Docket No. 50-423

Millstone Nuclear Power Station, Unit No. 3

Safety Parameter Display System

Safety Analysis Report

April, 1984

Table of Contents

Table of Contents (Cont.)

1.0 INTRODUCTION

1.1 Summary of the Safety Analysis

This report provides a written safety analysis for the Millstone Unit No. 3 Safety Parameter Display System (SPDS). Information is provided to show that the SPDS is being designed to meet the provisions of Supplement 1 to NUREG-0737.

The SPDS is part of an Emergency Response Information System (ERIS) that combines all plant process computer functions for emergency response tasks. The critical safety functions were selected to be consistent with the Westinghouse Owners' Group Emergency Response Guidelines from which Millstone Unit No. 3 Emergency Operating Procedures (EOPs) are being developed. The SPDS displays are being developed with the consideration of human factors principles. Signals input to SPDS shall be evaluated for quality and validation. A verification and validation program will be conducted, including an independent review of the SPDS.

In this manner, a SPDS design is being developed that will provide an effective aid to the operators in determining the safety status of the plant during abnormal and emergency conditions.

1.2 Discussion

The SPDS is one part of an integrated emergency response capability. It will be consistent with the Emergency Operating Procedures (EOPs) and the Operators' Training Program. For Millstone Unit No. 3, the EOPs will be based upon the Westinghouse Owners' Group Emergency Response Guidelines.

The Emergency Response Guidelines (ERGs) are composed of:

- Optimal Recovery Guidelines and Emergency Contingencies
- Critical Safety Function Status Trees and Restoration Guidelines

The Optimal Recovery Guidelines provide guidance for the operator to recover the plant from nominal design basis faulted and upset conditions. The Function Restoration Guidelines, when used with the Critical Safety Function Status Trees, provide a systematic means for addressing any challenge to plant critical safety functions, which is entirely independent of initiating event or plant state.

The structure of the Critical Safety Function Status Trees has been carefully chosen to be compatible with the existing basis for operator training, since the status trees provide an explicit tool to re-emphasize the necessity for the operator to be always aware of the state of his plant safety functions. An additional advantage derived from the introduction of the status tree concept directly into the procedures structure is that the operator is provided with a performance aid, to reinforce his training

and assist his memory, particularly during high-stress situations typical of transient or emergency conditions.

From this discussion of the Critical Safety Function Status Trees and the SPDS, it is clear that they perform the same functions and must be compatible. Thus, the Critical Safety Functions and Variables selection for SPDS has been based upon the Critical Safety Function Status Trees of the Emergency Response Guidelines.

1.3 NRC Criteria

1.3.1 Supplement 1 of NUREG-0737

Regarding the SPDS, Section 4.1 of Supplement 1 to NUREG-0737 identifies the following NRC criteria:

a. The 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 principal 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 plant 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.

b. 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.

c. The SPDS shall be suitably isolated from electrical or electronic interference with equipment and sensors that are in use for safety systems. 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 the SPDS. Furthermore, operators should be trained to respond to accident conditions both with and without the SPDS available.

d. The selection of specific information that should be provided for a particular plant shall be based on engineering judgment of individual plant licensees, taking into account the importance of prompt implementation.

e. The SPDS display shall be designed to incorporate accepted human factors principles so that the displayed information can be readily perceived and comprehended by SPDS users.

f. The minimum information to be provided shall be sufficient to provide information to plant operators about:

(i) Reactivity control

(ii) Reactor core cooling and heat removal from the primary system

(iii) Reactor coolant system integrity

(iv) Radioactivity control

(v) Containment conditions

The specific parameters to be displayed shall be determined by the licensee.

The remainder of this report defines the extent of compliance of the Millstone Unit No. 3 SPDS with the above NRC criteria.

1.3.2 Regulatory Guide 1.97

The variables needed to determine the status of the Critical Safety Functions (CSFs) and Radioactivity Releases are identical to the majority of the Types A, B, C and E variables of Regulatory Guide 1.97, and therefore these variables will be a major part of the SPDS data base. Type D variables, those needed to assess the performance and availability of safety systems, are not part of the SPDS data base. Although not part of the SPDS, most Type D variables will be part of the plant process computer data base.

The design criteria stated in Regulatory Guide 1.97 for Category 1 sensors infers that a third channel may be required if a failure of one channel results in information ambiguity. The SPDS will have the capability to use techniques such as analytic redundancy, to determine the valid reading and avoid the need to install a third channel.

1.3.3 Generic Letter 82-28 (NUREG-0737 Item II.F.2)

Another designated function of the SPDS is to monitor the overall status of core cooling adequacy. The Class 1E display for Inadequate Core Cooling (ICC) is presently provided in the instrument rack room. To resolve this potential Human Engineering Discrepancy (HED), the primary ICC display will be provided via the SPDS. In the event that the SPDS is not available during accident conditions, the ICC information will still be available on Class 1E qualified devices (ICC panels). As a minimum, the SPDS will include the capability to display the following ICC information.

a. Core map of all core exit thermocouples (CETs).

b. Pressure/Temperature Plots with the saturation curve, NPSH limits, heat-up/cooldown rates, subcooling to 200°F, superheat to 35°F.

c. Time history plots of all ICC related variables including reactor vessel level and selected temperature inputs.

2.0 SPDS DESIGN DESCRIPTION

2.1 Overview

One function of the Millstone Unit No. 3 plant process computer system is the supplying of information required for responses to an emergency condition. Because of the need to develop integrated emergency response facilities and data systems to aid in accident management, an Emergency Response Information System (ERIS) is being developed for Millstone Unit No. 3. This system will display information in the Technical Support Center and Emergency Operations Facility. This report covers only those functions of ERIS related to SPDS.

2.2 SPDS Definition

SPDS aids the control room operating crew in monitoring the status of the CSFs that constitute the basis of the plant-specific, symptom-oriented EOPs. Its principal purpose is to aid the control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to avoid a degraded core.

2.3 SPDS Availability

Although the SPDS need not be a safety-grade system, implementation of a highly reliable, state-of-the-art SPDS is an important design objective.

As a design objective, the availability of the SPDS will be greater than 99 percent during normal plant operation. In this context, design availability is understood to encompass the following minimal functional capabilities:

1) The ability to monitor and display the status of all critical safety functions.

2) The ability to determine the value of all variables which are used in the CSF status determination.

2.4 SPDS Use and Location

SPDS displays of CSF status and supporting displays of CSF-related parameters will be accessible to operators in the vicinity of the main control board. SPDS displays that include EOP logic, prompts and algorithm information will be available at the control room location where CSF monitoring will occur.

2.5 Modes of Operation

The CSFs defined for Millstone Unit No. 3 are not appropriate for all modes of operation. Specifically, it is assumed that a status tree is entered from either a Start-up or Power Operation mode and not from a Refueling or Cold Shutdown mode.

The design of the SPDS for Millstone Unit No. 3 therefore only requires the availability of the SPDS in modes 1, 2, 3 and 4 (power operation, startup, hot standby, and hot shutdown).

2.6 Display Flexibility

The SPDS hardware and software will have the capability to display plant information in the following types of common formats, both singly and mixed formats:

Alphanumeric prompts, messages and labels

EOP status trees

Horizontal or vertical bar graphs

Mimic/P&ID displays

Multivariable plots vs. time

Variable vs. variable

2.7 Data Storage

Capability will be provided to store up to 375 SPDS variables for the interval from two hour pre-event to twelve hours post-event.

2.8 Signal Validation

The SPDS will have the capability of validating individual signals used in SPDS displays and algorithms by use of simple analysis, checking and comparative methods to be specified for each SPDS variable.

2.9 Electric Power Sources

The SPDS, as part of the plant process computer system, will be powered from an uninterruptible power supply, capable of supplying power to the computer system after a loss of offsite power.

2.10 Electrical Separation

The SPDS, as part of the plant process computer system, will receive signals from both Class 1E and non-1E sources. Adequate electrical separation in accordance with the guidance of Regulatory Guide 1.75 will be provided for all signals, power sources and output devices.

3.0 SPDS CRITICAL SAFETY FUNCTION AND VARIABLE SELECTION

3.1 Selection Process

The SPDS is being designed to complement the EOPs, that is, to aid the operator in implementing the EOPs. It is not intended to require the operator to use the SPDS displays in the transient identifications. The major user of the SPDS during a transient would be the senior reactor operator to "see" the overall plant condition and how actions taken by the operator under his direction affect the maintenance of the six critical safety functions.

The plan for operator response to an Engineered Safeguards System actuation is shown in Figure 1. If the specific event can be diagnosed, the operator is directed to use a defined set of procedural steps to effect plant recovery. If no diagnosis is possible, the operator is trained to monitor certain critical safety functions which indicate overall plant safety status. If any safety function is challenged, the operator is directed to a contingency action through an evaluation and identification scheme of the critical safety functions. To complement this plan, the SPDS can be most effectively used to continuously monitor the critical safety functions and assist the operator in the evaluation scheme to determine the appropriate contingency action. In this manner, the SPDS will be consistent with the W Emergency Response Guidelines.

The W Emergency Response Guidelines have identified the critical safety functions (CSFs) and have developed critical safety function status trees for critical safety function evaluation.

The Critical Safety Functions were selected to monitor three barriers to the release of radioactivity. The Critical Safety Functions 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)

Situations can arise in which the integrity of a barrier is lost and cannot be restored even though all Critical Safety Functions are satisfied. The classic double-ended guillotine break of reactor coolant system piping constitutes an irrevocable failure of the reactor coolant system pressure boundary barrier. In this situation the reactor coolant system pressure boundary barrier is recognized to be failed, and all available resources are directed toward minimizing further degradation of the failed barrier and keeping the fuel matrix/cladding barrier and the containment barrier intact.

The SPDS will be used to assist in the CSF evaluation by monitoring the CSFs, using the same logic as the CSF status trees. This is necessary to facilitate operator use of the SPDS in support of the Millstone Unit No. 3 Emergency Operating Procedures. These status trees are shown in Figures 2a-2f.

The SPDS will also display information for Radioactivity Control. A display summarizing Radioactivity Control has been identified to aid the shift supervisor in performing his emergency response function prior to the staffing of the Emergency Response Facilities. Radioactivity Control is not a critical safety function, however, since radioactivity assessment has already been factored into the containment CSF.

3.2 Critical Safety Functions

The critical safety functions are shown in Table 1 in order of priority. The status of the critical safety function will be indicated by four states:

- Green - critical safety function is satisfied
- Yellow - critical safety function is not fully satisfied
- Orange - critical safety function is under severe challenge
- Red - critical safety function is in jeopardy

The state of the critical safety functions will be determined using the status tree logic given in Figures 2a-2f.

3.3 Critical Safety Function Variables

The variables for determining critical safety function status will be the decision points in the critical safety function status trees. These variables are listed in Table 2, grouped by safety function.

3.4 Radioactivity Control Function

The status of the radioactivity control function will also be indicated by four states:

- o Green - no abnormal releases
- o Yellow - releases exceed unusual event (Delta-2) criteria
- o Orange - releases exceed alert (Charlie-1) criteria
- o Red - releases exceed site area emergency (Charlie-2) criteria

These states were selected to correspond to the Emergency Action Levels identified in the Millstone Nuclear Power Station Emergency Plan.

3.5 Radioactivity Control Variables

The variables for determining the radioactivity control status were selected by identifying all potential release paths for radioactivity. These variables are listed in Table 3.

3.6 Instrumentation

The instruments used in measuring the critical safety and radioactivity function variables are given in the Appendices A and B.

3.7 Analytical Basis for Critical Safety Function and Variable Selection

The SPDS critical safety functions and variables have been chosen to be identical to the critical safety functions developed for the Emergency Response Guidelines. Thus, the analytical basis for the SPDS selection is the same as the basis for the ERGs. These ERG critical safety function status trees were reviewed and approved for implementation by the NRC in its Safety Evaluation of "Emergency Response Guidelines" (Generic Letter 83-22).

3.8 Emergency Response With and Without SPDS

The Emergency Response Guidelines contain CSF evaluations that are simple enough to allow manual evaluations. This manual evaluation will

be performed if the SPDS is not available. Since the SPDS is entirely compatible with the ERGs, only one set of procedures (EOPs) are required.

4.0 SPDS DISPLAYS

4.1 Display Philosophy

Each display location provides independent access to SPDS displays. Displays selected at one CRT can be different from those displays selected elsewhere. During an emergency, for example, this would allow operators to select SPDS displays that aid process control actions and permit supervisory personnel to simultaneously view SPDS displays oriented toward overview and safety assessment.

In order to maintain CSF status indication at all times, one SPDS display will include indication of the status of each CSF in a format that is common to all SPDS displays. CSF status will be supplemented on each display with a unique set of information and plant data developed to aid one or more of the following:

a. Assessment/Control of CSF plant variables.

b. EOP Entry Condition Indication.

c. CSF Status Tree Assessment.

The set of SPDS displays and access controls will be implemented with a hierarchy or structure that facilitates and systematizes passage between displays.

4.2 Primary Displays

At least one (1) control room CRT will continuously monitor the status of all CSFs during Modes 1, 2, 3 & 4. Other information may be displayed simultaneously as long as the status of the CSFs are still able to be determined. CSF monitoring will include indication of the need to enter a specific Function Recovery Procedure as defined in the ERGs and EOPs.

Each SPDS display will show a common set of indications of the status of the six CSFs and of Radioactivity Control. Status indication colors will correspond to the status colors in the ERGs and EOPs. When any Function Recovery entry condition is met, this will be indicated by the CSF to which it applies. The format for presenting this information will be common to all SPDS displays.

4.3 Secondary Displays

During normal, transient and accident conditions access will be provided to a certain number of predefined displays. These secondary displays will

support the CSF status indicators and enable the operating crew to determine/evaluate the reasons for changes in CSF status and the potential need to enter a Function Recovery Procedure.

The set of secondary displays will consist of at least one display oriented to each of the following functions.

a. Subcriticality CSF Variables and Status Tree.

b. Core Cooling CSF Variables and Status Tree.

c. Heat Sink CSF Variables and Status Tree.

d. Integrity CSF Variables and Status Tree.

e. Containment CSF Variables and Status Tree.

f. Coolant Inventory CSF Variables and Status Tree.

4.4 Other Displays

A set of supporting displays will be generated for displaying other important information such as:

a) Plant variable information to aid CSF assessment and EOP execution.

b) Inadequate core cooling variables not included in the primary display of core cooling CSF variables.

4.5 Display Change

Each secondary display will be accessible through a menu.

Once a secondary display is presented on the CRT, other supporting displays can be accessed in a timely manner.

All display page changes will be operator initiated and not computer initiated.

4.6 Variable Status Indication

All SPDS variables will be displayed with a visual indication of the associated quality level as determined by SPDS data processing and validation, e.g., invalid or unvalidated variables could be tagged. Appropriate visual indication will also be available on displays of SPDS variables when out-of-scan, substituted or dummy signals are involved.

5.0 SIGNAL VALIDATION

5.1 Quality Tags

A particular problem with all computer-based systems is the presentation to the operator of believable, validated data. In the real world environment, sensors fail, instrumentation drifts, and calculations (which depend on the quality of many sensors) become invalid if certain sensors are removed from scan. Often a group of sensors is involved in a variety of calculations. Then, if the sensor fails or is removed from scan, the operator has no knowledge of the calculation impact.

All presentation of information for the SPDS will be associated with Quality Tags which will indicate the quality of the processed sensor signal and the quality of calculated variables. Three distinct quality levels are required:

Validated - Validated quality applies when multiple sensors or analytically derived variables are compared for tracking within a specified error band and are within predefined limits.

Unvalidated - Unvalidated quality applies when a single sensor is correctly processed and has passed all limit checking and reasonability tests. Since this sensor is not compared with another sensor or group of sensors or an analytically derived variable, its quality remains unvalidated.

Invalid - Invalid quality applies when a sensor undergoing validation processing has failed that process or when a single sensor has failed processing quality standards.

6.0 VERIFICATION AND VALIDATION (V&V)

6.1 Verification and Validation Overview

This section provides an overview of the system verification and validation program. The objective of the Verification and Validation (V&V) program is to provide a quality system through independent technical review and evaluation conducted in parallel with system development.

The primary purposes of the V&V program is to:

a. Assure that system, procedural and documentation deficiencies are identified and corrected as early as possible in the development process.

b. Assure that system design reflects design specifications.

c. Assure that the installed system meets functional specifications.

d. Assure complete and auditable system documentation.

6.2 V&V Program

A team approach will be used for accomplishing V&V. The team composition will be multi-discipline, will include both user, systems and design functions, and will be independent from system development activities. The V&V team will develop and document a V&V plan as one of its initial activities.

Procedures and techniques to be used for conducting V&V activities will be determined. Examples of techniques that could be used to implement a balanced V&V program include:

a) Development and use of a functional capabilities matrix

b) Error identification and reporting system

c) Structured graphic techniques for analysis and presentation

d) Design walk-throughs

Procedures and techniques for each major V&V activity include:

- System Specifications Verification
- Design Verification
- System Validation

6.3 Verification and Validation of the Emergency Operating Procedures

Because the SPDS philosophy is to complement the Emergency Operating Procedures (EOPs), verification and validation of the EOPs is an important part of the V&V of the SPDS. Verification and validation has been performed for the Westinghouse ERGs and will be performed for the Millstone Unit No. 3 EOPs that are being developed from these guidelines.

6.3.1 V&V of the Westinghouse Emergency Response Guidelines

The Westinghouse Emergency Response Guidelines were submitted to the NRC Staff in 1982. The NRC reviewed these guidelines and issued a Safety Evaluation Report in June, 1983. The NRC Staff concluded that the guidelines were acceptable. In particular, they concluded that the six Critical Safety Functions were sufficient to protect the three physical barriers. While some areas of additional work on the ERGs were identified, the NRC Staff recommended implementation of the ERGs.

In addition, the Westinghouse Owners' Group developed a Validation Program for the guidelines which included a simulator test program at the Seabrook facility in October, 1983. The simulator test demonstrated that a computer-based status tree evaluation was a highly effective method of critical safety function monitoring.

Because of the extensive verification and validation performed on the ERGs, they represent a sound basis for the development of the Millstone Unit No. 3 SPDS and Emergency Operating Procedures.

6.3.2 Verification of the Millstone Unit No. 3 Emergency Operating Procedures

The Millstone Unit No. 3 Emergency Operating Procedures are being developed based upon the guidance of the Westinghouse Owners' Group Emergency Response Guidelines. To verify consistency between the ERGs and EOPs, a step by step comparison will be jointly made by the Millstone Unit No. 3 operators and the Control Room Design Review (CRDR) team. Justification for any differences will be provided and documented.

6.3.3 Validation of the Millstone Unit No. 3 Emergency Operating Procedures

When the Millstone Unit No. 3 EOPs are developed, a task analysis of the procedures will be performed by the Millstone Unit No. 3 operators and the CRDR team. Actions required to perform the steps in the EOPs will be defined and assessed. The control room operators' ability to efficiently and correctly perform the stated actions considering controls, instrumentation and physical layouts will also be assessed. This task analysis will therefore be used for verification of the selection of the instrumentation to be used for the critical safety function variables.

The Millstone Unit No. 3 Emergency Operating Procedures will be validated upon completion. A description of the Emergency Operating Procedure Validation Program will be submitted as part of the Emergency Operating Procedures Generation Package.

7.0 HUMAN FACTORS ENGINEERING

7.1 Human Factors Engineering

The fundamental SPDS design objective is to serve as an operator aid to monitor the overall safety status of the plant. Human factors considerations must be an integral part of a program to successfully develop such a system.

This section describes the role of the primary SPDS user, the context of use, and the human factors principles that will be incorporated into the SPDS design.

7.1.1 SPDS Use

The Millstone Unit No. 3 control room will be occupied by three or four licensed operators (i.e., one or two Senior Reactor Operators (SROs) and two Reactor Operators (ROs)). One of the SROs will be the Shift Supervisor (SS). The SS/SRO will be the primary SPDS user. The SPDS is intended to help the SS/SRO in managing the plant during unusual situations where problem detection and problem solving on a plant wide scale are involved. The major role of the SPDS is to help the operating crew maintain the plant in a safe condition or to show how to return the plant to a safe condition if it has departed from normality.

The present control room and the resources available to the SS/SRO are sufficient to carry out these tasks. The SPDS is intended as an aid to the SS/SRO, not as a replacement for necessary safety equipment. The SPDS serves as a concentrated data source and thus permits the SS/SRO to obtain desired information without walking the boards to check readings.

The role of the SS/SRO is as a decision maker and manager of the plant. The role of ROs and the other SRO is to assist the SS/SRO by carrying out the tasks deemed necessary by the SS/SRO. Although ROs are carrying out specific tasks such as maintaining levels, starting pumps, or checking instrument readings, they need to be cognizant of the impact their operations have on overall plant condition. SPDS displays will be accessible to RO personnel to help maintain the needed understanding of the overall picture and to foster a team approach to plant emergency response.

7.1.2 Control Room Design

The arrangement and number of SPDS display stations in the control room will provide separate SPDS stations for the SS/SRO (away from the boards) and for operators (visible from operating stations at the boards). This arrangement will provide the SS/SRO with a good view of the SPDS from his work station (he can see both the SPDS and the boards at the same time) and by the operators from their stations at the boards. Thus the arrangement will permit a flexible use pattern which is weighted towards the needs of the SS/SRO while still permitting RO use.

7.1.3 Human Factors Design Requirements

The final element in the SPDS applications environment relates to the imposed design constraints. One of the human factors design constraints is a direct consequence from analysis of the control room setting as it relates to viewing distances. Actually, the human factors design reflects a compromise between human factors, hardware/software limitations, and styles of use. To some extent the human factors ideal must be reconciled with existing hardware/software limitations. The characteristics of CRT displays, the screen resolution, and archive data retrieval times are operative examples. Style of use relates to the plant operating philosophy and preferences: Human factors must be consistent with the traditional style and information content operators expect and will use.

To deal with these somewhat competing objectives, it was encumbent to adopt a set of high-level design principles for SPDS. They are as follows:

- Design and functional simplicity
- Minimal set of SPDS display pages
- Critical safety function format

8.0 CONCLUSION

The SPDS for Millstone Unit No. 3 is being designed to adequately address the provisions of Supplement 1 to NUREG-0737. Specifically:

a) The SPDS will provide a concise display of critical plant variables to aid the control room operators in determining the safety status of the plant that is consistent with the Westinghouse Emergency Response Guidelines and the Millstone Unit No. 3 Emergency Operating Procedures.

b) The SPDS will display CSF information on colorgraphic terminals located in the control room. The SPDS will display the status of the CSFs continuously. The SPDS will be part of the plant process computer system and is being designed to meet availability considerations consistent with the SPDS function.

c) Since the SPDS will be completely consistent with the Westinghouse Emergency Response Guidelines, only one set of procedures is required for emergency response with and without the SPDS. Adequate electrical separation will be provided in accordance with the guidelines of Regulatory Guide 1.75.

d) The critical safety functions and variables have been selected to be consistent with the analytical basis of the Emergency Response Guidelines. In general, the Regulatory Guide 1.97 instruments will be the source of the variables.

e) The SPDS displays are being designed to meet human factors principles.

f) The SPDS provides information about:

   (1) reactivity control

   (2) core cooling and heat removal

   (3) RCS integrity

   (4) radioactivity control

   (5) containment conditions

This safety analysis shows that the SPDS will be consistent with Emergency Response Guidelines and the Millstone Unit No. 3 Emergency Operating Procedures, and provides an integrated approach to abnormal and emergency conditions. Human factors principles are being considered in the design to assure that the operators can use the SPDS effectively. A Verification and Validation Program will assure that independent reviews are conducted to assure proper implementation of the SPDS design.

The development of the SPDS will be an effective aid for the control room operators to determine the safety status of the plant during abnormal and emergency conditions.

TABLE 1: Critical Safety Functions

I.	Subcriticality	Highest Priority
II.	Core Cooling	
III.	Heat Sink	
IV.	Integrity	
V.	Containment	
VI.	Inventory	Lowest Priority

TABLE 2: Critical Safety Function Variables

SAFETY FUNCTION		VARIABLE	
I.	Subcriticality	1.	Reactor trip
		2.	Power level
		3.	Startup rate
		4.	Source range energized
II.	Core Cooling	1.	Core exit temperature
		2.	RCS subcooling
		3.	RC pump status
		4.	RV level
III.	Heat Sink	1.	S/G level
		2.	Total FW flow rate
		3.	S/G pressure
IV.	Integrity	1.	Cooldown Rate
		2.	RCS temperature
		3.	RCS pressure
V.	Containment	1.	Containment pressure
		2.	Containment level
		3.	Containment radiation
VI.	RCS Inventory	1.	Pressurizer level
		2.	Reactor vessel level

TABLE 3: Variables for Radioactivity Control

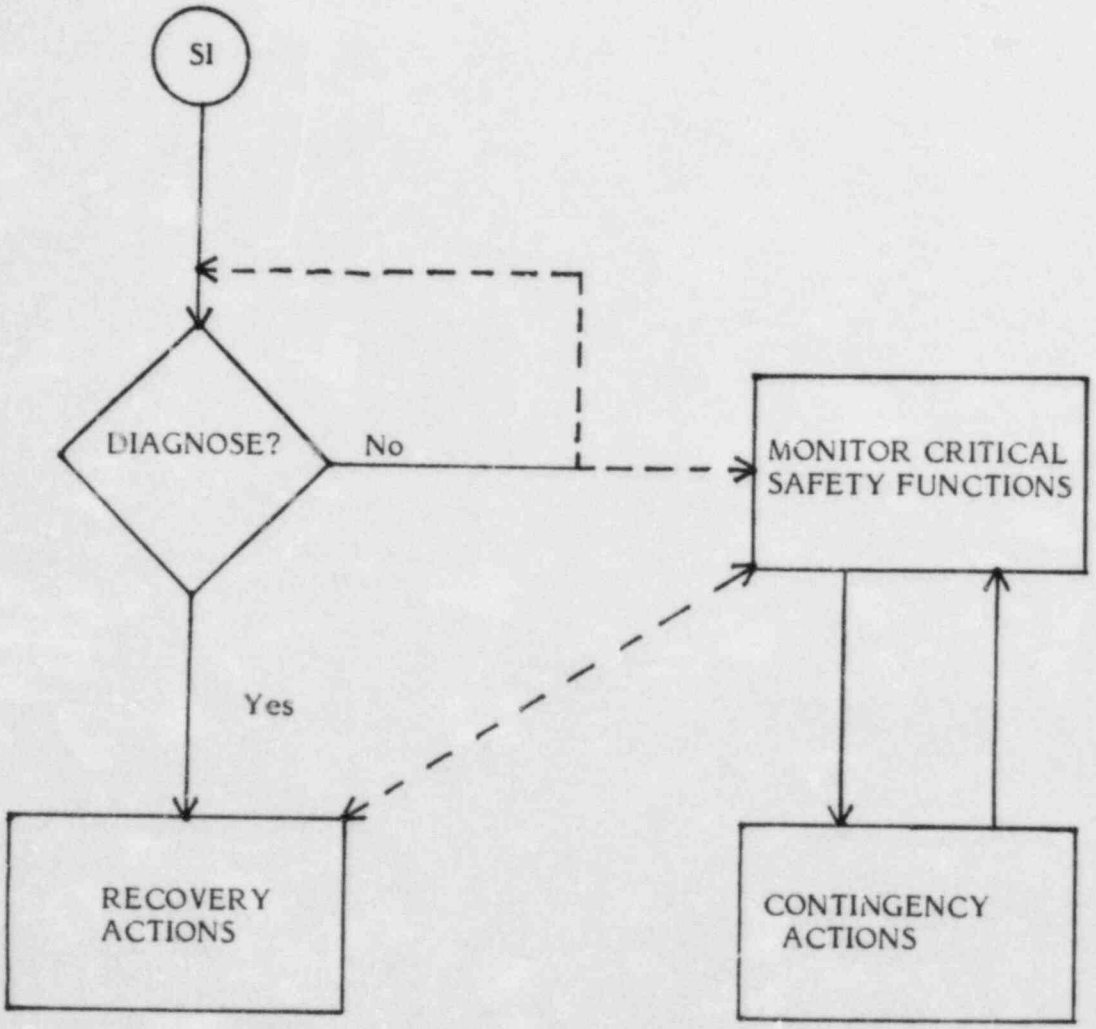
1. Main Steam Line Radiation

   a) main steam line radiation monitor
   b) steam generator safety valve status
   c) atmospheric dump valve status
   d) auxiliary feedwater pump steam status

2. Effluent Radiation

   a) stack monitor
   b) stack flow rate

FIGURES



OPERATOR RESPONSE LOGIC FOLLOWING

ACTUATION OF ENGINEERED SAFEGUARDS SYSTEM

FIGURE 1

Number:	Title:	Rev. Issue/Date:
F-0.1	SUBCRITICALITY	HP/LP, REV. 1 1 Sept., 1983

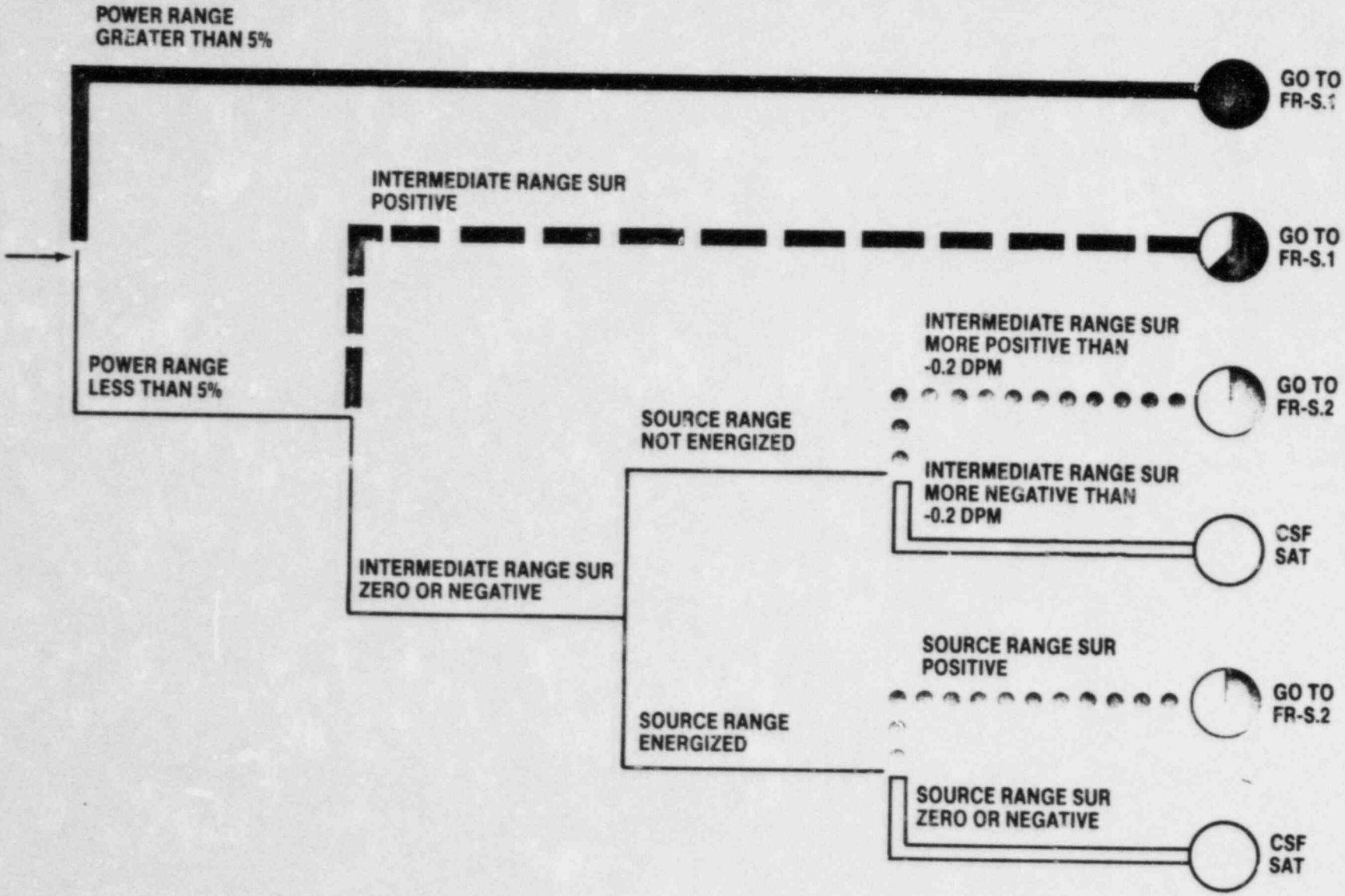


FIGURE 2a

Number:	Title:	Rev. Issue/Date:
F-0.2	CORE COOLING	HP/LP, REV. 1 1 Sept., 1983

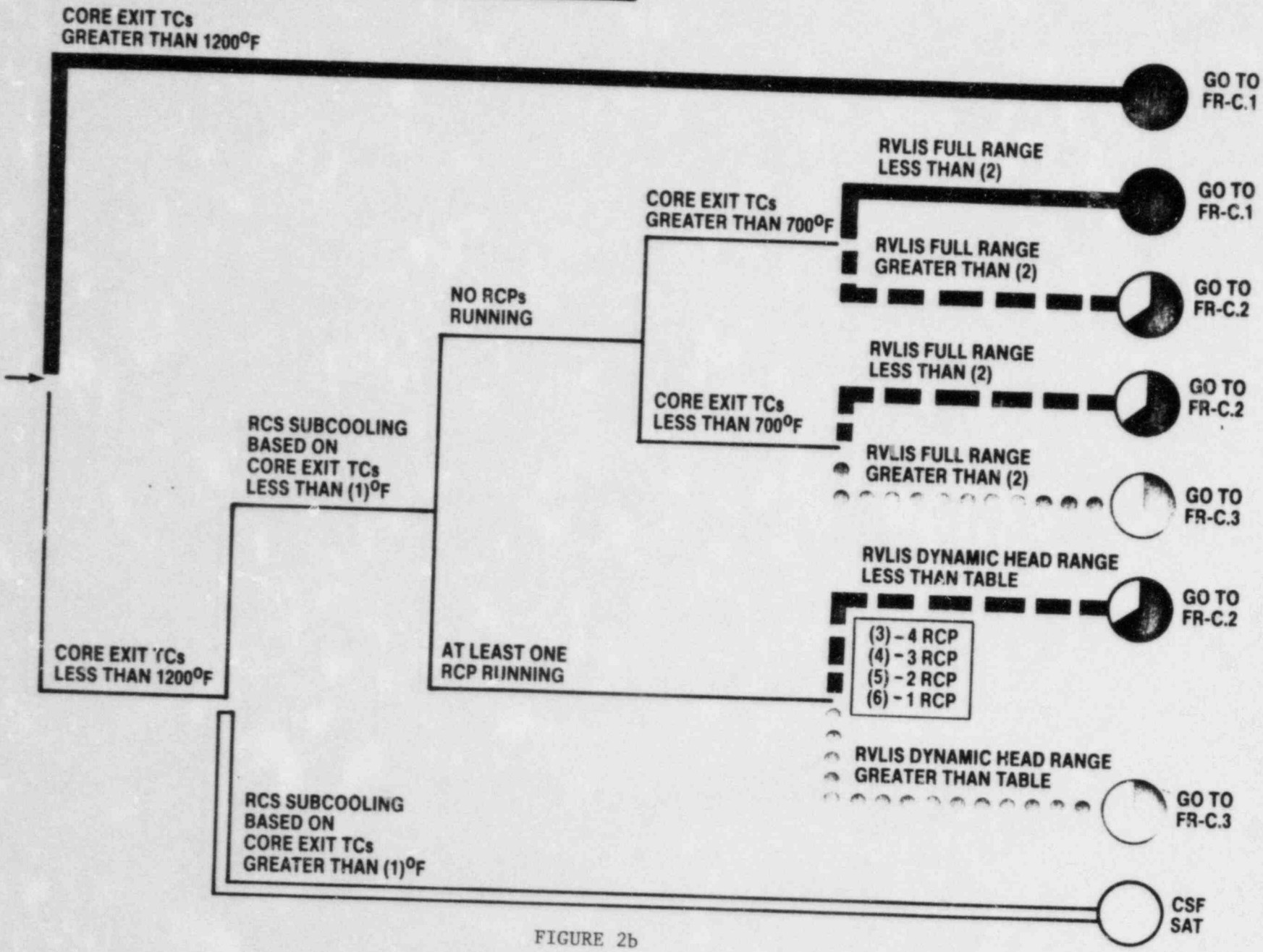


FIGURE 2b

Number:	Title:	Rev. Issue/Date:
F-0.3	HEAT SINK	HP/LP, REV. 1 1 Sept., 1983

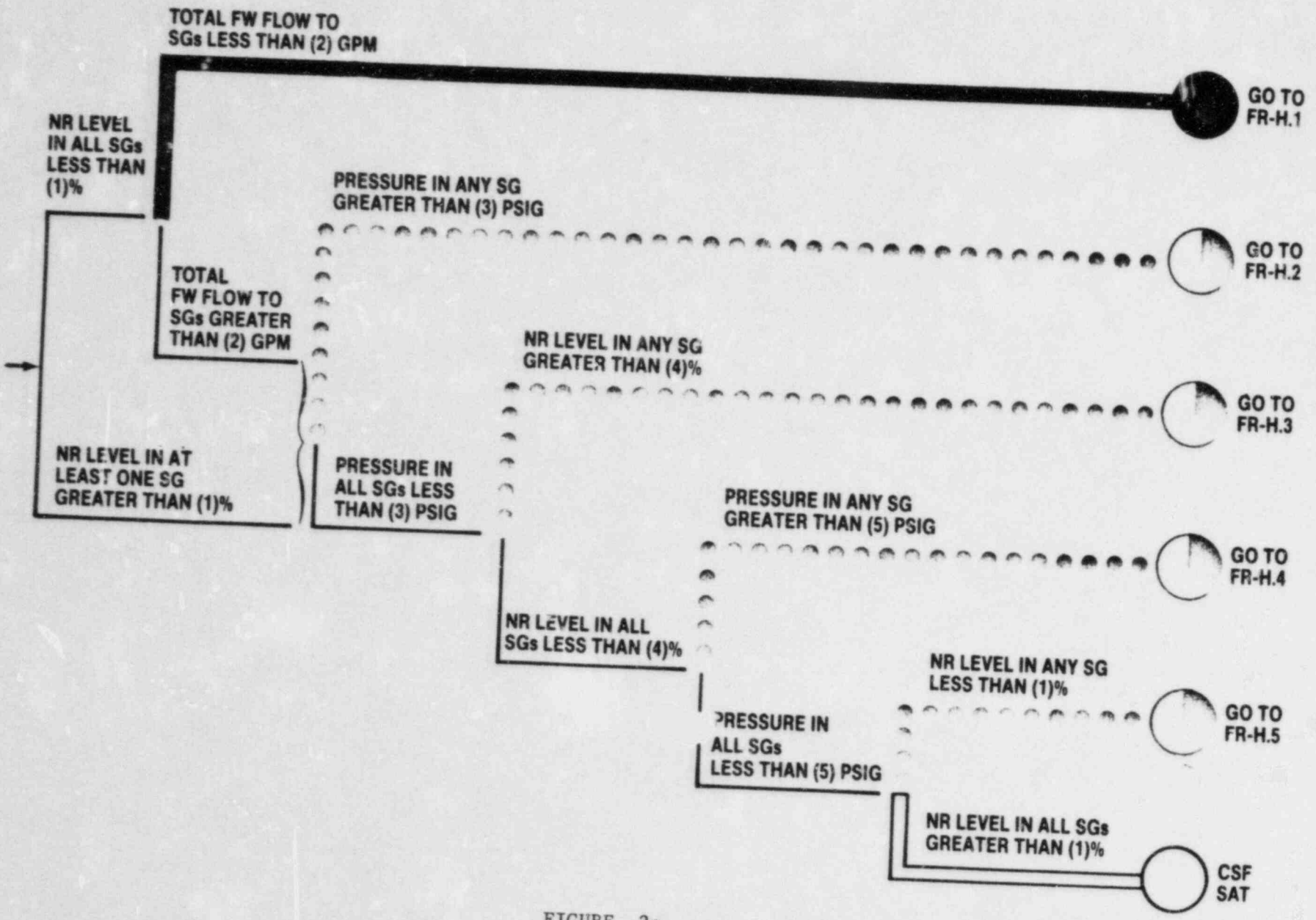


FIGURE 2c

Number:	Title:	Rev. Issue/Date:
F-0.4	INTEGRITY	HP/LP, REV. 1 1 Sept., 1983

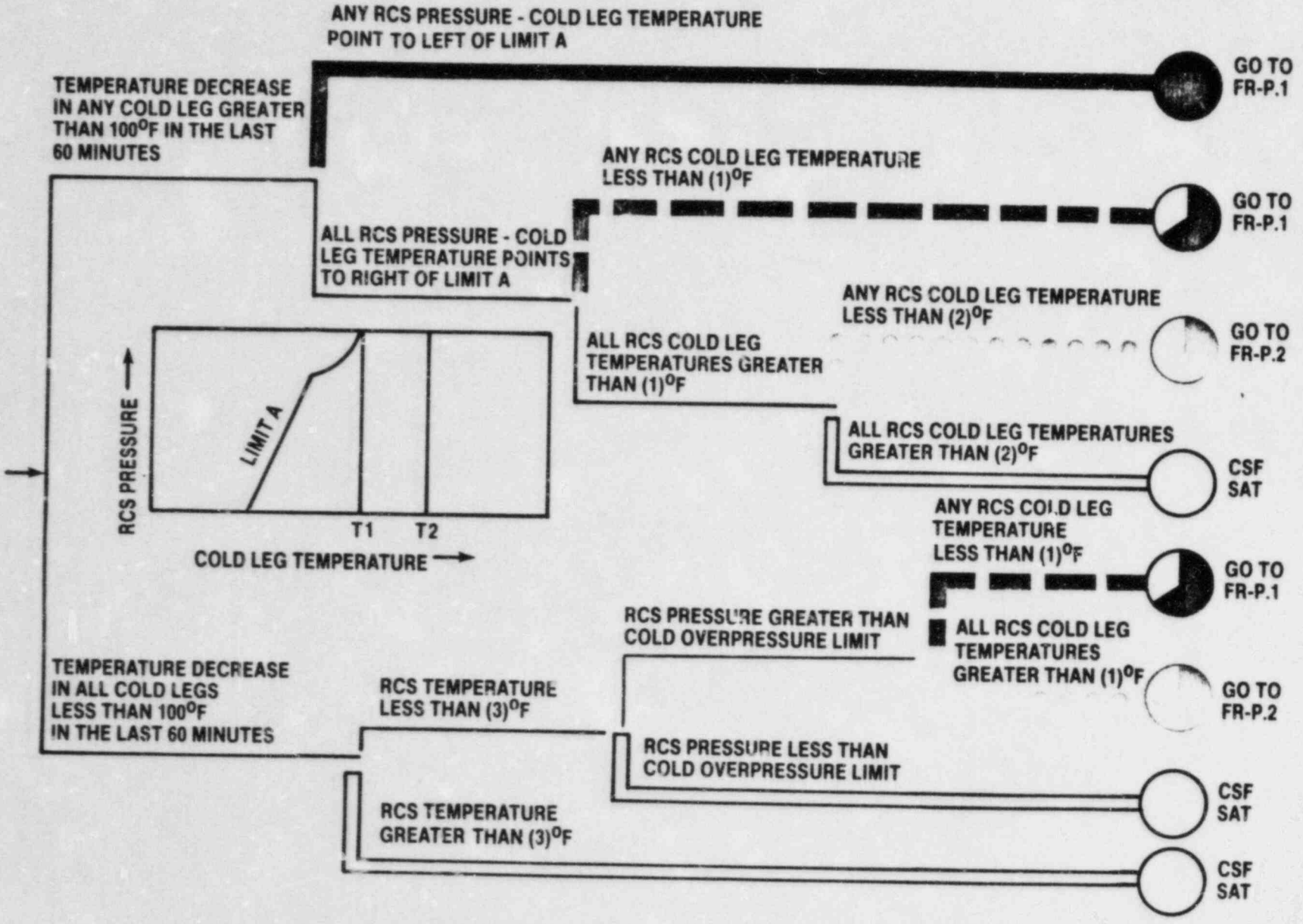


FIGURE 2d

Number:	Title:	Rev. Issue/Date:
F-0.5	CONTAINMENT	HP/LP, REV. 1 1 Sept., 1983

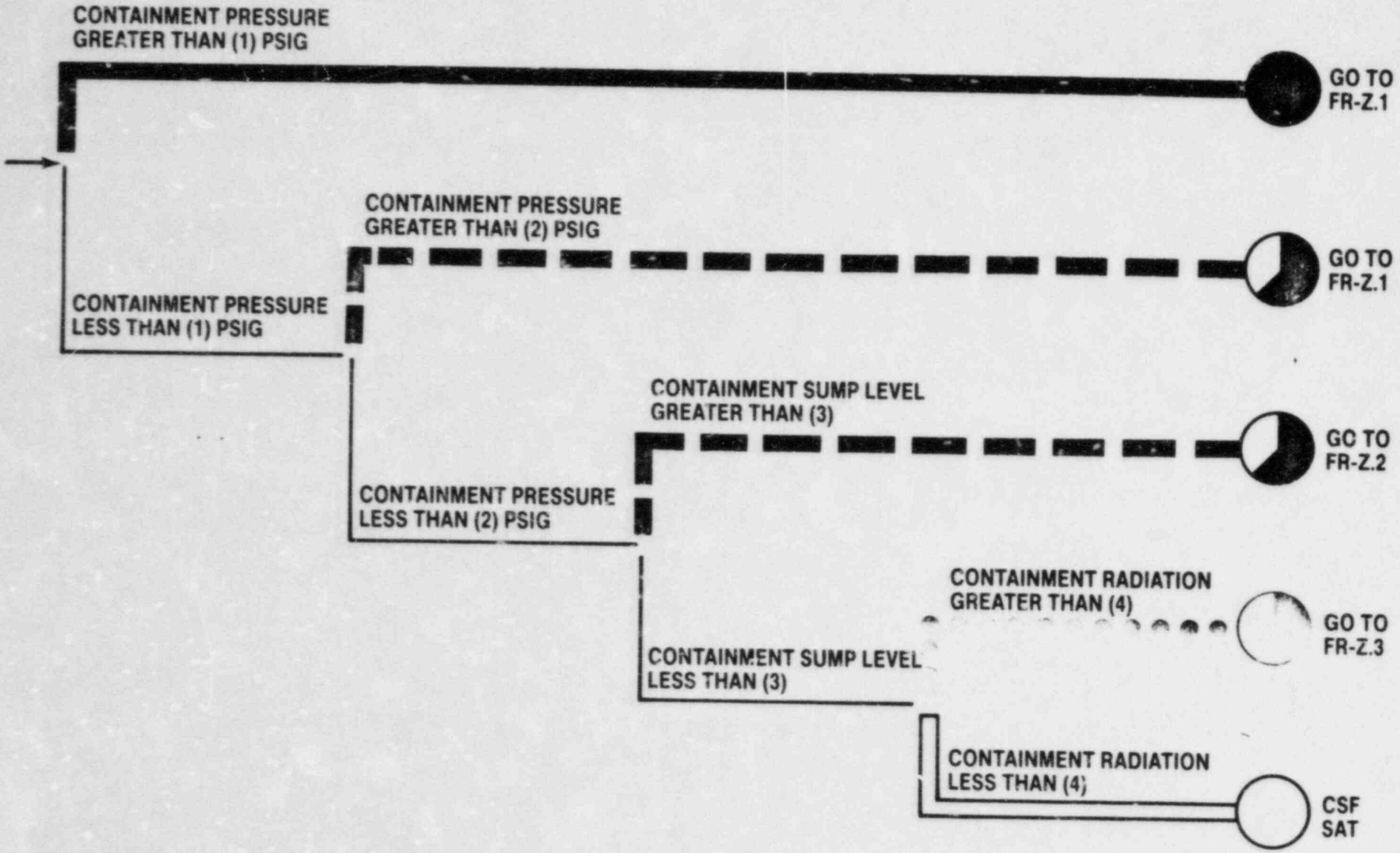


FIGURE 2e

Number:	Title:	Rev. Issue/Date:
F-0.6	INVENTORY	HP/LP, REV. 1 1 Sept., 1983

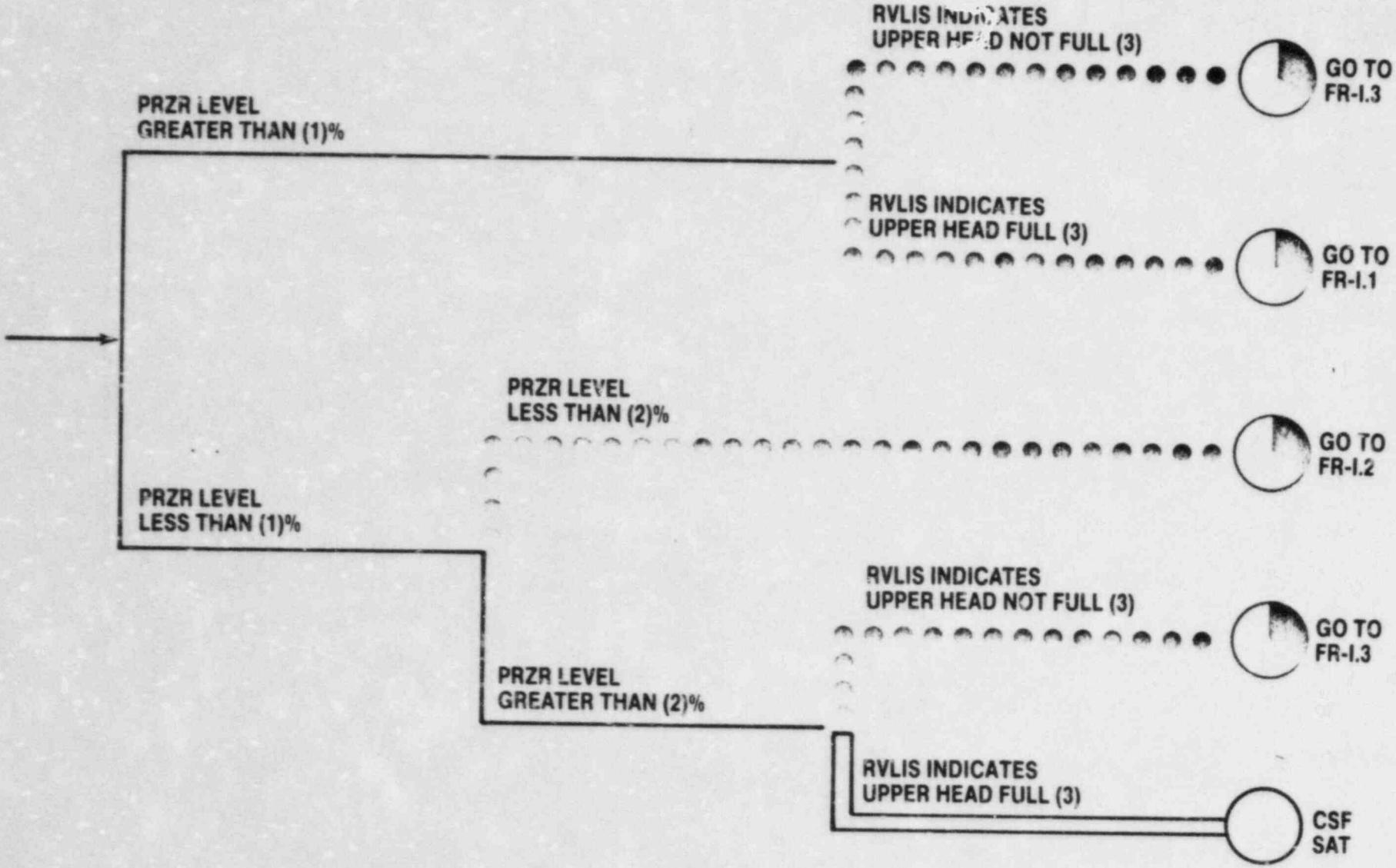


FIGURE 2f

APPENDIX A

INSTRUMENTATION FOR CRITICAL SAFETY FUNCTION MONITORING

CRITICAL SAFETY FUNCTION: Subcriticality

VARIABLE: Reactor Trip

Description	Instrument No.
Reactor Trip Breaker A	RP5RTA
Reactor Trip Breaker B	RP5RTB
Trip Signal	later

CRITICAL SAFETY FUNCTION: Subcriticality

VARIABLE: Power

Description	Instrument No.
Power Range Monitors	NM41F NM42F NM43F NM44F
Wide Range Fission Channels A and B	later

CRITICAL SAFETY FUNCTION: Subcriticality

VARIABLE: Startup Rate

Description	Instrument No.
Intermediate Range Monitor	NM35B NM36B
Source Range Monitor	NM31F NM32F
Wide Range Fission Channels A and B	later

CRITICAL SAFETY FUNCTION: Subcriticality

VARIABLE: Source R nge Energized

Description	Instrument No.
Source Range	NC31H
Loss of Voltage	NC32H

CRITICAL SAFETY FUNCTION: Core Cooling

VARIABLE: Core Exit Temperature

Description	Instrument No.
Core Exit Thermocouples	CTST1-CTST50

CRITICAL SAFETY FUNCTION: Core Cooling

VARIABLE: RCS Subcooling

Description	Instrument No.
ICC Processors	later
Unheated Junction of the HJTC from ICC Processors	later
Core Exit Thermocouples	CTST1-CTST50
Cold Leg RTDs	RCS-T413B/423B/433B/443B
Hot Leg RTDs	RCS-T413A/423A/433A/443A
Pressurizer Pressure	RCS-P455/456/457/458
RCS Pressure	RCS-P403/405

CRITICAL SAFETY FUNCTION: Core Cooling

VARIABLE: RC Pump Status

Description	Instrument No.
RC Pump Speed #1	RCP5475
2	RCP5476
2	RCP5477
3	RCP5478
RCS Loop Flow 1	RCS-F414/415/416
2	RCS-F424/425/426
3	RCS-F434/435/436
4	RCS-F444/445/446

CRITICAL SAFETY FUNCTION: Core Cooling

VARIABLE: RV level

Description	Instrument No.
ICC Processors	later

CRITICAL SAFETY FUNCTION: Heat Sink

VARIABLE: S/G level

Description	Instrument No.
Narrow Range S/G Level	
#1	FWS-L517/L518/L519
#2	FWS-L527/L528/L529
#3	FWS-L537/L538/L539
#4	FWS-L547/L548/L549
Wide Range S/G Level	
#1	FWS-L501/551
#2	FWS-L502/522
#3	FWS-L503/553
#4	FWS-L504/554

CRITICAL SAFETY FUNCTION: Heat Sink

VARIABLE: Total FW Flow

Description	Instrument No.
MFW 1	FWS-F510/511
2	FWS-F520/521
3	FWS-F530/531
4	FWS-F540/541
AFW 1	FWA-F33A
2	FWA-F33B
3	FWA-F33C
4	FWA-F33D

CRITICAL SAFETY FUNCTION: Heat Sink

VARIABLE: S/G pressure

Description	Instrument No.
S/G Outlet Pressure	
1	MSS-P514/5/6
2	MSS-P524/5/6
3	MSS-P534/5/6
4	MSS-P544/5/6

CRITICAL SAFETY FUNCTION: Integrity

VARIABLE: Cooldown Rate

Description	Instrument No.
Cold Leg RTD Loop #1	T413B
2	T423B
3	T433B
4	T443B

CRITICAL SAFETY FUNCTION: Integrity

VARIABLE: RCS Temperature

Description	Instrument No.
Cold Leg RTD's Loop #1	T413B
2	T423B
3	T433B
4	T443B

CRITICAL SAFETY FUNCTION: Integrity

VARIABLE: RCS pressure

Description	Instrument No.
Pressurizer Pressure	RCS P456
	RCS P457
	RCS P458
Wide Range RCS Pressure	RCS P403/405

CRITICAL SAFETY FUNCTION: Containment

VARIABLE: Containment Pressure

Description	Instrument No.
Wide Range Pressure	RMS-P24A
	RMS-P24B
Narrow Range Pressure	LMS-P934
	LMS-P935
	LMS-P936
	LMS-P937

CRITICAL SAFETY FUNCTION: Containment

VARIABLE: Water Level

Description	Instrument No.
Wide Range Sump Level	DAS-L-22
	DAS-L-39

CRITICAL SAFETY FUNCTION: Containment

VARIABLE: Containment Area Radiation

Description	Instrument No.
Wide Range Monitors	3RMS*RE04
	3RMS*RE05

CRITICAL SAFETY FUNCTION: Inventory

VARIABLE: Pressurizer Level

Description	Instrument No.
Pressurizer Level	RCS L459
	RCS L460
	RCS L461

CRITICAL SAFETY FUNCTION: Inventory

VARIABLE: RV level

Description	Instrument No.
ICC Processors	later

APPENDIX B

INSTRUMENTATION FOR RADIOACTIVITY CONTROL DISPLAY

RADIOACTIVITY CONTROL DISPLAY

VARIABLE: Main Steam Line Radiation

Description	Instrument No.
Main Steam Line Radiation Monitors	3MMS*RE75 3MMS*RE76 3MMS*RE77 3MMS*RE78
Safety Valve Flow Switches	later
Atmospheric Dump Valve Flow Switches	later
Auxiliary Feed Pump Steam Flow Switches	later

RADIOACTIVITY CONTROL DISPLAY

VARIABLE: Effluent Radiation

Description	Instrument No.
Stack Monitor	3HVR-RE19
Stack Flow Rate	3GWS-FT51/79