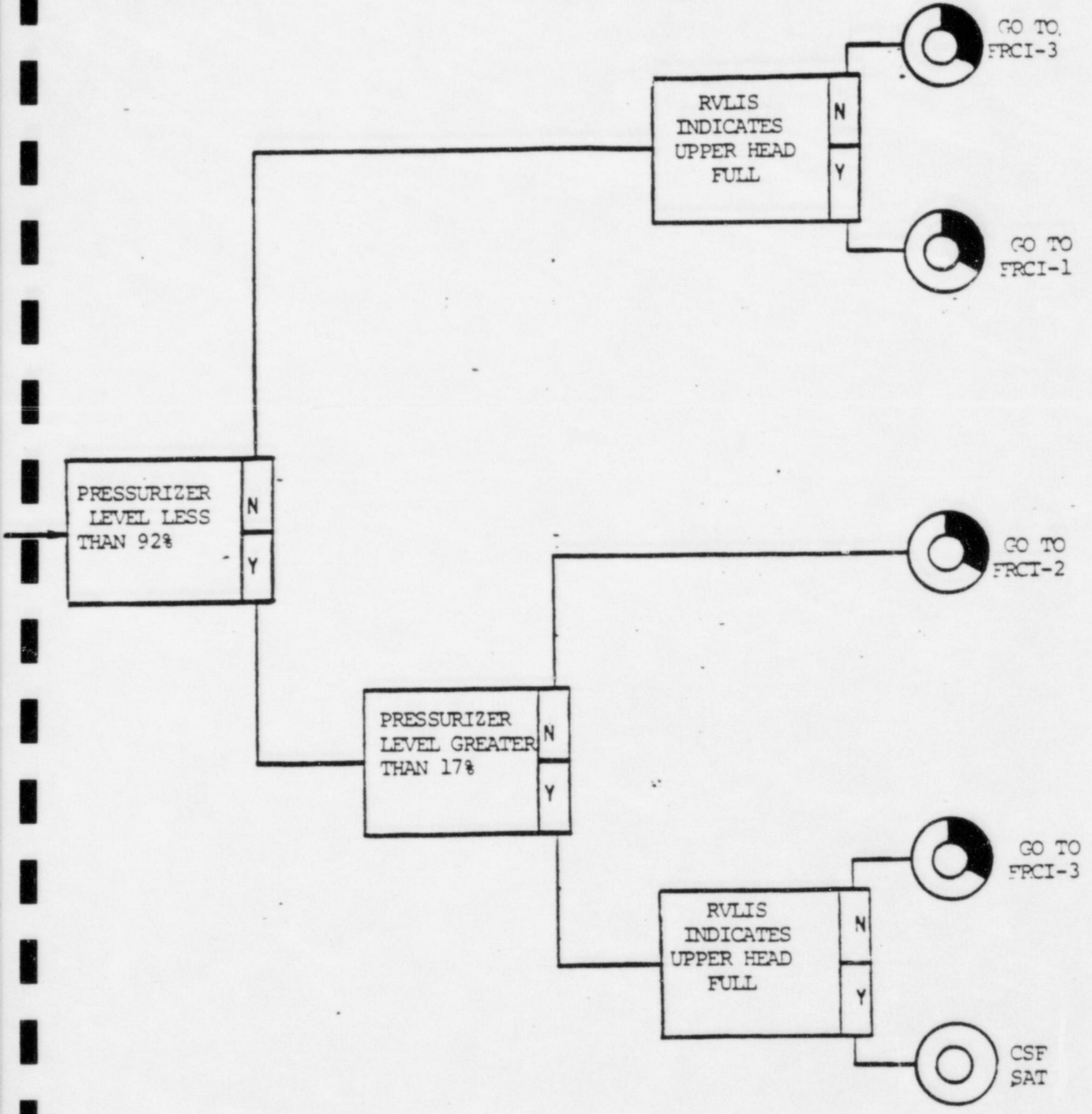
3.4 THERMAL SHOCK


RCS TEMPERATURE DECREASE LESS THAN 100°F IN THE LAST 60 MIN.
N
Y
RCS PRESSURE TEMPERATURE POINT TO RIGHT OF LIMIT A
N
Y
GO TO FRTS-1
ALL
RCS COLD LEG TEMPERATURE GREATER THAN 261 °F
N
Y
GO TO FRTS-1
ALL
RCS COLD LEG TEMPERATURE GREATER THAN 291 °F
N
Y
GO TO FRTS-2
CSF SAT
RCS TEMPERATURE GREATER THAN 312 F
N
Y
RCS PRESS LESS THAN COLD OVERPRESSURE SETPOINT 375 PSIG
N
Y
ALL RCS COLD TEMPERATURE GREATER THAN 261 F
N
Y
GO TO FRTS-1
GO TO FRTS-2
CSF SAT
CSF SAT

3.5 CONTAINMENT ENVIORNMENT


CONTAINMENT PRESSURE LESS THAN 47 PSIG
N
Y
GO TO FRCE-1
CONTAINMENT PRESSURE LESS THAN 23.5 PSIG
N
Y
GO TO FRCE-1
CONTAINMENT SUMP LEVEL LESS THAN MAX FLOOD LEVEL
N
Y
GO TO FRCE-2
CONTAINMENT RADIATION LESS THAN R-44 ALARM
N
Y
GO TO FRCE-3
CSF SAT

3.6 COOLANT INVENTORY


PRESSURIZER LEVEL LESS THAN 92%
N
Y
RVLIS INDICATES UPPER HEAD FULL
N
Y
GO TO FRCI-3
GO TO FRCI-1
PRESSURIZER LEVEL GREATER THAN 17%
N
Y
GO TO FRCI-2
RVLIS INDICATES UPPER HEAD FULL
N
Y
GO TO FRCI-3
CSF SAT

SAFETY PARAMETER DISPLAY SYSTEM IMPLEMENTATION PLAN

1. SCHEDULE

a.	DESIGN PHASE	9/84
b.	DEVELOPMENT PHASE	9/85
c.	INSTALLATION PHASE	12/85
d.	FIELD TESTING, OPERATION AND ACCEPTANCE PHASE	5/86
e.	FULLY OPERATIONAL	12/86

2. VERIFICATION AND VALIDATION PLAN

Verification and validation will be conducted by the computer system vendor. The program will be developed using NSAC-39 "Verification and Validation for Safety Parameter Display Systems" as guidance and will address the traceability of requirements of hardware and software and provide independent review. The V & V activities will be performed by a team which is completely independent of the development effort.

(REVISED) HUMAN FACTORS SPDS GUIDELINES

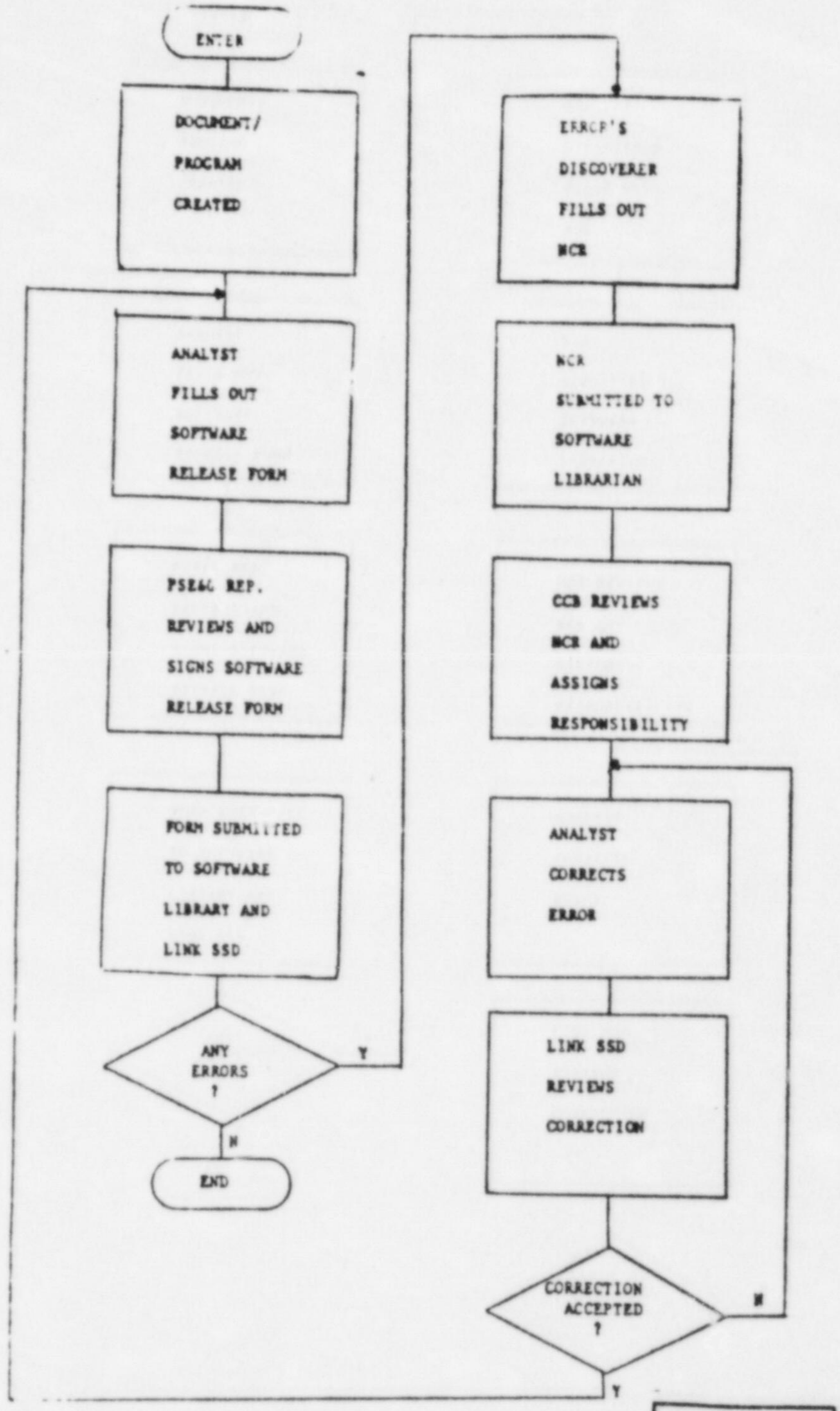
Prepared for
Public Service Electric and Gas
Salem Station Units 1 and 2

GP-R-211010

August 8, 1985

General Physics Corporation
Columbia, Maryland

TABLE OF CONTENTS



Link
SIMULATION SYSTEMS DIVISION
THE SINGER COMPANY

SOFTWARE RELEASE FORM

The following is submitted to configuration **management control:**

□ Document # ____________ Title ________________

□ Program Name ____________

This is a □ complete release

□ partial release

If partial release, explain: ______________________________

____

This is □ original release

□ revision

If revision, list all relevant NCRs ____________

____

____

____

____

Released by ________________ ____________
Systems Engineer Date

Approved by ________________ ____________
Systems Engineer Date

DOCUMENT #	DOCUMENT TITLE	LEVEL		DATE	ENGINEER	V&V REVIEW BY	DATE	NCR'S GENERATED	NCR'S INCORPORATED
		REVISION	CHANGE						
PS-LVC-006	Bulk Verification Program	0		6/5/85	RM	LR			
PS-LVC-017	Operational Limits Curve Display Background Generator	0		8/8/85	ML	TM			
PS-LVC-019	Alarms	0		8/16/85	RVW	TM	8/12/85	920-922	
PS-LVC-024	IDT/Host Communications Protocol	0		8/13/85	AM	TM	8/26/85	926-931	
PS-LVB-022	Report Formats	0		8/13/85	MM	LR	8/28/85		
PS-LVB-023	Alarm Message Format	0		8/13/85	MM	LR	8/29/85	950, 951	
PS-LVC-021	Fluid Property Calculations	0		8/16/85	ML	TM	8/23/85	925	
PS-LVC-001	ERF Computer Data Base	0		8/9/85	MM	TM/KO	8/22/85	923	
PS-LVB-025	Off-Line Diagnostics listing for Gould SEL 32/87	0		8/21/85	SB	TM/NL	9/18/85		
PS-LVB-026	Failover	0		8/28/85	ML	TM	9/10/85		
PS-LVB-022	Report Formats	0	1	8/26/85	MM	LR	9/10/85		
PS-LVC-001	ERF Computer Data Base	1		8/26/85	MM	TM	9/12/85		923
PS-LVB-017	SPDS Displays	0	1	8/26/85	MM	TM	9/16/85	975, 976	
PS-LVC-022	Report Formats	0		9/12/85	MM	LR	10/2/85	961-964	
PS-LVB-011	Sequence of Events	1		9/25/85	CB	TM	10/2/85		
PS-LVC-011	Sequence of Events	1		9/25/85	CB	TM	10/3/85	958,960	

PROGRAM NAME	DESCRIPTION	DATE	ENGINEER	NCR'S GENERATED	NCR'S INCORPORATED
BUBOLC	Bubblepic Operational Limits Curve	8/16/85	ML	924	
PTGEN	Generate Steam Table P(T)	8/20/85	ML	954	
TPGEN	Generata Steam Table T(P)	8/20/85	ML	934	
PSATT	Calculate saturation pressure for temperature	8/20/85	ML		
TSATP	Calculate saturation temperature for pressure	8/20/85	ML		
SOEFMT	SOE Print Formatter	9/17/85	CB		
SOEHFI	Initialize SOE History File	9/17/85	CB		
SOEP	SOE Processor	9/17/85	CB		
SOERPT	SOE Report Processor	9/17/85	CB		
SOETRP	Request SOE Trip Report	9/17/85	CB		
BOMNI	Build DC Data Base	9/17/85	CB		
DCDIG	Process DC Digital Input Points	9/17/85	CB		
DCDRVR	DC Driver/Receiver Program	9/17/85	CB		
DCERR	Process DIS/PIU Error/Return to Operation	9/17/85	CB		
DCINIT	Initialize DC Common	9/17/85	CB		
DCOUT	Process Digital and Analog Output Requests	9/17/85	CB		

REVISION HISTORY

REVISION #	DATE	CHANGE DATE	CHANGED PAGES	MCR # (S)

Figure 3-1 Revision History Page

Link

THE SINGER COMPANY

NON-CONFORMANCE REPORT

REPORT NO. ____________

SYSTEM NAME ____________

DEFICIENCY DISCOVERY SECTION

TEST INVESTIGATOR ____________ DATE ____________

LOCATION ____________ TIME ____________

SYSTEM MODULE NAME ____________

PROGRAM MODULE NAME ____________

MODULE(S) CONFIGURATION LEVEL NO. ____________

REFERENCE DESIGN DOCUMENT ____________

DEFICIENCY DESCRIPTION

EXPECTED RESULTS

CORRECTION IMPORTANCE/NEED DATE ____________

Link

THE SINGER COMPANY

NON-CONFORMANCE REPORT

REPORT NO. ____________ SYSTEM NAME ____________

DEFICIENCY ANALYSIS SECTION

NAME OF ANALYST ____________ DATE ____________

SYSTEM MODULE NAME ____________

PROGRAM MODULE NAME ____________

MODULE(S) CONFIGURATION LEVEL NO. ____________

REFERENCE DESIGN DOCUMENT ____________

ANALYSIS FINDINGS

DEFICIENCY CORRECTION IMPLEMENTATION

PROBLEM CATEGORY

□ DESIGN □ DATA DEFINITION □ LOGIC □ INTERFACE

□ DATA HANDLING □ SPECIFICATION □ OTHER ____________

NEW CONFIGURATION LEVEL NO. ____________

DOCUMENTATION UPDATED (Y/N) ____________ REV. NO. ____________

CORRECTED BY (ANALYST) ____________ DATE ____________

LINK ACCEPTANCE BY ____________ DATE ____________

REJECTION BY ____________ DATE ____________

Link

NONCONFORMANCE REPORT

REPORT NO. NCR-045

SYSTEM NAME Salem ERF

DEFICIENCY DISCOVERY SECTION

TEST INVESTIGATOR T. Morrow

DATE 4/18/85

LOCATION Singer-Link

TIME

SYSTEM MODULE NAME

PROGRAM MODULE NAME

MODULE(S) CONFIGURATION LEVEL NO.

REFERENCE DESIGN DOCUMENT PS-LVB-008 System Parameters Specification

DEFICIENCY DESCRIPTION P 4 SYMBOL ALACLR: comment states that value = 3 is blue. Value = 3 is yellow, 4 is blue per PACE Programmers Manual.

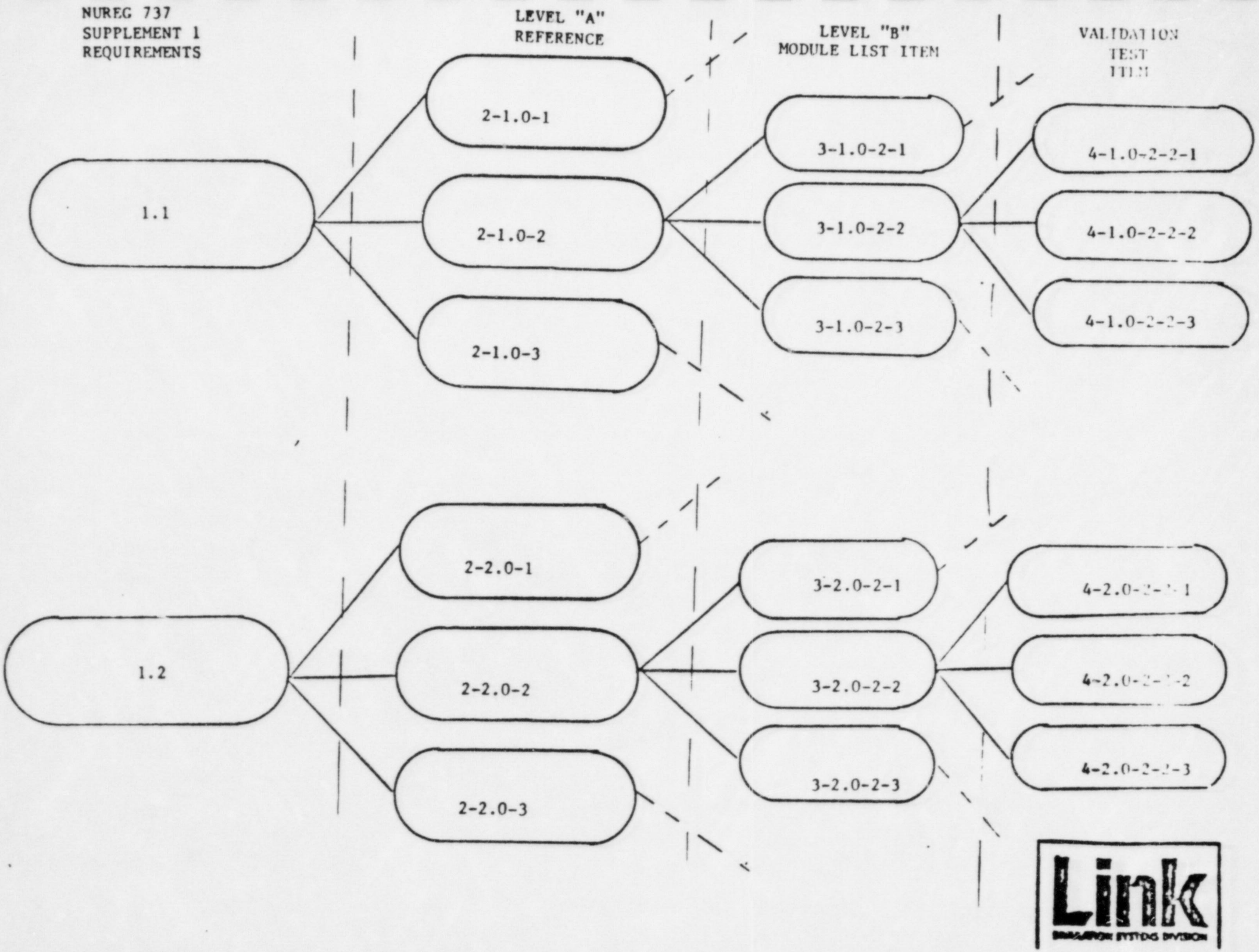
EXPECTED RESULTS Change comment to yellow or value to 4.

NCR #	DESCRIPTION	ACCEPTED/ REJECTED	DATE ASSIGNED	ANALYST	IMPORTANCE	CATEGORY	CORRECTION DATE	LINK ACCEPTANCE DATE
1	IDT Runtime Module-Appendix A 'functions missing'	A	5/8/85	AM	Necessity	Spec	5/9/85	9/13/85
2	IDT Runtime Module-Appendix A no introductory test	A	5/8/85	AM	Necessity	Spec.	5/9/85	9/13/85
3	IDT Runtime Module-SectionIV multiple defines	A	5/8/85	AM	Necessity	Spec.	5/9/85	9/13/85
4	IDT Dynamic Editor-Appendix B 'functions' missing	A	5/8/85	AM	Necessity	Spec.	5/9/85	9/13/85
5	IDT Dynamic Editor-Appendix B no introductory text	A	5/8/85	AM	Necessity	Spec.	5/9/85	9/13/85
6	IDT Dynamic Editor-SectionIV multiple defines	A	5/8/85	AM	Necessity	Spec.	5/9/85	9/13/85
7	SPDS Points List (D5/6 and D5/13)-point counts inconsistent	R (not a problem)				Spec.	5/9/85	9/13/85
8	OMNI Igtelligent DAS-'Applicable Documents' and 'Acceptance Test' missing	A	4/23/85	AM	Necessity	Documentation	5/8/85	9/13/85
9	OMNI Intelligent DAS-demand scan function need	A	4/23/85	AM	Necessity	Documentation	5/8/85	9/13/85
10	OMNI Intelligent DAS6 LevelA maximum EBC points/second	A	5/8/85	AM	Necessity	Documentation	5/8/85	9/13/85
11	OMNI Intelligent DAS format layouts for PV and DI missing	A	5/8/85	AM	Necessity	Documentation	5/8/85	9/13/85
12	Level A-3.15.2 Appendix missing	A	5/8/85	AM	Necessity	Documentation	5/8/85	9/13/85
13	Level A-3.15.3.4 -Figure 2 is missing	A	5/8/85	AM	Necessity	Documentation	5/8/85	9/13/85

Requirements PHASE REVIEW PROCESS

TEST FACTOR: Correctness

	REVIEW CRITERIA	ASSESSMENT				DESCRIPTION	APPROACH
		VA	A	IA	NA		
1.	Can the data required by the application be collected with the desired degree of reliability?			X		Confirm the data inputs can be generated with the desired degree of reliability.	Fact finding
2.	Can the data be collected within the time period specified?			X		Confirm the data base has been established within the required time frame.	Fact finding
3.	Have the user requirements been defined in writing?	X				Confirm with the user that the requirements in writing are complete.	Checklist
4.	Are the requirements stated in measurable terms?		X			Examine the reasonableness of the criteria for measuring successful completion of the requirements.	Walk-throughs
5.	Has the project solution addressed the user requirements?		X			Examine the system specifications to confirm that they satisfy stated objectives .	Walk-throughs
6.	Could test data be developed to test the achievement of the objectives?		X			Verify that the requirements are stated in enough detail that they could generate test data to verify compliance.	Test data
7.	Have procedures been specified to evaluate the implemented system to ensure the requirements are achieved?		X			Examine the specifications which indicate that a post-installation review will occur.	Confirmation/ examination


NUREG 737
SUPPLEMENT 1
REQUIREMENTS
LEVEL "A"
REFERENCE
LEVEL "B"
MODULE LIST ITEM
VALIDATION
TEST
ITEM
1.1
2-1.0-1
2-1.0-2
2-1.0-3
3-1.0-2-1
3-1.0-2-2
3-1.0-2-3
4-1.0-2-2-1
4-1.0-2-2-2
4-1.0-2-2-3
1.2
2-2.0-1
2-2.0-2
2-2.0-3
3-2.0-2-1
3-2.0-2-2
3-2.0-2-3
4-2.0-2-2-1
4-2.0-2-2-2
4-2.0-2-2-3
Link
SIMULATION SYSTEMS DIVISION

TRACEABILITY MATRIX - LEVEL 1

1-1.0 SPDS should provide a concise display of critical plant variables to the control room operators to aid them in rapidly and reliably determining the safety status of the plant. Although the SPDS will be operated during normal operations as well as during abnormal conditions, the principle purpose and function of the SPDS is to aid the control room personnel during abnormal and emergency conditions in determining the safety status of the palnt and in assessing whether abnormal conditions warrant corrective action by operators to avoid a degraded core. This can be particularly important during anticipated transients and the initial phase of an accident.

1-2.0 Each operating reactor shall be provided with a Safety Parameter Display System that is located convenient to the control room operators. This system will continuously display information from which the plant safety status can be readily and reliably assessed by control room personnel who are responsible for the avoidance of degraded and damaged core events.

1-3.0 The control room instrumentation required provides the operators with the information necessary for safe reactor operation under normal, transient, and accident conditions. The SPDS is used in addition to the basic components and serves to aid and augment these components. Thus, requirements applicable to control room instrumentation are not needed for this augmentation. The SPDS need not meet requirements of the single-failure criteria and it need not be qualified to meet Class 1E requirements.

1-3.1 SPDS shall be suitably isolated from electrical and electronic interference with equipment and sensors that are in use for safety systems. The SPDS need not be seismically qualified, and additional seismically qualified indication is not required for the sole purpose of being a backup for SPDS. Procedures which describe the timely and correct safety status assessment when the SPDS is and is not available will be developed by the licensee in parallel with SPDS.

1-3.2 Operators should be trained to respond to accident conditions both with and without the SPDS available.

1-4.0 There is a wide range of useful information that can be provided by various systems. This information is reflected in such staff documents as NUREG-0696, NUREG-0835, and Regulatory Guide 1.97. Prompt implementation of an SPDS can provide an important contribution to plant saftey.
The selection of specific information that should be provided for a particular plant shall be based on engineering judgement of individual plant licensees, taking into account the importance of prompt implementation.

TRACEABILITY MATRIX - LEVEL 2

2-1.0-1	3.15.8.1	SPDS will concentrate a set of plant parameters or derived variables onto the Safety Parameter Displays.
2-1.0-2	3.15.8.9	Alarms, alarm clears, and significant alarms are to be displayed.
2-1.0-3	3.15.8.10	Display area to be dedicated to graphic displays, graphic trending, operator guidance, etc.
2-1.0-4	3.15.8.12	Top Level Displays
2-1.0-5	3.15.8.13	Second Level Displays
2-1.0-6	3.15.8.14	Third Level Displays
2-1.0-7	3.15.8.15	Fourth Level Displays
2-2.0-1	3.15.8.1	SPDS will concentrate a set of plant parameters or derived variables onto the Safety Parameter Displays.
2-2.0-2	3.15.8.9	Alarms, alarm clears, and significant alarms are to be displayed.
2-2.0-3	3.15.8.10	Display area to be dedicated to graphic displays, graphic trending, operator guidance, etc.
2-2.0-4	3.15.8.12	Top Level Displays
2-2.0-5	3.15.8.13	Second Level Displays
2-2.0-6	3.15.8.14	Third Level Displays
2-2.0-7	3.15.8.15	Fourth Level Displays
2-3.0-1	3.15.8.1	SPDS
2-3.1-1	3.15.2.1	Multiplexor Subsystem to receive most of its inputs in parallel with existing process monitoring/control devices.
2-3.2-1	3.7	ERF offers the capability to aid qualified personnel to assess safety status during normal and abnormal operations.
2-4.0-1	3.15.8.1	SPDS
2-4.0-2	3.15.8.9	Alarm Area

TRACEABILITY MATRIX - LEVEL 3

3-1.0-1-1	PP-2.1.12	Display Retriever
3-1.0-1-2	PS-LVB-008	System Parameters
3-1.0-2-1	PP-2.1.15	CRT Alarm Acknowledge Service Program
3-1.0-2-2	PP-2.2.2	CRT Acknowledge All Alarm Service Program
3-1.0-2-3	PU-2.9	Alarms and Messages
3-1.0-2-4	PU-3.15	Alarms and Messages
3-1.0-2-5	PU-9	Alarms and Messages
3-1.0-2-6	PT-2.25	PV Alarm Checking Records
3-1.0-2-7	PT-2.31	PV Alarm Group File
3-1.0-2-8	PT-2.37	DI Alarm Group File
3-1.0-2-9	PS-LVB-008	System Parameters
3-1.0-2-10	PS-LVB-013	Processor Mode Alarm Message Data
3-1.0-2-11	PS-LVB-019	Alarms
3-1.0-3-1	PP-2.2.9	CRT Data Entry Service Program
3-1.0-3-2	PP-2.2.13	CRT Local Function Key Service Program
3-1.0-3-3	PS-LVB-013	Processor Mode Real Time Graphics
3-1.0-4-1	PS-LVB-017	Top Level Displays
3-1.0-5-1	PS-LVB-017	Second Level Displays
3-1.0-6-1	PS-LVB-017	Third Level Displays
3-1.0-7-1	PS-LVB-017	Fourth Level Displays
3-2.0-1-1	PP-2.1.12	Display Retriever
3-2.0-1-2	PS-LVB-008	System Parameters
3-2.0-2-1	PP-2.1.15	CRT Alarm Acknowledge Service Program
3-2.0-2-2	PP-2.2.2	CRT Acknowledge All Alarm Service Program
3-2.0-2-3	PU-2.9	Alarms and Messages

TRACEABILITY MATRIX - LEVEL 4

4-1.0-1-1-1	DISRET (PACE)
4-1.0-1-2-1	System Parameters (PACE)
4-1.0-2-1-1	ALMACK (PACE)
4-1.0-2-2-1	ACKALL (PACE)
4-1.0-2-3-1	PACE Alarms and Messages (General)
4-1.0-2-4-1	PACE Form 750A
4-1.0-2-4-2	PACE Form 750B
4-1.0-2-4-3	PACE Form 750C
4-1.0-2-4-4	PACE Form 750D
4-1.0-2-4-5	PACE Form 752A
4-1.0-2-4-6	PACE Form 752B
4-1.0-2-4-7	PACE Form 752C
4-1.0-2-5-1	Alarm Display/Acknowledgement
4-1.0-2-6-1	PACE File 152
4-1.0-2-7-1	PACE File 164
4-1.0-2-8-1	PACE File 178
4-1.0-2-9-1	System Parameters (PACE)
4-1.0-2-10-1	PRISM
4-1.0-2-11-1	ALAID
4-1.0-3-1-1	CPACTN (PACE)
4-1.0-3-2-1	CPLOCF (PACE)
4-1.0-3-3-1	CENTRY (PACE)
4-1.0-4-1-1	Top Level Displays
4-1.0-5-1-1	Second Level Displays

TRACEABILITY MATRIX - LEVEL 2

2-19.0-12	3.15.8.27	Add/Delete Trend
2-19.0-13	3.15.8.27	Date/Time Update
2-19.0-14	3.15.8.27	Calibrate Point
2-20		Display Editor
2-20.0-1	3.15.9	Display Editor
2-20.0-2	3.15.9.1	Shape Editor
2-21		SEL FORTRAN
2-21.0-1	3.15.3.19	Real-Time FORTRAN
2-21.0-2	3.15.3.20	FORTRAN Library

TRACEABILITY MATRIX - LEVEL 3

3-20.0-2-2	PS-LVB-005	IDT Run Time Module
3-21.0-1-1	PS-LVB-010	SEL FORTRAN I/O Support Routines
3-21.0-1-2	PS-LVB-012	SEL FORTRAN Translation Support Routines
3-21.0-2-1	PS-LVB-010	SEL FORTRAN I/O Support Routines
3-21.0-2-2	PS-LVB-012	SEL FORTRAN Translation Support Routines

PP: PACE32 Programmer Manual
PT: PACE32 Technical Manual
PU: PACE32 User Manual
CC: CPI RTP Digital Analog Loopback and Calibration Card Technical Manual
IRCU: CPI RTP Intelligent Remote Control Unit Technical Manual
DA: CPI Data Acquisition System Technical Manual
AI: CPI RTP7436 Series Universal Analog Input Card Set

TRACEABILITY MATRIX - LEVEL 4

4-19.0-14-1-1	PRISM
4-19.0-14-1-2	
4-20.0-1-1-1	REAL
4-20.0-1-2-1	ARCHIE
4-20.0-1-3-1	PRISM
4-20.0-2-1-1	REAL
4-20.0-2-2-1	ARCHIE
4-21.0-1-1-1	N:FCBIO
4-21.0-1-2-1	N:XLATE
4-21.0-2-1-1	N:FCBIO
4-21.0-2-2-1	N:XLATE

Software Design Phase Review Process
Test Factor: Completeness

		ASSESSMENT						
	REVIEW CRITERIA	VA	A	IA	UA	DESCRIPTION	APPROACH	NCR
1.	Are all subsystem interfaces defined?					Confirm all subsystem interfaces.	Confirmation/ examination	
2.	Have all operating sequences been addressed? (e.g., start-up, restart, initialization, error detection).					Verify all operating sequences.	Confirmation/ examination	
3.	Are all algorithms defined?					Verify all algorithms used have descriptions.	Checklist	
4.	Are all system requirements addressed?					Confirm requirements are addressed.	Traceability matrix	
5.	Are any special utility programs required?					Verify utilities are defined.	Checklist	
6.	Are all interfaces to the executive defined?					Verify executive interfaces are correct.	Confirmation/ examination	
7.	Are all interfaces to the I/O defined?					Verify I/O interfaces are correct.	Confirmation/ examination	
8.	Has the source of each item in the data base been defined? (e.g., operator entered, calculated, etc.)					Verify data base source definition	Checklist	
9.	Does system provide for the subsequent addition of new points?					Verify new points can be easily added to data base.	Confirmation/ examination	

USE OR DISCLOSURE OF PROPOSAL DATA IS SUBJECT TO THE RESTRICTION ON THE TITLE PAGE OF THIS PROPOSAL

Hardware Design Phase Review Process
Test Factor: Consistency

		ASSESSMENT						
	REVIEW CRITERIA	VA	A	IA	NA	DESCRIPTION	APPROACH	NCR
1.	Are design documents consistent with system diagrams in the requirement specification?					Verify design documentation is is consistent with requirements.	Confirmation/ examination	
2.	Is the hardware provided consistent with the hardware specified in the requirements?					Verify all specified hardware is provided.	Confirmation/ examination	
3.	Isthe actual I/O point count consistent with the system specification?					Verify I/O point count is consistent.	Confirmation/ examination	
4.	Are the interface requirements of the remote I/O equipment consistent with those provided in the computer complex?					Verify correct interfaces are provided.	Confirmation/ examination	
5.	Is the requirement specified redundancy provided?					Verify all specified hardware is provided.	Confirmation/ examination	

1.1.3 SHUTDOWN MARGIN DISPLAY TEST

PURPOSE: THE PURPOSE OF THE SHUTDOWN MARGIN DISPLAY TEST IS TO VALIDATE THE DISPLAYS ASSOCIATED WITH THE CRITICAL SAFETY FUNCTION FOR SHUTDOWN MARGIN.

FUNCTION: THE FUNCTIONS TO BE TESTED ARE THE DISPLAY FORMAT'S CONFORMITY TO DESIGN SPECIFICATION, INCLUDING COLOR, TEXT, FUNCTIONALITY AS A CRITICAL SAFETY FUNCTION STATUS TREE, PAGING, TABBING, AND ZOOMING.

INPUTS: THE FOLLOWING SIMULATED ANALOG INPUTS ARE REQUIRED:

1) POWER RANGE TRANSMITTERS XA5711, XA5712, XA5713, AND XA5714

2) INTERMEDIATE RANGE SUR TRANSMITTERS XA5705 AND XA5706

3) SOURCE RANGE TRANSMITTERS XA5699 AND XA5700
OPERATOR INPUTS WILL BE THROUGH THE CRT KEYBOARD

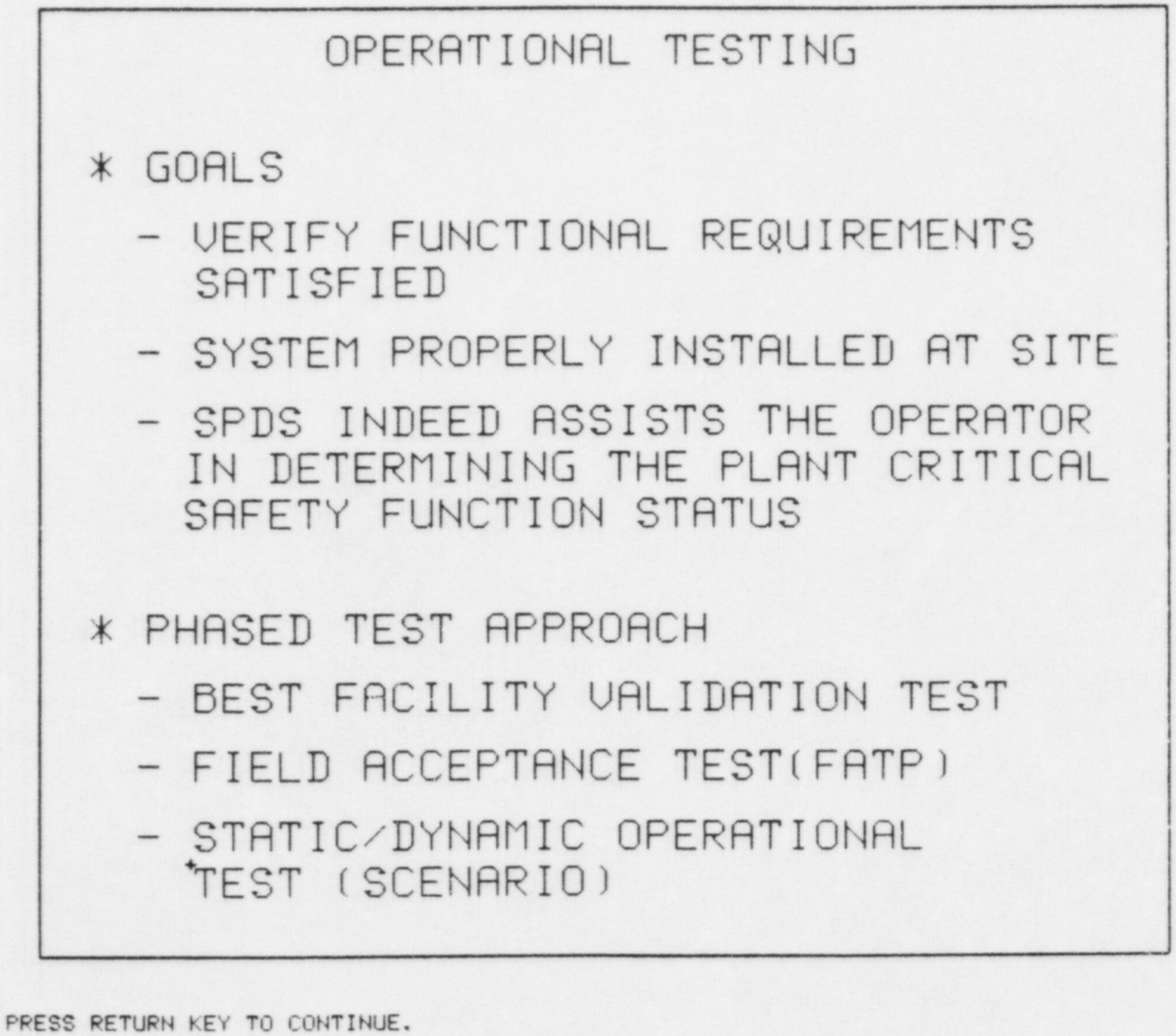
OUTPUTS: THE CRT DISPLAY WILL BE USED FOR OUTPUTS. THE VIDEO COPIER MAY BE USED TO COPY THE DISPLAYS FOR DETAILED EXAMINATION AT THE DISCRETION OF THE TESTER. RESPONSE TO KEYBOARD ENTRIES SHALL BE NO MORE THAN 1 SECOND.

TEST SETUP: THE SPDS WILL BE BROUGHT UP, IF IT IS NOT ALREADY UP. THE POWER RANGE TRANSMITTERS, THE INTERMEDIATE RANGE SUR TRANSMITTERS, AND THE SOURCE RANGE TRANSMITTERS WILL ALL BE SET TO 0 AND NOT FAILED. THE CSF BOX DISPLAY WILL BE BROUGHT UP ON ONE CRT.

PROCEDURE:

1.1.3 SHUTDOWN MARGIN TEST

STEP	TEST/EXPECTED RESULTS	DATE	RESULT	INIT
1	OBSERVE THE CSF BOX DISPLAY. THE "S" COLUMN SHALL BE GREEN.			
2	TAB TO THE "S" COLUMN AND PRESS THE ZOOM KEY. THE SHUTDOWN MARGIN DISPLAY SHALL BE DISPLAYED.			
3	VERIFY DISPLAY VERSUS DOCUMENTATION (PS-LVB-017 APPENDIX C) THERE SHALL BE A GREEN PATH FROM THE "START" BLOCK TO THE FIRST "SAT" BLOCK. ALL OTHER PATHS SHALL BE WHITE. THE "S" BLOCK SHALL BE GREEN.			
4	VERIFY THAT THE TAB KEY MOVES THE CURSOR THROUGH EACH OF THE CSF BLOCKS AND TO THE FRSM-1 AND FRSM-2 BLOCKS.			
5	CHANGE XA5699 (U#NM31FA_SP) TO A NEGATIVE VALUE. THERE SHALL BE NO CHANGE ON THE CRT.			
6	CHANGE XA5699 (U#NM31FA_SP) >0. THERE SHALL BE NO CHANGE ON THE CRT.			
7	CHANGE XA5700 (U#NM32FA_SP) >0. THE GREEN PATH SHALL BE REPLACED BY A YELLOW ONE TO THE LEFT-MOST FRSM-2 BLOCK. THE "S" BLOCK SHALL CHANGE TO YELLOW.			
8	PAGE UP TO THE CRITICAL SAFETY FUNCTION DISPLAY. THE "S" BLOCK SHALL BE YELLOW.			
9	ZOOM TO THE SHUTDOWN MARGIN DISPLAY. TAB TO THE DISPLAYED YELLOW BLOCK AND ZOOM TO THE FRSM-2 FUNCTIONAL RECOVERY GUIDELINE DISPLAY. VERIFY DISPLAY VERSUS PS-LVC-017 APPENDIX C/P11-11.			
10	PAGE UP TO SHUTDOWN MARGIN DISPLAY. OBSERVE THE DISPLAY HAS NOT CHANGED.			



OPERATIONAL TESTING

* GOALS

  - VERIFY FUNCTIONAL REQUIREMENTS SATISFIED
  - SYSTEM PROPERLY INSTALLED AT SITE
  - SPDS INDEED ASSISTS THE OPERATOR IN DETERMINING THE PLANT CRITICAL SAFETY FUNCTION STATUS

* PHASED TEST APPROACH

  - BEST FACILITY VALIDATION TEST
  - FIELD ACCEPTANCE TEST(FATP)
  - STATIC/DYNAMIC OPERATIONAL TEST (SCENARIO)

PRESS RETURN KEY TO CONTINUE.

APPENDIX C

SPDS PRE-IMPLEMENTATION AUDIT ATTENDEES

Appendix C
SPDS Pre-Implementation Audit Attendees
December 5, 1985

Name	Affiliation	Phone Number
Rod Patwell	PSE&G - Licensing	4750
Larry Curran	PSE&G Salem Ops	339-6000 x3026
Tom Morrow	Singer	301-964-4801
Richard Stark	SAIC	703-448-6470
Whitney Hansen	NRC/Comex	206-823-5092
Mark Archer	NRC/SAIC	703-821-5785
Leo Beltracchi	NRC/NRR	301-492-4879
M. Allicock	PSE&G	609-339-4839
Richard J. Eckenrode	NRC/NRR/PWR-A	301-492-4882
T.R. McGuire	PSE&G - Controls and Electrical Division	201-430-8744
A. Morgan	PSE&G - Controls and Electrical Division	201-430-8407
Catherine Gaddy	General Physics	301-964-6000
James F. Davis, Jr.	PSE&G - Controls and Electrical Division	201-430-8216
J.P. Whooley	PSE&G - Assistant Chief E&C Engineer	201-430-8221