INSTRUMENTATION AND CONTROLS

CHAPTER 7

TABLE OF CONTENTS

Section	Title	Page
7.0	INSTRUMENTATION AND CONTROLS	7.1-1
7.1	INTRODUCTION	7.1-1
7.1.1	IDENTIFICATION OF SAFETY RELATED SYSTEMS	7.1-1
7.1.2	IDENTIFICATION OF SAFETY CRITERIA	7.1-6
7.1A	RPS MATRIX POWER SUPPLY ISOLATION QUALIFICATION	7.1A-1
7.2	REACTOR PROTECTIVE SYSTEM	7.2-1
7.2.1	DESCRIPTION	7.2-1
7.2.2	ANALYSIS	7.2-16
	REFERENCES	7.2-29
7.3	ENGINEERED SAFETY FEATURES SYSTEM	7.3-1
7.3.1	DESCRIPTION	7.3-1
7.3.2	ANALYSIS	7.3-25
	REFERENCES	7.3-34
7.4	SYSTEMS REQUIRED FOR SAFE SHUTDOWN	7.4-1
7.4.1	DESCRIPTION	7.4-1
7.4.2	ANALYSIS	7.4-10
	REFERENCES	7.4-19
7.5	SAFETY RELATED DISPLAY INSTRUMENTATION (INCLUDES NON-SAFETY RELATED DISPLAY INSTRUMENTATION)	7.5-1
7.5.1	DESCRIPTION	7.5-1
7.5.2	ANALYSIS	7.5-6
7.5.3	TMI RELATED ADDITIONAL ACCIDENT MONITORING INSTRUMENTATION	7.5-15
7.5.4	INSTRUMENTATION FOR DETECTION OF INADEQUATE CORE COOLING	7.5-17

EC282743

EC282743

CHAPTER 7

TABLE OF CONTENTS (Cont'd)

Section	Title	Page
7.5.5	POST ACCIDENT EXCORE NEUTRON FLUX MONITORING SYSTEM	7.5-29
	REFERENCES	7.5-31
7.5A	SAFETY ASSESSMENT SYSTEM/EMERGENCY RESPONSE DATA ACQUISITION AND DISPLAY SYSTEM	7.5A-1
7.5A.1	DESCRIPTION	7.5A-2
7.5A.2	HUMAN FACTORS CONSIDERATIONS	7.5A-3
7.5A.3	VERIFICATION AND VALIDATION	7.5A-4
7.6	ALL OTHER SYSTEMS REQUIRED FOR SAFETY	7.6-1
7.6.1	DESCRIPTION	7.6-1
7.6.2	ANALYSIS	7.6-2
7.6.3	ADDITIONAL SYSTEMS REQUIRED FOR SAFETY	7.6-7
7.7	CONTROL SYSTEMS NOT REQUIRED FOR SAFETY	7.7-1
7.7.1	DESCRIPTION	7.7-1
7.7.2	ANALYSIS	7.7-14
7.7.3	SYSTEM EVALUATION - HUMAN FACTORS ENGINEERING	7.7-15

INSTRUMENTATION AND CONTROLS

CHAPTER 7

LIST OF TABLES

Table	Title	Page
7.2-1	REACTOR PROTECTIVE SYSTEM DESIGN INPUTS	T7.2-1
7.2-2	REACTOR PROTECTIVE SYSTEM BYPASSES	T7.2-2
7.2-3	REACTOR PROTECTIVE SYSTEM SENSORS	T7.2-3
7.2-4	REACTOR PROTECTIVE SYSTEM MONITORED INSTRUMENT RANGES	T7.2-4
7.2-5	REACTOR PROTECTIVE SYSTEM - FAILURE MODES AND EFFECTS ANALYSIS	T7.2-5
7.3-1	ESFAS SENSOR PARAMETERS AND SETPOINTS	T7.3-1
7.3-2	COMPONENTS ACTUATED ON SIAS	T7.3-2
7.3-3	COMPONENTS ACTUATED ON RAS	T7.3-8
7.3-4	COMPONENTS ACTUATED ON CSAS	T7.3-10
7.3-5	COMPONENTS ACTUATED ON CIAS	T7.3-11
7.3-6	COMPONENTS ACTUATED ON MSIS	T7.3-14
7.3-7	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FAILURE MODES AND EFFECTS ANALYSIS	T7.3-15
7.3-8	ESF SIGNAL INTERCONNECTIONS FOR AB SHARED SYSTEM EQUIPMENT CONTROL-FAILURE MODE ANALYSIS	T7.3-23
7.3-9	MSIV ISOLATION CIRCUIT FAILURE MODE ANALYSIS	T7.3-24
7.3-10	ESF BYPASSES OR INOPERABLE INDICATION SYSTEM	T7.3-25
7.3-11	COMPONENTS ACTUATED BY AFAS	T7.3-29
7.3-12	AUXILIARY FEEDWATER ACTUATION SYSTEM FAILURE MODES AND EFFECTS ANALYSIS	T7.3-30
7.4-1	INSTRUMENTS FOR MONITORING SAFE SHUTDOWN	T7.4-1
7.4-2	INSTRUMENTATION AND CONTROL - HOT SHUTDOWN PANEL OUTSIDE THE CONTROL ROOM	T7.4-5
7.4-3	EMERGENCY REACTOR HOT SHUTDOWN/HOT STANDBY FROM OUTSIDE OF THE CONTROL ROOM CONTROL & TRANSFER SWITCH LIST	T7.4-7

CHAPTER 7

LIST OF TABLES (Cont'd)

Table	Title	Page
7.4-4	EMERGENCY REACTOR COOLDOWN & SHUTDOWN FROM OUTSIDE OF THE CONTROL ROOM	T7.4-10
7.4-5	EMERGENCY REACTOR SHUTDOWN FROM OUTSIDE OF THE CONTROL ROOM – INSTRUMENTATION	T7.4-12
7.4-6	HOT SHUTDOWN PANEL SWITCH POSITIONS	T7.4-13
7.5-1	SAFETY-RELATED DISPLAY INSTRUMENTATION	T7.5-1
7.5-2	DELETED	T7.5-27
7.5-3	SAFETY RELATED ANNUNCIATOR WINDOWS	T7.5-28
7.5-4	ESF SYSTEM VALVE INDICATORS	T7.5-29
7.6-1	SHUTDOWN COOLING SYSTEM AND SAFETY INJECTION TANK INTERLOCKS	T7.6-1
7.6-2	ACOUSTIC VALVE FLOW MONITOR COMPONENTS	T7.6-2

INSTRUMENTATION AND CONTROLS

CHAPTER 7

LIST OF FIGURES

Figures	Title
7.2-1	Control Wiring Diagram Pressurizer Pressure Measurement Loop
7.2-2	Neutron Flux Monitoring System Safety Channel
7.2-3	Low Steam Generator Pressure Reactor Trip Bypass Functional Diagram
7.2-4	Core Protection Trips Block Diagram
7.2-5	Thermal Margin Trip
7.2-6	ΔT Power Calculation
7.2-7	Reactor Protective System Block Diagram
7.2-8	RPS Functional Diagram
7.2-9	Basic RPS Testing System
7.2-10	Simplified RPS Cabinet Layout (Rear View)
7.2-11	Typical RPS Bay Layout
7.2-12	Bistable Block Diagram
7.2-13	Variable High-Power Trip Operation (Typical)
7.2-14	Low Flow Protective System Functional Diagram
7.2-15a	Steam Generator 'A' Protective Channel Block Diagram
7.2-15b	Steam Generator 'B' Protective Channel Block Diagram
7.2-16	Local Power Density Trip
7.2-17	Schematic Trip Test System
7.2-18	RPS Schematic SH 4 of 4
7.2-19a	RPS Misc. Schematics Sheet 1 of 4
7.2-19b	RPS Misc. Schematics Sheet 3 of 4
7.2-20	RPS Misc. Schematics Sheet 2 of 4
7.2-21	Reactor Protective System Interface Logic Diagram
7.3-1	Block Diagram - Engineered Safeguards Logic System
7.3-2	Control Wiring Diagram Pressurizer Pressure P-1102A Measurement Loop

CHAPTER 7

LIST OF FIGURES (Cont'd)

Figures	Title
7.3-3	Deleted
7.3-4	Deleted
7.3-5	Deleted
7.3-6	Deleted
7.3-6a	ATWS/DSS Logic Channel
7.3-7	Deleted
7.3-8	Deleted
7.3-9	Deleted
7.3-10	Block Diagram Power Distribution For Engineered Safeguards Logic System
7.3-11	ESFAS Interconnection for AB Shared System Equipment
7.3-12	Auxiliary Feedwater Actuation System Simplified Functional Diagram
7.3-13	Auxiliary Feedwater Actuation System Testing System Diagram
7.3-14	AFW Actuation System Signal Logic Diagram
7.5-1a	ICC Detection Instrumentation
7.5-1b	Qualified Safety Parameter Display System
7.5-2	HJTC Sensor - HJTC/Splash Shield
7.5-3	Heated Junction Thermocouple Probe Assembly
7.5-4	Deleted
7.5-5	HJTC Probe Installation
7.5-6	HJTC Sensor Locations
7.5-7a	In-Core Instrument Assembly
7.5-7b	ICI Detector Assemblies/Core Exit Thermocouples Core Locations
7.5-8	Interaction of the DG and the Inoperable Status Board
7.5A-1	Deleted
7.5A-2	Deleted
7.5A-3	Data Link System Configuration
7.6-1	Shutdown Cooling Suction Valves Power and Control

CHAPTER 7

LIST OF FIGURES (Cont'd)

Figures	Title
7.6-2	ATWS Block Diagram
7.7-1	Reactor Regulating System Block Diagram
7.7-2	CEDMCS-RPS Interface Block Diagram
7.7-3	Deleted
7.7-4	Deleted
7.7-5	Feedwater Control System Block Diagram
7.7-6	Analog Display System Simplified Block Diagram
7.7-7	Deleted
7.7-8a	Boron Dilution Alarm System Functional Diagram
7.7-8b	Boron Dilution Alarm System Neutron Flux and Setpoint

7.0 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

The instrumentation and control systems which monitor and perform safety related functions are discussed in this chapter. Complete descriptions and analyses of these systems are provided in Sections 7.2 through 7.6.

I & E Bulletin 79-24 titled "Frozen Lines" required review of plant design to ensure adequate protection of safety-related process, instrument, and sampling lines from freezing during extremely cold weather. Insulation was added to selected instrument lines as a result of this bulletin.

7.1.1 IDENTIFICATION OF SAFETY RELATED SYSTEMS

The safety related instrumentation and controls are associated with the Reactor Protective System, engineered safety features systems, systems required for safe shutdown, safety related display instrumentation and all other systems required for safety.

- Combustion Engineering, Inc (CE)
- Ebasco Services Inc (E)

7.1.1.1 Reactor Protective System (RPS) (CE)

The RPS generates signals that actuate reactor trip. A description of the RPS, detailing the functions of the system, is found in Section 7.2.

7.1.1.2 Engineered Safety Features Actuation System (ESFAS) (E), (CE)

The ESFAS generates signals that actuate engineered safety feature (ESF) systems. The actuation signals and the actuated systems are discussed in Section 7.3. The ESFAS consists of devices and circuitry to actuate the following signals:

a. Safety Injection Actuation Signal (SIAS)
b. Recirculation Actuation Signal (RAS)
c. Containment Spray Actuation Signal (CSAS)
d. Containment Isolation Actuation Signal (CIAS)
e. Main Steam Isolation Signal (MSIS)
f. Auxiliary Feedwater Actuation Signal-1 (AFAS-1)
g. Auxiliary Feedwater Actuation Signal-2 (AFAS-2)

The ESF systems which are actuated by the ESFAS are the following:

a. Safety Injection System (CE)

b. Recirculation system (E)

c. Containment Spray System (E)

d. Containment Isolation (E)

e. Main Steam and Feedwater Isolation (E)

f. Containment Cooling System (E)

g. Shield Building Ventilation System (E)

h. ESF Support Systems (E); see Subsection 7.1.1.3 for a list of support systems

i. Auxiliary Feedwater System (E)

7.1.1.3 Systems Required for Safe Shutdown

The systems required for safe shutdown include those systems which are required to secure and maintain the reactor in a hot shutdown condition and bring it to cold shutdown.

The following are the systems normally used for safe shutdown:

a. Auxiliary Feedwater System (E)

b. Atmospheric Steam Dump Valves (Steam Dump and Bypass System) (E)

c. Shutdown Cooling System (CE)

d. Chemical and Volume Control System (CVCS) [Boron addition and charging portion only] (CE)

The following support systems are also required to be operable or to function:

a. Component Cooling Water System (E)

b. Intake Cooling Water System (E)

c. Onsite Power System, including diesel generator system (E)

d. Heating, Ventilating and Air Conditioning (HVAC) Systems as required for areas containing systems and equipment required for safe shutdown (E)

e. Diesel Fuel Oil Storage and Transfer System (E)

The instrumentation and controls for the systems required for safe shutdown are described in Section 7.4.

7.1.1.4 Display Instrumentation

This section describes non-safety and safety related display instrumentation. The safety related (Class 1E) display instrumentation provides timely information to the operator so that he may initiate appropriate safety actions if and when required. Non-safety instrumentation is used for normal operation and although not required may be available for operator information.

The following display instrumentation provides monitoring of the automatic or manually actuated systems associated with the operation of the plant during normal or accident conditions:

a. ESF Systems Monitoring (E)

b. ESF Support Systems Monitoring (E)

c. Reactor Protective System Monitoring (CE)

d. CEA Position Indication System (CE)

e. Plant Process Display Instrumentation (CE/E)

f. Control Board Annunciators (E)

g. Bypass and Inoperable Status Indication (E)

h. Control Room Habitability Instrumentation (E)

i. Post-Accident Monitoring Instrumentation (E)/(CE)

j. Shutdown Cooling System Instrumentation (CE)

Refer to Section 7.5 for a description of the above instrumentation systems.

7.1.1.4.1 Qualified Safety Parameter Display System (QSPDS)

The QSPDS provides Class 1E processing and display of inadequate core cooling monitoring instruments and calculations. A description of the QSPDS, specifically the functions of the system is found in Subsection 7.5.4.3.2.

7.1.1.4.2 Regulatory Guide 1.97, R3

EC286245

Instrumentation pertaining to RG 1.97, R3 is described in Subsection 7.5.2.9.

7.1.1.5 All Other Systems Required for Safety

Other systems required for safety include the following interlocks and systems:

a. Shutdown Cooling System Suction Line Valve Interlocks (CE) (see Subsection 5.4.7)

b. Safety Injection Tank Isolation Valve Interlocks (CE) (see Section 6.3)

c. Refueling Interlocks (CE) (see Subsection 9.1.4)

d. Fuel Pool Cooling and Purification System (CE) (see Subsection 9.1.3)

e. Reactor Coolant Leak Detection System (CE) (see Subsection 5.2.5)

f. Area and Process Radiation Monitoring (E) (see Subsection 12.3.4)

g. Containment Vacuum Relief System (E) (see Subsection 6.2.1)

h. Overpressurization Protection (CE) (see Subsection 5.2.2)

i. Shield Building Ventilation System Switchover from Fuel Handling Building (E) (see Subsection 6.2.3)

The above are described further in Section 7.6.

7.1.1.6 Comparison

The Reactor Protective System was designed and built functionally identical to the system provided for St. Lucie Unit 1 (Docket No. 50-335) with the following exceptions:

a. The number of CEAs for St. Lucie Unit 2 is 83 (Cycle 1). This change has resulted in minor changes in core protection calculator settings.

b. The RPS of St. Lucie Unit 2 has a loss of CCW trip for RCP (Equipment) protection. This trip is not credited in the safety analysis.

   The St. Lucie Unit 2 logic functions are identical to those used for St. Lucie Unit 1, but also include fuses in all matrix inter-bay connections as part of improved fault protection. In addition, a test circuit is provided for checking the fuses (associated with this matrix fault protection) periodically (See Note 2). Matrix fuse integrity is checked periodically in accordance with the RPS technical specifications.

   St. Lucie Unit 2 matrix relays are dry reed types, for improved reliability over the original St. Lucie Unit 1 mercury wetted reed type relay design.

   St. Lucie Unit 2 incorporates a new RPS bistable design which, while functionally identical, is characterized by: greater accuracy, input buffering for improved circuit isolation, improved noise immunity via an adjustable response time, less cycling due to a variable hysterisis feature, and a pull-up (down) circuit design which forces a bistable trip on a loss of input signal. Consequently, contrary to the St. Lucie Unit 1 UFSAR Subsection 7.2.2.2, the St. Lucie Unit 2 auctioneered input bistables utilizing negative inputs trip in an open circuit configuration (See Note 3).

   St. Lucie Unit 2 has incorporated RG 1.53, RG 1.22, RG 1.75, IEEE 323-74, 344-75, and 384-74 in the RPS design. These guides/standards were not in effect when St. Lucie Unit 1 was licensed.

c. Systems Required for Safe Shutdown

   St. Lucie Unit 2 conforms to RG 1.75, which identifies a 6-inch spatial separation requirement, versus the 12 inch criteria of St. Lucie Unit 1.

d. Safety Related Display Instrumentation

   The upper and lower CEA limits are indicated on the CEDMCS control panel for St. Lucie Unit 2, while St. Lucie Unit 1 displays this information on the core mimic display. The St. Lucie Unit 2 design is identical to the SONGS design (Docket No. 50-362).

Many aspects of the St. Lucie Unit 2 design for Post-Accident Monitoring are different from St. Lucie Unit 1. St. Lucie Unit 2 is identical to SONGS with the exception of invoking BTP EICSB No. 23, Qualification of Safety-Related Display Instrumentation for Post-Accident and Safe Shutdown. The associated changes in this area for invoking RG 1.97 (R3) are provided in Subsection 7.5.2.9. EC286245

St. Lucie Unit 2 utilizes the Analog Display System (ADS), which while functionally identical to the originally supplied St. Lucie Unit 1 Metroscope, exhibits improved reliability design features and incorporates improved human factors characteristics. The metroscope was subsequently replaced with the CEA position display system (CEAPDS), which is similar to ADS.

This indication is non-1E indication and is further described in Subsection 7.7.1.1.6.

e. Engineered Safety Features Actuation System (ESFAS)

The St. Lucie Unit 2 ESFAS is functionally identical to the St. Lucie Unit 1 System. Channel designation and parameter inputs are essentially the same except for the following specific differences: The St. Lucie Unit 2 main steam isolation signal (MSIS) is initiated by a low pressure signal from either steam generator or high containment pressure (Subsection 7.3.1.1.5). St. Lucie Unit 1 MSIS is initiated by a low pressure signal from either steam generator only. The St. Lucie Unit 2 containment isolation actuation signal (CIAS) is modified to actuate on safety injection actuation signal (SIAS) as well as high containment pressure or high containment radiation. This modification was incorporated in St. Lucie Unit 1 as required by USNRC TMI Action Items to satisfy a diversity requirement for containment isolation. Subsection 7.3.1.1.4 reflects this CIAS modification.

St. Lucie Unit 2 has incorporated RG 1.53, RG 1.22, RG 1.75, IEEE 323-1974, 344-1975, and 384-1974 in the ESFAS design. These guides/standards were not in effect when St. Lucie Unit 1 was licensed.

The ESF systems are designed and built functionally identical to the ESF systems used on St. Lucie Unit 1 (Docket No. 50-335). The following are ESF system differences when compared against St. Lucie Unit 1.

a. Containment fan cooling system has two speed motors.

b. Each safety injection train is provided with its own miniflow recirculation header.

c. Each LPSI pump has its own separate header and associated valves.

d. The HPSI pumps are comprised of two functionally separate and independent pumps and headers. There is no installed spare HPSI pumps.

e. The Shutdown Cooling System is designed with redundant valves and headers.

f. Piping and valves permit the diversion of HPSI flow from the cold leg into the hot leg of the Reactor Coolant System for simultaneous hot and cold leg injection.

g. Pressurizer pressure interlocks on the SIT isolation valves open the valves prior to an actual or simulated pressurizer pressure signal exceeding 515 psia and prevent closure of the valves if pressurizer pressure is greater than 276 psia.

NOTES:

1. Deleted

2. The fuses of this section are utilized in the System 80 Plant Protection System Design.

3. The bistable design is a modified System 80 design, since the System 80 design does not utilize auctioneering.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Comparison of the design with applicable Regulatory Guide recommendations and degrees of compliance with the appropriate design bases, criteria standards, and other documents used in the design of the systems listed in Subsection 7.1.1 are described in Subsections 7.1.2.1 through 7.1.2.2.

7.1.2.1 Design Bases

The technical design bases for specific instrumentation and controls of each safety-related system are presented in applicable Subsections of this chapter. Design bases that apply equally to all safety- related instrumentation and control systems are in this Subsection.

a. General Design Criteria (GDC) Appendix A to 10 CFR 50: Discussions of compliance with GDC are provided in Sections 3.1, 7.2 and 7.3.

b. IEEE 279-1971 (ANSI N42.7-1972), "Criteria for Protection Systems for Nuclear Power Generating Station,": Discussions of conformance to this standard are provided in Sections 7.2, 7.3, 7.4, 7.5, and 7.6.

c. Applicable Regulatory Guides and IEEE standards discussed in Subsection 7.1.2.2.

Reactor Protective System

The design bases for the RPS are presented in Section 7.2.

Engineered Safety Features Actuation System

The design bases for the ESFAS and the ESF support systems are described in Section 7.3.

Systems Required for Safe Shutdown

The design bases for the systems required for safe shutdown are given in Section 7.4.

Safety Related Display Instrumentation

The design bases for display instrumentation are delineated in Section 7.5.

All Other Systems Required for Safety

The design bases for all other systems required for safety are discussed in Section 7.6.

The ESFAS and RPS instruments and circuitry inaccuracies are taken into consideration during setpoint selection and the accident analyses discussed in Chapter 15.

7.1.2.2 Regulatory Guide Implementation

Section 1.8 discusses how the effective dates of the Regulatory Guides discussed below were selected. The following is a comparison of the St. Lucie Unit 2 instrumentation and control design with the listed Regulatory Guides:

Regulatory Guide 1.11, "Instrument Lines Penetrating Primary Reactor Containment," 3/71 (R0)

The vacuum relief and containment main purge sensing lines used to detect a negative pressure inside containment do not form part of the protection system (as defined in IEEE 279-1971); but based on regulatory position 2a, compliance with positions 1b, 1c, 1d, and 1e is discussed below.

The sensing lines are redundant, independent and are testable in accordance with the requirements for a protective system. The sensing lines are each 3/8 inch (OD). In the event of a postulated failure in this line or in the excess flow check valve located just outside the shield wall during normal operation, the small size of this line precludes a) gross leakage, b) coolant loss since this line does not carry reactor coolant, c) jeopardizing the integrity of the secondary containment and d) potential offsite doses in excess of guidelines established for design basis accidents. A self-actuated excess flow check valve is provided outside of and as close to the shield wall as practical in each of the sensing lines. The sensing lines and excess flow check valves are Quality Group B. The redundant lines are separated and provisions are incorporated to permit periodic visual in-service inspection.

Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," 2/72 (R0)

Periodic testing of protection system actuation functions is discussed in Subsection 7.2.1.1.9 for RPS, Subsection 7.3.1.1.1d for ESFAS, Subsection 7.3.1.1.8d for AFAS, Subsection 7.4.2.3 for systems required for safe shutdown, Subsection 7.5.2.9 for safety related instrumentation and Subsection 7.6.2.2 for all other instrumentation systems required for safety.

Regulatory Guide 1.29, "Seismic Design Classification," 9/78 (R3)

Class 1E instrumentation and control components are designed to withstand the effects of a safe shutdown earthquake (SSE) and are designed as seismic Category 1. The seismic Category I design requirements are applied to the instrumentation and controls for the safety related systems identified in Subsection 7.1.1.

Qualification of seismic Category I/Class 1E instrumentation and controls is discussed in Section 3.10.

Regulatory Guide 1.30,"Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment," 8/72 (R0)

For a discussion of Regulatory Guide 1.30 (R0), refer to Chapter 17.

Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants," 8/72 (R0)

The use of IEEE 308-1971 in conjunction with Regulatory Guide 1.32 (R0) is discussed in Subsection 8.3.1.2.

Regulatory Guide 1.40, "Qualification Tests of Continuous-Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plants," 3/73 (R0)

This regulatory guide is not applicable to any instrumentation. Information on qualification is provided in Section 3.11.

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems“ 5/73 (R0)

The design of the safety related display information conforms to the regulatory positions of Regulatory Guide 1.47 (R0). Refer to Subsection 7.5.2.7 for a discussion of bypassed and inoperable status indication.

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant ProtectionSystems," 6/73 (R0)

The instrumentation and controls for safety related equipment conform to the recommendations of IEEE 379-1972 and are consistent with the recommendations of Regulatory Guide 1.53 (R0).

Regulatory Guide 1.62, "Manual Initiation of Protective Actions," 10/73 (R0)

The recommendations of Regulatory Guide 1.62 (RO) are complied with by the following design:

a. Manual initiation of each protective action at the system level is provided.

b. Manual initiation of a system level protective action initiates all required supporting systems.

c. Manual initiation switches are located in the control room and are readily accessible by the operator.

d. The amount of equipment common to both manual and automatic initiation is kept to a minimum. No single failure within the manual, automatic or common portions of the protection system can prevent initiation of the protection action by manual or automatic means.

e. Manual initiation of protective action depends on the operation of a minimum of equipment consistent with the above.

f. Manual initiations at the system level are designed to go to completion once initiated as required by Section 4.16 of IEEE 279-1971.

Regulatory Guide 1.63, "Electric Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plants," 10/73 (R0)

Instrumentation wiring which penetrates the containment is through electric penetration assemblies. For a discussion of how the design of the penetrations complies with the Regulatory Guide, refer to Subsection 8.3.1.2.

Regulatory Guide 1.68, "Initial Test Programs for Water-Cooled Reactor Power Plants," 11/73 (R0)

Regulatory Guide 1.73, "Qualification Tests of Electric Valve Operators Installed Inside theContainment of Nuclear Power Plants," 1/74 (R0)

Information on qualification testing is discussed in Section 3.11.

Regulatory Guide 1.75, "Physical Independence of Electric Systems," 1/75 (R1)

The safety related instrumentation and control systems meet the intent of Regulatory Guide 1.75 (R1) and IEEE 384-1974. Additional discussions concerning the implementation of Regulatory Guide 1.75 (R1) are given in Subsection 8.3.1.2. Note that the majority of the regulatory positions are directed at electric energy levels significantly above the energy levels of instrumentation and control circuits.

The RPS cabinet is divided into four bays which are separated by barriers. Each bay contains one of the four redundant channels of the RPS. This provides the separation and independence necessary to meet the requirements of Section 4.6 of IEEE 279-1971.

Tests or analyses are performed to demonstrate that no single credible event in one RPS channel can propagate the fault created to any other channel.

The reactor trip switchgear components and its associated switches, contacts, relays, etc. is contained in a five bay switchgear cabinet (four safety bays and one neutral bay). Each bay is physically separated from the other bays. This method of construction ensures that a single credible failure in one reactor trip switchgear does not cause malfunction or failure in another cabinet.

These isolation techniques ensure that no credible failure on the output side of the isolation device affects the RPS side and that the independence of the RPS is not jeopardized.

Instrumentation and control channel independence is achieved by electrical and physical separation between redundant Safety Class 1E channels and between Class 1E and non-Class 1E circuits and equipment. The ESFAS is provided with six separate cubicles, one for each channel (MA, MB, MC, MD, SA and SB), consisting of four measurement channels separated by metal barriers and two actuation channels. Redundant bistables, modules, logic matrices and output relays are located in separate cabinets. The redundant components at the control boards in the control room are also electrically and physically separated, providing complete channel independence. Physical separation barriers and boxed in terminal boards are utilized to maintain these separations between electrical circuits of redundant components. Circuits

which perform a nonsafety function and share or come in contact with Class 1E circuits are identified as associated circuits up to the isolation device. Associated circuits are separated in the same manner as the Class 1E circuits with which they are associated. Associated circuits are connected to non-Class 1E circuits through an isolation device. Separation is maintained from the Class 1E equipment up to and including the isolation device.

The isolation and independence of the Reactor Protective System is discussed below within two classifications: 1) Isolation of external non-1E interface signals and 2) Internal isolation to maintain independence of redundant channels.

a. Below is a listing of the signals which interface with systems external to the RPS.

Signal	Transmission Type	Isolation Device
Reactor Coolant Pump Breaker Status Contacts	Digital	Relay
Reactor Trip Switchgear Trip Circuit Breakers	Digital	Relay
Bistable Trip to Sequence of Events	Digital	Relay
Bistable Trip & Pre-Trip to Plant Annunciator	Digital	Relay
Operating Bypass and Misc. Plant Annunciator settings	Digital	Relay
CEA Withdrawal Prohibit	Digital	Relay
10^{-4} % Power to Analog Display System	Digital	Relay
Power Operated Relief Valve Closure Signal	Digital	Relay
Q Power to Power Ratio Calculator	Analog	Isolation Amplifier
Q Power to Analog Display System	Analog	Isolation Amplifier

When reviewing the above list it should be noted that signals which are listed as not requiring an isolation device are maintained separate from signals classified as 1E or associated in accordance with the requirements set forth in Regulatory Guide 1.75 (R1). Also the isolation device identified as relay are physically a relay in conjunction with a fuse. The relay provides contact to coil isolation (dielectric strength) while the fuse maintains the integrity of the wire. The two devices together are considered to be the isolation device.

Each type isolation device is qualified for a fault of 480V ac and 325V dc. The actual test voltages are 600V ac and 400V dc.

The general acceptance criteria for RPS isolation devices is as follows:

1. Application of the fault to the appropriate side of the isolation device shall not propagate to the other side of the isolation device or adversely affect the operation of circuitry connected to the other side of this isolation device.

2. The integrity of the wire insulation must be maintained. The above acceptance criteria meets Regulatory Guide 1.75 and IEEE 384.

b. The following is a discussion of the means by which independence of the four RPS channels is maintained.

Process input signals are sent to bistable trip units within the RPS where the signal is first buffered and then compared to a setpoint to create an on/off type signal. This signal deenergizes five separate relays within the trip unit. At this point all signals, cablings, modules, dedicated power supplies and any associated test circuitry are maintained totally independent across the four channels.

One contact from each trip unit is wired in series together within each channel. This series string is produced three times within each channel. The strings are then combined with another channel such that each contact is in parallel with a contact from another channel. This forms the six possible combinations of logic matrices AB, AC, AD, BC, BD, CD. All connections of relay contacts between channels are fuse protected in the channel of origin and the channel of destination. This fuse in conjunction with its related contact and coil provide the required isolation between bistable and matrix.

Each matrix is powered from two diode isolated power supplies located in two different channels of the RPS. Each power supply has with it an isolation circuit which limits the fault to acceptable values and prevents the fault from disturbing the independent vital buses.

Each logic matrix drives four matrix relays. One matrix relay contact from each of the six matrices is connected in series to drive an initiation relay. This circuit is labeled the trip path. All connections of relay contacts between channels are fuse protected in the channel of origin and the channel of destination. This fuse in conjunction with its related contact and coil provide the required isolation between the trip path and each matrix.

Testing within each channel is maintained independent through the use of a test interlock circuit which provides the intelligence to allow testing in only one channel at a time. The test is performed in three levels: 1) bistable test, 2) matrix test and 3) trip path test. The bistable test is performed using an independent test source within each channel such that a fault would affect only one channel. The matrix and trip path test is performed through the matrix test

module by energizing bistable and/or matrix secondary relay coils. A combination of contact to contact, contact to coil, coil to contact and coil to coil isolation (all in conjunction with a fuse) are used to ensure a fault within the test circuit will not compromise the four channel redundancy.

All isolation devices discussed above are qualified to 480V ac and 325V dc and tested to 600V ac and 400V dc. The entire system is also subjected to an EMI test in accordance with MIL-STD-461A, "Electromagnetic Interference Characteristics Requirements for Equipment," for both conducted and radiated signals using tests CS01, CS02, CS06, RS03 and RS04. Additional information on qualification tests is provided in Appendix 7.1A.

In addition to the above, the safety portion of the pressurizer level channels are isolated from the non-safety portion by an analog voltage to analog voltage isolation. This isolation utilizes transformer coupling as its isolating/signal coupling medium.

Short circuits, open circuits, and high voltages (480 ac) are applied to the output circuitry as credible faults. The failure of these faults to perturb or propagate to the input circuitry form the basis of the acceptance criteria for this isolation.

There are no additional safety to non-safety interfaces nor process instrumentation interconnections between redundant safety circuits.

Regulatory Guide 1.80, "Preoperational Testing of Instrument Air Systems," 6/74 (R0)

Regulatory Guide 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants," 11/74 (R0)

For discussion of qualification of Class 1E equipment, see Section 3.11.

Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident" 12/75 (R0) and 12/80 (Rev. 2)

As indicated in the implementation section of Regulatory Guide 1.97 (R0), the positions of this guide are to be used to evaluate construction permit (CP) applications submitted after August 1, 1976; the St. Lucie Unit 2 CP application was docketed in September 1974. Although Regulatory Guide 1.97 (R0) was not applicable to this operating license application, the positions of this Regulatory Guide are discussed in Subsection 7.5.2.9. Implementation of the requirements of Regulatory Guide 1.97, Rev. 3 is discussed in Subsection 7.5.2.9. EC286245 EC286245

Regulatory Guide 1.100, "Seismic Qualification of Electric Equipment for Nuclear Power Plants," 3/76 (R0)

As indicated in the implementation section of Regulatory Guide 1.100 (R0), the positions of this guide are to be used to evaluate construction permit (CP) applications docketed after November 15, 1976. The St. Lucie Unit 2 (CP) application was docketed in September, 1974. Although RG 1.100 (R0) is not applicable to this operating license application, Section 3.10 presents a discussion of seismic qualification of Class 1E instrumentation and controls.

Regulatory Guide 1.105, "Instrument Setpoints," 11/76 (R1)

As indicated in the implementation section of Regulatory Guide 1.105 (R1), the method described in this guide is to be used in the evaluation of plants with construction permits docketed after July 1, 1976. Although Regulatory Guide 1.105 (R1) not applicable to the St. Lucie Unit 2 operating license, the intent of the regulatory positions is met as follows:

(C1) Setpoints are established with margins as indicated at the Technical Specification limits for the process variable and the nominal trip setpoint which include allowance for instrument inaccuracy, calibration uncertainty, and instrument drift anticipated between calibration intervals.

(C2) All setpoints are established in that portion of the instrument span which insures that accuracy is maintained. Instruments are calibrated so as to insure the required accuracy at the setpoint.

(C3) The range selected for the instrumentation encompasses the expected operating range of the process variable being monitored to the extent that saturation does not negate the required action of the instrument.

(C4) The accuracies of all instruments with setpoints are equal to or better than the accuracy assumed in the safety analysis. Instrument internals are chosen for the design conditions in which they are installed. Design verification is included as part of the equipment qualification program as recommended in Regulatory Guide 1.89 (R0).

(C5) Instruments important to safety have securing devices on the setpoint adjustment mechanism. The securing device is designed such that during securing or releasing it does not alter the setpoint. Such devices are under administrative control.

(C6) Documentation of bases used in selecting setpoint values are contained in the Technical Specifications. Chapter 15 contains assumptions used in the accident analyses whereby setpoint values are determined.

Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems" 6/76 (R0)

As indicated in the implementation section of Regulatory Guide 1.118 (R0), the positions of this guide are to be used to evaluate construction permit applications docketed after February 15, 1977. Although Regulatory Guide 1.118 (R0) is not applicable to this operating license application, the design meets the intent of Regulatory Guide 1.118 (R0) and IEEE 338-1971 except for response time testing. Periodic response time testing during reactor operation is required by the Regulatory Guide. The design calls for response time verification testing conducted during initial installation and subsequent plant shutdowns.

This Regulatory Guide is further discussed in Subsection 8.3.1.2.

APPENDIX 7.1A

RPS MATRIX POWER SUPPLY ISOLATION QUALIFICATION

APPENDIX 7.1A

RPS MATRIX POWER SUPPLY ISOLATION QUALIFICATION

The following provides further definition on the method of qualifying the RPS matrix power supply (with associated isolation networks) to the requirements of IEEE 323-1974, in accordance with CENPD-255(R1), "Qualification of Class 1E Instrumentation." The results of each test discussed below were provided to the NRC.[(1)(2)]

a. Fault Isolation Qualification

The test involves simulating a typical RPS matrix, including bistable trip units, bistable power supplies, matrix power supplies, matrix relays, and isolation relays. Vital bus power (120V ac) Is simulated by using two power isolation transformers. The isolation test consists of the application of 600V ac and 400V dc faults in the circuit in the common and transverse modes. The basis for the 600V ac and the 400V dc test voltage is as follows:

- 600V ac: The highest credible ac fault voltage which could appear within the RPS is 480V ac. This voltage is increased by 10 percent to 528V ac to account for normal voltage tolerances and then again increased by 10 percent to 581V ac to account for IEEE STD 323-1974 margin. This voltage is then rounded off to 600V ac.

- 400V dc: The highest credible dc fault voltage which could appear within the RPS is 325V dc. This voltage is increased by 10 percent to 358V dc to account for normal voltage tolerances and then again increased by 10 percent to 394V dc to account for IEEE STD 323-1974 margin. This voltage is then rounded off to 400V dc.

1. Common Mode Test

The common mode test is accomplished by applying a fault to the dc side of a matrix power supply. The fault voltage and current are monitored to define the fault characteristics. Also, the 120V ac line side of the power supply is monitored to document any effect as a result of application of the fault. All monitoring is by means of a light beam recorder.

2. Transverse Mode Test

The transverse mode test is accomplished by applying the fault directly to the output terminals of the isolation circuit. This fault voltage and current are monitored to define the fault characteristics. Also, the Input side of the Isolation circuit and the 120V ac line side of the power supply are monitored to document any effects as a result of application of the faults. All monitoring is by means of a light beam recorder.

3. AcceptanceCriterion

   The acceptance criterion for the above tests is that upon application of the fault the input power supply voltage does not vary more than ± 10 percent from the nominal voltage. It has been shown that before, during, and after a fault application the system will perform its protective function (trip actuation) when required.

b. SurgeQualification

A surge test is performed on the RPS according to the guidance of IEEE Standard 472-1974, to the extent practical.

The test involves simulating a typical RPS matrix, including bistable trip units, bistable power supplies, matrix power supplies, matrix relays, and isolation relays. Vital bus power (120V ac) is simulated by using two power isolation transformers. The test voltage from neutral to peak is 337 volts (120V ac + 10 percent) x 1.414 plus the neutral to peak surge 300V/2.

An ultra-isolation transformer has been added to the design of the vital bus inverter system in order to attenuate any line surges which may pass through the inverter system. The isolation transformer is surge qualified in accordance with the guidelines of IEEE Standard 472-1974. This includes application of a surge (2.5 kV to 3.0 kV) to the primary winding in both the common and transverse modes. The acceptance criterion for this test is that the transformer limits the surge on the secondary to 100 volts. Note that the credible surge seen by the RPS is limited to 100 volts which is two thirds of the surge being applied to the RPS. The transformer is also qualified to the requirements of IEEE Standard 344-1975 and IEEE Standard 323-1974, in accordance with CENPD-255(R1).

1. CommonModeTest

   The common mode test is accomplished by applying a surge to the ac side of the matrix power supply and the power supply chassis. During surge application the simulated RPS circuit is operated to show proper function and accuracy. Also, the 120V ac line of the associated power supply is monitored.

2. TransverseModeTest

   The transverse mode test is accomplished by applying a surge to the ac side of the matrix power supply. During application of the surge the simulated RPS circuit is operated to show proper function and accuracy. Also the 120V ac line of the associated power supply is monitored.

3. AcceptanceCriterion

   The acceptance criterion for the above tests is that all circuits shall operate correctly and within their normal accuracy requirements before,

during, and after the surge application. Also, the voltage observed at the input of the second power supply should not vary more than ± 10 percent of the nominal voltage.

APPENDIX7.1A:REFERENCES

1) FP&L Letter L-82-470 from Dr. R. E. Uhrig (FP&L) to Mr. D. G. Eisenhut (NRC) dated October 29, 1982.

2). FP&L Letter L-82-550 from Dr. R. E. Uhrig (FP&L) to Mr. D. G. Eisenhut (NRC) dated December 22, 1982.

7.2 REACTOR PROTECTIVE SYSTEM

This section describes the design and functions of the Reactor Protective System (RPS). Subsection 7.2.1 includes a summary description of the following:

- Reactor Trips Initiating
- Circuits Logic
- Actuated Devices Bypasses
- Interlocks Redundancy Diversity
- Testing
- Power Supply

Design bases are discussed in Subsection 7.2.1.2.

Analysis of the design of the RPS is discussed in Subsection 7.2.2, including the bases for the reactor trips, purpose of the trips, compliance with General Design Criteria and IEEE 279-1971, and a failure modes and effects analysis.

7.2.1 DESCRIPTION

7.2.1.1 System Description

The Reactor Protective System (RPS) consists of sensors, calculators, logic, and other equipment necessary to monitor selected Nuclear Steam Supply System (NSSS) conditions and to effect reliable and rapid reactor shutdown (reactor trip) if any or a combination of the monitored conditions approach specified safety system settings. The RPS functions are to assure that reactor coolant pressure boundary (RCPB) and fuel performance guidelines are not exceeded during moderate frequency events and infrequent events and also to provide assistance in limiting conditions for certain limiting faults.

The system is designed such that the single failure criterion and performance requirements are met with three channels in service. A coincidence of any two like trip signals generates a reactor trip signal. However, four measurement channels with electrical and physical separation are provided for each parameter. To enhance plant availability, a fourth channel is provided as a spare and allows bypassing of one channel while maintaining the requisite two-out-of-three logic.

A reactor trip initiated by the Reactor Protective System causes the input motive power to be removed from the control element drive mechanism control system (CEDMCS) by the trip switchgear, which in turn causes all control element assemblies to be inserted by gravity.

Provisions were originally made for future operations with one or more reactor coolant pumps inoperative, in that the low reactor coolant flow trip setpoint and the thermal margin/low pressure trip setpoints could be simultaneously changed to the setpoints for the selected pump conditions. However, power operation with less than four pumps in operation is not allowed by the operating license, and this flow dependent setpoint capability was subsequently eliminated.

The RPS trip setpoints are provided in the Technical Specifications. RPS bypasses are summarized on Table 7.2-2.

7.2.1.1.1 Reactor Trips

7.2.1.1.1.1 High Power Level

A reactor trip on variable high power level is provided to trip the reactor in the event of reactivity excursions that may be too rapid for the high pressurizer pressure trip function to respond. High power level trips also provide backup protection for steam line break accidents.

High Power levels trip the reactor when the reactor power (the higher of neutron flux power or thermal power) reaches a high preset value. During startups, this setpoint is manually increased to a fixed increment above the existing reactor power level up to a maximum value. As reactor power decreases, the high power level trip setpoint automatically decreases, maintaining the fixed increment between the reactor power level and the setpoint. The high power trip has a 15% lower and a 10% upper limit (RTP).

7.2.1.1.1.2 High Rate-of-Change of Power

The high rate-of-change of power trip is not credited in any of the Chapter 15 accident analyses; however, the trip is considered in the safety analysis in that the presence of this trip function precluded the need for specific analyses of other events initiated from subcritical conditions (events not discussed in Chapter 15). This trip is provided to trip the reactor when the rate-of-change of neutron flux power reaches a high preset value.

7.2.1.1.1.3 High Local Power Density

The high local power density trip is provided to trip the reactor when the axial offset exceeds a high calculated value or falls below a low calculated value. The calculated setpoints are generated in the analog core protection calculators as a function of reactor power (the higher of neutron flux power or thermal power), and assure a core peak local power density below fuel performance guidelines for infrequent events and moderate frequency events (See Chapter 15). The trip is automatically bypassed when reactor power falls below a low preset value.

7.2.1.1.1.4 Thermal Margin/Low Pressure

The thermal margin/low pressure (TM/LP) trip is provided to trip the reactor when the Reactor Coolant System pressure falls below a low preset value, or a low calculated value, whichever is higher. The calculated setpoint is a function of reactor inlet temperature, and axial offset. The calculated setpoint assures a core departure from nucleate boiling (DNB) ratio above the fuel performance guidelines for infrequent events and moderate frequency events. The preset setpoint provides protective action assistance to the engineered safety feature (ESF) systems during certain LOCA limiting faults. The trip signal can be manually bypassed when the neutron flux power falls below a low preset value. The bypass is automatically removed when the flux power exceeds the bypass value.

The Asymmetric Steam Generator Transient Protective Trip Function (ASGTPTF) consists of SG pressure inputs to the TM/LP calculator, causing a reactor trip when the difference in pressure between the two SGs exceeds the trip setpoint. The ASGTPTF is designed to provide a reactor

trip on secondary system malfunctions which result in asymmetric primary loop coolant temperatures.

7.2.1.1.1.5 High Pressurizer Pressure

The high pressurizer pressure trip is provided to trip the reactor when measured pressurizer pressure reaches a high preset value.

7.2.1.1.1.6 Low Reactor Coolant Flow

The low reactor coolant flow trip is provided to trip the reactor when the reactor coolant flow reaches a low preset value. The low reactor coolant flow trip signal may be manually bypassed when the neutron flux power falls below a low preset value. The bypass is automatically removed when the flux power exceeds this value.

7.2.1.1.1.7 Low Steam Generator Water Level

The low steam generator water level trip is provided to trip the reactor when the lower of the measured steam generator water levels for the two steam generators falls to a low preset value.

7.2.1.1.1.8 Low Steam Generator Pressure

The low steam generator pressure trip is provided to trip the reactor when the lower of the measured steam generator pressures for the two steam generators falls to a low preset value. The low steam generator pressure trip signal may be manually bypassed when the steam generator pressure falls below a low preset value. The bypass is automatically removed when the steam generator pressure exceeds this value.

7.2.1.1.1.9 High Containment Pressure

The high containment pressure trip is provided to trip the reactor when measured containment pressure reaches a high preset value.

7.2.1.1.1.10 Turbine Trip

The reactor trip on turbine trip is an equipment protective trip and is not required for reactor protection. The reactor trip on turbine trip is automatically bypassed when the reactor power falls below a low preset value. The bypass is automatically removed when the reactor power exceeds this value.

7.2.1.1.1.11 Loss of Component Cooling Water Trip

The reactor trip upon a loss of component cooling water to the reactor coolant pumps is not required for reactor protection. The reactor trip upon loss of component cooling water is delayed 10 minutes after it reaches the preset setpoint. Four channels of Class 1E indication of component cooling water flow out of all reactor coolant pumps is provided on the RTGB.

In addition, indicators are provided on the reactor turbine generator board (RTGB) for reactor coolant pump component cooling water flow for each reactor coolant pump.

7.2.1.1.1.12 Manual Trip

A manual reactor trip is provided to permit the operator to trip the reactor. Actuation of two adjacent pushbutton switches in the control room causes interruption of the AC power to the CEDMs. Two independent sets of trip pushbuttons are provided; either one of which causes a reactor trip. There are also manual reactor trip switches at the reactor trip switchgear.

The remote manual initiation portion of the reactor trip system is designed as an input to the reactor trip switchgear system (RTSS). This design is consistent with the recommendations of Regulatory Guide 1.62, "Manual Initiation of Protective Actions," October 1973 (R0). The amount of equipment common to both automatic and manual initiation is kept to a minimum. Once initiated, the manual trip goes to completion as required in Section 4.16 of IEEE 279-1971.

7.2.1.1.2 Initiating Circuits

7.2.1.1.2.1 Process Measurements

Various pressures, water levels, and temperatures associated with the NSSS and the containment atmosphere are continuously monitored to provide signals to the RPS trip bistables. All protective parameters are measured with four independent process instrument channels each of which is powered by an independent instrument power supply. A detailed listing of the parameters measured is contained in Table 7.2-3.

A typical protective channel as shown on Figure 7.2-1, consists of a sensor/transmitter, power supply, current loop resistors, indicating meter or recorder, trip bistable/calculator inputs.

7.2.1.1.2.2 Excore Neutron Flux Monitoring and Protective Systems

The excore nuclear instrumentation includes neutron detectors located around the reactor core, and signal conditioning equipment located within the containment and Reactor Auxiliary Building. Neutron flux is monitored over a 10 decade span from $2x10^{-8}$ percent to 200 percent reactor power and outputs are provided for reactor protection and information display.

There are four channels of safety instrumentation (see Figure 7.2-2). Each channel comprises both linear "Power Range" circuitry and logarithmic "Wide Range" circuitry located within the same drawer. Each channel has separate detectors and amplifiers (where required) for the linear and logarithmic portions of the safety channel.

7.2.1.1.2.2.1 Wide Range Logarithmic Safety Channels

The four wide range logarithmic safety channels measure neutron flux from $2x10^{-8}$ percent of full power through 200 percent of full power. A fission chamber detector and amplifier, both located within containment, provide a signal input to the signal processing electronics, located in the safety channel drawer in the RPS cabinet.

The wide range logarithmic safety channels are used by the RPS as input signals to the high rate of change of power trip, input to the zero power mode bypass circuitry and to the low power bypass of this trip.

7.2.1.1.2.2.2 Power Range Safety Channels

The four power range channels measure neutron flux linearly over the range of 1.0 percent to 200 percent of full power. The detector assembly provided for each power range safety channel consists of two uncompensated ionization chambers stacked vertically along the length of the reactor core. The use of two subchannel detectors in this arrangement permits the measurement of axial offset during power operation. The dc current signal from each of the ionization chambers is fed directly to the signal processing electronics, located in the safety channel drawer. The power range safety channels are used by the RPS as input signals to the core protection calculators to determine the neutron flux power and axial offset, and as input signals to the high power bypass circuitry for the high rate of change of power trip.

7.2.1.1.2.3 Reactor Coolant Flow Measurements

The reactor coolant flow measurement signals are provided by summing a function of the differential pressure across each steam generator to provide an indication of the total coolant flow through the reactor. This measurement of differential pressure (Δ p) is directly proportional to the actual flow. The low flow reactor trip is actuated directly by the summed Δ p signals.

7.2.1.1.2.4 Analog Core Protection Calculators

The core protection calculators are analog computers that provide input to the thermal margin/low pressure trip, the local power density trip, and the high power trip.

A calculated low pressure limit related to departure from nucleate boiling ratio (DNBR) is determined using preset coefficients as a function of the measured cold leg temperature, axial offset, and the higher of the thermal power or neutron flux power. This calculated low pressure limit is an input to the thermal margin/low pressure trip.

The difference between steam generator pressures is monitored and compared to a predetermined setpoint, above which a reactor trip is initiated to protect against secondary system malfunctions which result in asymmetric primary loop coolant temperatures.

The functions of the analog core protection calculators are shown on Figures 7.2-4 through 7.2-6.

The upper and lower subchannel neutron flux signals from the power range safety channels are processed to determine the neutron flux power and the axial offset. The axial offset is an input to the local power density trip, and the thermal margin/low pressure trip.

The hot and cold leg temperatures from precision resistance temperature detectors are processed to determine the thermal power. The higher of the thermal power or neutron flux power is an input to the high power trip, the thermal margin/low pressure trip, and the local power density trip.

7.2.1.1.2.5 Trip Generation

Signals from the process trip unit measurement loops are sent to bistables where the input signals are compared (trip setpoint) to predetermined trip values. Whenever a parameter reaches the trip value, the bistables deenergize three bistable relays. The bistable relay contacts

change state, effecting the appropriate coincidence logic (refer to Subsection 7.2.1.1.3). Auxiliary bistables are provided for contact input process signals.

The bistable setpoints are adjustable from the front of the RPS cabinet through recessed potentiometers. The setpoints within a channel can be monitored on a meter located on the front of the RPS cabinet.

Pretrip and trip circuitry is also provided to generate visible indication on the front of each RPS cabinet.

7.2.1.1.2.6 Pressurizer and Steam Generator Level Measurements

Both steam generators and the pressurizer at St. Lucie Unit 2 have open-column reference legs susceptible to containment temperature changes. The effect of a High Energy Line Break inside the containment would be to heatup the reference legs and cause a decrease in the density of the water columns. The resultant effect on the level measurement system would be an indicated level that is reading higher than the actual level. The main concern for an accurate level reading during an accident such as a main steam break would be to maintain an inventory level in the intact steam generator(s) using the auxiliary feedwater system to allow a controlled cooldown and also to record an accurate pressurizer level as a means of reacting to changing RCS conditions.

The level error is accounted for in the determination of safety setpoints.

7.2.1.1.3 Logic

Tripping of a bistable (or trip contact opening as in the case of turbine trip, loss of component cooling water to the reactor coolant pumps, or a calculated trip) results in a channel trip which is characterized by the deenergization of three bistable trip relays (see Figures 7.2-7 and 7.2-8).

Contacts from the bistable relays of the same parameter in the four protective channels are arranged into six logic ANDs, designated AB, AC, AD, BC, BD, and CD, which represent all possible coincidence of two combinations. To form an AND circuit, the bistable trip relay contacts associated with two like measurement channels are connected in parallel (e.g., one from A and one from B). This process is continued until all combinations have been formed.

Since there is more than one parameter that can initiate a reactor trip, the parallel pairs of bistable trip relay contacts for each monitored parameter are connected in series (logic OR) to form six logic matrices. The six matrices are designated AB, AC, AD, BC, BD, and CD.

Each logic matrix is connected in series with a set of four matrix output relays. Each logic matrix is powered from two separate 120v Class 1E instrument power supply buses through dual dc power supplies as shown on Figure 7.2-8. The power supplies are protected from overload by means of input and/or output fuses or circuit breakers.

The contacts of the matrix relays are combined into four trip paths, one trip path per channel.

Each initiation circuit is formed by connecting six contacts (one matrix relay contact from each of the six logic matrices) in series. The six series contact are in series with the initiation relay. The initiation relays open the reactor trip switchgear system (RTSS) circuit breakers as discussed in Subsection 7.2.1.1.4.

7.2.1.1.4 Actuated Devices

The logic matrices cause the four initiation relays to be deenergized. Each initiation relay in turn causes two of the trip circuit breakers in the RTSS to open (see Figures 7.2-7 and 7.2-8).

Power input to the RTSS comes from two full-capacity motor-generator sets, so that the loss of either set does not cause a release of the CEAs. Each line passes through two trip circuit breakers (each actuated by a separate trip-path) in series so that, although both sides of the branch lines must be deenergized to release the CEAs, there are two separate means of interrupting each side of the line. Upon removal of power to the CEDM power supplies, all of the CEAs are inserted into the reactor core by gravity.

Two independent sets of manual trip pushbuttons are provided on the RTGB 201 and 204 to open the trip circuit breakers, if desired. The manual trip completely bypasses the trip logic. As can be seen on Figure 7.2-8, both manual trip pushbuttons in a set must be depressed to initiate a reactor trip.

The reactor trip switchgear system is housed in a cabinet separate from the Reactor Protective System and is located in the electrical equipment room below the control room. In addition to the trip circuit breakers, the cabinet also contains current monitoring devices for testing purposes, bus undervoltage relays for auxiliary functions, and a bus tie breaker.

Pushbuttons are provided at the RTSS to allow circuit breaker testing at a location other than the control room.

7.2.1.1.5 Bypasses

The bypasses listed in Table 7.2-2 are provided to permit testing, startup, and maintenance.

a. Operating Bypasses

The zero power mode and low steam generator pressure bypasses are provided for two conditions: system tests at low power and low temperature, and heatup and cooldown with shutdown CEAs withdrawn. The bypasses may be used in mode 3 and below consistent with Technical Specifications and operating procedures. The bypasses are manually initiated and removed within each channel, with automatic removal as a backup to assure full system capability. The functions affected by this bypass are listed in Table 7.2-2.

The turbine trip bypass is provided to remove this equipment protective trip below the value shown in Table 7.2-2 so that the reactor can be started up with the turbine tripped.

The high local power density trip bypass is provided to remove this trip in the low power range where it is not required for reactor protection.

The high rate of change of power trip bypass is provided to remove this equipment protective trip in the range of low power operation where its function is not required.

All operating bypasses are visibly displayed to the operator.

b. Trip Channel Bypass

A bypass is provided to remove a trip function from one of the RPS channels from service for maintenance or testing. The requisite two-out-of-three trip logic is unaffected by this bypass. The remaining trip functions in that channel are unchanged. The bypass is manually initiated and manually removed. The bypass is initiated by the use of a key operated switch. By the use of administrative controls only one key is available for each trip parameter. Each of the CCW low flow to RCP trip channels may be manually bypassed (one key per channel) to remove this trip when not required by Technical Specifications. By the use of administrative controls, only one key is used to bypass a trip function when required by the Technical Specifications.

Therefore, only one channel of a given parameter can be bypassed at a time, except as detailed above.

7.2.1.1.6 Interlocks

The following interlocks are provided:

a. An electrical interlock allows only one set of four matrix relays in one matrix to be held at a time during system testing. The same circuit allows only one pair of bistable trip relays, for a given parameter, to be actuated at a time (see Figure 7.2-9).

b. An interlock is provided to initiate a variable high power, thermal margin/low pressure and local power density trips when test signals are applied to the calculators. This occurswhen the nuclear instrument summer control switch is removed from the (A + B)/2 position or a linear channel high voltage trip is produced or the calibration panel mode select switch is removed from the operating position.

c. A mechanical interlock in conjunction with administrative control prevents the operator from bypassing more than one trip channel at a time for any one type of trip. Different type trips may be simultaneously bypassed, however, either in one channel or in different channels.

7.2.1.1.7 Redundancy/Independence

The four channel independence begins at the output of the 4 ac UPS inverters, designated inverter 2A, 2B, 2C and 2D or the Maintenance Bypass Transformer 2A, 2B, 2C and 2D and their associated instrument Buses as shown on Figure 8.3-3. Independence of the four channels of RPS or ESFAS is maintained in accordance with Subsections 8.3.1.3, 8.3.1.4, and 7.3.1.1.1h.

Redundant features of the Reactor Protective System include:

a. Four independent channels, from process sensor through and including channel trip relays

b. Six logic matrices which provide the trip logic. Dual power supplies are provided for the matrix relays

c. Four trip paths, including four control logic paths and four initiation relays

d. CEDM power from two power buses, including two full capacity motor-generator sets

e. Two sets of manual trip pushbuttons with either set being sufficient to initiate a reactor trip

f. AC power for the system from four separate Class 1E instrument power supply buses. DCpower for trip circuit breaker control logic is provided from four separate dc buses powered from two separate battery trains.

The result of the redundant features is a system that meets the single failure criterion, can be tested during reactor operation, and maintains the requisite two-out-of-three logic.

The benefit of a system that includes four independent and redundant channels is that the system can be operated, if need be, with up to two channels out of service (one bypassed and another tripped) and still meet the single failure criterion. The system logic must be restored to at least a three operating channel condition prior to removing another channel for Maintenance.

7.2.1.1.8 Diversity

The failure modes of redundant channels and the conditions of operation that are common to them are analyzed to assure that credible common failure modes do not exist. The design provides reasonable assurance that:

a. The monitored variables provide adequate information during the events listed in Subsections 7.2.2.1.1 and 7.2.2.1.2.

b. The equipment can perform as required.

c. The interactions of protective actions, control actions and the environmental changes that cause, or are caused by, the events listed in Subsection 7.2.2.1.1 and 7.2.2.1.2 do not prevent the mitigation of the consequences of the event.

d. The RPS cannot be made inoperable by the inadvertent actions of operating or maintenance personnel.

In addition, the design is not encumbered with additional components or channels without reasonable assurance that such additions are beneficial.

In accordance with 10 CFR 50.62, a high degree of diversity is required between the RPS and the Diverse Scram and Auxiliary Feedwater Actuation Systems (see further discussion in section 7.6.3.11).

The bistable and matrix relay cards found in the AFAS cabinets have a high level of diversity with respect to the relays found in the RPS. In general the AFAS relays have different types of reed switch assemblies than the RPS relays. These relays are the only area of concern identified by the NRC relevant to the mitigation requirement of the ATWS Rule (10 CFR 50.62) and they maintain diversity between the RPS and AFAS. It has been concluded that the different relay cards are sufficient to show compliance with the NRC ATWS Rule on auxiliary feedwater initiation, 10 CFR Part 50.62.

7.2.1.1.9 Testing

Provisions are made to permit periodic testing of the RPS, with the reactor operating at power or when shut down. These tests cover the trip actions from sensor input through the logic and the trip switchgear. The system test does not interfere with the protective function of the system. The testing system meets the criteria of IEEE 338-1971," IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," and is consistent with the recommendations of Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," February 1972 (R0).

RPS functions can be tested one channel at a time while the plant is operating by using the built in test circuits, with the following exceptions:

a. PORV Actuation - This logic circuit requires two out of four trip actuations and therefore can only be tested during plant shutdown when the PORV control circuit external of the RPS can be defeated. Testing the PORV will also initiate a reactor trip.

b. CEA Withdrawal Prohibit (CWP) - This logic circuit requires two out of four pre-trip actuations and should be tested only during plant shutdown.

c. Response Time Testing - This test requires two out of four actuations of the RPS and can only be performed during plant shutdown.

NI detectors and amplifiers where utilized are not capable of being tested during operation. Proper operation of these channels is verified by periodic channel comparisons.

Process transmitters and sensors feeding the RPS not accessible during operation are also checked for proper operation by periodic channel comparisons.

The individual tests are described briefly below. Overlap between individual tests exists so that the entire RPS can be tested. Frequency of accomplishing these tests is listed in the Technical Specifications.

7.2.1.1.9.1 Sensor Check

During reactor operation, the measurement channels providing an input to the RPS are checked by comparing the outputs of similar channels and crosschecking with related measurements.

These measurement channels are checked and calibrated in accordance with plant Technical Specifications.

7.2.1.1.9.2 Bistable Trip Unit Tests

Testing of the bistable trip units is accomplished by manually varying the input signal up to or down to the trip setpoint level on one bistable at a time and observing the trip action.

Varying the input signal is accomplished by means of a trip test circuit consisting of a digital voltmeter and a test circuit used to vary the magnitude of the signal supplied by the measurement channel to the trip input. The trip test circuit is interlocked electrically so that it can be used if only one channel at a time. A switch is provided to select the measurement channel,

and a pushbutton is provided to apply the test signal. The digital voltmeter indicates the value of the test signal. Trip action (deenergizing) of each of the bistable trip relays is indicated by individual lights on the front of the cabinet, indicating that these relays operate as required for a bistable trip condition.

When one of the bistables of a protective channel is in the tripped condition, a channel trip exists and is annunciated on the RTGB. In this condition, a reactor trip would take place upon receipt of a trip signal in one of the other like trip channels. The trip channel under test is therefore bypassed for this test. Full protection is maintained.

7.2.1.1.9.3 Analog Core Protection Calculator Test

This test is accomplished by simulating selected calculator sensor inputs values and monitoring the corresponding output signals.

The checking of the trip relays for the calculator generated trips is conducted as described in Subsection 7.2.1.1.9.2, for thermal margin/low pressure, or by initiating a calculator trip, for local power density, and observing the individual bistable relay trip lights.

7.2.1.1.9.4 Logic Matrix Test

This test is carried out to verify proper operation of the six logic matrices, any of which can initiate a system trip for any possible coincidence of two trip condition from the signal inputs from each measurement channel.

Only the matrix relays in one of the six logic matrix test modules can be held in the energized position during tests. If, for example, the AB logic matrix hold pushbutton is depressed, actuation of the other matrix hold pushbuttons can have no effect upon their respective logic matrices.

Actuation of the pushbutton applies a test voltage to the test system hold coils of the selected double coil matrix relays. This voltage provides the power necessary to hold the relays in their energized position when deactuation of the bistable trip relay contacts in the matrix ladder being tested causes deenergization of the primary matrix relay coils.

The logic matrix to be tested is selected using the system channel trip select switch. While holding the matrix hold pushbutton in its actuated position, rotation of the channel trip select switch releases only those bistable trip relays that have operating contacts in the logic matrix under test. The channel trip select switch applies a test voltage of opposite polarity to the bistable trip relay test coils, so that the magnetic flux generated by these coils opposes that of the primary coil of the relay. The resulting flux will be zero, and the relays are released. A simplified diagram of this testing system is shown on Figure 7.2-9 using the AB matrix.

Trip action can be observed by illumination of the trip relay indicators located on the front panel of the RPS cabinet and by loss of voltage to the four matrix relays, which is indicated by extinguishing indicator lights connected across each matrix relay coil. Test equipment may be used for monitoring if status lights are not available.

During this test, the matrix relay "hold" lights remain on, indicating that a test voltage has been applied to the holding coils of the matrix relays of the logic matrix module under test.

Each logic matrix tested consists of series/parallel contact arrangements of the trip unit bistable relays in two RPS bays. Each wire crossing a channel boundary is fused. A two-position fuse test switch is provided for each matrix. Operation of the matrix push button applies a test voltage to the holding coils of the matrix relays, while at the same time operation of the fuse test switch places alternate trip unit relays in the tripped condition. This in turn changes the series/parallel matrix to a series circuit. Fuse status is determined by observing the normal matrix lights and the bistable relay status lights.

The test is repeated for all six matrices. This test verifies that the bistable relay contacts operate correctly and that the logic matrix relays will deenergize if the matrix continuity is violated. The opening of the matrix relay contact is tested in the trip path tests (see Subsection 7.2.1.1.9.5).

7.2.1.1.9.5 Trip Path/Circuit Breaker Tests

Each trip path is tested individually by depressing a matrix hold pushbutton (holding matrix relays), selecting any trip position on the channel trip select switch (opening the matrix), and selecting a matrix relay on the matrix relay trip select switch (deenergizing one of the matrix relays).

This causes one, and only one, of the trip paths to deenergize, causing two trip circuit breakers to open. CEDMs remain energized via the other trip circuit breakers.

The dropout lamps shown on Figures 7.2-8 and 7.2-9 are used to provide additional verification that the matrix relay is deenergized, (e.g., the AB-1 matrix relay contact energized the dropout lamp). Proper operation of the actual trip path matrix relay contacts is verified by the trip path lamp located on the trip status panel.

Proper operation of all trip circuit breakers is verified by lights on the RPS status panel; final proof of opening of the trip circuit breakers is the lack of indicated current through the trip breakers. Test equipment may be used for monitoring if status lights are not available.

The matrix relay trip select switch is turned to the next position, reenergizing the tested matrix relay and allowing the trip breakers to be manually reset.

This sequence is repeated for the other three trip paths from the selected matrix. Following this, the entire sequence is repeated for the remaining five matrices. Upon completion, all 24 matrix relay contacts and all four trip paths and breakers have been tested.

7.2.1.1.9.6 Manual Trip Test

The manual trip feature is tested by depressing one of the four manual trip pushbuttons, observing a trip of two of the trip breakers and resetting the breakers prior to depressing the next manual trip pushbutton.

7.2.1.1.9.7 Bypass Test

The system bypasses, as itemized in Table 7.2-2, are tested by appropriate test circuitry. Testing includes both initiation and removal features.

7.2.1.1.9.8 Response Time Test

Response time testing of the Reactor Protective System is required at refueling intervals per the Technical Specifications. Response time test requirements and acceptance criteria are discussed in Section 13.7.2.1. These tests are conducted on a system basis or an overlapping subsystem basis.

7.2.1.1.10 Class 1E Instrument Power Supply

The adequacy of a four (4) channel based ac UPS system deriving its stored energy power source from two divisions of dc power requires a brief review of the philosophy of ac UPS power for RPS and ESFAS power supply.

The ac UPS power supply four channel concept is selected for plant availability and not plant safety as the loss of power to the RPS and ESFAS will result in channel trip.

Furthermore, the number of channels, whether three or four, provides a design basis in excess of that required for safety by providing for spurious channel trips or testing during plant operation without plant trip for the specific purpose to enhance plant availability or provide testing during operation.

In fact, the requirement for the ac UPS system is actually the ability to "ride-through" a momentary power loss without plant trip. Boiling Water Reactors (e.g., WPPSS No. 2) utilize non-Class 1E "ride- through flywheel motor-generator power systems" to power the reactor protection systems.

Table 7.3-7, "Engineered Safety Features Actuation System Modes and Effects Analysis," clearly indicates that the loss of a battery will not preclude completion of safety function. Furthermore, the two redundant Class 1E divisions of onsite ac power deriving its onsite power generation from Class 1E diesel-generators forms the basis for compliance with 10 CFR 50 Appendix A GDC 17. These two divisions provide the source of power to the ac UPS RPS & ESFAS power supplies through the dc power distribution system battery chargers in Light Water Reactors. Provision of four batteries for utility convenience or symmetry, each in support of a RPS and ESFAS channel, would typically only support RPS and ESFAS loads for the short time necessary to resequence the battery chargers on the Class 1E ac system subsequent to a Loss of Offsite Power. A review of licensed nuclear plants demonstrates the acceptability of the two safety related battery design (References 1 & 2).

On the basis of the referenced information, the St. Lucie Unit 2 design is considered acceptable.

The Class 1E instrument power supply requirements are discussed in Chapter 8.

7.2.1.2 Design Bases

The RPS is designed to assure that acceptable RCPB and fuel performance guidelines are not exceeded during Moderate Frequency Events and Infrequent Events. In addition, the system is designed to assist the ESF systems in limiting the consequences of limiting Faults. To ensure that these objectives are achieved, the reactor must be maintained within the limiting conditions and the limiting safety system settings implemented consistent with the Technical Specifications.

The system is designed on the following bases to assure adequate performance of its protective function:

a. The system is designed in compliance with the applicable criteria of, "General Design Criteria for Nuclear Power Plants," Appendix A of 10 CFR 50.

b. Instrumentation, function, and operation of the system conform to the requirements of IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

c. System testing conforms to the requirements of IEEE 338-1971, "IEEE Trial-Use Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems."

d. The system designed is consistent with the recommendations of Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," June 1973 (R0) and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," February 1972 (R0).

e. The system is designed to determine the following conditions in order to provide adequate protection during Moderate Frequency Events and Infrequent Events.

    1. Neutron flux power, thermal power
    2. Reactor Coolant System pressure
    3. Thermal margin in the limiting coolant channel in the core
    4. Axial offset
    5. Steam generator water level
    6. Reactor Coolant System flow

f. The system is designed to determine the following conditions in order to provide protective action assistance to the ESF during Limiting Faults:

    1. Neutron flux power
    2. Reactor Coolant System pressure
    3. Steam generator pressure
    4. Containment pressure
    5. Reactor Coolant System flow
    6. Steam generator water level

g. The system is designed to monitor variables that are needed to assure adequate determination of the conditions given in listings e) and f) above, over the entire range of normal operation and transient conditions. The full power nominal

values and the maximum and minimum values that can be sensed for each monitored plant variable are given in Table 7.2-4.

The type, number, and location of the sensors provided to monitor these variables are given in Table 7.2-3.

h. The system is designed to alert the operator when any monitored condition is approaching a condition that would initiate a protective action.

i. The system is designed so that a protective action is not initiated due to normal operation.

Nominal full power values of monitored conditions and their corresponding nominal protective action (trip) setpoints are given in Table 7.2-1 and St. Lucie Unit 2 Technical Specifications respectively.

The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays and inaccuracies are taken into account. Response times and analysis setpoints used in the safety analyses are provided in Chapters 6 and 15.

The trip delay times and analysis setpoints provided in Chapter 15 are representative of the manner in which the RPS instrumentation operates. These quantities are used in the transient analysis shown in Chapters 6 and 15. Actual RPS uncertainties and delay times are obtained from calculations and tests performed on the RPS and associated instrumentation. The verified system uncertainties are factored into RPS settings and/or setpoints to assure that the system adequately performs its intended function when the errors and uncertainties combine in an adverse manner. The final equipment settings are then included in the Technical Specifications.

j. System components are qualified for environmental and seismic conditions in accordance with IEEE 344, and IEEE 323 as defined in Section 3.10 and referenced in Section 3.11

Electrical transmitters are mounted on open instrument racks, insulated cabinets with heaters are not utilized.

7.2.1.3 System Drawings

The signal logics, block diagrams, and test circuit block diagrams are shown on Figures 7.2-1 through 7.2-21. Electrical wiring diagrams, block diagrams, logic diagrams and location layout drawings are listed and provided by reference in Section 1.7.

7.2.2 ANALYSIS

7.2.2.1 Introduction

The RPS is designed to provide the following protective functions:

a. Initiate automatic protective action to assure that acceptable RCPB and fuel performance guidelines are not exceeded during Moderate Frequency Events and Infrequent Events.

b. Initiate automatic protective action during Limiting Faults to aid the ESF systems in limiting the consequences of these events.

A description of the reactor trips provided in the RPS is given in Subsection 7.2.1.1.1. Subsection 7.2.2.2 provides the bases for all the RPS trips and the Technical Specifications provide nominal trip setpoints.

Most of the trips in the RPS are single parameter trips (i.e., a trip signal is generated by comparing a single measured variable with a fixed setpoint). The RPS calculated trips that do not fall into this category are as follows:

a. Low Steam Generator Level Trip.

   This trip is determined as a function of the lower of the measured steam generator water levels for the two steam generators.

b. Low Steam Generator Pressure Trip.

   This trip is determined as a function of the lower of the measured steam generator pressures for the two steam generators.

c. High Local Power Density Trip.

   This trip is calculated as a function of several measured variables.

d. Thermal Margin/Low Pressure Trip.

   This trip is calculated as a function of several measured variables.

e. High Power Level Trip.

This trip is determined as a function of the higher of neutron flux power or thermal power. The trip employs a setpoint that can be manually increased to a fixed increment above the existing power level (higher of the two power levels). The setpoint tracks the power (remaining this fixed increment above it) when the power decreases.

All RPS trips except turbine trip are provided with a pretrip alarm in addition to the trip alarm. Pretrip alarms are provided to alert the operator to an approach to a trip condition and play no part in the safety evaluation of the plant. The pretrip alarms associated with the high power level trip, thermal margin/low pressure trip, high local power density, and high rate-of-change of power initiates a control rod withdrawal prohibit (CWP) to the CEDMCS.

RPS setpoints are chosen in the following manner: nominal RPS trip setpoints are selected on the basis of past performance of similar plants. Considering expected uncertainties and delay

times, an analysis setpoint is selected to verify the adequacy of the nominal setpoint for the conditions described in Subsections 7.2.2.1.1 and 7.2.2.1.2. The analysis setpoint along with actual instrument uncertainties provides the basis for the calculation of the final equipment setpoints to be reported in the Technical Specifications. These final equipment setpoints assure that a trip signal is generated at or before the analysis setpoint. The manner by which these delay times and uncertainties are verified is discussed in Subsection 7.2.1.2.

7.2.2.1.1 Moderate Frequency Events and Infrequent Events

Moderate Frequency Events and Infrequent Events are those events that may occur one or more times during the life of the plant. In particular, the occurrences considered include single component failures or control system failures resulting in transients which may require protective action.

The RPS provides proper protective actions when required to assure that the fuel performance and RCPB guidelines are not exceeded for Moderate Frequency and Infrequent Events.

7.2.2.1.2 Limiting Faults

The Limiting Faults are those events that are not expected to occur during the life of the plant. The consequences of these Limiting Faults are limited by the actions of the Engineered safety features systems. The RPS provides actions when required to assist in limiting the consequences of the Limiting Faults to assume that the fuel performance and RCPB guidelines are not exceeded.

7.2.2.2 Trip Bases

The RPS consists of eleven trips in each channel that initiates the required automatic protective action utilizing a coincidence of two like trip signals.

A brief description of the inputs and purpose of each trip is presented in Subsections 7.2.2.2.1 through 7.2.2.2.11.

Due to the significance of the Loss of Component Cooling Water Trip and the Turbine Trip, an analysis of these trips has been included in Subsections 7.2.2.2.10 and 7.2.2.2.11, respectively.

7.2.2.2.1 High Power Level Trip

<u>Inputs</u>

a. Neutron flux power from the Excore Neutron Flux Monitoring System;

b. Thermal power derived from the hot and cold leg coolant temperature.

<u>Purpose</u>

Trip to assist the ESF systems in the event of an ejected CEA Limiting Fault.

7.2.2.2.2 High Rate-of-Change of Power Trip

Input

Neutron flux power from the Excore Neutron Flux Monitoring System.

Purpose

To provide equipment protection and to protect against an exceedingly high rate of change of power resulting from large reactivity insertions during periods of low power operation.

7.2.2.2.3 High Local Power Density Trip

Inputs

a. Neutron flux power and axial offset from the Excore Neutron Flux Monitoring System;

b. Thermal power derived from the hot and cold leg coolant temperature measurements.

Purpose

To prevent the linear heat rate (kW/ft) in the limiting fuel pin in the core from exceeding the fuel performance guidelines in the event of any Moderate Frequency Event or Infrequent Event.

7.2.2.2.4 Thermal Margin/Low Pressure Trip

Inputs

a. Neutron flux power and axial offset from the Excore Neutron Flux Monitoring System;

b. RCS pressure from pressurizer pressure measurement;

c. Thermal power derived from the hot and cold leg coolant temperature measurements, and

d. Steam generator pressure from each steam generator

Purpose

To prevent the DNB ratio in the limiting coolant channel in the core from exceeding the fuel performance guidelines in the event of defined Moderate Frequency Events. In addition, this trip provides a low pressure reactor trip to assist the ESF systems in limiting the consequences of certain LOCA Limiting Faults.

7.2.2.2.5 High Pressurizer Pressure Trip

Input

Pressurizer pressure from narrow range pressurizer pressure measurement.

Purpose

To help assure the integrity of the RCS boundary for any defined Moderate Frequency Events or Infrequent Events that could lead to an overpressurization of the RCS, and to provide a reactor trip to assist the ESF systems in the event of a feedwater line break (FWLB) Limiting Fault.

7.2.2.2.6 Low Reactor Coolant Flow Trip

Input

Reactor coolant flow from summing the differential pressure across each steam generator.

Purpose

To provide a reactor trip to prevent the DNB ratio in the limiting coolant channel in the core from exceeding the fuel performance guidelines in the event of a change of forced reactor coolant flow Infrequent Event or Moderate Frequency Events. In addition, this trip will assist the ESF systems in limiting the consequences of a RCP shaft seizure Limiting Fault, RCP sheared shaft Limiting Fault, and certain steam line break Limiting Faults.

7.2.2.2.7 Low Steam Generator Water Level Trip

Input

Level of water in each steam generator downcomer region from narrow range differential pressure measurements.

Purpose

To provide protective action to assure that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of steam generator water inventory.

Should feedwater not be recoverable, the increased EPU core decay power and the associated decreased boil-off time impacts the timing and equipment set required for successful implementation of once-through-cooling operation. A risk informed change to increase the steam generator narrow range low level reactor trip setpoint from 20.5 percent to 35 percent was implemented to address this potential loss of capability.

7.2.2.2.8 Low Steam Generator Pressure Trip

Input

Steam pressure in each steam generator.

Purpose

To assist the ESF systems in the event of a steam line break Limiting Fault.

7.2.2.2.9 High Containment Pressure Trip

Input

Pressure inside containment.

Purpose

To assist the ESF systems in the event of certain LOCA or FWLB Limiting Faults.

7.2.2.2.10 Loss of Component Cooling Water Trip

Input

A reactor trip following a loss of Component Cooling Water (CCW) to the reactor coolant pumps is provided as an equipment protective feature, but is not required for reactor protection. See Subsection 7.2.2.5.5.

The return flow of CCW to the reactor coolant pumps is sensed at the discharge header. Four flow transmitters are located on the CCW common return header to monitor CCW flow from the RCPs. These four transmitters are powered from redundant Class 1E power supplies (MA, MB, MC, and MD) are physically and electrically separated in accordance with Regulatory Guide 1.75 (R1).

Purpose

The trip setting corresponds to a reduction in flow to the four reactor coolant pumps. System evaluation is described in Subsection 9.2.2.

7.2.2.2.11 Loss of Load, Turbine Trip

Input

A reactor trip initiation following a turbine trip is provided as an equipment protective feature, and is not required for reactor protection. See Subsection 7.2.2.5.4.

Turbine trip is taken from four non-Class 1E hydraulic oil pressure switches associated with the Turbine Control System. A coincidence of low hydraulic oil on two of the pressure switches initiates the reactor trip signal. The signal is fed to the Reactor Protective System through an isolation device.

The turbine trip circuit for the reactor trip up to the isolation device is classified as non-safety. Special cable routing provisions are provided. After the isolation device the circuit (including the isolation device) meets all IEEE 279-1971 requirements as described in Subsection 7.2.2.3.2. The circuit testing is in accordance with the Subsection 7.2.1.1.9 and the plant technical specification.

Purpose

To provide equipment protection rather than reactor protection. This trip is intended to precede a high pressurizer pressure trip, which is the safety related reactor protective trip, as a result of a

turbine trip at power operation above the bypass setpoint shown in Table 7.2-2. The Turbine Control System is described in Subsection 7.7.1.1.10.

7.2.2.3 Design

7.2.2.3.1 General Design Criteria

Conformance to Appendix A of 10 CFR 50, "General Design Criteria for Nuclear Power Plants," are given in Section 3.1.

7.2.2.3.2 Equipment Design Criteria

IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations", establishes minimum requirements for safety related functional performance and reliability of the Reactor Protective System.

This section describes how the requirements as listed in Section 4 of IEEE 279-1971 are satisfied.

4.1, "General Functional Requirement"

The RPS is designed to assure that acceptable RCPB and fuel performance guidelines are not exceeded for Moderate Frequency Events and Infrequent Events. In addition, the RPS is designed to assist the ESF in limiting the consequences of Limiting Faults. Instrument performance characteristics, response time, and accuracy are selected for compatibility with and adequacy for the particular function. Trip setpoints are established by analyses of the system parameters. Factors such as instrument accuracies, trip times, CEA travel times, circuit breaker trip times, and pump starting times are considered in the design of the system.

4.2, "Single Failure Criterion"

The RPS is designed so that any single failure within the system does not prevent proper protective action at the system level. No single failure defeats more than one of the protective channels associated with any one trip function. The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, negates protective system operation. Signal conductors are protected and routed independently.

Signal conductors and power leads coming into or going out of each cabinet are protected and routed separately for each channel of each system to minimize possible interaction.

Single failures considered in the design of the RPS are described in the failure modes and effects analysis (FMEA) shown in Table 7.2-5.

4.3, "Quality Control of Components and Modules"

The quality assurance program complies with 10 CFR 50, Appendix B. This program includes appropriate requirements for design review, procurement, inspection and testing to ensure that the system components are of a quality consistent with minimum maintenance requirements and low failure rates.

4.4, "Equipment Qualification"

The RPS meets the equipment qualification requirements described in Sections 3.10 and 3.11.

4.5, "Channel Integrity"

Type testing of components, separation of sensors and channels, and qualification of the cabling are utilized to ensure that the channels maintain their functional capability required under applicable extremes of environment, power supplied, malfunction and fault conditions. Loss of or damage to any one channel does not prevent the protective action of the RPS. Sensors are connected so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the containment are specified and rated for the intended service. Components which must operate during or after a Limiting Fault are qualified for the most limiting environment for the period of time for which they must maintain their functional capability. Results of type tests are used to verify this.

4.6, "Channel Independence"

Each channel is independent of its redundant channels. The sensors are separated, cabling is routed separately and, in cabinets, each redundant channel is located in a separate compartment which provides thermal and mechanical barriers. This minimizes the possibility of a single event causing more than one channel failure. The outputs from these redundant channels are isolated from each other so that a single failure does not cause impairment of the system function.

Outputs from the RPS channels to non-Class 1E systems are isolated so that a failure in the non- Class 1E system does not cause loss of the safety system function.

Conformance with the requirements of IEEE 384-1974, "IEEE Trial Use Standard Criteria for Separation of Class 1E Equipment and Circuits," and Regulatory Guide 1.75, "Physical Independence of Electric Systems," January, 1975 (R1) is discussed in Subsection 7.1.2.2.

4.7, "Control and Protection System Interaction"

a. 4.7.1 - Classification of Equipment

   Equipment that is used for both protective and control functions is designed in accordance with IEEE 279-1971. The following is a list of such cases:

   - The RPS thermal margin/low pressure, local power density high power level, high rate-of-change of power and high pressurizer pressure bistable pre-trips are formed into logic which initiates a CEA withdrawal prohibit. This circuit is classified as non- Class 1E and its signal is isolated prior to being sent to the CEDMCS.

   - The RPS high pressurizer pressure bistable trips are arranged into a logic to initiate opening of the pressurizer relief valves upon a coincidence of two channels. This circuit is classified as non-Class 1E and is isolated prior to leaving the RPS cabinet.

- Meter relays located within the steam generator level measuring loops are arranged such that a high level in the steam generator produces a feedwater regulating valve closure and high-high level trips the turbine and feedwater pumps. The circuits are classified as non-Class 1E and are isolated accordingly.

b. 4.7.2 - Isolation Devices

Signals from the RPS are isolated such that a failure does not affect protective action of the RPS.

c. 4.7.3 - Single Random Failures

Provisions are included such that a single random failure does not cause a control action that results in a condition requiring a protective action, and does not concurrently prevent proper action of RPS channel even when degraded by a second random failure. The control feature is manually bypassed when the associated protective channel is bypassed or removed from service.

d. 4.7.4 - Multiple Failures Resulting from a Credible Single Event

No credible single event results in multiple failures.

4.8, "Derivation of System Input"

Insofar as is practicable, system inputs are derived from signals that are direct measures of the desired variables. Variables that are measured directly include neutron flux, temperatures, and pressures. Level information is derived from appropriate differential pressure measurements. Flow information is derived from steam generator differential pressure.

4.9, "Capability for Sensor Checks"

RPS sensors are checked by cross-channel comparison. Each channel has a known relationship with the other channels of the same parameter.

4.10, "Capability for Test and Calibration"

The RPS design complies with IEEE 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," and Regulatory Guide 1.22 (R0), as discussed in Subsection 7.2.2.3.2.

4.11, "Channel Bypass or Removal From Operation"

Any one of the four protection channels can be tested, calibrated, or repaired without impairing the protective action capability of the RPS. Within any RPS channel, individual trip functions may be bypassed. The requisite two-out-of-three logic is unaffected.

4.12, "Operating Bypasses"

Operating bypasses are provided as shown in Table 7.2-2. The operating bypasses are automatically removed when the conditions which permitted the bypass are no longer present.

4.13, "Indication of Bypasses"

RPS trip channel bypasses are not automatically annunciated on the control board but are indicated on the RPS which is in the control room in view of the operator.

Indication of test or bypass conditions or removal of any channel from service is given by lights and annunciation. Bypasses that are automatically removed at specified setpoints are indicated when in the bypass condition. Bypassing for maintenance or testing is visually indicated on the front of the respective RPS cabinet. System level bypass indication (zero power mode bypass, SG pressure bypass) of the RPS is furnished on the reactor protection annunciators RTGB-204.

4.14, "Access to Means for Bypassing"

A key is required to bypass a protective system channel (refer to Figure 7.2-20). Only one key is available for bypassing the channels of a given parameter. Therefore, only one of the four channels of any one type trip may be bypassed at any one time. All bypasses are visually indicated. The CCW low flow to RCP trip may be manually bypassed via multiple keys to remove this trip when not required by Technical Specifications. By the use of the administrative controls, only one key is available when the function is required to be operable by Technical Specifications.

4.15, "Multiple Setpoints"

Manual setpoint changes are not required during normal plant operation, except high power level.

Manual incrementing of high power level setpoints is used for the controlled increasing of reactor power as discussed in Subsection 7.2.1.1.1.1. Incrementing of setpoints is initiated by an RTGB pushbutton, one for each channel. This method of increasing setpoints provides a positive assurance that the setpoint is never increased above existing power by more than a predetermined margin.

A variable setpoint is provided for Thermal Margin/Low Pressure (TM/LP) and Local Power Density (LPD) for the purposes defined in Subsections 7.2.1.1.1.4 and 7.2.1.1.1.3 respectively. The setpoints are continuously calculated with limits being applied to restrict the setpoints to a prescribed range.

4.16, "Completion of Protective Action Once It is Initiated"

The system is designed to ensure that protective action (reactor trip) goes to completion once initiated. Operator action is required to clear the trip and return to operation. Protective action is initiated when the reactor trip circuit breakers open. Protective action is completed when the CEAs arrive at their full-in position.

4.17, "Manual Initiation"

A manual trip is effected by depressing either of two sets of trip pushbuttons on the RTGB for the RPS or the pushbuttons on the RTSS. No single failure prevents a manual trip.

4.18, "Access to Setpoint Adjustments, Calibration and Test Points"

Setpoint or calibration adjustments are either internal to the protective system or under direct administrative control.

4.19, "Identification of Protective Action"

Indication lights are provided for all protective actions, including identification of channel trips. The breaker status and current indication are available to the operator.

4.20, "Information Readout"

Means are provided to allow the operator to monitor trip system inputs, outputs and calculations. The specific displays that are provided for continuous display are described in Section 7.5.

4.21, "System Repair"

Identification of a defective input channel is accomplished by observation of system status lights or by testing as described in Subsection 7.2.1.1.9. Replacement or repair of components is accomplished with the affected input channel bypassed. The affected trip function then operates in its requisite two-out-of-three trip logic.

4.22, "Identification"

Equipment, including panels, modules, and cables, associated with the trip system are marked in order to facilitate identification.

A color coding scheme is used to identify the physically separated channel cabling from sensor to the RPS. The same color code is used for interbay or intercabinet identification.

Cabling or wiring within a bay at the cabinet which is in the channel of its circuit classification is not color coded. The cabinet nameplates and cabling are color coded as follows:

Protective	Associated	Non-Class 1E
Channel MA: Red	Channel J-(AMA): Red/White	All channels black
Channel MB: Yellow	Channel K-(AMB): Yellow/White	
Channel MC: Green	Channel L-(AMC): Green/White	
Channel MD: Blue	Channel M-(AMD): Blue/White	

7.2.2.3.3 Testing Criteria

Conformance to IEEE 338-1971 and Regulatory Guide 1.22 (R0) are discussed in Subsection 7.1.2.2. Test intervals and their bases are included in the Technical Specifications. A complete channel can be tested without causing a reactor trip and without affecting system operability. Overlap in the RPS channel tests is provided to assure that the entire channel is functional. The testing scheme is discussed in detail in Subsection 7.2.1.1.9.

The RPS is periodically and routinely tested to verify its operability. A complete channel can be individually tested without initiating a reactor trip, without violating the single failure criterion, and without inhibiting the operation of the system. The system can be checked from the sensor signal through the circuit breakers of the RTSS. The RPS logic can be tested during reactor operation. The sensors can be checked by comparison with similar channels or channels that involve related information. Minimum frequencies for checks, calibration, and testing of the RPS instrumentation are given in the Technical Specifications. Overlap in the checking and testing is provided to assure that the entire channel is functional. The use of individual trip and ground detection lights, in conjunction with those provided at the Class 1E instrument power supply bus, assure that all possible grounds are detected.

The periodic test of the RPS utilize the built in test circuitry. No additional test equipment or fuse removal procedures are required. The installed test equipment contains its own power supply, checks the logic and trip relays which conforms to Regulatory Guide 1.118 (R0) position C.13.

7.2.2.4 Failure Modes and Effects Analysis (FMEA)

A FMEA for the RPS is provided in Table 7.2-5. The FMEA is for protection systems' sensors, and coincidence and actuating logics. The logic interface for the protection systems is shown on Figure 7.2-21.

7.2.2.5 Effects of Other Associated Functions

7.2.2.5.1 Instrument Air

The loss of plant instrument air systems has no effect upon the safety channel sensors, Reactor Protective System or actuated devices.

7.2.2.5.2 Cooling Water

Loss of cooling water can in no way degrade the safety channel sensors, Reactor Protective System or actuated devices.

7.2.2.5.3 Plant Load Rejection

The original 45 percent steam bypass capability of the Steam Dump and Bypass System (Subsection 7.7.1.1.5) was restored as part of the Extended Power Uprate. A load rejection of greater magnitude is reflected into the Reactor Coolant System and, if severe enough, initiates a Reactor Protective System response by either a high pressurizer pressure trip (Subsection 7.2.1.1.1.5) or a low thermal margin trip (Subsection 7.2.1.1.1.4) to prevent the occurrence of an unacceptable approach to the DNB or RCPB limit.

7.2.2.5.4 Turbine Trip

A reactor trip initiation following a turbine trip (Subsection 7.2.1.1.1.10) is provided as an equipment protective feature and is not required for reactor protection.

7.2.2.5.5 Loss-of-Component Cooling Water Trip

A reactor trip following a loss of component cooling water to the reactor coolant pumps is provided but is not required for reactor protection.

7.2.2.6 Protection System Setpoint Methodology and Determination of Surveillance Procedure Acceptance Criteria

The RPS low SG level trip setpoint was changed for the extended power uprate (EPU). In accordance with References 1 and 2, this section was added to document the methodology used to determine the trip setpoint, the as-found acceptance criteria band, and the as-left acceptance criteria.

A combination of three documents is used to initially establish, and subsequently maintain compliance with, each TS setpoint value. These three documents are the instrument channel uncertainty calculation, the safety analysis plant parameters document, and the instrument channel setpoint calculation.

An instrument uncertainty calculation exists for each safety system input parameter. These calculations determine the various elements of uncertainty applicable to each component within that instrument channel from the sensor/transmitter up to the protection system cabinet input. These loop uncertainty calculations have been prepared in accordance with FPL discipline standard IC-3.17, Instrument Setpoint Methodology. IC-3.17 is in turn based on ISA Standard 67.04, Setpoints for Nuclear Safety Related Instrumentation, and Regulatory Guide (RG) 1.105, Instrument Setpoints for Safety Related Systems. Elements of uncertainty for individual components, such as setting tolerance, measuring & test equipment (M&TE) and drift are specifically based on associated surveillance procedure requirements and test frequencies. Environmental effects for both normal and harsh conditions are determined for each loop component as applicable.

The safety analysis plant parameters (SAPP) document serves as a bridge between the instrument channel setpoint calculations and the safety analysis. The bounding uncertainty allowance applicable to each protection system function is documented and managed in the SAPP. Where applicable, the SAPP includes individual bounding uncertainty allowances for both normal and harsh conditions. The rationale for managing the trip function uncertainty allowances in the SAPP is as follows:

- All inputs used for the safety analysis are managed in the SAPP. This organization facilitates the safety analysis work required for each reload.

- Including bounding trip function uncertainty allowances in one common document promotes consistent use of analytical limit values throughout the safety analysis which facilitates effective margin management.

- Including bounding trip function uncertainty allowances in the SAPP eliminates the need for documenting the analytical limits in the setpoint calculations. Therefore the purpose of the setpoint calculations is to verify that the trip function uncertainty allowances in the SAPP are bounding with respect to the calculated total channel uncertainty.

A second calculation exists for each safety system input parameter. Each of these calculations combines the loop component uncertainties with the protection system cabinet uncertainties to determine an overall total loop uncertainty (TLU). These setpoint calculations also verify that the uncertainty allowances defined in the SAPP may be left anywhere within the as-left band. This allowed setting tolerance must be treated as a bias in the setpoint determination. RIS 2006-17 further stipulates that the surveillance procedures must ensure that the trip setpoint is restored to within the as-left band before the channel is returned to service. To address this NRC guidance,

the setpoint calculations are structured to ensure that TLU plus setting tolerance (ST) is less than or equal to the SAPP allowance (TLU + ST ≤ SAPP uncertainty allowance). The ST is also included as a random / independent term in the root-sum-square TLU calculation. Protection system surveillance procedures require that trip setpoints are restored to within the as-left band before the channel is returned to service.

NRC guidance provided in RIS 2006-17 stipulates use of an as-found acceptance criteria band centered about the nominal equipment setpoint as a measure of instrument channel operability. To address this NRC guidance, the setpoint calculations are structured to include determination of an operability limit (OL) band. The OL band is synonymous with the as-found acceptance criteria band. The OL band is based on 2 times the ST and is normally centered about the nominal equipment setting. For trip functions where the ST is non-symmetrical about the nominal trip setpoint, the OL band is structured to provide equal tolerance above and below the ST limits.

NRC guidance also required the addition of two notes to TS Table 4.3-1 pertaining to the monthly functional surveillance requirement for the Low Steam Generator Level function. For the Low SG Level function, note #8 of TS Table 4.3-1 requires that if the as-found setpoint is outside of the as-found tolerance band then the channel must be declared inoperable and must be evaluated under the corrective action program (CAP). The CAP evaluation must conclude that the channel is functioning as required before returning the channel to service. For the Low SG Level function, note #9 of TS Table 4.3-1 requires that this trip setpoint be reset to a value within the as-left band before the channel is returned to OPERABLE status. In addition, Note 9 required specificity of the Field Trip Setpoint along with the as-found acceptance criteria band and the as-lefl acceptance criteria. Those values are:

- Field Trip Setpoint 35.5% (-2.420 VDC)
- Trip Setpoint As-Found Band 35.0 to 36.0% (-2.400 to -2.440 VDC) Trip Setpoint As-Left Band 35.25 to 35.75% (-2.410 to -2.430 VDC)

REFERENCES: SECTION 7.2

1) NRC Regulatory Issue Summary (RIS) 2006-17, NRC Staff Position on the Requirements of 10 CFR 50.36, "Technical Specifications," Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels

2) TSTF-493, Clarify Application of Setpoint Methodology for LSSS Functions

3) FPL Letter L-2011-346, Response to NRC Instrumentation & Controls Branch Request for Additional Information Regarding Extended Power Uprate License Amendment Request,

TABLE 7.2-1

REACTOR PROTECTIVE SYSTEM DESIGN INPUTS

	Nominal Value (Full Power)	Nominal Trip Setpoint
High Rate-of-Change of Power, dpm	0	c
High Power Level, % Full Power [a]	100	c
Thermal Margin, psia	Variable	c
Low Pressure, psia	2250	c
High Local Power Density, kw/ft	Variable	c
High Pressurizer Pressure, psia	2250	c
Low Steam Generator Water Level, %[b]	65	c
Low Steam Generator Pressure, psia	888	c
High Containment Pressure, psig	0	c
Low Reactor Coolant Flow, %	100	c
Loss of CCW to RCPs, gpm	1368	c
Steam Generator Pressure Difference, psid	0	c
Turbine Trip	Not-Tripped	c

a. Setpoint can be manually increased to a fixed increment above existing power level as power is increased and is automatically decreased as power is decreased maintaining a fixed increment. This fixed increment is 10 percent power.

b. Percent of the distance between the instrument nozzles above the lower nozzle.

c. Refer to the St Lucie Unit 2 Technical Specifications, for setpoint values.

TABLE 7.2-2

REACTOR PROTECTIVE SYSTEM BYPASSES

Title	Function	Initiated by	Removed by	Notes
Zero Power Mode bypass	Disables TM/LP Trip Disables TM/LP CWP Disables Low Reactor Coolant Flow Trip Disables ΔT Power input to High Power Level Trip	Manually	Automatically above .5% power*	Allows system tests and low temperature, and low power heatup and cooldown with shutdown CEAs withdrawn.
Low Steam Generator (SG,) Pressure trip bypass	Disables Low SG Pressure trip	Manually	Automatically if SG pressure is above 705 psig*	Allows system tests at low power and low temperature and heatup and cooldown with shutdown CEAs withdrawn.
High Local Power Density (LPD) trip bypass	Disables High LPD trip	Automatically below 15% power*	Automatically above 15% power*	Protection from this trip is not required in this power range.
High Rate-of-Change of Power trip bypass	Disables High Rate-of-Change of Power trip	Automatically above 15% power and below 10^{-4}% power*	Automatically below 15% power and above 10^{-4}% power*	This equipment protective trip is not required in this power range.
Turbine trip bypass	Disables reactor trip on turbine trip	Automatically below 15% power*	Automatically above 15% power*	Allows reactor start-up with the turbine tripped. Trip is equipment protective only.
Trip Channel bypass	Disables any given trip channel	Manually by controlled access switch	Same switch	Captive key allows only one channel for anyone type trip to be bypassed at one time.

* - Nominal values

TABLE 7.2-3

REACTOR PROTECTIVE SYSTEM SENSORS

Monitored Variable	Type	Number of Sensors	Location
Neutron flux power	Fission chambers Ion chambers	4 4	Biological shield
Cold leg temperature	Precision RTD	8	Cold leg piping
Hot leg temperature	Precision RTD	8	Hot leg piping
Pressurizer pressure	Pressure Transducers	4 [(a)]	Pressurizer
Steam generator ΔP	Differential pressure transducers	4 per steam generator	Between hot leg and steam generator output plenum
Steam generator level	Differential pressure transducers	4 per steam generator	Steam generators
Steam generator pressure	Pressure Transducers	4 per steam generator[(a)]	Steam generators
Containment pressure	Pressure Transducers	4[(a)]	Reactor Auxiliary Building
Turbine trip sensors	Pressure Switches	4	Turbine Building
Component Cooling Water Flow from RCPs	Flow Transducers	4	Reactor Auxiliary Building

(a) Common with Engineered Safety Feature Actuation System.

TABLE 7.2-4

REACTOR PROTECTIVE SYSTEM MONITORED INSTRUMENT RANGES

Cycle 1

Monitored Variable	Minimum	Nominal (Full Power)	Maximum
Neutron flux power, % full power	2×10^{-8}	100	200
Cold leg temperature, F	465	548	615
Hot leg temperature, F	515	596	665
Pressurizer Pressure psia	1,500	2,250	2,500
Steam generator Primary ΔP, psid	0	45	50
Steam generator water level [(a)] %	0	70	100
Steam generator pressure, psia	0	815	1,200
Containment pressure, psia	0	0	15
Component cooling water flow from RCPs, gpm	-	1,368	-

(a) Percent of the distance between the level instrument nozzles (above the lower nozzle).

TABLE 7.2-5

REACTOR PROTECTIVE SYSTEM

FAILURE MODES AND EFFECTS ANALYSIS

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
1.	Local Power Density	Axial off-set index for one of 4 power range safety channel fails low	The ioniza-tion chamber detector failure.	The axial offset index for the affected safety channel will be negative. This can lead to exceeding a power-dependent limit, resulting a trip of the auxiliary trip unit, and thus a channel trip.	Pre-trip alarm Periodic test	3 channel redun-dancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	a) Failure of this measure-ment channel could also affect the TM/LP and the High Power Bistables b) The operator can restore the Reactor Trip Logic 2/3 coincidence by re-storing the bypassed 4th channel operability and then bypassing the failed channel.
		Axial off-set index for one of the 4 power range safety channels fails high	The ioniza-tion chamber detector failure	The axial offset index for the affected measurement will exceed a calculated power dependant limit, resulting a trip of the associated auxiliary trip unit, and thus the effected trip channel trips.	Pre-trip alarm Periodic test	3 channel redun-dancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	
2.	High Power Level	Fails low	Maximum sel-ect circuit in ΔT power calculation network failure in low output.	Calculated reactor power, Q, will be too low. Affected trip channel will not trip even when bonafide high power level con-dition exists.	Periodic test	3 channel redund-ancy (4th chan-nel in Bypass)	Logic becomes 2/2 coincidence	a) Failure of this measure-ment channel could also affect the TM/LP and the Local Power Density Bistables. b) See Item 1, Remark b.
		Fails high	Maximum sel-ect circuit in ΔT power calculation network fails in high out-put voltage	Calculated reactor power, Q, will be too high. Affected trip chan-nel trips.	Pre-trip alarm Periodic test	3 channel redund-ancy (4th chan-nel in Bypass)	Logic becomes 1/2 coincidence	

TABLE 7.2-5(Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
3.	Loop 2A core outlet temperature (T hot) (Typical for Loop 2B)	Channel A fails low (Typical for channels B, C, and D)	Power supply failure. RTD shorted.	The averaged T hot decreases △ power decreases in TM/LPT calculation for channel A.	Periodic test Sensor test	3 channel redundancy (4th channel in Bypass)	Makes reactor trip logic for TM/LPT 2-out-of-2 coincidence.	a) Failure of this measurement channel could also affect the Local Power Density and the High Power Bistables. b) See Item 1, Remark b.
		Channel A fails high (Typical for channels B, C, and D)	RTD open	The averaged T hot increases △T power increases in TM/LPT calculation for channel A. Channel A will trip on TM/LPT.	Periodic test Sensor test Pre-trip alarm	3 channel redundancy (4th channel in Bypass) .	Makes reactor trip logic for TM/LPT 1-out-2 coincidence	
4.	Core inlet temperature Loop 2A (Typical for Loop 2B) (T cold)	Channel A fails low (Typical for channel B, C, and D)	Power supply failure RTD network failure	Low value for T cold input to TM/LP calculation for Ch. A.	Periodic test Sensor test	The maximum T cold among the 2 loops is chosen. So one loop temperature failing low does not affect the TM/LPT	Changes Setpoints	a) Failure of this measurements channel could affect the TM/LP, Local Power Density and High Power Bistables. b) See Item 1, Remark b.
		Channel A fails high (Typical for channels B, C, and D)	RTD open	Loop 2A T cold is used in △T power calculation for channel A. So △T power decreases for channel A. Whether channel A will trip or not will depend upon sensitivity of pressure setpoint as a function of T cold.	Periodic test Sensor test	3 channel redundancy (4th channel in bypass)	Reactor trip logic for TM/LPT becomes 2/2 coincidence	
5.	Pressurizer Pressure	One measurement channel fails low	Pressure transmitter failure; dc power supply failure	Low pressurizer pressure signal to the high pressurizer pressure Bistable trip unit (BTU) will not trip even when bonafide high pressurizer pressure exists.	Periodic testing Sensor check	3 channel redundancy (4th channel In Bypass)	Trip logic becomes 2-out-of 2 coincidence	a) See Item 1, Remark b. .

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
				Thermal margin/low pressure trip function (TM/LPT) will trip the affected channel.	Pre-trip alarm		TM/LPT logic becomes 1/2 coincidence.	
		One measurement channel fails high	Pressure transmitter failure, component failure	High pressurizer pressure signal to the high pressurizer pressure BTU and the thermal margin BTU. Affected channel trips.	Pre-trip alarm Periodic testing	3 channel redundancy (4th channel in Bypass)	Trip logic becomes 1-out-of 2 for TM/LP and Hi Pressurizer Pressure Trips	
6.	Core Flow Summer	Fails low	Power supply failure; grounded output.	Flow bistable trip unit will trip the affected channel.	Flow bistable trip unit trip alarm & pre-trip alarm Periodic test	3 channel redundancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	a) See Item 1, Remark b.
		Fails High	Sensor failure; component saturated output	Flow bistable trip unit will not trip for bonafide low flow condition.	Periodic test	3 channel redundancy (4th channel in Bypass)	Logic becomes 2/2 coincidence	
7	Loss of Load Trip Input	Fails off	Failure of auxiliary trip unit. Turbine auto-stop oil pressure switch fails closed.	Affected channel will not trip even if bonafide loss of load condition exists.	Periodic test	3 redundant channels (4th channel in Bypass)	Logic becomes 2/2 coincident	a) See Item 1, Remark b.
		Fails on	Pressure switch fails open	Auxiliary trip unit trips	Pre-trip alarm	3 redundant channels (4th in Bypass)	Logic becomes 1/2 coincident	
8.	Steam Generator Level No. 1 (Typical For No. 2)	Fails low Channel A (Typical for Channels B, C, & D)	Transmitter failure DC power supply failure.	Channel A trips on low S.G. level	Pre-trip alarm	3 channel Redundancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	a) See Item 1, Remark b.

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		Fails high channel A	Transmitter failure, component failure	The lower of the 2 S.G. levels is chosen for each channel. If the failure affects the S.G. with the lower level, the channel will not trip.	Periodic test	3 channel redundancy (4th channel in Bypass).	Logic become 2/2 coincidence	
9.	Steam generator pressure (SG 1) (Channel A Typical)	a) Channel fails low	Transmitter failure, DC power supply failure or high line resistance	A low pressure signal from SG 1 is input to the steam generator low pressure trip bistable and the asymmetric steam generator trip portion of the TM/LP calculator. If pressure signal is low enough, one SG low pressure bistable will trip. TM/LP calculator might sense an SG 1 Pres. <SG 2 Pres. condition and initiate one bistable trip on an asymmetric steam generator transient condition.	Pre-trip alarm on either "Low SG Pressure" or "Asymmetric Steam Generator Transient". Periodic testing otherwise.	3 channel redundancy (4th channel Bypass)	Logic become 1-out-of-2 coincident for "Low Steam Generator Pressure" and/or "Asymmetric Generator Trip".	See Item 1, Remark b
		b) Channel fails high	Transmitter failure, component failure	A high pressure signal from SG I is input to the steam generator low trip bistable and the asymmetric steam generator trip portion of the TM/LP calculator. For the low steam generator trip, the lower of the two steam generator pressures is chosen. If the failure affects the steam generator with the lower pressure, the channel will not respond properly. The TM/LP calculator will sense SG 2 Press. <SG 1 Press. and trip one bistable on an asymmetric steam generator transient condition.	If Annunciating TM/LP calculator initiates a channel trip, otherwise periodic testing.	3 channel redundancy (4th channel in Bypass)	SG low pressure logic is 2-out-of 2 for transients affecting SG 1 and 2-out-of-three for transient affecting SC 2. Asymmetric steam generator pressure trip logic becomes 1-out-of-2	
		c) Signal fails as is or at a point trip setting.	Sensor malfunction transmitter malfunction.	Pressure changes in SG I will not be input to the RPS. For transients affecting SG 1, the low pressure trip bistable and the TM/LP "Asymmetric Steam Generator Pressure" bistable will not trip. For transients involving SG 2, both bistables	Periodic test. Also detectable due to a spurious "Asymmetric Steam Generator Press." Trip on a	3 channel redundancy (4th channel in Bypass)	Low steam generator pressure and asymmetric steam generator pressure trip logics become 2-out-of-2 for transients affecting SG 1.	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
				will respond properly. For transients involving both steam generators, the "Low Steam Generator Pressure" bistable will trip properly and the "Asymmetric Steam Generator Pressure" bistable will trip spuriously on SG 2 Press.< SG 1 Press.	Transient affecting both steam generators			
10	Steam generator pressure (SG 2), (Channel A Typical)	This item is equivalent to line item 9 a), b), c) for steam generator 2 instead of steam generator 1.						
11.	Containment Pressure	Fails High	Transmitter Failure Component Failure	Affected channel will not respond to bonafide high containment pressure condition	Periodic test Sensor test	3 channel redundancy (4th channel in Bypass	Logic becomes 2/2 coincidence	a) See Item 1, Remark b b) Transmitter is reverse acting
		Fails Low	Transmitter failure	Affected channel trips	Pre-trip alarm	3 channel redundancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	
12.	CCW Flow to RCP signal	Fails high	Transmitter failure	Affected channel will not respond to a decrease in CCW flow to RCPs	Periodic test	3 channel redundancy (4th channel in Bypass)	Logic becomes 2/2 coincidence	a) See Item 1, Remark b
		Fails low	Transmitter failure, sensor failure, power supply failure	Spurious indication of low CCW flow to RCPs	Annunciating	3 channel redundancy (4th channel in Bypass)	Logic becomes 1/2 coincidence	
13	Log Flux Monitor	One channel output fails high	Transmitter failure, noise	The high signal level will cause one High Rate-of-Change of Power Bistable to trip	Annunciating	3 channel Redundancy (4th channel in Bypass)	Trip logic for High Rate-of-Change of Power becomes 1/2 coincidence	See Item 1, Remark b

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		One channel output fails low	Transmitter failure, DC Power supply fault	The High Rate-of-Change of Power Bistable associated with the failed measurement channel will not trip on an actual high rate of change of power	Periodic Testing	3 channel redundancy (4th channel in Bypass)	Trip logic for High Rate-of-Change of Power becomes 2/2 coincidence	
		One channel output fails open	Open circuit	The affected High Rate-of-Change of power bistable will trip	Annunciating	3 channel redundancy (4th channel in Bypass)	Trip logic for High Rate of Change of power becomes 1/2 coincidence	
14	Linear Flux Monitor	One channel output fails high	Transmitter failure, electronic noise	High Flux Input to Core Protection Calculator (CPC). This will cause one Local Power Density Bistable and possibly one High Power Bistable to trip. TM/LP calculation will also be affected.	Annunciating	3 channel redundancy (4th channel in Bypass)	RPS trip logic for Local Power Density and High Power becomes 1/2 coincidence	a) See Item 1, Remark b
		One channel output fails low	Transmitter fault, D.C. Power supply fault	Linear flux input to one CPC will be low, the associated Local Power Density Bistable will not trip on a high flux condition. The TM/LP and High Power Bistables will also be affected.	Periodic Test	3 channel redundancy (4th channel in Bypass)	RPS Trip Logic for Local Power Density becomes 2/2 coincidence	
		Loss of output from one channel	Open circuit	Flux input to CPC lost, Local Density Bistable will trip High Power and TM/LP Bistables also affected.	Annunciating	3 channel redundancy (4th channel bypass)	RPS trip logic for large power density becomes 1/2 coincidence	
15.	High rate of change of Power Bistable Trip Unit (Channel A Typical)	Output fails low	Open circuit, component failure	Bistable Trip Unit relays are deenergized. Contacts in the "A" leg of the logic matrices AB, AC, and AD open. The AB, AC and AD logic matrices are in the half trip state.	Pre-trip alarms	3 channel redundancy (4th channel in Bypass)	RPS Trip Log for high rate of change of power becomes 1/2 coincidence	See Item 1, Remark b.
		Output fails high	Short circuit, set-point comparator failure, component failure	Bistable Trip unit relays will not be deenergized when a valid high rate of change of power condition occurs	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for high rate of change of power becomes 2/2	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
16.	Local power density bistable trip unit (Channel A Typical)	Output fails low	Power supply failure, open circuit, component failure	Bistable trip unit relays will be deenergized and their contacts in the trip logic matrices will open. Trip logic matrices AB, AC, and AD will be in a half-trip state.	Annunciating	3 channel redundancy (4th channel in Bypass)	Trip logic for high local power density becomes 1/2 coincidence. Trip logic for other parameters unaffected.	See Item 1, Remark b
		Output fails high	Short circuit, component failure	Bistable trip unit relays will not be deenergized on a valid high local power density	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for high local power density becomes 2/2 coincidence Trip logic for other parameters unaffected.	
17.	High Power bistable trip unit (Channel A Typical)	Output low	Open circuit, power supply failure, component failure	Bistable trip unit relays are deenergized and their contacts in the trip logic matrices AB, AC, and AD are in half-trip state	Annunciating	3 channel redundancy (4th channel in Bypass)	Trip logic for High Power becomes 1/2 coincidence. Other parameters unaffected	See Item 1, Remark b
		Output high	Short circuit, variable setpoint comparator failure.	Bistable trip unit relays will not deenergize for a valid overpower condition	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for High Power becomes 2/2 coincidence. other parameters unaffected	
18.	Thermal Margin/ Low Pressure Bistable Trip unit (Channel A Typical)	a) Output fails low	Open circuit power supply failure component failure	Bistable trip unit relays will be deenergized, and their contacts in the trip logic matrices will open. Trip logic matrices AB, AC, and AD will be in the half-trip state.	Annunciating	3 channel redundancy (4th channel in Bypass)	Trip logic for thermal margin/ low pressure and asymmetric steam generator pressure will become 1/2 coincidence. Other parameters unaffected.	See Item 1, Remark b

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		b) Output fails high	Short circuit, setpoint comparator failure	Bistable trip unit relays will not deenergize for a valid TM/LP condition	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for thermal margin low pressure and asymmetric steam generator pressure will become 2/2 coincidence. Other parameters unaffected.	
19.	Pressurizer bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	See Item 17	See Item 17	See Item 17	Trip logic for high pressurizer pressure becomes 1/2 coincidence Other parameters unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit, setpoint comparator failure	Bistable trip unit relays will not deenergize on a valid high pressurizer pressure condition	Periodic test	3 channel redundancy (4th channel bypass)	Trip logic for high pressurizer 2/2 coincidence. Other parameters are unaffected.	
20.	Low reactor coolant flow bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	See Item 17	See Item 17	See Item 17	Trip logic for low reactor coolant flow becomes 1/2 coincidence. Other parameters are unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit setpoint comparator failure	Bistable trip unit will not deenergize for a valid low reactor coolant flow condition	Periodic test coolant	3 channel redundancy (4th channel in bypass)	Trip logic for low reactor coolant flow becomes 2/2 coincidence. Other parameters are unaffected.	
21.	Loss of load Bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	Same as Item 17	Same as Item 17	Same as Item 17	Trip logic for loss of load becomes 1/2 coincidence. Other parameters are unaffected.	See Item 1, Remark b.

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		Output fails high	Short circuit	Bistable trip unit relays will not deenergize on a valid loss of load	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for loss of load becomes 2/2 coincidence. Other trip parameters are unaffected.	
22.	Low steam generator water level Bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure	Same as Item 17	Same as Item 17	Same as Item 17	Trip logic for low steam generator level becomes 1/2 incidence. Other parameters are unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit, setpoint comparator failure	Bistable trip unit relays will not deenergize on a valid low steam generator level	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for steam generator level become 2/2 coincidence. Other parameters are unaffected.	
23.	Low steam generator steam pressure bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	Same as Item 17	Same as Item 17	Same as Item 17	Trip logic for low steam generator steam pressure becomes 1/2 coincidence. Other parameters are unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit, setpoint comparator failure	Bistable trip unit relays will not deenergize on a valid low steam generator pressure condition	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic low steam generator steam pressure becomes 2/2 coincidence. Other parameters are unaffected.	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
24.	High containment pressure bistable trip unit (Channel A Typical)	Output fails low	Open circuit, component failure, power supply failure	Same as 17	Same as 17	Same as 17	Trip logic for high contain-pressure becomes 1/2 coincidence. Other parameters are unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit, setpoint comparator failure	Bistable trip relays will not deenergize for a valid high containment pressure condition	Periodic test	3 channel redundancy (4th channel in Bypass)	Trip logic for high containment pressure becomes 2/2 coincidence. Other parameters unaffected.	
25.	Loss of RCP CCW low Bistable trip unit (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	Same as 17	Same as 17	Same as 17	Trip logic for loss of RCP flow becomes coincidence. Other parameters unaffected.	See Item 1, Remark b.
		Output fails high	Short circuit,	Bistable trip unit relays will not deenergize on loss of CCW flow to the RCPs	Periodic test	3 channel redundancy	Trip logic for loss of RCP CCW flow becomes 2/2 coincidence Other parameters are unaffected.	
26.	Loss of RCP CCW flow trip timer (Channel A Typical)	Output fails low	Open circuit, power supply failure, component failure	Equivalent to 17	Equivalent to 17	Equivalent to 17	Same as 24	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		Output fails high	Short circuit, component failure	Same as 24	Same as 24	Same as 24	Same as 24	
		Time delay changes	Component degradation	When loss of RCP CGW flow bistable trips, contacts in the logic matrices will open either earlier or later than the contacts for the other two channels (dependent on which direction time delay changes)	Periodic test	3 channel redundancy (4th channel in Bypass)	No impact on trip logic	
27.	Logic Matrix (AB Typical) (See Figure 7.2-7)	Fails OFF	Concurrent opening of 2 parallel paths	Reactor Trip	Annunciating	N/A	Reactor Trip	There is no single component failure within the logic matrix that can cause this failure
		Fails ON	Failure of 1 of 2 parallel paths to open on signal - contact short, short circuit	The logic matrix will not deenergize the logic matrix relays and hence not trip the reactor on a coincidence of trip signals in the A and B channels for a given trip parameter	Periodic	There are five other logic matrices which can initiate a reactor trip on a coincidence of 2 trip signals for a given trip parameter (i.e., AC, BC, BD, CD, AD)	The Reactor Trip Logic becomes 2-out-of-4 selective, with the AB combination not effective for a given parameter.	
28.	Logic Matrix Relay -AB1 (Typical of 24) (See Figure 7.2-7)	Fails Energized	Short to power, contact weld	When the AB logic matrix deenergizes, the AB contact in Trip Path 1 will not open.	Periodic Test	The contacts for the other 3 AB logic matrix relays in the other three Trip Paths will open and trip the reactor. In addition, Trip Path 1 can be deenergized by	No significant effect	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
						the No. 1 logic matrix relay from any one of the other 5 logic matrices.		
		Fails Deenergized	Open circuit, Power Supply Failure	The AB contact in Trip Path 1 will open, the Trip Path will deenergize, and two reactor trip circuit breakers will open	Annunciating	None Required	One of two parallel paths providing power to the CEDM buses is open, Reactor is in a half trip state, The trip path logic changes from 2/4 selective to 1/3 selective.	
29.	Trip Path 1 (Typical of 4) (See Figure 7.2-7)	a) One Trip Path Contact Fails open	Mechanical failure, open circuit	The Trip Path relay (K1) is deenergized and two reactor trip circuit breakers are open.	Annunciating	None Required	Reactor is in a half-trip state. Trip Path Logic changes from 2/4 selective to 1/3 selective.	
		b) One Trip Path Contact fails closed	Contact weld, short circuit	Deenergization of one of six logic matrices will not deenergize the Trip Path 1 circuit breaker control relay (K1)	Periodic Test	Trip Paths 2, 3 & 4 not affected and can trip reactor, plus deenergization of any one of the five other logic matrices will deenergize Trip Path one	No significant effect	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
		c) Trip circuit breaker control relay (K1) fails open	Open winding, Power supply failure	Same as 28a)	Annunciating	None Required	Same as 28a)	
		d) Trip circuit breaker control relay (K1) fails energized	Short to power, contact weld	Trip Path 1 cannot be deenergized by a valid signal coincidence. Two of eight circuit breakers will not open.	Periodic Test	Trip Paths 2,3 and 4 are not affected and can trip reactor	Trip Path Logic becomes 2/3 selective in-stead of 2/4 selective.	
30.	Trip Circuit Breaker I (Typi-cal of 8)	a) Fails open	Failure of under voltage relay coil, open circuit Mechanical failure	One of two parallel paths supplying power to one half of the Control Element Drive Mechanisms (CEDM) will be interrupted.	Annunciating plus zero reading from current indicator in circuit.	Parallel redun-dant path to supply power to the CEDMS	RPS Trip Logic not affected.	
		b) Fails closed	Contact weld, Mechanical binding, Short to power, under voltage coil shorted.	One of two series redundant breakers in one of two parallel redundant paths to supply power to the CEDMS will not open on a trip signal.	Periodic Test	The series redun-dant breaker can interrupt power on the affected path.	RPS Trip Logic not affected.	

TABLE 7.2-5 (Cont'd)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon RPS	Remarks and Other Effects
31.	Power Operated Relief Valve Actuation Logic Matrices	a) One fails off	Failure in two parallel paths which cause open circuits	Spurious opening of the power operated relief valve	Annunciating	N/A	No effect on RPS Trip Logic will result in RCS Depressuriza-tion, and Loss of RCS inventory	There is no single component failure within a logic matrix that can produce this fault.
		b) One fails on	Short circuit in one of two parallel paths, contact short	The affected Logic Matrix will not produce a Power Operated Relief Valve (PORV) Actuation Signal when the pressurizer pressure reaches the pretrip setpoint	Periodic Test	Three redundant Logic Matrices for actuation of the PORV. (One of four pressu-rizer pressure channels assumed to be bypassed, hence only three of six Logic Matrices	The RPS Trip Logic unaffected. The actuation logic for the PORVs becomes 2-out-of 3 selective.	
32.	Control Rod With-drawal Prohibit Logic Matrix	a) Fails off	Concurrent failure in two parallel paths which result in a open circuit in both paths	Spurious actuation of the Control Rod Withdrawal Prohibit.	Annunciating	N/A	No effect on RPS Trip Logic, but control rods cannot be with-drawn.	There is no single component failure that can cause a Logic Matrix to fall off.
	(Matrix AB Typi-cal of 6)	b) Fails on	Short circuit or shorted contact in one of the two parallel paths in the Logic Matrix	A Control Rod Withdrawal (CWP) actuation signal will not be generated by the affected Logic Matrix when a valid condition exists.	Periodic Tests	The three Logic Matrices are each capable of initiating a CWP actuation signal (Note: one channel, i.e., Ch. D, is assumed to be bypassed, hence only 3 of 6 Logic matrices are active.	RPS Trip Logic not affected. CWP actuation logic becomes 2/4 selective.	See Item 1, Remark b.

Refer to Drawing
2998-B-327
Sh. 372, 373, 374, 375

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

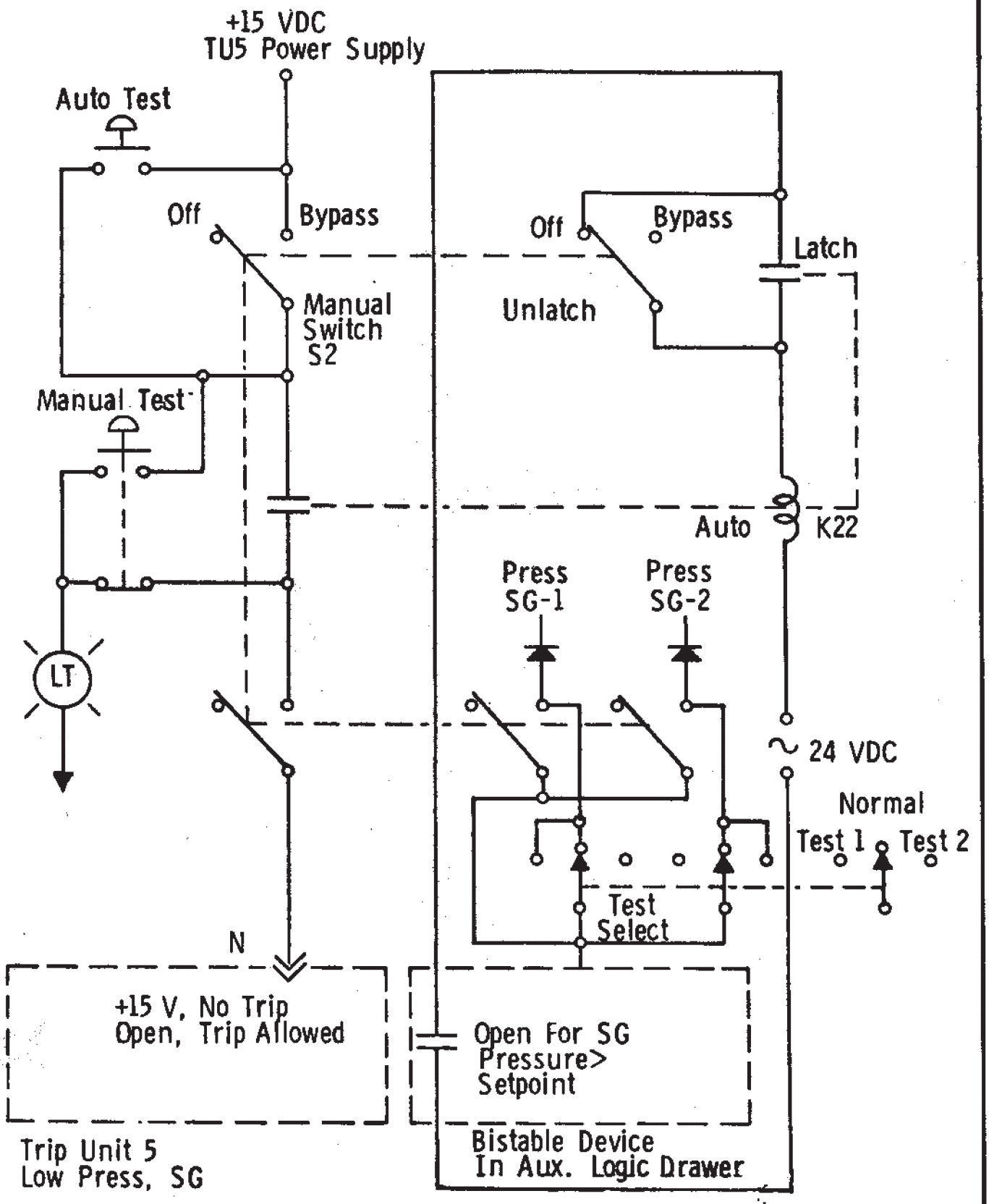
CONTROL WIRING DIAGRAM
PRESSURIZER PRESSURE
MEASUREMENT LOOP
FIGURE 7.2-1

Refer to Drawing
2998-15345

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

NEUTRON FLUX MONITORING
SYSTEM SAFETY CHANNEL

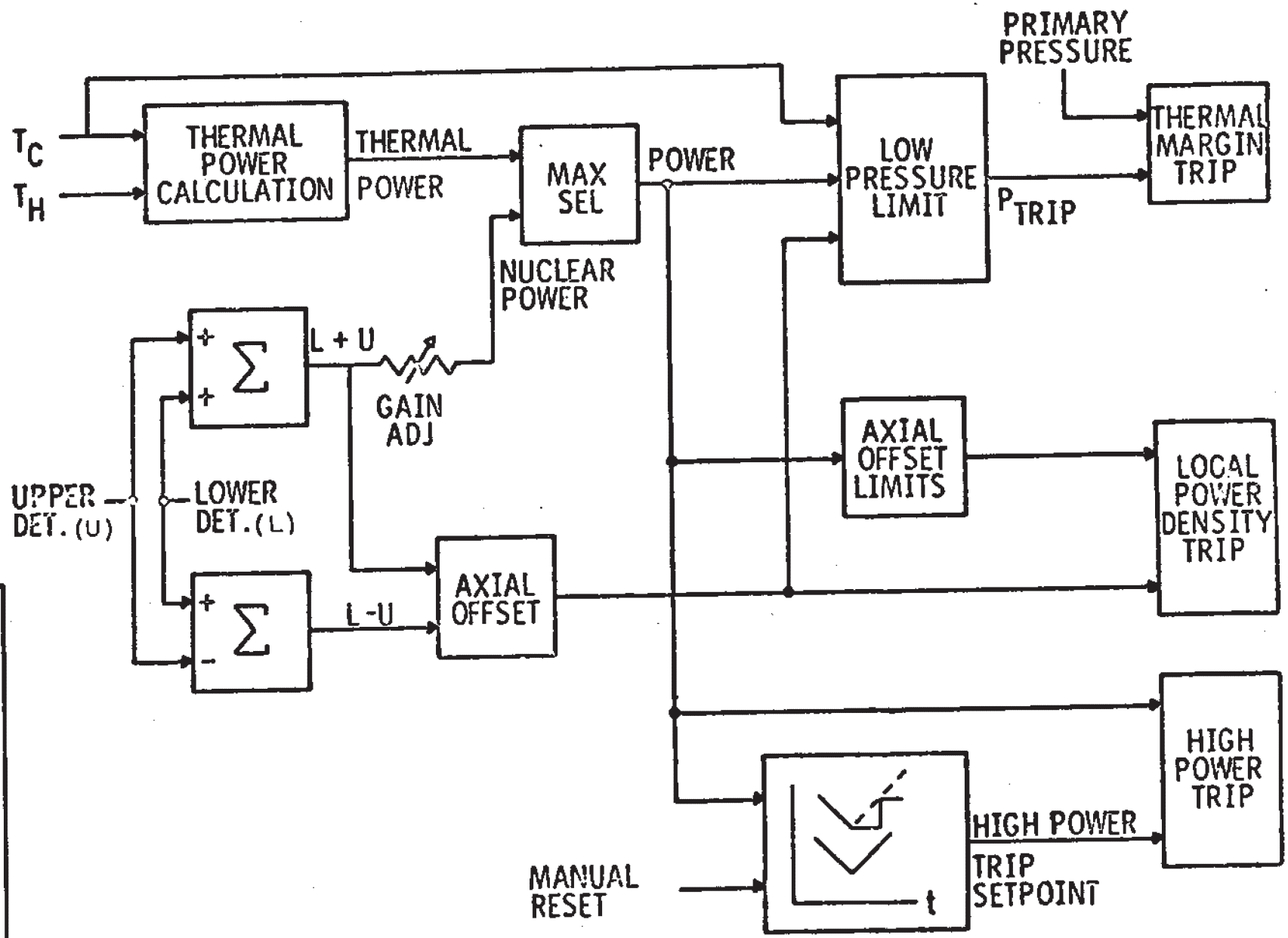
FIGURE 7.2-2



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

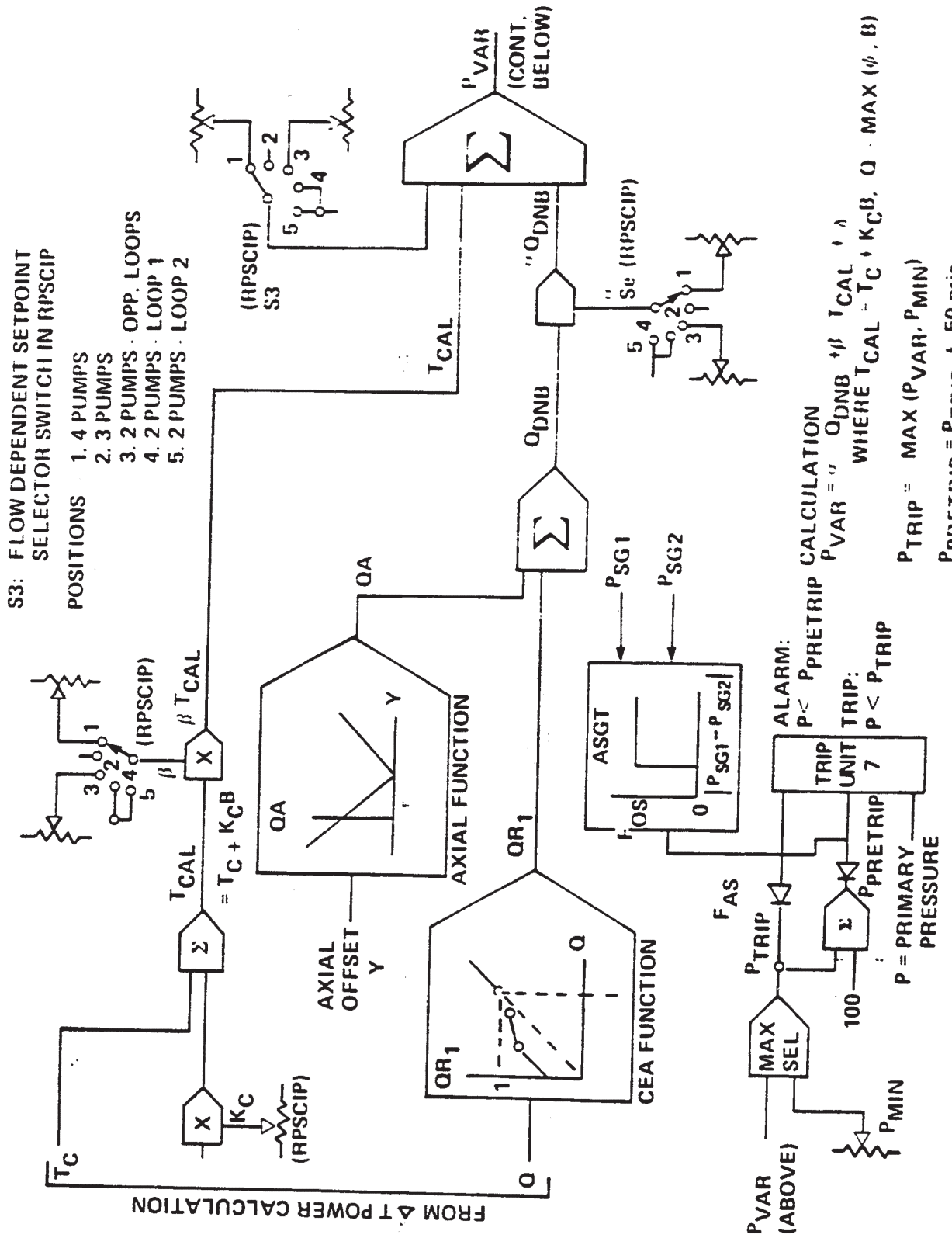
LOW STEAM GENERATOR PRESSURE
REACTOR TRIP BYPASS FUNCTIONAL
DIAGRAM

FIGURE 7.2-3



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

CORE PROTECTION TRIPS
BLOCK DIAGRAM
FIGURE 7.2-4



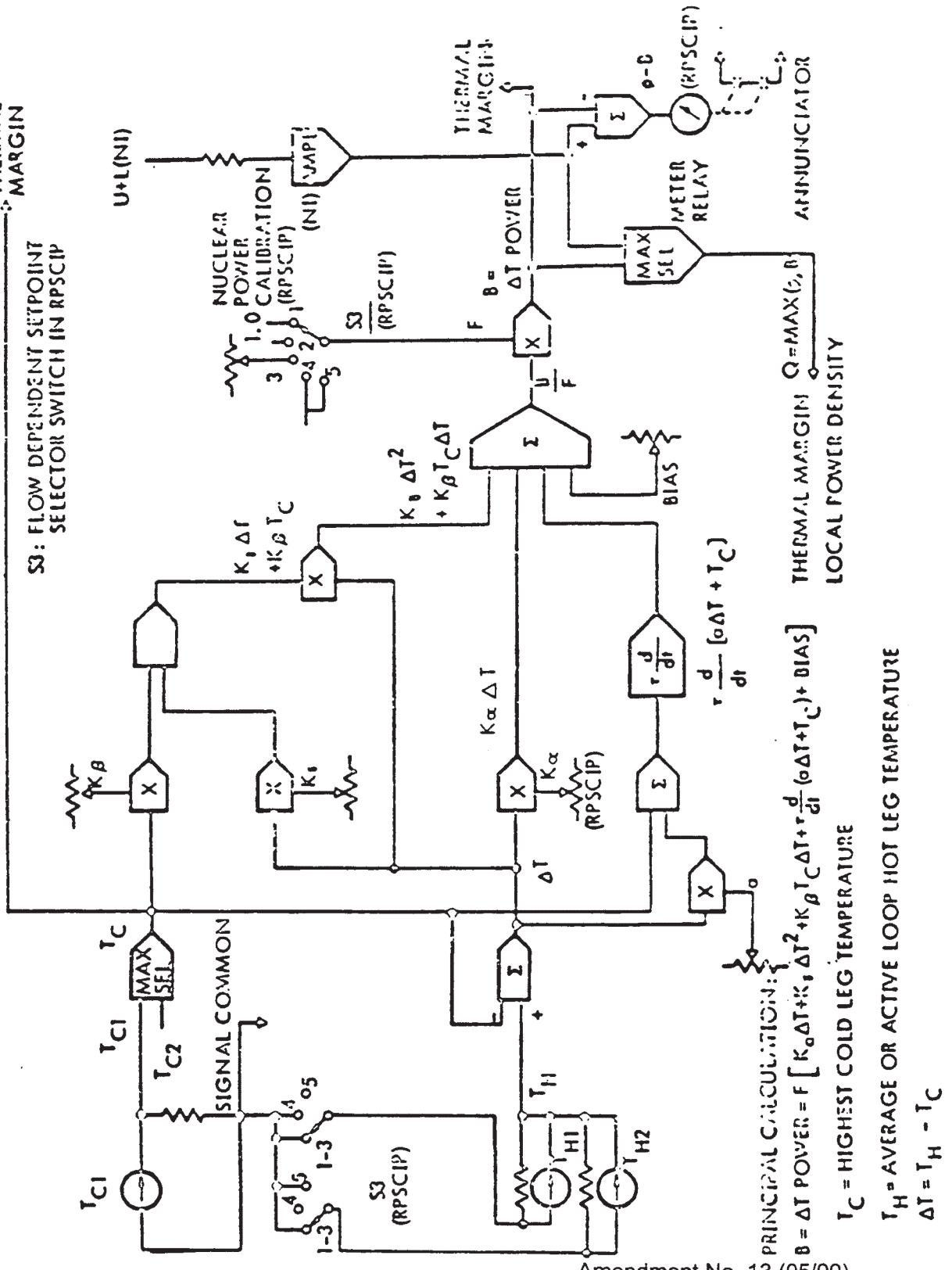
Amendment No. 13 (05/00)

Note:
At power operation with less than four (4) Reactor Coolant Pumps is not allowed by plant Technical Specifications, and the Flow Dependent Setpoint Selector Switch has been hardwired in the 4-Pump position.

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

THERMAL MARGIN TRIP

FIGURE 7.2-5



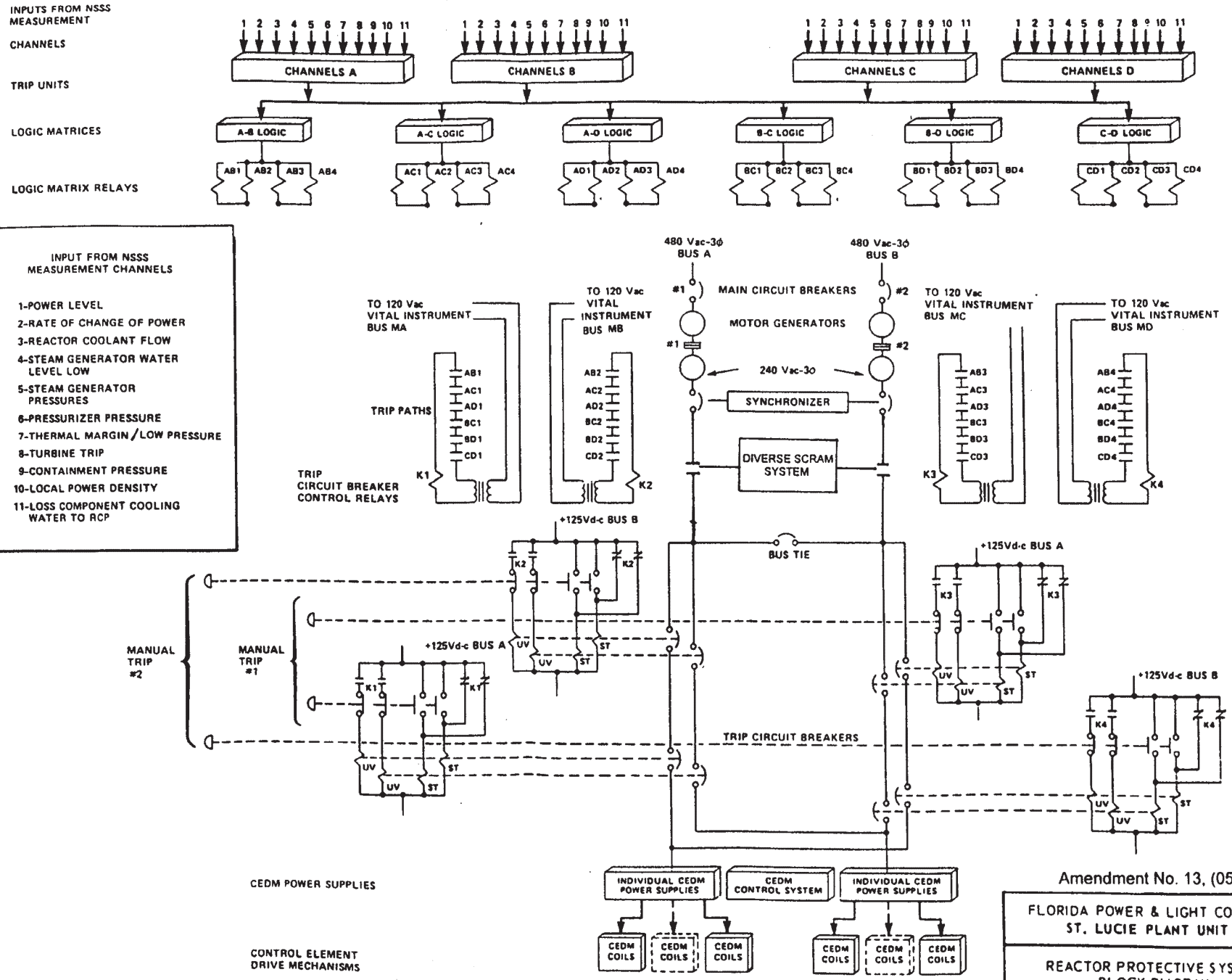
Amendment No. 13 (05/00)

Note:
At power operation with less than four (4) Reactor Coolant Pumps is not allowed by plant Technical Specifications, and the Flow Dependent Setpoint Selector Switch has been hardwired in the 4-Pump position.

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ΔT POWER CALCULATION

FIGURE 7.2-6



Amendment No. 13, (05/00)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

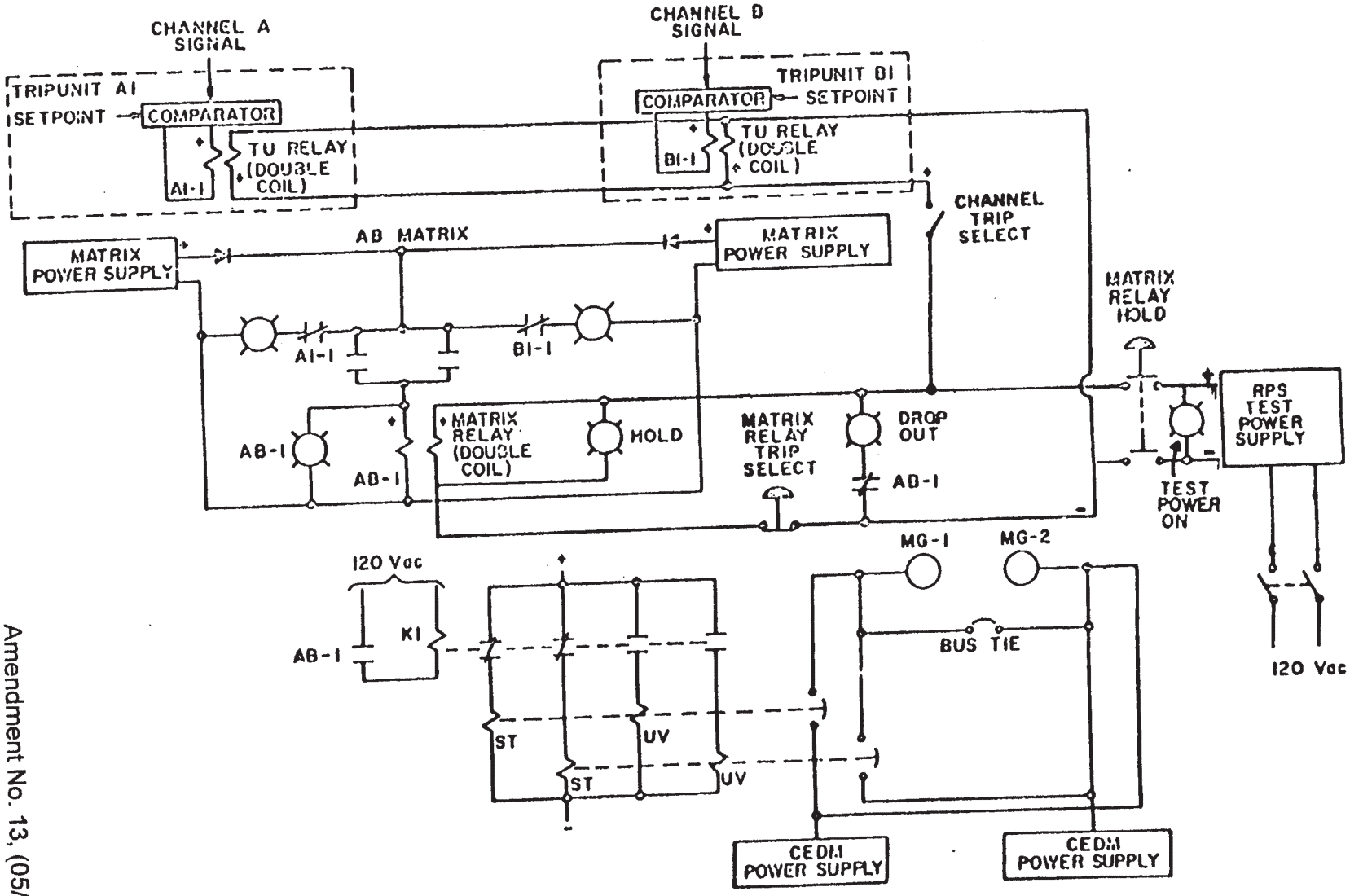
REACTOR PROTECTIVE SYSTEM
BLOCK DIAGRAM
FIGURE 7.2-7

Refer to Drawing
2998-4991

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

RPS FUNCTIONAL DIAGRAM

FIGURE 7.2-8

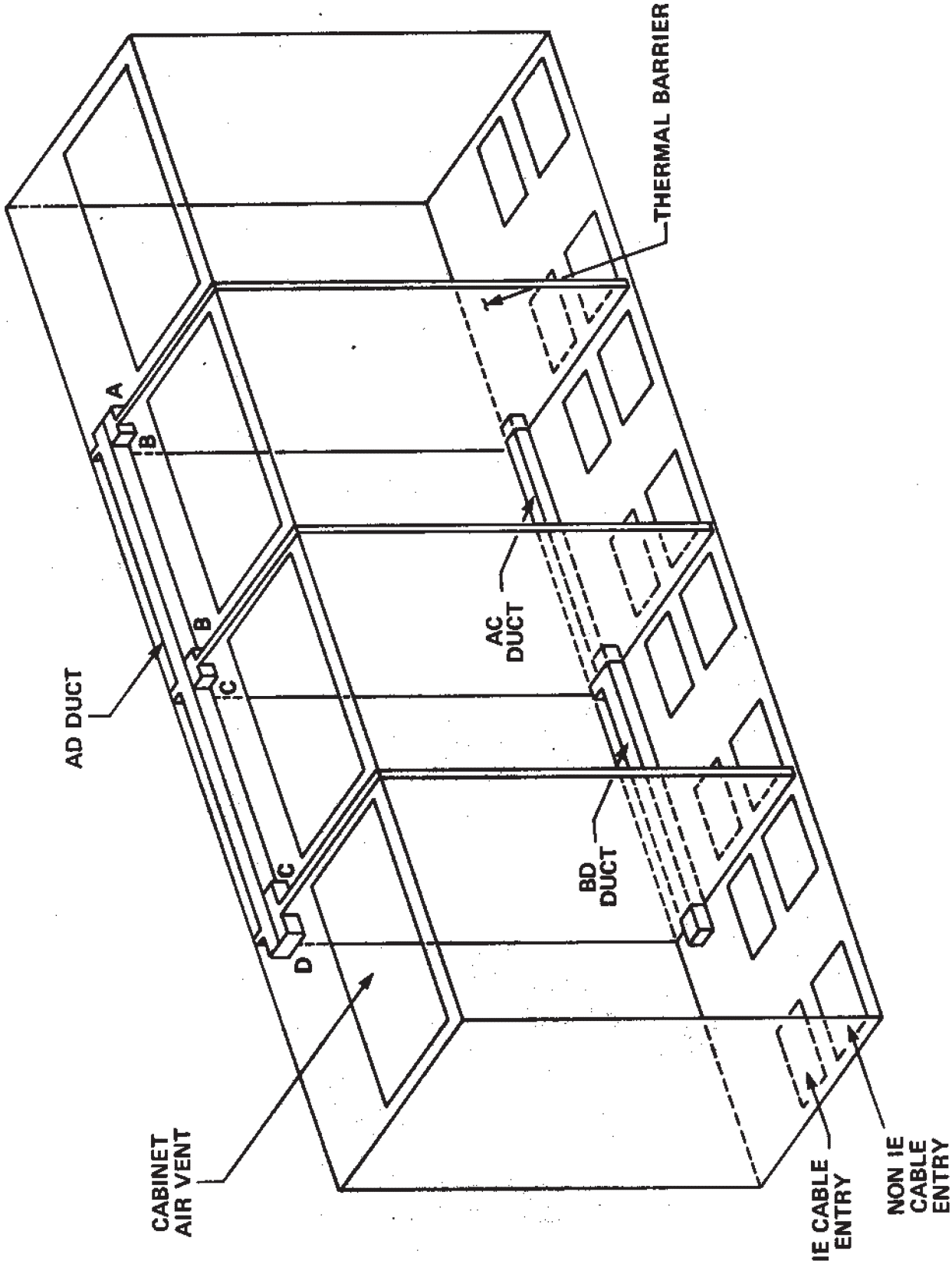


FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BASIC RPS TESTING SYSTEM

FIGURE 7.2-9

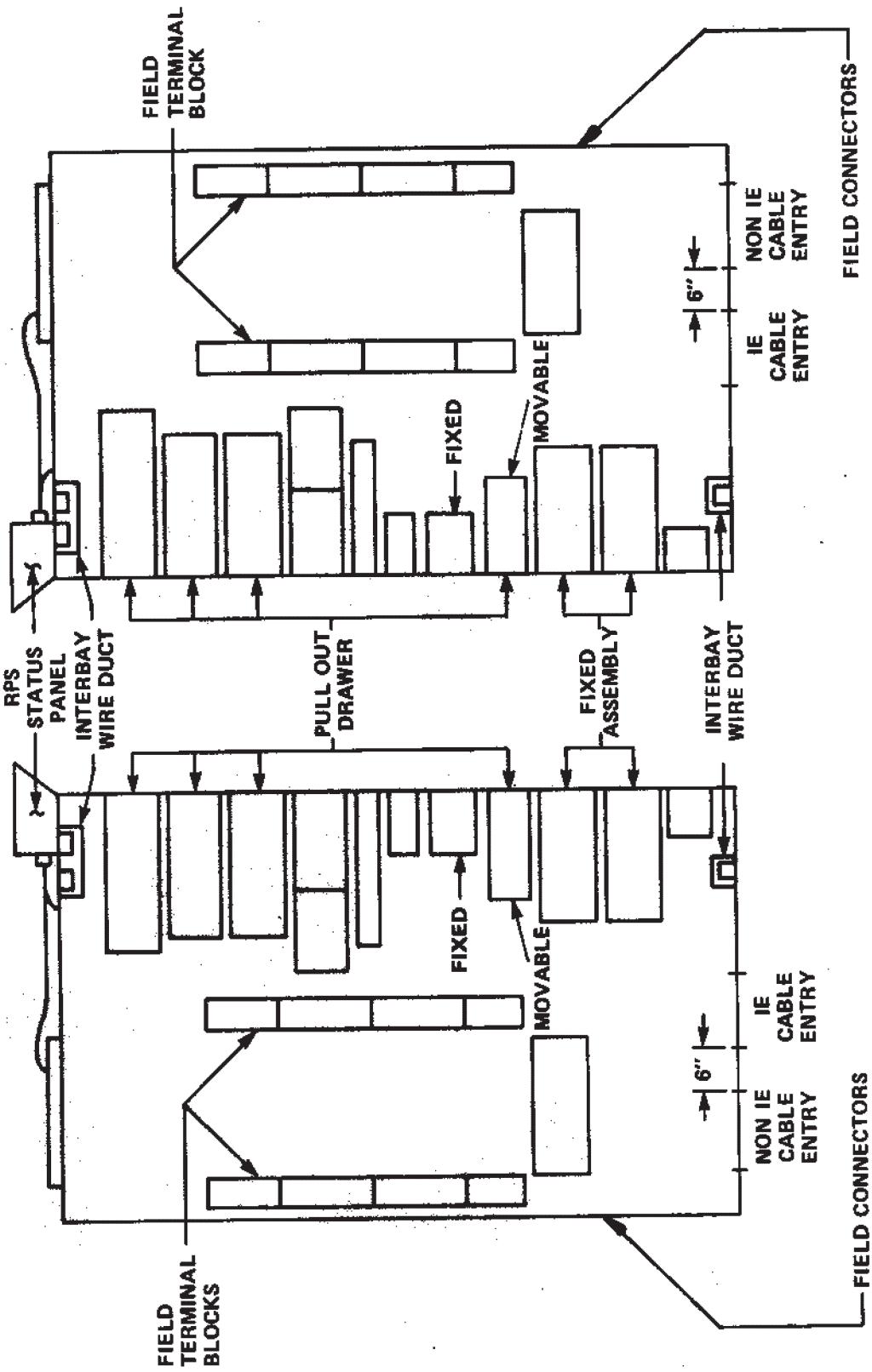
Amendment No. 13, (05/00)



AMENDMENT NO. 0 (12/80)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

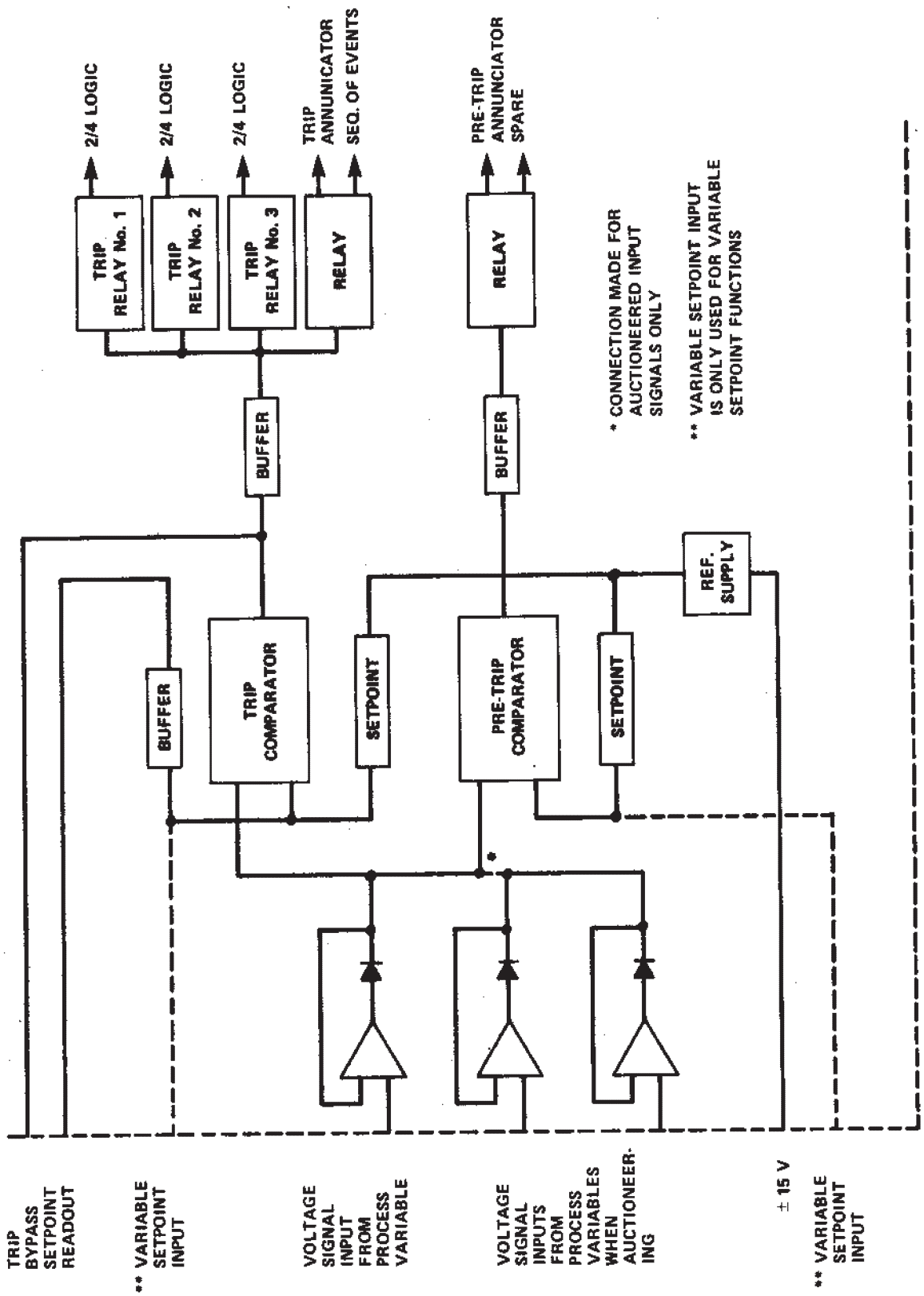
SIMPLIFIED RPS CABINET LAYOUT
(REAR VIEW)
FIGURE 7.2–10



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

TYPICAL RPS BAY LAYOUT

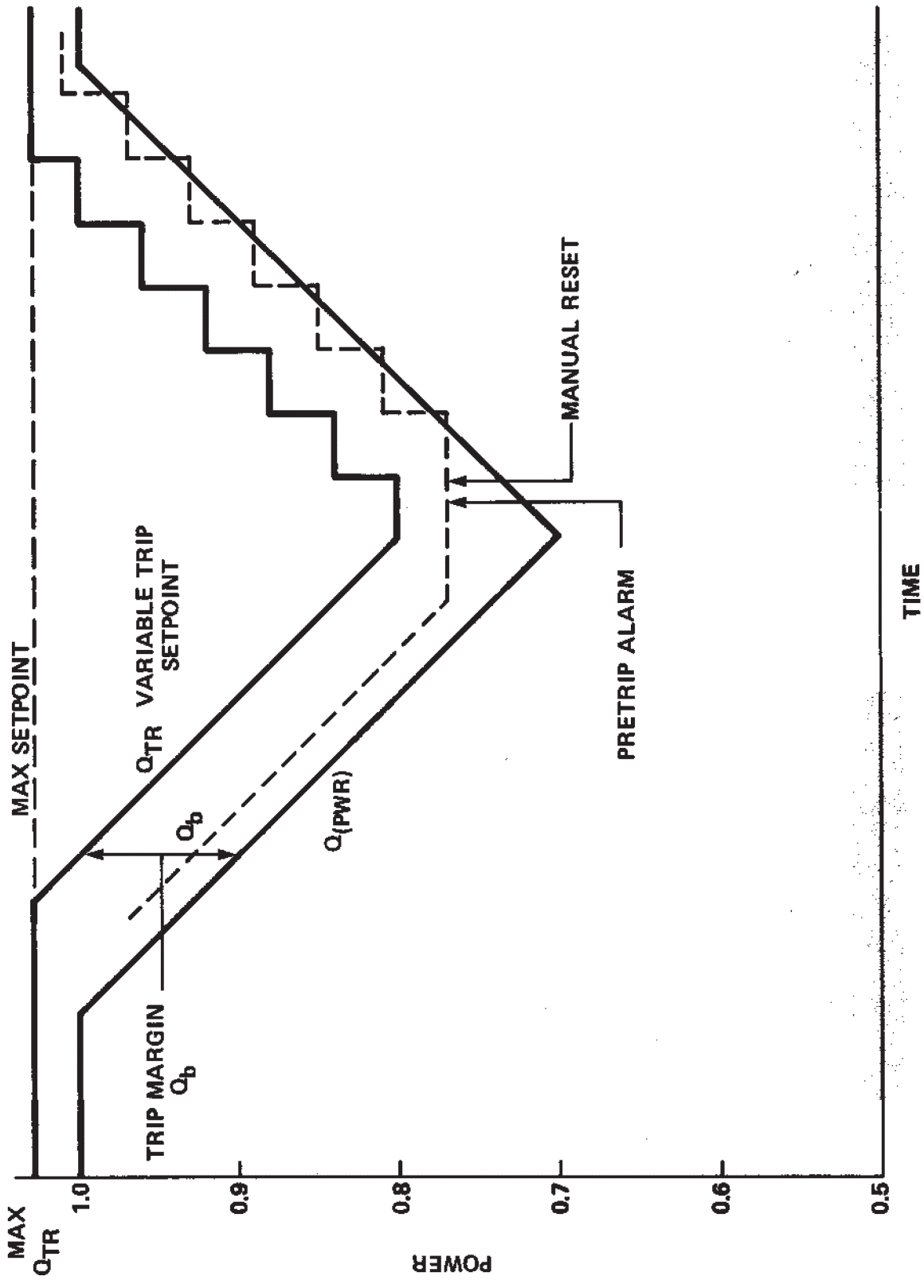
FIGURE 7.2–11



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BISTABLE BLOCK DIAGRAM

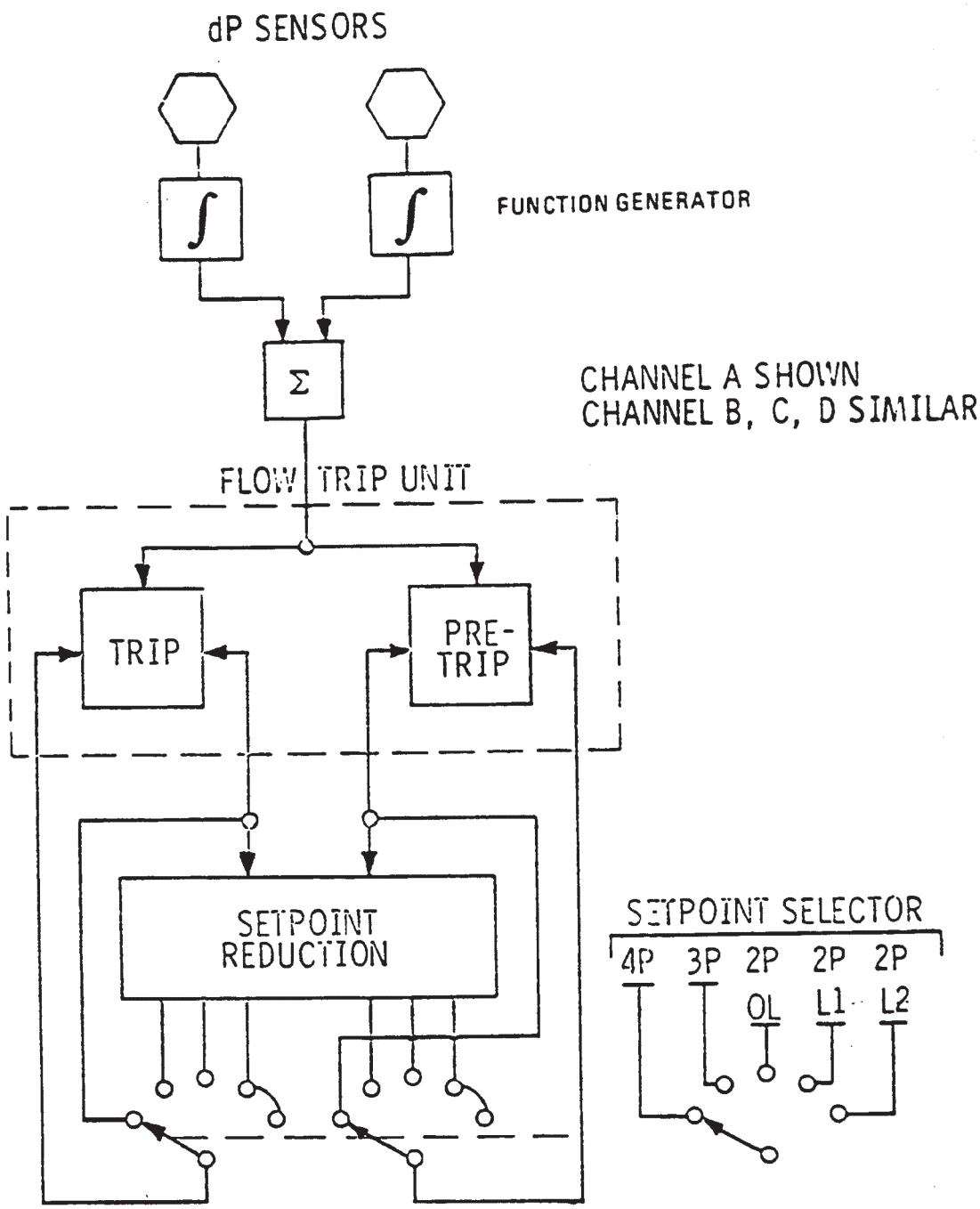
FIGURE 7.2–12



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

VARIABLE HIGH-POWER TRIP OPERATION (TYPICAL)

FIGURE 7.2-13



Amendment No. 13 (05/00)

Note:
At power operation with less than four (4) Reactor Coolant Pumps is not allowed by plant Technical Specifications, and the Flow Dependent Setpoint Selector Switch has been hardwired in the 4-Pump position.

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

LOW FLOW PROTECTIVE SYSTEM
FUNCTIONAL DIAGRAM
FIGURE 7.2-14

Refer to Drawing
2998-8342

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

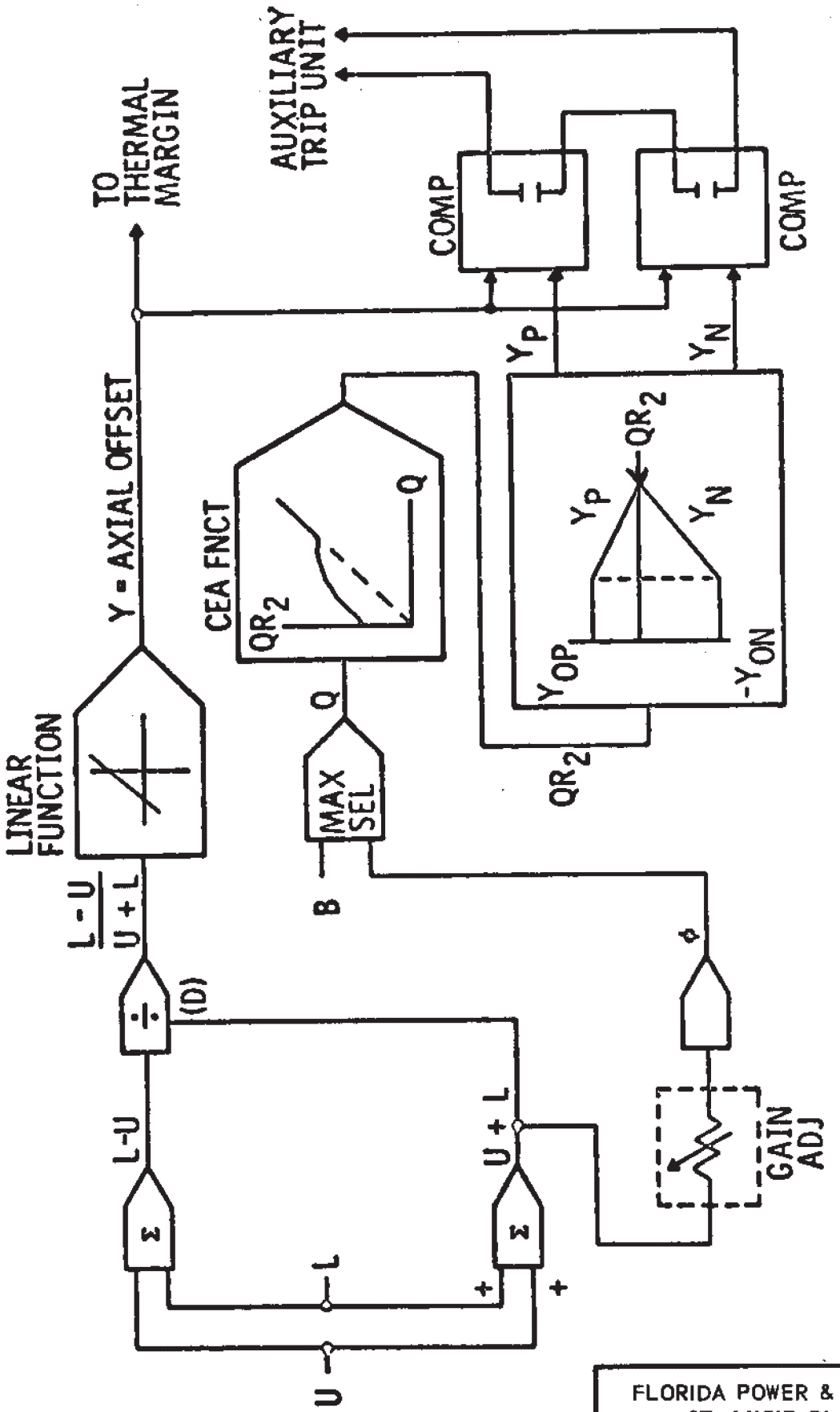
STEAM GENERATOR 'A'
PROTECTIVE CHANNEL BLOCK
DIAGRAM
FIGURE 7.2-15a

Amendment No. 18 (01/08)

Refer to Drawing
2998-8341

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

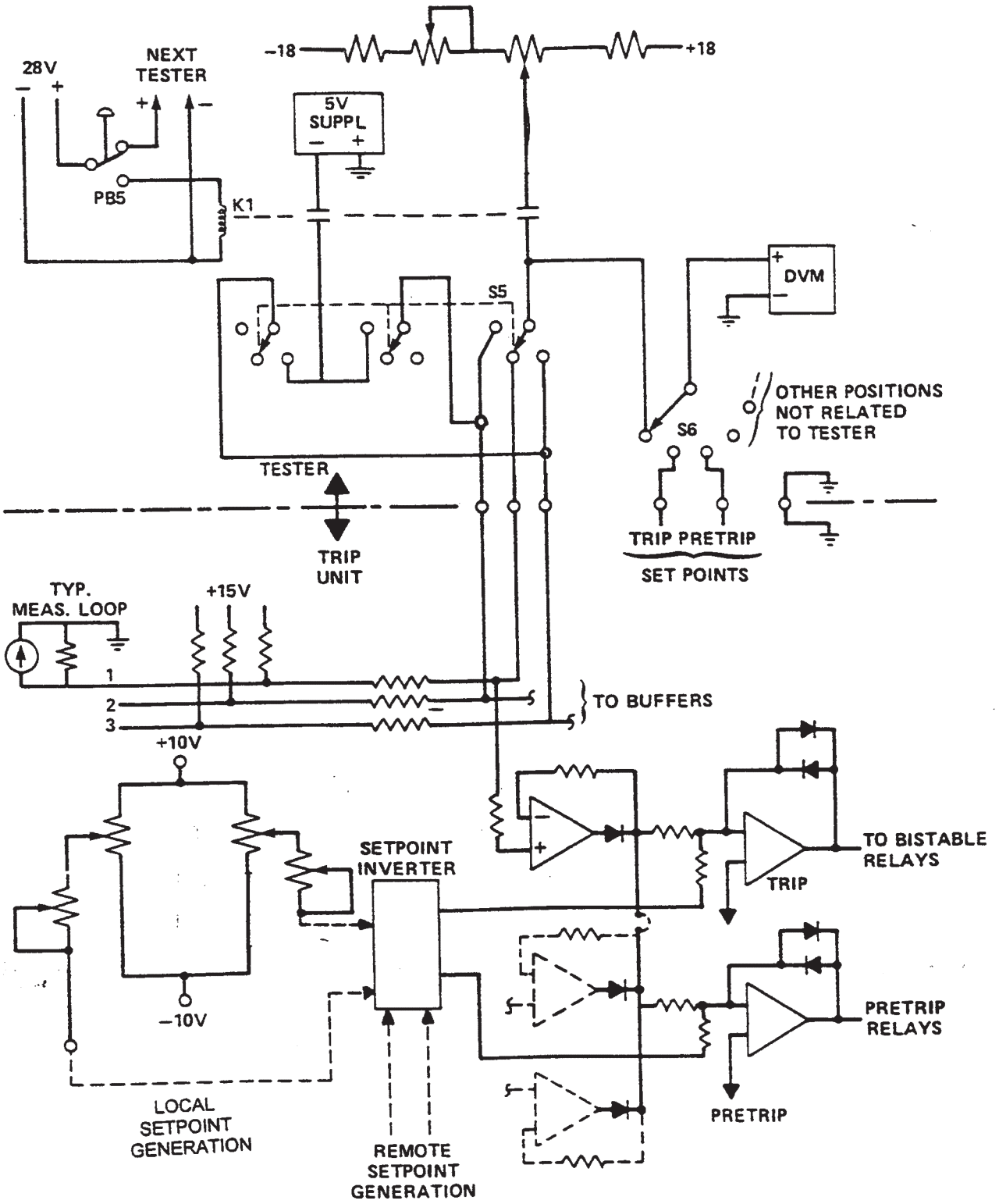
STEAM GENERATOR 'B'
PROTECTIVE CHANNEL BLOCK
DIAGRAM
FIGURE 7.2-15b



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

LOCAL POWER DENSITY TRIP

FIGURE 7.2-16



Amendment No. 13, (05/00)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

SCHEMATIC TRIP TEST SYSTEM

FIGURE 7.2-17

Refer to Drawing
2998-4967

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

RPS SCHEMATIC
SH 4 OF 4

FIGURE 7.2-18

Refer to Drawing
2998-4972

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

RPS MISC. SCHEMATICS
SHEET 1 OF 4

FIGURE 7.2-19a

Refer to Drawing
2998-4973

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

RPS MISC. SCHEMATICS
SHEET 3 OF 4

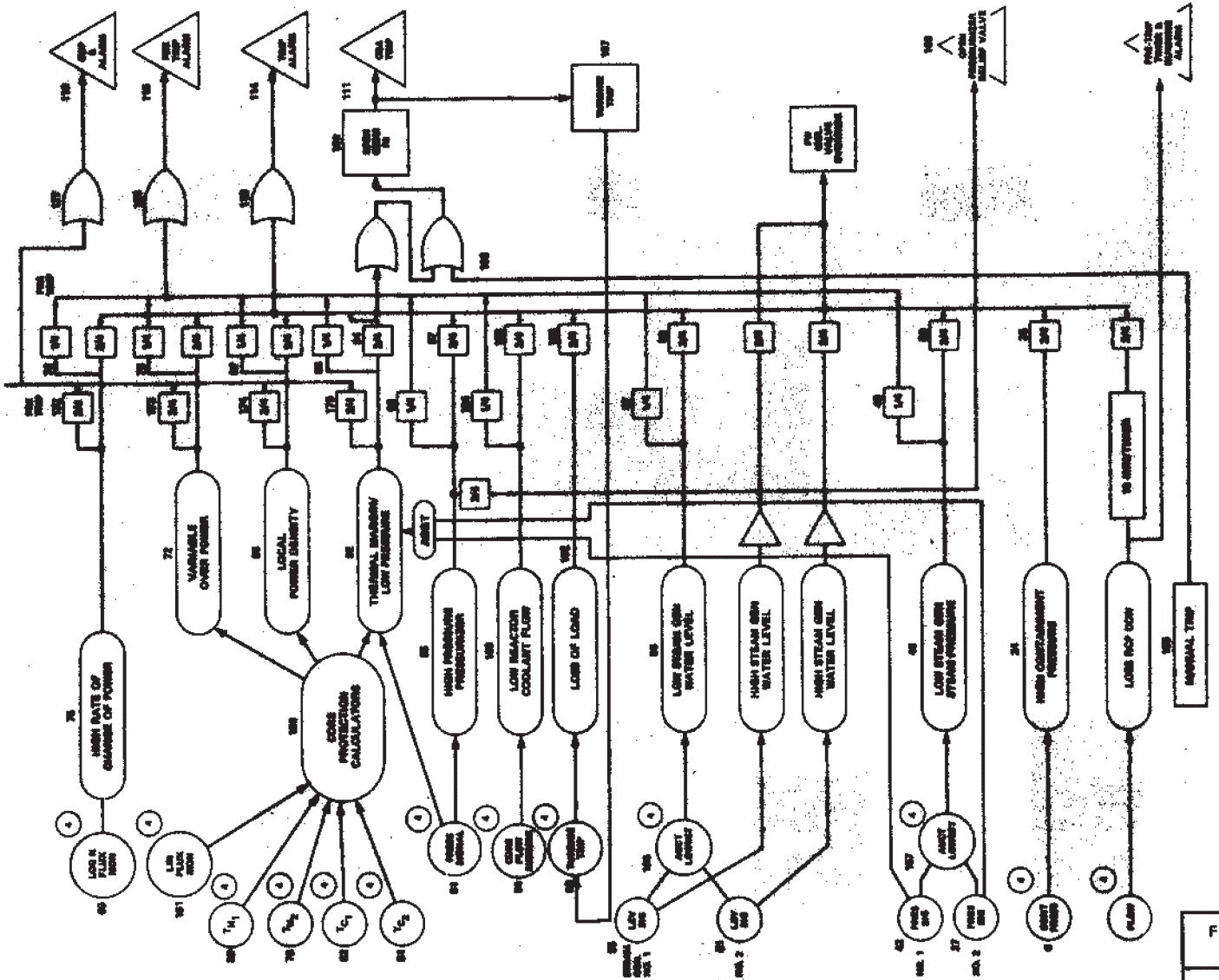
FIGURE 7.2-19b

Refer to Drawing
2998-4974

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

RPS MISC. SCHEMATICS
SHEET 2 OF 4

FIGURE 7.2-20



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

REACTOR PROTECTIVE SYSTEM
INTERFACE LOGIC DIAGRAM
FIGURE 7.2-21

7.3 ENGINEERED SAFETY FEATURES SYSTEM

The safety related instrumentation and controls of the engineered safety features (ESF) systems include (1) the Engineered Safety Feature Actuation System (ESFAS), which consists of the electrical and mechanical devices and circuitry (from sensors through the contacts of the output relays) involved in generating those signals that actuate the required ESF systems, (2) the initiation of components that perform the protective actions after receiving an actuation signal generated by the ESFAS (or by the operator), and (3) the instrumentation and control of supporting systems to the ESF.

The ESFAS contains devices and circuitry needed to generate the following signals, when the monitored variables reach levels that are indicative of conditions which require protective action (see Table 7.3-1):

a. Safety Injection Actuation Signal (SIAS)

b. Recirculation Actuation Signal (RAS)

c. Containment Spray Actuation Signal (CSAS)

d. Containment Isolation Actuation Signal (CIAS)

e. Main Steam Isolation Signal (MSIS)

f. Auxiliary Feedwater Actuation Signal-1 (AFAS-1)

g. Auxiliary Feedwater Actuation Signal-2 (AFAS-2)

The ESFAS circuitry includes the redundant initiating variable measurement devices, trip bistables, the coincidence logic matrices, actuation modules, output relays, manual and automatic test circuitry and the separated channel cabinets for housing the components.

7.3.1 DESCRIPTION

The actuation signals sent to the following systems are discussed herein:

a. ESF systems and components (and actuation signal(s) are identified in parentheses)

   1. Safety Injection System (SIAS)

   2. Recirculation (SIS Subsystem) (RAS)

   3. Containment Spray System (CSAS)

   4. Containment Isolation (CIAS)

   5. Main Steam and Feedwater Isolation (MSIS)

   6. Containment Cooling System (SIAS)

   7. Shield Building Ventilation System (CIAS)

8. ESF Support System (SIAS)

9. Auxiliary Feedwater System (AFAS-1, AFAS-2)

b. ESF Systems Not Actuated by ESFAS

1. Combustible Gas Control System, although an ESF, is manually actuated if required following a LOCA.

The system P&I diagrams for the ESF systems are shown on Figures 6.3-1(a-c), 6.2-41, 9.4-9, 9.4-11, 10.1-1(a-f) and 10.1-2(a&b).

7.3.1.1 Signal Description

7.3.1.1.1 Safety Injection Actuation Signal

This description deals with the instrumentation and controls for the safety injection actuation signal (SIAS). Refer to Section 6.3, Emergency Core Cooling System, for a description of the Safety Injection System (SIS) and Subsection 6.2.2 for a description of the Containment Cooling System. The safety related display information which provides the operator with information to monitor the required safety functions is described in Section 7.5.

The instrumentation and controls for the components and equipment in channel SA are physically and electrically separate and independent of the instrumentation and controls for the components and equipment in channel SB. This independence maintains the redundancy required to ensure the functional capability of the equipment following a design basis event which is mitigated by the SIS.

A SIAS automatically actuates the Safety Injection System and the supporting systems as listed in Table 7.3-2. The SIAS is initiated by a coincidence of either two-out-of-three low pressurizer pressure signals or two-out-of-three high containment pressure signals, shown on Figure 7.3-1. There are four independent pressurizer pressure transmitters (PT-1102A, B, C, D) and four independent containment pressure transmitters (PT-07-2A, B, C, D) to provide signal inputs. A bypass is provided to remove a trip function from one of the measurement channels for maintenance or testing. The requisite two-out-of-three trip logic is unaffected by this bypass. The remaining trip functions in the channels are unchanged. The two-out-of-three logic meets full safety requirements including the requirements of single failure criteria.

Separate control switches, for optional manual actuation of the equipment, are located on the reactor turbine generator board (RTGB) in the control room. Automatic actuation of the equipment is initiated by the SIAS output relay contacts. Control board instrumentation (eg., flow, temperature, pressure) is provided to enable the operator to evaluate system performance. Alarms are provided; see Subsection 7.5.1 for a discussion of the ESF system/support monitoring display instrumentation.

A safety injection block is provided to permit shutdown depressurization of the Reactor Coolant System (RCS) without initiating safety injection. This block is accomplished manually after pressurizer pressure has been reduced and a permissive signal is generated by the Engineered Safety Features Actuation System. This blocking procedure is under strict administrative control; block and block permissive is annunciated and indicated in the control room. It is not possible to block above a preset pressure, if the system is blocked and pressure rises above that point, the

block is automatically removed. The block circuit complies with the signal failure criterion in IEEE 279-1971.

The actuation circuits for the ESFAS are all similar except for specific inputs, operating bypasses, and actuation devices. The SIAS described below is typical of all ESFAS. The specific instruments and controls associated with each actuation signal are discussed separately in the appropriate subsection.

a. Initiating Circuit

Pressure measurement channels associated with the pressurizer and the containment are continuously monitored to provide signals to the SIAS. The protective parameters are measured with four independent instruments, utilized to perform the following functions:

i) Monitor pressurizer pressure and containment pressure

ii) Provide indication of operational availability of each sensor to the operator

iii) Transmit analog signals to bistables within the SIAS initiating logic.

The measurement channels consist of instrument sensing lines, sensors, transmitters, power supplies, bistables, isolation devices, indicators, current loop resistors, and interconnecting wiring. A typical protective measurement channel functional diagram is shown on Figure 7.3-2.

Each measurement channel is separated from its redundant measurement channels to provide physical and electrical isolation of the signals to the SIAS initiating logic. The output of each transmitter is an ungrounded current loop which has a live zero. Each channel is supplied from its separate 120 volt safety related ac distribution bus.

Display information, which provides the operator with the operational availability of each measurement channel, is described and tabulated for the ESFAS in Section 7.5.

b. Logic

The SIAS logic matrices are physically separated into channel related sections within the ESFAS cabinets.

The SIAS initiation signals generated in the four measurement channels (MA, MB, MC, MD) are received by four trip bistables from each parameter. At the bistables the signals are compared to predetermined setpoints. Whenever a channel parameter reaches the predetermined setpoint, the bistable initiates a channel trip.

The signals of the four trip bistables from each parameter, feed two separate SIAS coincidence logic matrices (SA & SB) via channel separated isolation modules. The isolation modules maintain separation between the measurement channels and the logic matrices.

One of the four measurement channels serves as an active standby, which can be removed for maintenance or testing, while still maintaining a two-out-of-three logic. The output of the SIAS matrices feed the actuation relays.

Four separate power buses from safety related inverters (described in Section 8.3), supply 120 volt ac to the ESFAS cabinets. The MA, MB, MC, and MD cabinets have power supplies fed from the MA, MB, MC and MD buses respectively, while cabinet SA is powered by two auctioneered supplies fed from MA and MC buses and cabinet SB is powered by two auctioneered supplies fed from MB & MD buses (see Figure 7.3-10).

c. Output Relays

The SIAS output relays are located in the two redundant cabinets SA and SB of the ESFAS.

Initiation signals from the coincidence logic matrices associated with each actuation channel. (SA & SB) de-energize the SIAS output relays, which in turn initiate the ESF and supporting equipment listed in Table 7.3-2. The SIAS output relays in both redundant channels are divided into groups, for individual actuation of specific ESF equipment during manual periodic testing. Components of each group are actuated by one group relays. Group relay contacts are directly connected in the actuating device control circuit for the actuated components of each ESF system. In the unlikely event of an actual SIAS, all groups of output relays are de-energized to actuate automatically the equipment listed in Table 7.3-2.

d. Manual and Automatic Test Circuitry

Periodic testing of the SIAS and its associated components is conducted from the ESFAS cabinets by means of separate manually operated switches and pushbuttons provided at each of the redundant cabinets.

The tests are conducted periodically during normal plant operation in accordance with Technical Specifications to verify operability of the SIAS. The grouping of the relays provides the verification tests without interrupting normal plant operation.

Jumpers or temporary forms of bypassing are not used during testing. The system testing in no way interferes with the protective function of the system and meets the intent of IEEE 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," and of Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," 2/72(R0).

The periodic test of the ESFAS utilizes the built in test circuitry. No additional test equipment or fuse removal procedures are required. The installation test equipment contains its own power supply and checks logic and trip relays, which conforms to Regulatory Guide 1.118 Rev. 0, position C.13.

The individual tests are described below:

i) Sensor Checks

The four redundant measurement channels providing inputs to the SIAS (i.e., pressurizer pressure and containment pressure) are checked by comparing the reading of the indicators of the four channels in the control room, and by cross checking with related measurements.

ii) Trip Bistable Tests

Testing of the trip bistable calibration setpoint is accomplished by manually varying a test input signal to the trip setpoint level (on one bistable at a time) and observing the trip action. An adjustable voltage source provides the calibration input signal and digital voltmeter indicates the value of this signal. During this bistable trip setpoint calibration test the bistable trip output is blocked to the logic matrices. An additional pushbutton on each bistable in concert with the selector switch allows to trip test the bistable and to provide one test input to the logic matrices.

The bistable test circuit uses a momentary, spring return "Auto" calibration switch. After calibration test, the bistable is returned to its normal automatic position. The bistable trip test uses momentary spring return pushbutton located on the bistable. After observing trip test lights and releasing the button, the bistable returns to its normal position.

iii) Logic Matrices Tests

Each group logic matrix requires two inputs for a test trip. One test signal is obtained by the trip tested bistable described above and the second one is provided by the activation of a test group selector switch and simultaneously pressing a momentary test button on the tested logic matrix. This causes the logic matrix undergoing the test to trip and to de-energize the output relays connected to this test group. It should be noted that any test selector switch position chosen does not block an incoming SIAS resulting from a design basis accident (DBA). The matrix does not reset after the test and requires operator action on the main control board to actuate the systems reset switch.

iv) Actuating Device and Actuated Component Test

Operational testing of the group output relays as described in (iii) above is accomplished by individually selecting one group (refer to Table 7.3-2 for the test group assignment). Components were grouped to maximize their testability at power without impacting plant operation. For example, when SIAS test group 1A is tested the LPSI pump 2A starts but LPSI discharge valves remain closed since they are assigned to test group 2A. This overlapping test method causes the ESF components to actuate; therefore the propagation of a valid trip during testing is not impeded and the ESF system proceeds to full actuation. Group 0 was originally intended to include all components not testable at power; however, design development precluded this limitation.

v) Response Time Tests

Response time tests of the ESFAS are conducted at refueling intervals in accord with the Technical Specifications. Response time test requirements and acceptance criteria are discussed in Section 13.7.2.2.

vi) Automatic Testing

An automatic test inserter (ATI) provides automatic and continuous on-line testing without disturbing the ESFAS functions. During each test interval, two ATI pulses (less than 2 Milliseconds) are applied to selected groups of bistables. The first ATI pulse is lower than the trip level and it sets a flip-flop in each bistable for a test interval memory. The second ATI pulse is above the trip point so that the bistables provide the trip signals through the isolation modules and actuation modules, and the pulses are returned to the bistables if the equipment performs properly. If the first pulse trips a bistable, or if the second pulse is not transmitted, an ATI fault is then indicated and alarmed on the ESFAS front panel. The control room annunciator does not have reflash capability, therefore, the annunciator "locks in" after the first detected fault. The operator then performs manual tests at the indicated area, to determine and replace the faulty components. The ATI and its components are completely independent from the ESFAS.

vii) Engineered Safety Feature (ESF) Reset Controls (IE Bulletin 80-06)

In order to maintain safety equipment in its emergency mode upon reset of an engineered safety features actuation signal, (ESFAS) design changes on several systems have been performed to assure that protective action of the equipment, initiated by ESFAS, is not compromised once the associated actuation signal is reset.

The circuitry for reset has been tested and verified to comply with IE Bulletin 80-06 Item 2 during plant startup.

The only exception is the circuitry for the Diesel Generator where in the emergency mode all protective trips, except differential current and overspeed, are bypassed by an ESFAS. ESFAS reset restores the DC trip circuits provided the emergency bus tie breakers are closed manually upon restoration of offsite power. Since the ESFAS reset restores all DG trips only if the emergency bus tie breakers are closed (offsite power available), no changes are planned for these circuits.

e. Bypasses

A key-operated trip channel bypass is provided to remove a trip function from service for maintenance or testing. The bypass is manually initiated and manually removed. The pressurizer pressure bypass is designed as a safety injection block during shutdown depressurization of the RCS. Manual block is induced only during shutdown when the pressurizer pressure has been reduced. Pressurizer pressure signals generated by the measurement channels are received through

separate bistables whereby a 3-out-of-4 channel coincident permissive bypass signal is generated by the ESFAS. This permissive signal must be available before the manual block can be induced. The block function is automatically removed when pressurizer pressure returns above setpoint.

f. Interlocks

A key interlock prevents the operator from, bypassing more than one measurement channel at a time. During system testing the electrical interlocks allow only one matrix logic to be held in the test position at one time, and only one process measurement loop signal can be perturbed at one time.

g. Sequencing

Each ESFAS simultaneously actuates components listed in Tables 7.3-2, 3, 4, 5 and 6. However, to ensure that emergency diesel generator loads are properly assigned in the event of loss of offsite power, individual time relays are provided to delay starting of the equipment in accordance with the emergency diesel generator loading sequence (see Table 8.3-2).

h. Redundancy

Redundant features of the SIAS include:

i) Four independent channels, from process sensor through and including bistables and channel isolation modules.

ii) Two redundant logic matrices which provide the coincidence logic. Independent power supplies are provided for each logic matrix.

iii) Two trip paths are present for each actuation signal.

iv) Four independent bistables are utilized to provide block permissive signals for the pressurizer pressure actuation signal.

v) The actuation signal is generated by relays within two output trains so that redundant system components are actuated from separate trains. Separate relays in each of the redundant trains are also provided for the actuation of the equipment. In the third channel (channel SAB). ESFAS interconnections for AB shared system equipment are shown on Figure 7.3-11. A discussion of channel SAB is presented in Subsection 8.3.1.

Equipment actuated by redundant actuation trains (SA and SB) for SAB shared system equipment are as follows:

1) Intake Cooling Water Pump 2C

2) Charging Pumps 2C

3) Component Cooling Water Pump 2C

vi) Two independent sets of control switches and pushbuttons are provided at two locations on the main control board for optional operator actions to initiate SIAS.

vii) The four channel independence begins at the output of the 4 ac UPS inverters, designated inverter 2A, 2B, 2C and 2D or the Maintenance Bypass Transformer 2A, 2B, 2C and 2D and their associated instrument Buses as shown on Figure 8.3-3. Independence of the four channels of RPS or ESFAS is maintained in accordance with Subsections 8.3.1.3, 8.3.1.4, and 7.2.1.1.7.

AC power for the actuation system is provided from four separate 120V AC instrumentation buses. Power for control and operation of redundant actuated components comes from separate buses.

The above redundant features provide a system which meets the single failure criterion, is testable during plant operation, and is operable with a two-out-of-three logic.

The benefit of a system that includes four independent and redundant channels is that the system can be operated with up to two channels out of service (one bypassed, one tripped) and still meet the single failure criterion. While in this condition (one-out-of-two logic), it is impossible to bypass another channel for testing or maintenance: the system logic must be restored to at least a two-out-of- three condition prior to removing another channel for maintenance. In fact, the plant basis (Figure 7.3-1) is a three channel protection system with an "Installed spare" for the RPS, and ESFAS functions of SIAS, MSIS, and CIAS. However, the design basis for the ESFAS functions of RAS and CSAS is the energization of actuation relays (Figure 7.3-1) to make it incredible for spurious actuation of Containment Spray or Recirculation which can be detrimental to equipment in a non-accident condition. Therefore, the NRC position of trip instead of continuous bypass for one of the four channels used for RAS or CSAS is acceptable to the applicant.

i. Diversity

The ESFAS incorporates functional diversity to accommodate the unlikely event of a common mode failure during accident conditions.

j. Auxiliary Supporting Systems Required

Support systems are identified in Subsection 7.3.1.1.6.

7.3.1.1.2 Recirculation Actuation Signal

This description deals with the instrumentation and controls for the recirculation actuation signal (RAS). Refer to Section 6.2 for a description of the Containment Spray System, and Section 6.3 for a description of the Safety Injection System.

All actions required to effect the change over from injection to recirculation are automatically initiated by the RAS. No operator interaction is required.

The RAS is automatically initiated by two-out-of-four low refueling water tank level signals rather than two-out-of-three, because it is designed to energize to actuate rather than de-energize to actuate; see Figure 7.3-1. The four measurement channels for the refueling water tank level are physically and electrically separated and all four channels are active during plant operation. A bypass is provided to remove a trip function from one of the measurement channels for maintenance or testing. The requisite two-out-of-three trip logic is unaffected by this bypass. The remaining trip functions in the channels are unchanged. Due to the energize-to-activate design, technical specifications require that the channel be placed in trip condition after a specified time; the trip of one-out-of-three remaining channels actuates the RAS.

Based on the following considerations, Technical Specification action statements pertaining to one inoperable RAS (RWT level) measurement channel were revised (via Technical Specification Amendment #132 and Engineering Evaluation PSL-ENG-SENS-00-024) to restrict the amount of time an inoperable channel could remain in either trip or bypass. With one inoperable channel in bypass, RAS actuation could be precluded by a single failure (i.e., failure of a DC Bus that results in loss of both associated 120 VAC measurement channel busses) due to the energize to actuate RAS design. The second consideration is that with one inoperable channel in trip, premature RAS actuation could occur due to single failure of another channel.

The RAS automatically transfers the suction of the high pressure safety injection pumps and the containment spray pumps from the refueling water tank (RWT) to the containment sump, by opening the two sump outlet valves while simultaneously closing the refueling water tank outlet valves, and closing the pump miniflow recirculation valves to the tank. Concurrent with transfer of pump suction from the refueling water tank to the containment sump, the low pressure safety injection pumps are automatically stopped on RAS. The RAS measurement channels and logics are designed as "energize to actuate" in order to prevent spurious RAS initiation in the unlikely event of a loss of power to the channels. Consequences due to spurious RAS initiation are summarized below:

a. Normal Plant Operation

   The LPSI, HPSI and containment spray are not operating. On a spurious RAS initiation, (LPSI, HPSI and Containment Spray Pumps remain not operating) one outlet valve opens and one refueling water tank outlet valve closes. This should not affect normal plant operation because the other ESFAS channel will remain operational. Adequate valve position, sump/tank levels instrumentation, and alarms in the control room are provided. The operators are alerted to correct the abnormal condition promptly.

b. Emergency Reactor Shutdown Condition (i.e., SIAS and/or CIAS)

   The HPSI, LPSI and Containment Spray Pumps are running with their suction headers lined up with the Refueling Water Tank (RWT). If RAS signal of one (1) safety channel actuated, the corresponding LPSI pump will be stopped. The HPSI and Containment Spray Pumps of that channel will be connected to the dry sump. However, the remaining redundant safety pump trains will remain intact and perform the required safety functions. The control room operator has adequate alarms and instrumentation to recognize the abnormal pump-valve line up and correct it manually from the control room prior to pump damage.

c. Normal Shutdown Cooling

The LPSI pumps are isolated from RWT and containment sump by V3444 and V3432. Pump suctions are obtained from RCS. Spurious RAS switchover signal should not affect the Decay Heat Removal System or damage the pumps.

No single failure prevents initiation of the RAS. Valve circuitry permits optional manual closing of any containment sump suction line or manual opening of any RWT outlet line after an RAS initiation, from either the control room or from a local control station. Control room alarms are provided to annunciate possible maloperations (see Subsection 7.5.1).

Redundant safety class instrumentation is provided for RWT level and containment sump level. Annunciations are available to the control room operator to alert him of abnormal valve positions, and pump operating conditions. Furthermore, RAS annunciation is provided in the control room.

The reset of SIAS prior to automatic switchover from injection to recirculation does not affect RAS. The RAS actuation strictly depends on RWT levels (2 out of 4 channels) and is independent of SIAS.

The containment sump valves (MV-07-2A, 2B) open in 30 seconds and the refueling water tank outlet valves (MV-07-1A, 1B) close in 90 seconds, such that RWT or containment sump water is always available at the suction of the pumps during the transfer. Further, enough water is maintained below the low level (RAS) setpoint in the RWT to sustain pump suction throughout the closure of the RWT isolation valves. In the event one or both of the RWT valves fails to close, the water seal created by the difference in elevation between the containment sump and RWT water levels would prevent air from being drawn into the system. No credit is taken for the height of water in the RWT above the suction line in the calculation of the available Net Positive Suction Read (NPSH). Thus, even if tank level is drawn down to the suction line, pump operation is assured. (Note: This information is historical and based on the original NPSH calculation. The calculation did not include the effects of vortex formation).

Components actuated by the RAS are listed in Table 7.3-3.

a. Initiating Circuits

The RAS initiating circuits are similar to the initiating circuits described in Subsection 7.3.1.1.1a for SIAS other than the fact that RWT water level is the only parameter monitored.

b. Logic

The logic for the RAS is shown on Figure 7.3-1.

c. Output Relays

Output relays for the RAS are similar to those described in Subsection 7.3.1.1.1c for SIAS except relays are energized to actuate the RAS.

d. Manual and Automatic Test Circuitry

Provisions for testing the RAS are similar to those described in Subsection 7.3.1.1.1d.

e. Bypasses

Bypasses for the RAS are similar to those described in Subsection 7.3.1.1.1e for SIAS except there is no blocking for shutdown.

f. Interlocks

Interlock provision for RAS are similar to those described in Subsection 7.3.1.1.1f for SIAS.

g. Sequencing

Sequencing equipment and functions for RAS are described in Subsection 7.3.1.1.1g.

h. Redundancy

Redundancy features for the RAS are similar to those described in Subsection 7.3.1.1.1h.

i. Diversity

The only parameter being measured is RWT water level; therefore functional diversity is not applicable.

j. Auxiliary Supporting Systems Required

Support systems are identified in Subsection 7.3.1.1.6.

7.3.1.1.3 Containment Spray Actuation Signal

This description deals with the instrumentation and controls for the containment spray actuation signal (CSAS). Refer to Subsection 6.2.2 for a description of the Containment Spray System (CSS). The containment heat removal function is also performed by the Containment Cooling System which is actuated by SIAS.

The CSAS automatically actuates the CSS. The CSAS is initiated by a coincidence of two-out-of-four high-high containment pressure signals (rather than two-out-of-three, because it is designed to energize to actuate rather than de-energize to actuate) and a simultaneous SIAS signal as shown on Figure 7.3-1. The four measurement channels for high-high containment pressure are physically and electrically separated and all four channels are active during plant operation. A bypass is provided to remove a trip function from one of the measurement channels for maintenance or testing. The requisite two-out-of-three trip logic is unaffected by this bypass. The remaining trip functions in the channels are unchanged. Due to the energize-to-actuate design, technical specifications require that the channel be placed in trip condition after a specified time; the trip of one-out-of-three remaining channels in conjunction with a SIAS actuates the CSAS.

The system is composed of four redundant channels, MA, MB, MC, and MD. The instrumentation and controls in a channel are physically and electrically separate and independent of the instrumentation and controls in other channels. This independence maintains the redundancy required to ensure equipment functionality following any design basis event.

The two redundant CSAS actuation channels (SA and SB) initiate the operation of the containment spray pumps (A and B) and their associated valves (see Figure 6.2-41). Each spray system isolation valve (FCV-07-1A and 1B) is opened by its associated CSAS actuation channel (SA or SB).

The CSAS containment pressure measurement channels and CSAS actuation logics are designed as "energize to actuate" to prevent spurious spray system operation on loss of power to one of the two 125V dc buses.

The 125V dc system is designed such that no single failure results in loss of power to both of the 125V dc buses (see Subsection 8.3.2). In the event of loss of power to one bus, CSAS is initiated when required by the measurement channels associated with the unaffected bus. Each CSAS actuation channel can also be initiated manually from the control room. Thus, no single failure prevents proper CSAS actuation.

a. Initiating Circuits

   Initiating circuits are similar to the initiating circuits described in Subsection 7.3.1.1.1a for SIAS except that the parameter monitored is containment pressure only.

   The SIAS and high-high containment pressure signals are combined in two AND circuits within the ESFAS initiating logic. The AND circuits prevent inadvertent operation of the Containment Spray System upon generation of an SIAS only.

b. Logic

   The CSAS logic is shown on Figure 7.3-1.

c. Output Relays

   The output relays for CSAS are similar to those described in Subsection 7.3.1.1.1c for SIAS except relays are energized to actuate the CSAS.

d. Manual and Automatic Test Circuitry

   Manual and automatic testing for CSAS is similar to that described in Subsection 7.3.1.1.1d for SIAS.

e. Bypasses

   Bypasses for the CSAS are similar to those described in Subsection 7.3.1.1.1e for SIAS except there is no blocking for shutdown.

f. Interlocks

   Interlock provisions for CSAS are similar to those described in Subsection 7.3.1.1.1f for SIAS.

g. Redundancy

Redundancy features for CSAS are similar to those described in Subsection 7.3.1.1.1h for SIAS.

h. Diversity

The only parameter being measured is Containment Pressure, therefore Functional Diversity is not applicable.

i. Sequencing

Sequencing equipment and functions for CSAS are similar to those described in Subsection 7.3.1.1.1g.

j. Auxiliary Supporting Systems Required

The auxiliary supporting systems are identified in Subsection 7.3.1.1.6.

7.3.1.1.4 Containment Isolation Actuation Signal

This description deals with the instrumentation and controls for the containment isolation actuation signal (CIAS). Refer to Subsection 6.2.4 for a description of the containment isolation system (CIS), and to Subsection 6.2.3 for a description of the Shield Building Ventilation System (SBVS). The CIS is automatically actuated by a CIAS. A list of the isolation valves with valve size, type of actuator, normal position, and position on loss of power is given in Tables 6.2-52 and 53.

The logic which initiates the CIAS is shown on Figure 7.3-1. CIAS is actuated on high containment pressure, or high containment radiation or on SIAS actuation. The CIAS measurement channels include four independent pressure transmitters and four independent containment radiation monitors. The measurement channel signals for each of these two diverse parameters are combined in two-out-of-three logic matrices. Each measurement channel is physically and electrically separated, enabling the bypass of any one of the four channels for maintenance or testing while remaining with a two-out-of-three logic for automatic actuation. The two-out-of-three logic meets full safety requirements including the requirement of the single failure criterion.

The output signals from the high containment pressure, high radiation, and SIAS logic matrices are combined in an "OR" logic circuit to form the CIAS. There are two redundant independent CIAS actuation channels (SA and SB). The instrumentation and controls of the components and equipment in channel A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in channel B. This independence maintains the redundancy required to ensure the functional capability necessary to isolate the containment. The safety related display instrumentation for the containment isolation system provides the operator with sufficient information to monitor the required safety functions.

Each CIAS actuation channel (SA and SB) also actuates the Shield Building Ventilation System (SBVS) fans (A and B) and its associated dampers and valves.

Each CIAS actuation channel may also be initiated manually from the control room.

a. Initiating Circuits

The initiating circuits for the CIAS are similar to those described in Subsection 7.3.1.1.1a for the SIAS with the exception that the parameters monitored are containment pressure and containment radiation.

b. Logic

The CIAS logic is shown on Figure 7.3-1.

c. Output Relays

The output relays for CIAS are similar to those described in Subsection 7.3.1.1.1.c for SIAS.

d. Manual and Automatic Test Circuitry

Manual and automatic testing for CIAS is similar to that described in Subsection 7.3.1.1.1d for SIAS.

e. Bypasses

Bypasses for CIAS are similar to those described in Subsection 7.3.1.1.1e for SIAS except there is no blocking for shutdown.

f. Interlocks

Interlock provisions for CIAS are similar to those described in Subsection 7.3.1.1.1f for SIAS.

g. Redundancy

Redundancy features for CIAS are similar to those described in Subsection 7.3.1.1.1h for SIAS.

h. Diversity

Diversity aspects for CIAS are similar to those described in Subsection 7.3.1.1.1i for SIAS.

i. Sequencing

Sequencing equipment and functions for CIAS are similar to those described in Subsection 7.3.1.1.1g for SIAS.

j. Auxiliary Supporting Systems Required

The auxiliary supporting systems are identified in Subsection 7.3.1.1.6.

7.3.1.1.5 Main Steam (and Feedwater) Isolation Signal

This description deals with the Instrumentation and controls for main steam and feedwater isolation. Refer to Section 10.3 for a description of the Main Steam System (MSS) and see Subsection 10.4.7 for a description of the Feedwater System.

The main steam isolation signal (MSIS) is initiated by two-out-of-three low pressure signals from either steam generator and/or upon high containment pressure. The MSIS terminates blowdown of steam from the steam generators, and stops the normal feedwater flow to the steam generators by closing the main steam and main feedwater Isolating valves.

The logic which initiates MSIS is shown on Figure 7.3-1. The MSIS measurement channels consist of four steam generator pressure transmitters for each steam generator and four high containment pressure transmitters. Two-out-of-three logic signals from low steam generator pressure and two-out-of-three logic signals from high containment pressure are combined in OR logic to provide closure of both the main steam isolation valves (MSIVs) and the main feedwater isolation valves (MFIVs). Each one of the four measurement channels is physically and electrically separated, enabling the bypass of any one channel for maintenance or testing while remaining with a two-out of-three logic for automatic actuation. The two-out-of-three logic meets full safety requirements including the requirement of the single failure criterion.

The measurement channels logic and actuation channels associated with steam generator A are separated from those associated with steam generator B. An MSIS signal on either channel closes the MSIV, the main feedwater isolation valve, and the backup feedwater isolation valve on that channel, and sends a signal through an isolation device to close the MSIV, the main feedwater isolation valve, and the backup feedwater isolation valve of the other channel. Each isolation device is designed as an energize-to-actuate device and is powered from the same safety related ac power source as the MSIS activation signal. The effects of ac or dc power loss in combination with the isolation device have been evaluated in Table 7.3-9 to insure conformance to single failure criteria for the MSIS features. In addition, annunciation is provided to alert the operator of power loss to the isolation device. This ensures that in the unlikely event of a steam line break accident upstream of the MSIVs; the MSIVs close and limit the blowdown to the faulted steam generator. The consequences of such an occurrence are evaluated in Chapter 15.

A manual block on the MSIS is provided to permit shutdown depressurization of the Main Steam System without initiating MSIS. This process is under strict administrative control with block and block permissive annunciated and indicated in the control room. It is not possible to block above a preset pressure: if the system is blocked and pressure rises above this point, the block is automatically removed. The block circuit is designed to comply with the single failure criterion specified in IEEE 279-1971. Each MSIS actuation channel can be initiated manually from the control room. A list of components activated on a MSIS is given in Table 7.3-6.

a. Initiating Circuits

   The initiating circuits for the MSIS is similar to that described in Subsection 7.3.1.1.1a for SIAS except that the parameters monitored are the steam generator pressure for each steam generator and containment pressure.

b. Logic

   The MSIS logic is shown on figure 7.3-1.

c. Output Relays

   The output relays for MSIS are similar to those described in Subsection 7.3.1.1.1c for SIAS.

d. Manual and Automatic Test Circuitry

Manual and automatic testing for MSIS is similar to that described in Subsection 7.3.1.1.1d for SIAS.

e. Bypasses

Bypasses for MSIS are similar to those described in Subsection 7.3.1.1.1e for SIAS.

f. Interlocks

Interlock provisions for MSIS are similar to those described in Subsection 7.3.1.1.1f for SIAS.

g. Redundancy

Redundancy features for MSIS are similar to those described in Subsection 7.3.1.1.1h for SIAS.

h. Diversity

The parameters being measured are steam generator pressure and containment pressure; therefore functional diversity is applicable.

i. Sequencing

Sequencing equipment and functions for MSIS are similar to those described in Subsection 7.3.1.1.1g for SIAS.

j. Auxiliary Supporting Systems Required

The auxiliary supporting systems required are identified and described in Subsection 7.3.1.1.6.

7.3.1.1.6 ESF Supporting Systems

The ESF supporting systems listed below are described in the referenced sections:

a. Component Cooling Water System (Subsection 9.2.2)

b. Intake Cooling Water System (Subsection 9.2.1)

c. Onsite Power System, including the diesel generator system (Section 8.3)

d. Diesel Fuel Oil Storage and Transfer System (Subsection 9.5.4)

e. Heating, Ventilating and Air Conditioning (HVAC) Systems as required for areas containing systems and equipment required for safe shutdown (Section 9.4).

7.3.1.1.7 Systems Not Actuated by ESFAS

a. Combustible Gas Control System

The Combustible Gas Control System is provided to control the concentration of hydrogen that may be released into containment following a LOCA; see Subsection 6.2.5.

7.3.1.1.8 Auxiliary Feedwater Actuation Signals

This description deals with the instrumentation and controls for the auxiliary feedwater actuation signals (AFAS-1, AFAS-2). Refer to Subsection 10.4.9 for a description of the "Auxiliary Feedwater System" (AFWS).

The safety related display information which provides the operator with information to monitor the required safety functions is described in Section 7.5.

The instrumentation and controls for the components and equipment in channel MA, MB, MC and MD are physically separated and electrically isolated and independent of each other. This independence maintains the redundancy required to ensure the functional capability of the equipment following a design basis event which is mitigated by the AFWS.

The AFAS actuation logic is shown functionally on Figures 7.3-12 and 7.3-14. It initiates auxiliary feedwater to a steam generator on a low level signal following a variable preset initiation delay period that performs in accordance with the Technical Specifications. However, the initiation of AFW to a steam generator with a low level condition will be prevented by the AFAS logic if the steam generator or its associated auxiliary feedwater supply header is identified as being ruptured.

A steam generator is identified as being ruptured when its pressure is approximately 275 psi below the other steam generator coincident with its own low level signal and with the other steam generator and auxiliary feedwater header being identified as not ruptured, per Technical Specification ESFAS trip value requirements.

An auxiliary feedwater supply header is identified as ruptured when its pressure is approximately 150 psi below the other feedwater header pressure coincident with its associated steam generator low level signal and with the other steam generator and auxiliary feedwater header being identified as not ruptured, per Technical Specification ESFAS trip value requirements.

The AFAS actuation logic isolates auxiliary feedwater flow to a steam generator upon recovery of steam generator level.

A separate auxiliary feedwater actuation signal is generated for each steam generator (AFAS-1, AFAS-2).

The AFAS logic employs three channels of initiating signals to provide a two-out-of-three actuation sequence of system components. However, to enhance plant availability, a fourth channel is provided as a spare and allows by-passing of one channel while maintaining the requisite two-out-of-three logic. The components actuated by the AFAS-1 and AFAS-2 logic are provided on Table 7.3-11. The failure modes and effects analysis for the AFAS logic is provided on Table 7.3-12.

a. Initiating Circuits

The AFAS initiation circuits are similar to the initiation circuits described in Subsection 7.3.1.1.1a for SIAS except that Steam Generator 2A and 2B pressure, Feedwater Header Pressure 1 and 2 and Steam Generator Level 2A and 2B are the parameters monitored as shown in Figure 7.3-12.

b. Logic

1. The steam generator low level initiation signals generated in the four measurement channels (MA, MB, MC, MD) are received by four bistable comparators for each parameter. At the bistables, the signals are compared to predeteremined setpoints. Whenever a channel parameter reaches the predetermined setpoint, the bistable initiates a channel trip which is characterized by the deenergization of three bistable trip relays.

Channel trip reset, characterized by the energization of the bistable relays, occurs whenever a channel parameter returns to a value representing the setpoint plus a predetermined bistable hysteresis resetpoint.

Two bistable hysteresis resetpoints operate to reset the channel trip before and after completion of a predetermined initiation time delay period.

Contacts from the bistable relays of the same system in the four protective channels are arranged into six logic AND'S, designated AB, AC, AD, BC, BD and CD, which represent all possible coincidence of two combinations. To form an AND circuit, the bistable trip relay contacts associated with the same AFAS (AFAS-1 or AFAS-2) are connected in parallel (eg, one from channel A and one from channel B). This process is continued until all combinations have been formed.

Each logic matrix is connected in series with a set of four matrix output relays. Each logic matrix is powered from two separate 120v Class 1E instrument power supply buses through dual dc power supplies. The contacts of the matrix relays are combined into four initiation circuits, one circuit per channel per AFAS.

Each initiation circuit is formed by connecting six contacts (one matrix relay contact from each of the six logic matrices) in series. The six series contacts are in series with the initiation delay circuit and the initiation relay. The initiation relay outputs are combined to form the actuation logic.

2. Actuation Logic

The actuation logic is formed by combining the initiation circuit output signals from the four channels into a selective two-out-of-three logic within each channel. Upon actuation of this logic the appropriate (AFAS 1 or 2) AFAS actuation relays will deenergize to control the individual AFWS components.

The actuation relays are subdivided into two categories as follows:

a. Cycling Relays - These relays control the auxiliary feedwater isolation valves and will automatically reset when the steam generator has refilled or a steam generator or feedwater header has been identified as being ruptured. The main feedwater isolation valves also utilize cycling relays, which close the isolation valves to the affected steam generator. After relay reset valve control is returned to the operator, however, the valve will remain closed.

b. Latching Relays - These relays control the auxiliary feedwater pumps and the AFW system turbine inlet valves, and will remain in the actuated condition until manually reset.

c. Trip Generator (Output Relays)

Signals from the process measurement loops are sent to bistables where the input signals are compared to the predetermined trip setpoints. Whenever a parameter reaches the trip value, the bistable output deenergizes. This and other similar signals form the AFAS logic signal which deenergizes three bistable relays when the appropriate conditions are met. The bistable relay contacts change state, effecting the appropriate coincidence logic (Sub-section 7.3.1.1.8b(1)).

The bistable and differential bistable setpoints are adjusted at the AFAS cabinet. Access to the adjustments is administratively controlled by means of a key locked cover. The initiation delay time setpoints and bistable hysteresis resetpoints are adjusted internal to the AFAS cabinet. The setpoints within each channel can be monitored through test jacks located on the AFAS cabinet.

d. Testing Circuitry

Provisions for testing the AFAS are similar to those described in Subsections 7.2.1.1.9.1, 7.2.1.1.9.2, 7.2.1.1.9.4 and 7.2.1.1.9.5 except as discussed below:

1. Bistable Comparator Test

Operation of bistable hysteresis resetpoints are verified using hysteresis test switches for each low steam

generator level bistable (see Figure 7.3-13). The bistable is placed in a tripped condition by test methods defined in Subsection 7.2.1.1.9.2, then the test input signal is increased until reset occurs.

2. Actuation Logic Test

This test verifies the proper operation of the AFAS actuating logic circuits (refer to Figure 7.3-13). The selective two-outof-three logic circuit, located in AFAS Cabinet, of each AFAS channel is tested in a manner identical to the Trip Path/Circuit Breaker System (see Subsection 7.2.1.1.9.5). One current leg of the selective two-out-of-three logic matrix is interrupted by opening one of the current legs contacts and loss of current in that current leg is verified. Each contact in both current legs is checked in this manner.

Initiation delay operation is tested using an initiation delay test switch (see Figure 7.3-13). One current leg of the selective two-out-of-three logic matrix is interrupted and loss of current in that leg is verified by the extinguishing of an AFAS panel indicator. Upon completion of the delay time period, the initiation delay function under test is automatically reset and the restoration of current is verified by the illumination of the panel indicator.

The manual trips are checked one at a time from the MAIN CONTROL BOARD and the lockout relay contacts are checked via the individual relay test system.

3. Actuating Device Test

Proper operation of the AFAS relays in the AFAS Cabinet is verified by deenergizing the relays one at a time via a test relay contact (see Figure 7.3-12) and noting the proper operation of all actuated components in that trip function (AFAS-1 or AFAS-2). The relay will automatically reenergize and return its components to the pretest condition when the test pushbutton is released.

The design of the test system is such that only one relay may be deenergized at a time. The test switch must be positioned to the function relays (AFAS-1 or AFAS-2) to be tested; selection of more than one function is impossible. The test circuit is electrically locked out upon actuation of a particular AFAS function.

e. Bypasses

1. Trip Channel Bypass

A bypass is provided to remove an AFAS function from one of the channels from service for maintenance or testing. The requisite two-out-of-three trip logic is unaffected by this bypass. The remaining trip functions in that channel are unchanged. The bypass is manually initiated and manually removed. The bypass is initiated by use of a pushbutton behind a key locked panel. When an AFAS is bypassed there is an audible and visible alarm to indicate which channel is being bypassed.

Based on the following considerations, Technical Specification action statements pertaining to one inoperable AFAS or AFW Isolation measurement channel were revised (via Technical Specification Amendment #132 and Engineering Evaluation PSL-ENG-SENS-00-024) to restrict the amount of time an inoperable channel could remain in a tripped condition. With one inoperable channel placed in trip, single failure of another AFW Isolation logic channel could compromise the rupture detection logic. This same Technical Specification Amendment also restricted the amount of time that either AFAS-1 or AFAS-2 could remain in bypass without bypassing both AFAS actuation functions in the affected channel. This change was also required to ensure the rupture detection logic could not be compromised by a postulated single failure.

2. Battery Fail Bypass

A bypass is provided upon battery failure defined as the loss of inverter output power to two AFAS channels. The bypass is automatically initiated and removed. Upon loss of power, the bypass is applied in one affected channel while the other affected channel trips. This results in a one-out-of-two trip logic for the remaining two unaffected channels. There is an audible and visible alarm to indicate which channel is bypassed. The automatic bypass operates on a priority basis in conjunction with trip channel bypass to preclude bypassing of more than one channel at a time.

f. Interlocks

Two interlocks are provided within the AFAS cabinet as follows:

1. Bypass Interlock - A priority bypass system prevents the operator from bypassing more than one AFAS function in a channel at a time.

2. Test System Interlock - A priority interlock prevents more than one channel of the AFAS from being tested at a time.

g. Sequencing

The AFAS simultaneously actuates the following AFW components:

1. The AFWS pumps and the Auxiliary Feedwater turbine inlet valves are latched on.

2. The AFWS isolation valves supplying feedwater to Steam Generator 2A and 2B are opened but are not latched.

   If a minimum pressure differential exists between steam generators or feedwater headers indicating a rupture, the associated AFWS isolation valves will remain closed. Once the steam generator level has reached its high level setpoint, the AFAS trip condition will no longer be generated, and the AFWS isolation valves will close.

3. The main feedwater isolation valves also utilize cycling relays, which close the isolation valves to the affected steam generator. After relay reset valve control is returned to the operator, however, the valve will remain closed.

Each AFAS actuates the components listed on Table 7.3-11. However, to ensure that the emergency diesel generator loads are properly assigned in the event of loss of offsite power, individual time relays are provided to delay starting of the equipment in accordance with the diesel generator sequence in Table 8.3-2.

h. Redundancy

Redundancy features for the AFAS-1 and AFAS-2 are similar to those described in Subsection 7.2.1.1.8.

i. Diversity

The system is designed to eliminate credible multiple channel failures originating from a common cause. The failure modes of redundant channels and the conditions of operation that are common to them are analyzed to assure that a predictable common failure mode does not exist.

The design provides reasonable assurance that the protective system cannot be made inoperable by the inadvertent actions of operating or maintenance personnel. The design is not encumbered with additional channels or components without reasonable assurance that such additions are beneficial.

The bistable and matrix relay cards found in the AFAS cabinets have a high level of diversity with respect to the relays found in the RPS. In general the AFAS relays have different types of reed switch assemblies than the RPS relays. These relays are the only area of concern identified by the NRC relevant to the mitigation requirement of the ATWS Rule (10 CFR 50.62) and they maintain diversity between the RPS and AFAS. It has been concluded that the different relay cards are sufficient to show compliance with the NRC ATWS Rule on auxiliary feedwater initiation, 10 CFR Part 50.62. (See Section 7.6.3.11)

j. Auxiliary Supporting Systems Required

The auxiliary supporting systems required are described in Subsection 7.3.1.1.6.

7.3.1.2 Design Basis Information

The ESFAS conforms to IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," and contains the following actuations:

a. Safety Injection Actuation Signal (SIAS) - De-energized to Actuate

b. Recirculation Actuation Signal (RAS) - Energized to Actuate

c. Containment Spray Actuation Signal (CSAS) - Energized to Actuate

d. Containment Isolation Actuation Signal (CIAS) - De-energized to Actuate

e. Main Steam Isolation Signal (MSIS) - De-energized to Actuate

f. Auxiliary Feedwater Actuation Signal - 1 (AFAS-1) - De-energize to Actuate

g. Auxiliary Feedwater Actuation Signal - 2 (AFAS-2) - De-energize to Actuate

Per Section 3 of IEEE 279-1971 "Design Basis", the design bases for the ESFAS are listed below:

<u>Basis 1</u>

Design basis events requiring protective actions are as follows:

a. Loss of Reactor Coolant - the actuating signals are SIAS, CIAS, CSAS, MSIS

b. Steam Generator Tube Rupture - the actuating signal is SIAS

c. Steam or Feedwater Line Break (Inside Containment) - the actuating signals are: SIAS, CSAS, CIAS, MSIS, AFAS-1, AFAS-2

d. Steam or Feedwater Line Break (Outside Containment) - the actuating signals are: MSIS, AFAS-1, AFAS-2

Basis 2

The station variables which must be monitored to provide protective actions are listed in Table 7.3-1.

Basis 3

None of the station variables referred to in Basis 2 are spatially dependent.

The locations of the ESFAS sensors are listed in Table 7.3-1.

Bases 4,5,6

Table 7.3-1 lists normal operating conditions, and the nominal actuation setpoints for the ESFAS monitored variables.

Basis 7,8

The ESFAS is designed to function so that:

a. The ranges of transient and steady-state conditions, during circumstances in which the system must perform, fall within the operating ranges of the equipment.

b. Any single failure does not prevent system action when required.

c. A loss of power to the measurement channels and/or to the logic system causes system actuation except for the containment spray and recirculation actuation signals.

d. The environmental conditions that accompany the design basis accident do not interfere with the ability of the systems to perform their safety function. Environmental design conditions for ESFAS instrumentation are discussed in Section 3.11.

e. The systems are designed to withstand safe shutdown earthquake loads without loss of their safety functions as discussed in Section 3.10,

Basis 9

a. ESFAS response times are discussed in UFSAR Table 13.7.2-2. For the CIAS Radiation Detectors, see Subsection 7.3.2.1.3.

b. Sensor accuracies and processing time delays are taken into account in the selection of each ESFAS trip setpoint. Response times and analysis setpoints used in the safety analysis are provided in Chapters 6 and 15. Accuracies and processing time are provided in appropriate vendor manuals and design calculations.

c. The ranges for the sensed variables that are accommodated by the ESFAS until proper conclusion of the protective action is assured as shown on Table 7.3-1.

In addition to conforming to IEEE 279-1971, the ESFAS meets the following design bases:

a. The systems meet the applicable criteria of 10 CFR 50, Appendix A and General Design Criteria as discussed in Subsection 7.3.2.1.1.

b. Channel independence is maintained by electrical and physical separations between redundant channels.

c. Equipment, including panels, components and cables associated with the protection system are uniquely identified.

d. The systems can be tested during reactor operation as far as practical without interrupting operation.

7.3.1.3 System Drawings

Control wiring diagrams, block diagrams, final logic diagrams, and location layout drawings are listed and provided by reference in Section 1.7.

7.3.2 ANALYSIS

7.3.2.1 Engineered Safety Feature Actuation System

The design of each of the ESF systems, including design bases and evaluation, is presented in Chapter 6. The ESFAS and the instrumentation addressed here are designed to provide the following protective functions:

a. Initiate automatic protective action to assure that acceptable RCS pressure and fuel performance guidelines are not exceeded.

b. Initiate automatic protective action, during certain postulated incidents of moderate frequency, infrequent events and limiting faults, to aid the ESF systems in mitigating the consequences of an accident.

7.3.2.1.1 Design

As previously described, the major portion of the ESFAS is functionally identical to the Reactor Protective System (RPS). Because of this, many of the responses to the requirements of the General Design Criteria, IEEE 279-1971 and IEEE 338-1971 are identical to the responses for the RPS. Where responses for the two systems are identical, reference is made to the appropriate section.

Section 3.1 provides a discussion of all General Design Criteria. This subsection describes how the requirements that are applicable to the ESFAS are satisfied.

Criterion 1: Quality Standards and Records

For a discussion of the Quality Assurance program, see Chapter 17.

Criterion 2: Design Bases For Protection Against Natural Phenomena

The design bases for protection against natural phenomena are described in Chapter 3.

Criterion 3: Fire Protection

For a discussion of separation criteria see Subsection 8.3.1. The design bases for fire protection is described in the Fire Protection Design Basis Document (Reference 1). EC282743

Criterion 4: Environmental and Missile Design Bases

Environmental design bases are described in Section 3.11. Missile design bases are described in Section 3.5.

Criterion 5: Sharing of Structures, Systems, and Components

No ESFAS components are shared with future or existing reactor facilities.

Criterion 10: Reactor Design

The ESFAS in conjunction with the plant control systems and Technical Specification requirements, provides sufficient margin to trip setpoints so that: (1) during normal operation spurious protective action is not initiated, and (2) during plant transients RCS pressure and fuel performance guidelines are not exceeded. Parameter actuation setpoints are shown in Table 7.3-1.

Criterion 13: Instrumentation and Control

Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls are provided to maintain these variables and systems within prescribed operating ranges.

Criterion 19: Control Room

Instrumentation and controls are provided in the control room to safely operate the plant under normal conditions and to maintain it in a safe condition under accident conditions. Emergency shutdown from outside the control room is described in Subsection 7.4.1.5.

Criterion 20: Protection System Functions

The ESFAS is designed to initiate automatically the operation of appropriate systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and to sense accident conditions and to initiate the operation of systems and components important to safety.

Criterion 21: Protection System Reliability and Testability

Functional reliability is ensured by compliance with the requirements of IEEE 279-1971. Testing is in compliance with IEEE 338-1971, and consistent with the recommendations of Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," 2/72 (R0).

Criterion 22: Protection System Independence

The ESFAS independence is assured through redundancy and diversity as described in Subsection 7.3.1.1.

Criterion 23: Protection System Failure Modes

Failure modes of the ESFAS components are discussed in Subsection 7.3.2.1.4.

Where protective action is required under adverse environmental conditions during certain incidents of moderate frequency, infrequent events and limiting faults, the ESFAS components are designed to function under such conditions.

Criterion 24: Separation of Protection and Control Systems

The ESFAS systems is separated from the control systems. No single failure of any control system component can impair the safety functions of ESFAS.

Criteria 34, 35, 37, 38, 40, 41, 43, 44 and 46

The ESF systems and the ESF support system are designed to comply with the above criteria. The instrumentation and control for these systems are discussed in Subsection 7.3.1.1.

Criteria 54, 55, 56, 57:

The instrument sensing lines for monitoring containment pressure are discussed in Subsection 7.1.2.2.

7.3.2.1.2 Equipment Design Criteria

IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," establishes minimum requirements for safety related functional performance and reliability of the ESFAS. This subsection describes how the requirements listed in Section 4 of IEEE 279-1971 are satisfied.

4.1 "General Functional Requirements"

The ESFAS is designed to automatically actuate the appropriate ESF systems, where required, and to mitigate the effects of a DBA. Instrument performance characteristics, response time, and accuracy are selected for compatibility with and adequacy for the particular function. Trip setpoints are established by analysis of the system parameters. Factors such as instrument inaccuracies, bistable trip times, valve travel time, and pump starting times are considered in establishing the margin between the trip setpoints and the safety limits. The time response of the sensors and protective systems are evaluated for abnormal conditions. Since uncertainty factors are considered as cumulative for the derivation of these times, the actual response time may be more rapid. However, even at the maximum time, the system provides conservative protection.

4.2 "Single Failure Criterion"

The ESFAS is designed so that any single failure within the system does not prevent proper protective action at the system level. Single failures considered include electrical faults (e.g.,

open, aborted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with the single failure criterion is accomplished by providing redundancy of power supplies and actuation circuits, and by separating the redundant elements electrically and physically to achieve the required independence. Each of these provisions is discussed below:

a. Redundancy

   The ESFAS consists of redundant subsystems and/or components for maximum system reliability. Each of the redundant components has automatic and/or manual actuation circuits which are separate from those provided for its redundant counterpart. Redundant instrumentation is provided to monitor ESFAS parameters.

b. Electrical Separation

   Electrical separation is achieved through the provision of independent power supplies and the elimination of electrical interconnection between redundant elements. Control power for redundant circuits is fed from separate 125V dc buses, through four redundant 125V dc to 120V ac inverters.

   The ac UPS power supply four channel concept is described in Subsection 7.2.1.1.10.

   The provision of separate power supplies and elimination of electrical connections between redundant circuits ensures that loss of power or electrical faults on any circuit cannot affect the redundant circuit.

c. Physical Separation

   Protection against the possibility of mechanical damage to both redundant portions of any instrumentation and control system required for the ESFAS is achieved by spatial separation and/or the provision of physical barriers between redundant elements.

   Physical separation within control panels is achieved by providing at least six inches of spatial separation between redundant circuitry or by a metal barrier. This separation is provided between control switches, bistables, relays and wiring necessary to actuate and control redundant components.

d. Cable trays and conduit containing redundant wiring and cables necessary to actuate and control redundant components are physically separated as discussed in Subsection 8.3.1.2.

e. The four channel independence is as described in Subsection 7.3.1.1.1h.

f. The redundant wiring and circuitry of the instrumentation and control systems required for ESFAS are marked and identified as described in Subsection 8.3.1.3.

The evaluation of the effects of specific single faults in the logic portion of the system included electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires,

missiles) resulting in mechanical damage. Compliance with the single failure criterion is accomplished by providing redundancy of sensors, measurement channels, logic matrices and actuation channels and separating these redundant elements electrically and physically to achieve the required independence.

4.3 "Quality Control of Components and Modules"

For a discussion of the Quality Assurance Program see Chapter 17.

4.4 "Equipment Qualification"

The ESFAS meets the equipment qualification requirements described in Sections 3.10 and 3.11.

4.5 "Channel Integrity"

Type testing of components, separation of sensors and channels, and qualification of cabling are utilized to ensure that the channels maintain the functional capability required under applicable extremes of conditions relating to environment, energy supply, malfunctions, and accidents.

Loss of or damage to any one path does not prevent ESF actuation. Sensors in lines are routed so that failure of any one line does not prevent timely ESF actuation. The components located in the containment are capable of operating in their specified environment described in Section 3.11.

4.6 "Channel Independence"

Channel independence is provided in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems," 1/75 (R1). The locations of the sensors, and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the channels, thereby precluding a situation in which a single event could remove or negate a protective function. Sensing lines are routed together in channel pairs. Redundant sensing lines are routed separately and are separated either by a barrier or a distance of four ft. These separations start from as close to the process taps as practical and continue out to the sensor mounting locations. This includes separation at the containment penetration areas. In the control room, protective system trip channels are located in individual compartments. Mechanical and thermal barriers between these compartments minimize the possibility of common event failure. Outputs from the components in this area to the control boards are isolated so that shorting, grounding, or the application of the highest available local voltages (120V ac, 125V dc) do not cause channel malfunction. Separate cabinets are provided in the control room for each of the ESFAS channels to separate components, logic and cable terminations associated with each channel.

Engineered safety features A and B actuating circuits are maintained independent with respect to signal interconnections for the AB shared system equipment control by both physical separation and electrical isolation.

Figure 7.3-11 shows this arrangement. A welded sheet metal box is located in each ESFAS logic cabinet and contains AB equipment actuation relays. These relays with 24 volt dc coils are hermetically sealed. The AB cables are routed from an AB tray through steel conduit to the AB1 and AB2 boxes and connected to the terminal boards. Tefzel insulated wires connect the

terminal board and relay contacts. The two relay coils are connected to a 2 out-of 4 actuation module which is used for AB relay only. A failure mode and effects for ESFAS AB system is given in Table 7.3-8. All other design concepts which meet the requirements of IEEE Standard 279-1971 and IEEE Standard 384-1977.

The isolation box is located in both the 9N38-5 and 9N38-6 cabinets and a single normally closed contact is used to provide a start signal to the C pump. The isolation characteristic is provided by a relay (coil to contacts) in each of the isolation boxes. The approximate isolation barrier is 500 volts ac or dc between the coil and contacts of this relay. The response time is approximately 12 milliseconds and the relay coil and contact wiring within the isolation box is routed so that the input (coil) and other (contacts) wires do not come in proximity.

4.7 "Control and Protection System Interaction"

No portion of the ESFAS is used for both control and protection functions.

4.8 "Derivation of Systems Inputs"

ESFAS inputs are derived from signals that are direct measures of the desired variables.

4.9 "Capability for Sensor Checks"

The ESFAS monitoring sensors are checked by comparing the monitored variables of redundant channels or by observing the effects of introducing and varying a substitute input to the sensor similar to the measured variable.

4.10 "Capability for Test and Calibration"

IEEE 338-1971 and Regulatory Guide 1.22 (R0) provides guidance for the development of procedures, equipment and documentation of periodic testing. The measurement signals for the ESFAS have the capability of being tested and calibrated under the design requirements of the system.

4.11 "Channel Bypass or Removal from Operation"

Any one of the four protective system channels may be tested, calibrated, or repaired without detrimental effects on the system. The single failure criterion is met during this condition. Redundant two channel systems are not bypassed during testing. Their tests are conducted in the actuated or safety position.

4.12 "Operating Bypasses"

Operating bypasses in the form of blocks for the SIAS and MSIS are discussed in Subsections 7.3.1.1.1 and 7.3.1.1.5, respectively. The operating by-passes are automatically removed when the permissive conditions are not met. The circuitry and devices which function to remove these inhibits are designed in accordance with IEEE 279-1971.

4.13 "Indication of Bypasses"

Indication of test or bypass conditions or removal of any channel from service is given by lights and annunciation at the system level and at the component level. Bypasses that are automatically removed at fixed setpoints are alarmed and indicated (see Table 7.3-10).

Conformance to ICSB 21 Position B.3, B.4, and B.5 can be summarized as follows:

B.3) St. Lucie Unit 2 ESF bypass indicating system provides availability (or bypass) indications of all ESF systems. These indications are at a system level. Means are not provided to cancel erroneous bypass indication. However, the operator can always assure the system status by cross checking the associated component operating status through their corresponding annunciation windows.

B.4) The ESF bypass indicating system is strictly status indication available to the control room operator. Based on the bypass informations and other related instrumentations, the operator can intelligently coordinate all maintenance/test activities throughout the plant, without compromising the plant safety.

B.5) Proper isolation devices are provided between the bypass indicating system and all safety-related systems to assure adverse effects cannot propagate from the indicating systems to the plant safety systems. Isolation devices are in accordance with Regulatory Guide 1.75 (R1).

4.14 "Access to Means for Bypassing"

The design of the ESFAS logic cabinets permits the administrative control of the means for manually bypassing measurement or actuation channels. The cabinets are located in the control room adjacent to the RTG boards. An administratively controlled key is required to permit only authorized access to the logic cabinets. Any channel that is bypassed is visibly indicated and annunciated on system and component level annunciators.

4.15 "Multiple Setpoints"

There are no multiple setpoints used for the ESFAS.

4.16 "Completion of Protective Action Once it Is Initiated"

The system is designed to ensure that protective action goes to completion once initiated.

4.17 "Manual Initiation"

For each ESFAS actuation a manual spring return switch and a "think" pushbutton is provided in each of the redundant channels. The operator must turn the switch while simultaneously pressing the "think" pushbutton in order to manually initiate the ESFAS channel. The switch and the pushbutton for each channel are located together on the control boards.

4.18 "Access to Setpoint Adjustments, Calibration and Test Points"

A key is required for access to setpoint adjustments, calibration and test points. Access is also visually and audibly annunciated. Setpoints are periodically checked during each periodic test.

4.19 "Identification of Protective Action"

Indication lights and/or annunciators are provided for identification of ESFAS status or trips in the control room.

4.20 "Information Readout"

Instruments are provided in the control room to allow the operator to monitor ESFAS measurement channel inputs. The specific displays that are provided for continuous monitoring are described in Subsection 7.5.1.

4.21 "System Repair"

Identification of a defective channel is accomplished by observation of system status lights or by testing as described in Subsection 7.3.1.1.1d. Replacement or repair of components is accomplished with the affected channel bypassed.

4.22 "Identification"

The ESFAS equipment, including panels, modules, and cables associated with the actuation system, are uniquely identified. Interconnecting cables are color coded on a channel basis (see Subsection 8.3.1.3).

7.3.2.1.3 Testing Criteria

IEEE 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Generating Station Protection Systems," and Regulatory Guide 1.22, (R0) provides guidance for development of procedures, equipment, and documentation of periodic testing. The basis for the scope and means of testing are described in this section. Test intervals and their bases are included in the Technical Specifications. Since operation of the ESF system, is not expected, the systems are periodically tested to verify operability. The system is tested from the sensor signal through the actuation devices. Complete channels can be individually tested without initiating protective action, without violating the single failure criterion, and without inhibiting the operation of the systems. The organization for testing and for documentation is described in Chapter 13.

Minimum frequencies for checks, calibration and testing of the ESFAS instrumentation are given in the Technical Specifications. Overlap in the checking and testing is provided to assure that the entire channel is functional.

The operability of the measurement channel sensors is verified during reactor operation by cross- checking between sensor output signals. Each of the ESFAS sensors has a control room readout and the operator can detect sensor malfunction through anomalous indication of the failed sensor.

Testing of ESFAS subgroup relays is performed on a staggered basis such that all relays are tested at least once every fuel cycle. Those components which cannot be tested during reactor operation because of their potential impact are tested during scheduled reactor shutdown.

During refueling the ESFAS sensors are checked and calibrated against known standards. The test equipment which is used to verify the sensor accuracies is checked periodically against

shop reference standards traceable to nationally recognized standards. The pressure and electronic calibration standards are as accurate or better than the devices to be checked.

Testing of ESFAS sensor response times is in accordance with Section 13.7.2.2 and the requirements of the Technical Specifications.

However, sensor response time testing is not required for the CIAS radiation detectors. This is because preoperational response time tests have shown that the response time is negligible with respect to the rest of the radiation detection system, and that this response will not change through the life of the detectors.

7.3.2.1.4 Failure Modes and Effects Analysis

Failure modes and effects analyses for the ESFAS are provided in Table 7.3-7. Figure 7.3-1 shows the typical logic, bistables, and isolation modules.

7.3.2.1.5 Consideration of Selected Plant Contingencies

a. Loss of Instrument Air System

None of the essential control or monitoring instrumentation is pneumatic. Electrical instrumentation is powered from the emergency power system. Therefore, the loss of instrument air does not degrade instrumentation and control systems required for shutdown of the plant.

b. Loss of Cooling Water to Vital Equipment

None of the instrumentation and controls required for safe shutdown rely on cooling water for operation. Air conditioning systems required to maintain the environment within the instrument design parameters are redundant and described in Sections 6.4 and 9.4.

REFERENCES

EC282743

1. DBD-FP-1, Fire Protection Design Basis Document.

TABLE 7.3-1

ESFAS SENSOR PARAMETERS AND SETPOINTS

Sensor	Location	Tag Nos.	Instrument[c] Range	Normal Operating Conditions	Nominal Actuation Setpoint
Pressurizer Pressure	See Table 1.7-1, Dwg. No. G226	PT-1102 A,B,C,D		2170-2330 psia	(a)
Containment Pressure	See Table 1.7-1, Dwg. No. G226	PT-07-2 A,B,C,D		0	(a)
Steam Generator Pressure	See Table 1.7-1. Dwg. No. G226	PT-8013 A,B,C,D PT-8023 A,B,C,D		815-915 psia	(a)
Steam Generator Delta Pressure	See Table 1.7-1. Dwg. No. G226	PT-8013 A,B,C,D PT-8023 A,B,C,D		0	(a)
Containment Radiation[b]	See Figures 1.2-8, 1.2-10 & 1.2-11	RD-26-3 RD-26-4 RD-26-5 RD-26-6		200 mR/hr	(a)
Refueling Water Tank Water Level	See Table 1.7-1, Dwg. No. G226	LT-07-2 A,B,C,D		32.5' to 38'	(a)
Feedwater Header Delta Pressure	Dwg. No. G226 Sh 3	PT-09- 9A,B,C,D PT-09-10A,B,C,D		0 psid	(a)
Steam Generator Level	See Table 1.7-1 Dwg No. G226	LT-9013A,B,C,D LT-9023A,B,C,D		65%	(a)

(a) Specific setpoint values are provided in the Technical Specifications.

(b) Due to the configuration of these detectors, response time testing is not required. Also see Subsection 7.3.2.1.3.

(c) Instrument ranges are selected in accordance with standard engineering practices.

TABLE 7.3-2

COMPONENTS ACTUATED ON SIAS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	Low Pressure Safety Injection Pump	2 A	x		1A
Start	Low Pressure Safety Injection Pump	2 B		x	1B
Start	High Pressure Safety Injection Pump	2 A	x		1A
Start	High Pressure Safety Injection Pump	2 B		x	1B
Open	LPSI Discharge Valve to Loop 2A-2	HCV-3615	x		2A
Open	LPSI Discharge Valve to Loop 2A-1	HCV-3625	x		2A
Open	LPSI Discharge Valve to Loop 2B-1	HCV-3635		x	2B
Open	LPSI Discharge Valve to Loop 2B-2	HCV-3645		x	2B
Open	HPSI Header A Disch. Valve to Loop 2A-2	HCV-3617	x		2A
Open	HPSI Header A Disch. Valve to Loop 2A-1	HCV-3627	x		2A
Open	HPSI Header A Disch. Valve to Loop 2B-1	HCV-3637	x		2A
Open	HPSI Header A Disch. Valve to Loop 2B-2	HCV-3647	x		2A
Open	HPSI Header B Disch. Valve to Loop 2A-2	HCV-3616		x	2B
Open	HPSI Header B Disch. Valve to Loop 2A-1	HCV-3626		x	2B
Open	HPSI Header B Disch. Valve to Loop 2B-1	HCV-3636		x	2B
Open	HPSI Header B Disch. Valve to Loop 2B-2	HCV-3646		x	2B
Close	HPSI Hot Leg Line Check Leak Drain Valve	V3572	x		3A
Close	S.I. Tank Test Line Valve to RWT	SE-03-2A	x		3A
Stop	Reactor Cavity Cooling Fan	HVS-2A	x		3A
Start Inhibit	Reactor Cavity Cooling Fan	HVS-2A	x		3A
Stop	Reactor Support Cooling Fan	HVE-3A	x		3A
Start Inhibit	Reactor Support Cooling Fan	HVE-3A	x		3A
Stop	CEDM Cooling Fan	HVE-21A	x		3A
Start Inhibit	CEDM Cooling Fan	HVE-21A	x		3A
Close	S.I. Tank 2A1 Recirc Drain Valve	HCV-3628	x		0A
Close	S.I. Tank 2A2 Recirc Drain Valve	HCV-3618	x		0A
Close	S.I. Tank 2B1 Recirc Drain Valve	HCV-3638		x	0B
Close	S.I. Tank 2B2 Recirc Drain Valve	HCV-3648		x	0B

TABLE 7.3-2 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	Diesel Generator	2 A	x		7A
Start	Diesel Generator	2 B		x	7B
Trip	Diesel Generator Breaker (for DG Loading)	2 A	x		8A
Trip	Diesel Generator Breaker (for DG Loading)	2 B		x	8B
Close	CCW to Fuel Pool HX Isolation Valve	MV-14-18	x		8A
Open Inhibit	CCW to Fuel Pool HX Isolation Valve	MV-14-18	x		8A
Close	CCW to Fuel Pool HX Isolation Valve	MV-14-17		x	8B
Open Inhibit	CCW to Fuel Pool HX Isolation Valve	MV-14-17		x	8B
Close	Hot Leg Line Check Valve Leak Drain Valve	V3571		x	3B
Stop	Reactor Cavity Cooling Fan	HVS-2B		x	3B
Start Inhibit	Reactor Cavity Cooling Fan	HVS-2B		x	3B
Stop	Reactor Support Cooling Fan	HVE-3B		x	3B
Start Inhibit	Reactor Support Cooling Fan	HVE-3B		x	3B
Stop	CEDM Cooling Fan	HVE-21B		x	3B
Start Inhibit	CEDM Cooling Fan	HVE-21B		x	3B
Close	Boric Acid Make-up Valve to VCT	V2512		x	6B
Open	Boric Acid Tank 2A Gravity Feed Valve to Charging Pumps	V2509		x	5B
Close Inhibit	Boric Acid Tank 2A Gravity Feed Valve to Charging Pumps	V2509		x	5B
Open	Boric Acid Tank 2B Gravity Feed Valve to Charging Pumps	V2508		x	5B
Close Inhibit	Boric Acid Tank 2B Gravity Feed Valve to Charging Pumps	V2508		x	5B
Close	Letdown Line Isolation Valve	V2516	x		0A
Close	Letdown Line Isolation Valve	V2515		x	0B
Close	VCT Discharge Valve	V2501		x	0B
Start	Component Cooling Water Pump	2 A	x		5A
Start	Component Cooling Water Pump	2 B		x	5B
Start	Component Cooling Water Pump	2 C	x	x	9A,9B
Close	CCW Header A Supply to Non-essential Header Isolation Valve	HCV-14-8A / 9		x	6A

TABLE 7.3-2 (Cont'd

Action	Component	Tag Number	Actuation Channel		Test Group
			A	B	
Override Close	CCW Hdr. Supply B to Non-essential Header Isolation Valve	HCV-14-8B/10		X	6B
Override Close	CCW Non-Essential Header Return to Hdr. A Isolation Valve	HCV-14-8A/9	X		6A
Close	CCW Non-essential Header Return to Hdr. B Isolation valve	HCV-14-8B/10		X	6B
Open	CCW Outlet Valve from Shutdown HX 2A	HCV-14-3A	X		5A
Open	CCW Outlet Valve from Shutdown HX 2B	HCV-14-3B		X	5B
Start	Intake Cooling Water Pump	2A	X		5A
Start	Intake Cooling Water Pump	2B		X	5B
Start	Intake Cooling Water Pump	2C	X	X	9A, 9B
Close	ICW Hdr. A Disch. to TCW Heat Exch. Isolation valve	MV-21-3	X		0A
Close	ICW Hdr. B Disch. to TCW Heat Exch. Isolation valve	MV-21-2		X	0B
Start Inhibit	RCP 2A-1 Oil Lift Pump	P-2A1-B		X	0B
Start Inhibit	RCP 2A-2 Oil Lift Pump	P-2A2-B	X		0A
Start Inhibit	RCP 2B-1 Oil Lift Pump	P-2B1-B	X		0A
Start Inhibit	RCP 2B-2 Oil Lift Pump	P-2B2-B		X	0B
Start	Reactor Aux. Bldg. Main Supply Fan	HVS-4A	X		1A
Start	Reactor Aux. Bldg. Main Supply Fan	HVS-4B		X	1B
Start	ECCS Area Exhaust Fan	HVE-9A	X		1A

TABLE 7.3-2 (Cont'd

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	ECCS Area Exhaust Fan	HVE-9B		x	1B
Open	Air Supply Dampers to ECCS Pump Room A	D-1, D-2	x		1A
Open	Air Supply Dampers to ECCS Pump Room B	D-3, D-4		x	1B
Close	ECCS Area Isolation Dampers	D-8A, D-9A	x		1A
Close	ECCS Area Isolation Dampers	D-8B, D-9B		x	1B
Close	ECCS Area Isolation Dampers	D-7A, 5A	x		1A
Close	ECCS Area Isolation Dampers	D-7B, 5B		x	1B
Close	ECCS Area Isolation Dampers	D-6A	x		1A
Close	ECCS Area Isolation Dampers	D-6B		x	1B
Close	ECCS Area Isolation Dampers	D-12A	x		1A
Close	ECCS Area Isolation Dampers	D-12B		x	1B
Start	Containment Fan Cooler	HVS-1A	x		8A
Start	Containment Fan Cooler	HVS-1B	x		8A
Start	Containment Fan Cooler	HVS-1C		x	8B
Start	Containment Fan Cooler	HVS-1D		x	8B
Close	RCP Cooling Water Supply Isolation Valve	HCV-14-1	x		0A
Close	RCP Cooling Water Supply Isolation Valve	HCV-14-7		x	0B
Close	RCP Cooling Water Return Isolation Valve	HCV-14-2	x		0A
Close	RCP Cooling Water Return Isolation Valve	HCV-14-6		x	0B
Close	Reactor Cavity Sump Pump Isolation Valve	LCV-07-11A	x		5A

TABLE 7.3-2 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Close	Reactor Cavity Sump Pump Isolation Valve	LCV-07-11B		x	5B
Open	Safety Injection Tank 2A1 Disch Valve	V3624	x		6A
Close Inhibit	Safety Injection Tank 2A1 Disch Valve	V3624	x		6A
Open	Safety Injection Tank 2A2 Disch Valve	V3614	x		7A
Close Inhibit	Safety Injection Tank 2A2 Disch Valve	V3614	x		7A
Open	Safety Injection Tank 2B1 Disch Valve	V3634		x	7B
Close Inhibit	Safety Injection Tank 2B1 Disch Valve	V3634		x	7B
Open	Safety Injection Tank 2B2 Disch Valve	V3644		x	8B
Close Inhibit	Safety Injection Tank 2B2 Disch Valve	V3644		x	8B
Close	Safety Injection Tank Fill and Drain Valves	SE-03-1A/V3621	x		2A
Close	Safety Injection Tank Fill and Drain Valves	SE-03-1B/V3611	x		2A
Close	Safety Injection Tank Fill and Drain Valves	SE-03-1C/V3631		x	2B
Close	Safety Injection Tank Fill and Drain Valves	SE-03-1D/V3641		x	2B
Close	Safety Injection Tank Test Line Valve to RWT	SE-03-2B		x	3B
Close	Boric Acid Supply Valve	FCV-2210Y	x		4A
Open Inhibit	Boron Load Control Valve	V2525		x	4B
Close	Boron Load Control Valve	V2525		x	4B
Start	Charging Pump 2A(1)	2A	x		4A
Close	Recirculation Valve to VCT	V2555	X		4A
Start	Charging Pump 2B(1)	2B		x	4B
Close	Recirculation Valve to VCT	V2554		x	4B
Start	Charging Pump 2C(1)	2C	x	x	9A,9B
Close	Recirculation Valve to VCT	V2553	x	x	9A,9B
Start	Boric Acid Make-up Pump 2A	2A	x		5A

TABLE 7.3-2 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	Boric Acid Makeup Pump	2B	x		5A
Close	Boric Acid Tank 2A Recirculation Line Valve	V2650	x		6A
Close	Boric Acid Tank 2B Recirculation Line Valve	V2651	x		6A
Open	Boric Acid Makeup Pump Bypass to Charging Pumps	V2514	x		5A
Close Inhibit	Boric Acid Makeup Pump Bypass to Charging Pumps	V2514	x		5A
Trip	4160 Swgr UV Interlock	2A3	x		7A
Trip	4160 Swgr UV Interlock	2B3		x	7B
Trip	Non-Essential Load		x		0A
Trip	Pressurizer Heater 2A3 Breaker	2A3	x		0A
Close Inhibit	Pressurizer Heater 2A3 Breaker	2A3	x		0A
Status	SAS Input		x		3A
Trip	Non-Essential Load			x	0B
Trip	Pressurizer Heater 2B3 Breaker	2B3		x	0B
Close Inhibit	Pressurizer Heater 2B3 Breaker	2B3		x	0B
Status	SAS Input			x	0B
Close	CCW Heat Exchanger Inlet Strainer Debris Discharge Valve	HCV-21-7A	x		6A
Close	CCW Heat Exchanger Inlet Strainer Debris Discharge Valve	HCV-21-7B		x	6B
Stop	Feedwater Pump 2A	2A1-3	x		3A, 8A
Stop	Feedwater Pump 2B	2B1-3		x	3B, 1B
Stop	Heater Drain Pump 2A	2A2-8	x		3A, 8A
Stop	Heater Drain Pump 2B	2B2-3		x	3B, 1B
Trip	Generator Main Leads (IPBD) Fan 2A	2A1-6D	x		3A, 8A
Trip	Generator Main Leads (IPBD) Fan 2B	2B1-2D		x	3B, 1B
Trip	Main Transformer 2A Coolers (Normal)	2A1-5C	x		3A, 8A
Trip	Main Transformer 2B Coolers (Normal)	2B1-2C		x	3B, 1B
Trip	Main Transformer 2A Coolers (Alternate)	2B1-1B		x	3B, 1B
Trip	Main Transformer 2B Coolers (Alternate)	2A1-6A	x		3A, 8A

TABLE 7.3-3

COMPONENTS ACTUATED ON RAS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Stop	LPSI Pump	2A	x		1A
Stop	LPSI Pump	2B		x	1B
Close	S.I. Pump Recirc. Line Valve to RWT	V3659	x		2A
Open Inhibit	S.I. Pump Recirc. Line Valve to RWT	V3659	x		2A
Close	S.I. Pump Recirc. Line Valve to RWT	V3660		x	2B
Open Inhibit	S.I. Pump Recirc. Line Valve to RWT	V3660		x	2B
Open	Containment Sump Outlet Valve to Recirc. Header A	MV-07-2A	x		4A
Alarm	Containment Sump Outlet Valve to Recirc. Header A	MV-07-2A	x		4A
Open	Containment Sump Outlet Valve to Recirc. Header B	MV-07-2B		x	4B
Alarm	Containment Sump Outlet Valve to Recirc. Header B	MV-07-2B		x	4B
Close	RWT Outlet Valve to S.I. Header A	MV-07-1A	x		3A
Alarm	RWT Outlet Valve to S.I. Header A	MV-07-1A	x		3A
Close	RWT Outlet Valve to S.I. Header B	MV-07-1B		x	3B
Alarm	RWT Outlet Valve to S.I. Header B	MV-07-1B		x	3B
Manual Start Permissive	LPSI Pump	2A	x		1A
Manual Start Permissive	LPSI Pump	2B		x	1B
Failure to Stop Alarm	LPSI Pump	2A	x		1A

TABLE 7.3-3 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Failure to Stop Alarm	LPSI Pump	2B		x	1B
Close	Minimum Flow Isolation Valve	V3495	x		5A
Close	Minimum Flow Isolation Valve	V3496		x	5B

TABLE 7.3-4

COMPONENTS ACTUATED ON CSAS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	Containment Spray Pump & Hydrazine Pump	2A	x		1A
Start	Containment Spray Pump & Hydrazine Pump	2B		x	1B
Open	Containment Spray Header A Inlet Valve	FCV-07-1A	x		2A
Open	Containment Spray Header B Inlet Valve	FCV-07-1B		x	2B
Resequence block 6 & 7	Diesel Generator Loading	2A	x		3A
Resequence block 6 & 7	Diesel Generator Loading	2B		x	3B
Open	Iodine Removal System Pump Isolation Valve	SE-07-3A	x		2A
Open	Iodine Removal System Pump Isolation Valve	SE-07-3B		x	2B

TABLE 7.3-5

COMPONENTS ACTUATED ON CIAS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Start	Shield Building Vent System Fan	HVE-6A	X		7A
Start	Shield Building Vent System Fan	HVE-6B		X	7B
Start	Control Room Isolation & Emergency Filtration System	HVE-13A FCV-25-16,17,18,24	X		7A
Start	Control Room Isolation & Emergency Filtration System	HVE-13B, FCV-25-14,15,19,25		X	7B
Start	Control Room Air Conditioning Unit (note 1)	HVA/ACC-3A	x		7A
Start	Control Room Air Conditioning Unit (note 1)	HVA/ACC-3B		x	7B
	(note 1) CRAC fan start required to support control room emergency filtration system function				
Close	Letdown Line Isolation Valve	V2516	X		0A
Close	Letdown Line Isolation Valve	V2522		X	0B
Close	RCS Sample Line Isolation Valve	V5200	X		1A
Close	RCS Sample Line Isolation Valve	V5203		X	1B
Close	RCS Surge Line Sample Isolation Valve	V5201	X		1A
Close	RCS Surge Line Sample Isolation Valve	V5204		X	1B
Close	Pressurizer Sample Line Isolation Valve	V5202	X		1A
Close	Pressurizer Sample Line Isolation Valve	V5205		X	1B
Close	Primary Water Line Isolation Valve	HCV-15-1		X	5B
Close	Safety Injection Tank Test Line Valve to RWT	SE-03-2A	X		1A
Close	Instrument Air Isolation Valve	HCV-18-1	X		OA
Close	Station Air Isolation Valve	HCV-18-2	X		5A
Close	Main Purge Inlet Isolation Valve	FCV-25-1	X		2A
Close	Main Purge Inlet Isolation Valve	FCV-25-3	X		2A
Close	Main Purge Inlet Isolation Valve	FCV-25-2		X	2B
Close	Main Purge Inlet Isolation Valve	FCV-25-5	X		2A
Close	Main Purge Inlet Isolation Valve	FCV-25-4		X	2B
Close	Main Purge Inlet Isolation Valve	FCV-25-6		X	2B

TABLE 7.3-5 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Stop	Containment Main Purge Exhaust Fan	HVE-8A	X		2A
Stop	Containment Main Purge Exhaust Fan	HVE-8B		X	2B
Close	Nitrogen Supply Isolation Valve	V6741		X	2B
Close	Waste Gas Header Isolation Valve	V6750	X		3A
Close	Waste Gas Header Isolation Valve	V6718		X	3B
Close	Reactor Cavity Sump Pump Discharge Isolation Valve	LCV-07-11A	X		4A
Close	Reactor Cavity Sump Pump Discharge Isolation Valve	LCV-07-11B		X	4B
Close	Containment Sample Isolation Valve	FCV-26-2,-4,-6	X		3A
Close	Containment Sample Isolation Valve	FCV-26-1,-3,-5		X	3B
Close	Steam Generator A Blowdown Isolation Valve	FCV-23-3	X		3A
Close	Steam Generator B Blowdown Isolation Valve	FCV-23-5	X		3A
Close	RCP Controlled Bleed-off Isolation Valve	V2505	X		0A
Close	Reactor Drain Tank Discharge Isolation Valve	V6341	X		4A
Close	Reactor Drain Tank Discharge Isolation Valve	V6342		X	4B
Close	Steam Generator A Blowdown Sample Isolation Valves	FCV-23-7 & 9	X		4A
Close	RCP Controlled Bleed-off Isolation Valve	V2524		X	0B
Open	Shield Building Ventilating System Isolation Valve	FCV-25-32	X		6A

TABLE 7.3-5 (Cont'd)

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Close Inhibit	Shield Building Ventilating Sys Isolation Valve	FCV-25-32	X		6A
Close	Safety Injection Tank Sample Isolation Valve	SE-05-1E	X		6A
Open Inhibit	Fuel Hdlg Bldg Emergency Ventilation Isol Valve	FCV-25-30	X		6A
Open Inhibit	Fuel Hdlg Bldg Emergency Ventilation Isol Valve	FCV-25-31		X	6B
Close	Fuel Hdlg Bldg Emergency Ventilation Isol Valve	FCV-25-30	X		6A
Close	Fuel Hdlg Bldg Emergency Ventilation Isol Valve	FCV-25-31		X	6B
Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-20	X		6A
Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-21		X	5B
Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-26	X		7A
Close	Continuous Containment/H_2 Purge Valve	FCV-25-36		X	6B
Override/Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-20	X		6A
Override/Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-21		X	5B
Override/Close	Continuous Containment/H_2 Purge Isol Valve	FCV-25-26	X		7A
Override/Close	Continuous Containment/H_2 Purge Valve	FCV-25-36		X	6B
Open	SBVS Isolation Valve	FCV-25-33		X	6B
Close Inhibit	Shield Building Ventilating Sys Isolation Valve	FCV-25-33		X	6B
Close	Safety Injection Tank Sample Isolation Valve	SE-05-1A SE-05-1B SE-05-1C SE-05-1D		X	6B
Close	Safety Injection Tank Test Line Valve to RWT	SE-03-2B		X	1B
Start	Unit 1 Control Room Isolation & Emergency Filtration System	HVE-13B, FCV-25-14,15,19 & 25		X	0B
Start	Unit 1 Control Room Isolation & Emergency Filtration System	HVE-13A, FCV-25-16,17,18 & 24	X		0A

TABLE 7.3-6

COMPONENTS ACTUATED ON MSIS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	Test Group
Close	Main Steam Line A Isolation Valve	HCV-08-1A	X	X(1)	0A
Close	Main Steam Line B Isolation Valve	HVC-08-1B	X(1)	X	0B
Close	Main Steam Isolation Valve A Bypass Valve	MV-08-1A	X	X(1)	1A
Open Inhibit	Main Steam Isolation Valve A Bypass Valve	MV-08-1A	X		1A
Close	Main Steam Isolation Valve B Bypass Valve	MV-08-1B	X(1)	X	1B
Open Inhibit	Main Steam Isolation Valve B Bypass Valve	MV-08-1B		X	1B
Close	Main FW Isolation Valve to SG 2A	HCV-09-1B	X(1)	X	0B
Open Inhibit	Main FW Isolation Valve to SG 2A	HCV-09-1B		X	0B
Close	Main FW Isolation Valve to SG 2B	HCV-09-2B	X(1)	X	0B
Open Inhibit	Main FW Isolation Valve to SG 2B	HCV-09-2B		X	0B
Close	Main FW Isolation Valve to SG 2A	HCV-09-1A	X	X(1)	0A
Open Inhibit	Main FW Isolation Valve to SG 2A	HCV-09-1A	X		0A
Close	Main FW Isolation Valve to SG 2B	HCV-09-2A	X	X(1)	0A
Open Inhibit	Main FW Isolation Valve to SG 2B	HCV-09-2A	X		0A
Status	SAS Input (MSIS-A)		X		0A
Status	SAS Input (MSIS-B)			X	0B

(1) Actuates through an isolation device

TABLE 7.3-7

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
FAILURE MODES AND EFFECTS ANALYSIS
ILLUSTRATION FIGURE 7.3-1
(3-Channels Operational 1-Channel Bypassed, See Note D)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
3	Pressurizer Pressure Sensing Circuit**	One spurious low signal (dropping to zero at output)	Open circuit, dc power failure, or shorted resistor (I/V converter)	Measurement channel pre-trip & trip alarms; meters indicate trip condition	Makes both channel Logics 1-out-of-2 to actuate (also makes SIAS & MSIS block permissive logic 2-out-of-f-2)	Notes A&B
3	Containment Pressure Sensing Circuit**					
3	Refueling Water Tank Level Sensor					
3	Steam Generator 2A Pressure Sensing Circuit**	One spurious high signal (reaching scale maximum at output)	Component failure, open resistor (I/V converter)	Test and comparison with redundant channel indicators; alarms	Makes both channel logics 2-out-of 2 (also makes SIAS & MSIS block permissive logic 3-out-of-2*)	Notes A&C
3	Steam Generator 2B Pressure Sensing Circiut**					
3	Pressurizer Pressure, Containment Pressure, SG 2A Pressure and SG 2B Pressure, Sensing Circuit Power Supply	One fails low	Open circuit, ac supply failure. Inverter failure	Measurement channel trip & pre-trip alarms; indicating meters read low. Power Loss alarm	Makes both channel logics 1-out-of-2 (also makes SIAS & MSIS block permissive logic 2-out-of2)	Notes A&B
3	RWT Level Sensor Power Supply	Failure of two on loss of one 125V dc battery	Open battery circuit	Alarms, Reactor & turbine-gen.trip.	Initiates SIAS, MSIS, CIS and makes one channel logic 1-out-of-1 or 1-out-of-2 for CSAS and RAS	Notes A,B&D
		One fails high	Component failure	Test and comparison with redundant channel indicators	Makes both channel logics 2-out-of-2 (also makes SIAS & MSIS block permissive logic 3-out-of 2)*	Notes A&C

Notes:
- A - Single failure with a measurement channel bypassed does not prevent system actuation.
- B - Immediate detection
- C - Possible immediate detection
- D - Bypassed measurement channel of the containment pressure or RWT level should be placed in trip mode or promptly restored to its operable status, in order to fulfill the logic for automatic actuation of the CSAS & RAS during a single failure of one battery
- * - SIAS & MSIS actuation cannot be blocked until bypassed channel of the pressurizer pressure of SG pressure is placed in trip mode.
- ** - Sensing circuit includes transmitter, converter and E/I converter.

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
3	Pressurizer Pressure SIAS Trip Bistable	One fails off	Open circuit, dc supply failure	Bistable indicator low reading	Makes both channel logics 1-out-of-2	Notes A&B
3	Containment Pressure SIAS Trip Bistable			Channel trip alarm; Auto test light & alarm		
3	Containment Pressure CIAS Trip Bistable					
		One fails on	Electronic circuit failure	Manual and automatic test	Makes both channel logics 2-out-of-2	Notes A&B
3	Containment Pressure CSAS Trip Bistable					
3	Refueling Tank Level RAS Trip Bistable			Automatic test light & alarm		
3	Containment Radiation CIAS Trip Bistable					
3	Steam Generator 2A Pressure MSIS Trip Bistable	Bistable removed	Bistable removed	Alarm when cabinet door opened	Makes both channel logics 2-out-of-2	Notes A&B
3	Steam Generator 2B Pressure MSIS Trip Bistable			Automatic test light and alarm Module removed alarm		
12	Isolation Module for Trip Block Bistables	One fails off	Electronic circuit damaged	Manual test	Makes one channel block logic 2-out-of-2	Note A
		One fails on	Open circuit	Manual test	Makes one channel block logic 3-out-of-2*	Note A
		Module removed	Module removed	Alarm when cabinet door opened; module removed alarm	Makes one channel block logic 2-out-of-2	Note A, B

Note: A - Single failure with a measurement channel bypassed does not prevent system actuation.

B - Immediate detection

* - SIAS & MSIS actuation cannot be locked until bypassed channel of the pressurizer pressure of SG pressure is placed in trip mode.

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
48	Isolation Module for Trip Bistables	One fails off	Electronic circuit Damaged	Manual and automatic test, auto test light & alarm	Makes one channel logic 1-out-of-2	Notes A&B
		One fails on	Electronic circuits Shorted	Automatic and manual test auto test light & alarm	Makes one channel logic 2-out-of-2	Notes A&B
		Module removed	Module removed	Alarm when cabinet door opened Module removed alarm; automatic test light & alarm	Makes one channel logic 1-out-of-2	Notes A&B
3	Containment Radiation Monitor	One spurious low signal	Open circuit, ac supply failure	Test and comparison with redundant channel indicators; meters read low	Makes both channel logics 2-out-of-2	Notes A&B
3	Containment Radiation MV/I Converter	One spurious high signal	Component failure	Measurement channel pre-trip & trip alarms: indicating meters read high	Makes both channel logics 1-out-of-2	Notes A&C
	I/V Converter					Notes A&B
6	Pressurizer Press. (R-1, 2)	One fails open	Component failure	Open resistor indicator reads high; measurement channel trip alarm	Makes both channel logics to actuate 1-out-of-2	
3	Containment Press. (R-6)				(Resistors R-1, 2, and 15, also make SIAS & MSIS block permissive logic 2-out-of-2)	
3	Containment Rad. (R-9)					
3	RWT Level (R-12)	One shorts	Short circuit	Indicator reads low; pre-trip alarm	None	Notes A&B
3	SG 2A Press (R-15)					
3	SG 2B Press (R-15 Typical)					

Notes:
- A - Single failure with a measurement channel bypassed does not prevent system actuation.
- B - Immediate detection
- C - Possible immediate detection

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
	I/V Converter					Notes
3	Pressurizer Press. (R-5)	One fails open	Component failure	Bistable indicator high reading	Makes both channel logics 2-out-of-2	A&C
3	Containment Press. (R-8)			Test and comparison with redundant channel indicators	(Resistors R-5, 14 make SIAS & MSIS block logic 3-out-of-2)*	
3	Containment Rad. (R-10)					
3	RWT Level (R-11)	One shorts	Short circuit	Bistable indicator low reading, channel trip alarm	Makes both channel logics 1-out-of-2	Notes A&B
3	SG 2A Press. (R-14)				(Resistors R-5, 14 also make SIAS & MSIS block logic (2-out-of-2)	
3	SG 2B Press. (R-14 typical)					

Notes: A - Single failure with a measurement channel bypassed does not prevent system actuation.

B - Immediate detection

C - Possible immediate detection

* - See note page 7.3-41.

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
3	Pressurizer Pressure SIAS Trip Block Bistable	One fails off	Open circuit, dc supply failure	Manual test	Makes both channel logics 2-out-of 2	Note A
3	Steam Generator 2A Pressure MSIS Trip Block Bi-stable	One fails on	Electronic circuit failure	Manual test	Makes both channel logics 3-out-of 2*	Note A
3	Steam Generator 2B Pressure MSIS Trip Block Bi-stable	Module removed	Module removed	Alarm when cabinet door opened; module removed alarm	Makes both channel logics 3-out-of 2*	Notes A&B
	2-out-of-4 Matrix and Actuation Module:	One fails off	Open circuit, dc supply failure	ESFAS channel actu-ation alarm	De-energizes output relays and starts components associated with failed test group	Notes A&B
2	SIAS A, B Test Group 0					
2	SIAS A, B Test Group 1					
2	SIAS A, B Test Group 2	One fails on	Electronic circuit shorted	Manual and auto-matic test	Prevents auto starts of components asso-ciated with failed test group	Notes A&B
2	SIAS A, B Test Group 3					
2	SIAS A, B Test Group 4					
2	SIAS A, B Test Group 5			Alarm test light & alarm		
2	SIAS A, B Test Group 6					
2	SIAS A, B Test Group 7	Module removed	Module removed	Alarm when cabinet door opened	De-energizes output re-lays and starts compon-ents associated with failed test group	Notes A&B
2	SIAS A, B Test Group 8					
2	SIAS A, B Test Group 9					

Notes: A - Single failure with a measurement channel bypassed does not prevent system actuation.

B - Immediate detection

* - See note on page 7.3-41

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
2	CIAS A, B Test Group 0					
2	CIAS A, B Test Group 1	One fails off	Open circuit, dc supply failure	ESFAS channel actu-ation alarm	De-energizes output relays and starts components with failed test group	Notes A&B
2	CIAS A, B Test Group 2					
2	CIAS A, B Test Group 3	One fails on	Electronic circuit shorted	Manual and auto-matic test	Prevents auto starts of components associated with failed test group	Notes A&B
2	CIAS A, B Test Group 4					
2	CIAS A, B Test Group 5			Auto test light & alarm		
2	CIAS A , B Test Group 6					
2	CIAS A, B Test Group 7	Module removed	Module removed	Alarm when cabinet door opened	De-energizes output re-lays and starts compon-ents associated with failed test group	Notes A&B
2	MSIS A, B Test Group 0					
2	MSIS A, B Test Group 1					
	2-out-of-4 Matrix and Actuation Module	One fails on	Electronic circuits shorted	ESFAS channel actuation alarm	Energize output re-lays and starts com-ponents associated with failed Test Group	Notes A&B
2	CSAS A, B Test Group 1					
2	CSAS A, B Test Group 2					
2	CSAS A, B Test Group 3					
2	RAS A, B Test Group 1					
2	RAS A, B Test Group 2					
2	RAS A, B Test Group 3	One fails off	Component failure	Manual-auto test	Prevents auto start of components asso-ciated with failed Test Group	Notes A&B
2	RAS A, B Test Group 4			Auto test light & alarm		
2	RAS A, B Test Group 5					

Notes: A - Single failure with a measurement channel bypassed does not prevent system actuation.

B - Immediate detection

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
		Module removed	Module removed	Alarm when cabinet door opened. Automatic test light & alarm	Prevents auto start of components associated with failed Test Group	Notes A&B
	3-out-of 4 Matrix and Actuation Module	One fails on	Electronic circuit shorted	Block permissive indication & alarm	Completes permissive signal for manual block of SIAS or MSIS on one channel only	Notes A&B
2	SIAS, A, B Block		dc supply failure			
2	MSIS, A, B Block					
		One fails off	Component failure	Manual test	Prevents SIAS or MSIS channel block	Notes A&C
		Module removed	Module removed	Alarm when cabinet door opened	Prevents SIAS or MSIS channel block	Notes A&B
	Pushbutton "think":	One fails open	Component failure	Manual test	Blocks ESFAS channel manual actuation	Notes A&C
2	SIAS A, B			Pushbutton and control switch actuated alarm		
2	CIAS A, B					
2	RAS A, B	One fails closed	Component failure	Pushbutton and control switch actuated alarm	None	Notes A&B
2	CSAS A, B					
2	MSIS A, B					

Notes
- A - Single failure with a measurement channel bypassed does not prevent system actuation.
- B - Immediate detection
- C - Possible immediate detection

TABLE 7.3-7 (Cont'd)

OPERATIONAL COMPONENTS	NAME	FAILURE MODE	FAILURE MECHANISM	DETECTION	EFFECTS ON ESFAS LOGIC	REMARKS
	Control Switch	One fails open	Component failure	Manual Test	Blocks ESFAS channel manual actuation	Notes A&C
2	SIAS A, B			Pushbutton and control switch actuated alarm		
2	CIAS A, B					
2	RAS A, B	One fails closed	Component failure	Pushbutton and control switch actuated alarm	None	Notes A&B
2	CSAS A, B					
2	MSIS A, B					
	Output relays:	One relay coil fails open or shorted. Contacts fail in actuated position	Component failure	Component running lights on control board on.	Starts components assigned to this relay	Notes A&B
36	SIAS A, B					
4	CIAS A, B	One relay's contacts fail to actuate	Component failure	Manual test	Prevents automatic start of components assigned to this relay	Note A
4	MSIS A, B					
	Output relays:	One relay coil fails open or shorted. Contacts fail to actuate.	Component failure	Manual test	Prevents auto start of components assigned to this relay	Note A
6	CSAS A & B					
10	RAS A, B	One relay's contacts fail in actuated position	Component failure	Component running lights on control board on	Starts components assigned to this relay	Notes A&B

Notes:
- A - Single failure with a measurement channel bypassed does not prevent system actuation.
- B - Immediate detection
- C - Possible immediate detection

TABLE 7.3-8

ESF SIGNAL INTERCONNECTIONS FOR AB SHARED SYSTEM
EQUIPMENT CONTROL-FAILURE MODE ANALYSIS

Component	Function	Failure Mode	Effects on ESF System	Detection	Failure Mechanism	Remarks
AB Equipment Control Board	Centralized Control of AB Equipment	AB Control Power Failure	AB Equipment Control Lost	Circuit Monitoring, Alarms, Indicating Lights	Open Circuits Or Cables Power Supply Failure	Immediate Detection ESF A and B Not Effected
		Control Power High Voltage or Fire	AB Equipment Control Lost Including Relay Contact Failure in Relay Boxes AB1 & AB2		Imposed High Voltage on AB Circuits Relay Coils, Shorted Wires	Possible Immediate Detection ESF A & B System Not Effected
ESF Logic Cabinet SA	Centralized ESF A & AB Initiation	Control Power Failure	Failure or ESF A & AB Initiation, or Spurious Initiation	Various Alarms	Power Supply Failure Electronic Components Shorted	Immediate Detection ESF B System Not Effected
		Fire			Shorted Wires	
ESF Logic Cabinet SB	Centralized ESF B & AB Initiation	Control Power Failure	Failure of ESF B & AB Initiation or Spurious Initiation	Various Alarms	Power Supply Failure Electronic Components Shorted	Immediate Detection ESF A System Not Effected
		Fire			Shorted Wires	
Box AB1 Located in ESF Cabinet SA	Provides Separation Between A & AB	Fire	Failure of ESF AB Initiation	Various Alarms	Shorted Wires Faulty Relays	Immediate Detection ESF A & B System Not Effected
Box AB2 Located in ESF Cabinet SB	Provides Separation Between B & AB	Fire	Failure of ESF AB Initiation	Various Alarms		Immediate Detection ESF A & B System Not Effected

Table 7.3-9

MSIV ISOLATION CIRCUIT FAILURE MODE ANALYSIS

Item	Power Supply	Function	Failure Mode & Effect	Detection	Failure Mechanism	Meets Single Failure Criteria
1	125 VDC supply MSIV A Control Circuit	Provides power for HCV-08-1A closing circuit	Low HCV-08-1A remains open but inoperational	Control room alarm	Open fuse, CKT ground test	Yes. HCV-08-1B will operate on MSIS-A or MSIS-B. FW isolation valves will operate also.
2	125 VDC Supply to isolation relay 29/312 circuit	Provides power to MSIS A signal isolation to train B	Low Disables MSIS-A signal to train B	Control room alarm	Open fuse, CKT ground test	Yes. MSIS A will close valve HCV-08-1A & train A FW isolation valves. MSIS B will operate both trains.
3	125 VDC Battery A	Provides power through MA & MC inverters to ESFAS A train	Low Train A valves inoperational. Train B MSIS is spuriously actuated. Note (2)	Control room alarm	Battery A or 125 VDC bus failure	Yes. MSIS B will close HCV-08-1B & train B FW isolation valves.

Notes:

(1) Train B similar
(2) MSIS B trip logic 2 out of 4 (2 out of 3) is spuriously actuated by de-energizing MA & MC ESFAS measurement cabinet bistables & isolation modules.

TABLE 7.3-10

ESF BYPASSES OR INOPERABLE INDICATION SYSTEM

Channel	Bypass Indication Window	System	Bypassed Components Causing Automatic Indication	Connection From	Manual Capability To Activate Bypass Indication	Remarks
A	1	L.P. Safety Injection	Diesel Generator 2A LPSI Pump 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator	Yes	
A	2	H.P. Safety Injection	Diesel Generator 2A CCW Header HPSI Pump 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
A	3	Charging and Boron	Diesel Generator 2A Charging Pump 2A Boric Acid Make-up Pump 2A Boric Acid Make-up Pump 2B 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator Annunciator Annunciator	Yes	
A	4	Control Room Habita-bility	Diesel Generator 2A Control Room Air Conditioning 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator	Yes	
A	5	Aux. Building H&V	Diesel Generator 2A RRAB Exhaust Fans RAB Supply Pans 125V DC Battery 2A BKR Open	Annunciator HVCB HVCB Annunciator	Yes	
A	6	Containment Spray	Diesel Generator 2A CCW Header Containment Spray Pump 2A 125VDC Battery 2A BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
A	8	Containment Vacuum Relief	Cont. Vacuum Relief Va. Contr. Pwr. Cont. Vacuum Relief Air Low Press.	HVCB Annunciator	Yes	
A	9	Containment Air Cooler	Diesel Generator 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator	Yes	
			CCW Header Containment Air Recirc. Coolers	Annunciator Annunciator	Yes	
A	10	Main Steam Isolation	Diesel Generator 2A Main Steam Isolation Valve 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator	Yes	

TABLE 7.3-10(Cont'd)

Channel	Bypass Indication Window	System	Bypassed Components Causing Automatic Indication	Connection From	Manual Capability To Activate Bypass Indication	Remarks
A	11	Recirc. Actuation	Diesel Generator 2A Refueling Water Tank Valve Containment Sump Valve 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
A	12	Fuel Pool Emerg Vent	Diesel Generator 2A Fuel Bldg Emerg Vent 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator	Yes	
A	13	H_2 Systems	Diesel Generator 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator	Yes	
A	14	Shield Bldg. Vent	Diesel Generator 2A Shield Bldg Vent Exh. Fan 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator	Yes	
A	15	Aux. Feed Water	Diesel Generator 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator	Yes	
A	16	Spare			Yes	
A	17	Spare				
A	18	Spare				
A	19	Spare				
A	20	Component Cooling Water	Diesel Generator 2A Intake Cooling Water Pump 2A Component Cooling Water Pump 2A 125V DC Battery 2A BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
B	1	L.P. Safety Injection	Diesel Generator 2B LPSI Pump 2B 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator	Yes	
B	2	H.P. Safety Injection	Diesel Generator 2B CCW Header HPSI Pump 2B 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
B	3	Charging and Boron	Diesel Generator 2B Charging Pump 2B Boric Acid Gravity Valves 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator Annunciator	Yes	

TABLE 7.3-10(Cont'd)

Channel	Bypass Indication Window	System	Bypassed Components Causing Automatic Indication	Connection From	Manual Capability To Activate Bypass Indication	Remarks
B	4	Control Room Habitability	Diesel Generator 2B Control Room Air Conditioning 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator	Yes	
B	5	Aux. Building H&V	Diesel Generator 2B RAB Exhaust Fans RAB Supply Fans 125V DC Battery 2B BKR Open	Annunciator HVCB HVCB Annunciator	Yes	
B	6	Containment Spray	Diesel Generator 2B CCW Header Containment Spray Pump 2B 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
B	8	Containment Vacuum Relief	Cont. Vacuum Relief Va. Contr. Pwr. Cont. Vacuum Relief Va. Air Low Press.	HVCB Annunciator	Yes	
B	9	Containment Air Cooler	Diesel Generator 2B CCW Header Contain Air Recirc. Coolers 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
B	10	Main Steam Isolation	Diesel Generator 2B Main Steam Isolation Valve 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator	Yes	
B	11	Recirc. Actuation	Diesel Generator 2B Refueling Water Tank Valve Containment Sump Valve 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
B	12	Fuel Pool Emerg Vent	Diesel Generator 2B Fuel Bldg Emerg. Vent Valve 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator	Yes	
B	13	H_2 Systems	Diesel Generator 2B 125V DC Battery 2B	Annunciator Annunciator	Yes	
B	14	Shield Bldg Vent	Diesel Generator 2B Shield Bldg. Exh. Fan 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator	Yes	

TABLE 7.3-10(Cont'd)

Channel	Bypass Indication Window	System	Bypassed Components Causing Automatic Indication	Connection From	Manual Capability To Activate Bypass Indication	Remarks
B	15	Aux. Feed Water	Diesel Generator 2B 125V DC Battery 2B BKR Open	Annunciator Annunciator	Yes	
B	16	Spare				
B	17	Spare				
B	15	Spare				
B	19	Spare				
B	20	Component Cooling Water	Diesel Generator 2B Intake Cooling Water Pump 2B Component Cooling Water Pump 2B 125V DC Battery 2B BKR Open	Annunciator Annunciator Annunciator Annunciator	Yes	
C	1	Charging and Boron	Charging Pump 2C	Annunciator	Yes	
C	2	Control Room Habita-bility	Cont. Room Air Cond Sys. C	Annunciator	Yes	
C	3	Spare				
C	4	Component Cooling Water	Intake Cooling Water Pump 2C Component Cooling Water Pump 2C	Annunciator Annunciator	Yes	

TABLE 7.3-11
COMPONENTS ACTUATED BY AFAS

Action	Component	Tag Number	Actuation Channel A	Actuation Channel B	AFAS
Start(1)	AFW Pump	2A	X		AFAS-1
Start(1)	AFW Pump	2B		X	AFAS-2
Open/Close	AFW Pump 2A Disch to SG 2A	MV-09-9	X		AFAS-1
Open/Close	AFW Pump 2B Disch to SG 2B	MV-09-10		X	AFAS-2
Open/Close	AFW Pump 2C Disch to SG 2A	MV-09-11		X	AFAS-1
Open/Close	AFW Pump 2C Disch to SG 2B	MV-09-12	X		AFAS-2
Open(1)	STM From SG 2B to AFWP 2C	MV-08-12	X		AFAS-2 or AFAS 1
Open(1)	STM From SG 2A to AFWP 2C	MV-08-13		X	AFAS-1 or AFAS 2
Open/Close	AFW Pump 2A Disch to SG 2A	SE-09-2	X(2)		AFAS-1
Open/Close	AFW Pump 2B Disch to SG 2B	SE-09-3		X(3)	AFAS-2
Open/Close	AFW Pump 2C Disch to SG 2A	SE-09-4		X(3)	AFAS-1
Open/Close	AFW Pump 2C Disch to SG 2B	SE-09-5	X(2)		AFAS-2
Close	MFIV to SG 2A	HCV-09-1A	X		AFAS-1*
Close	MFIV to SG 2A	HCV-09-1B		X	AFAS-1*
Close	MFIV to SG 2B	HCV-09-2A	X(2)		AFAS-2*
Close	MFIV to SG 2B	HCV-09-2B		X(3)	AFAS-2*

* The AFAS may be overridden and the valve re-opened by the control room operator only during 2-EOP-06, total loss of feedwater.

(1) Indicates components that are latched. All other components are unlatched (cycling).
(2) Indicates that components are actuated by Channel C which is diverse from Channel A for single failure considerations.
(3) Indicates that components are actuated by Channel D which is diverse from Channel B for single failure considerations.

TABLE 7.3-12
AUXILIARY FEEDWATER ACTUATION SYSTEM
FAILURE MODES AND EFFECTS ANALYSIS

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
1 Feedwater header pressure sensor-1 (Channel A, Typical)	a. Fails off (low pressure Signal)	Sensor failure, open circuit, D/C power supply failure	Low P_1 pressure signal to $P_1 < P_2$ differential pressure bistable. Bistable changes logic state and initiates input to the channel A AFAS1 block circuit.	Annunciating, pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS1 becomes 2-out-2 coincident. The block logic becomes 1-out-of-2 coincident.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel function.
	b. Fails as is	Sensor failure, component failure	Erroneous P_1 pressure signal to $P_2 < P_1$ differential pressure bistable during actual SG1 trip. Bistable changes logic state and initiates input to channel A AFAS2 block circuit when SG2 trips.	Annunciating, pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 2-out-of-2 coincident. The block logic becomes 1-out-of-2 coincident.	Same as above
	c. Fails on (high pressure signal)	Sensor failure, component failure	Erroneous high P_1 pressure signal to $P_2 < P_1$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS2 block circuit.	Annunciating, pre-trip and trip alarms.	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 2-out-of-2 coincident. The block logic becomes 1-out-of-2 coincident.	Same as above
2 Feedwater header pressure sensor-2	a. Fails off	Sensor failure, open circuit, D/C power supply failure	Low P_2 pressure signal to the $P_2 < P_1$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS2 block circuit.	Annunciating, pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 2-out-of-2 coincident. The block logic becomes 1-out-of-2 coincident.	Same as above
	b. Fails as is	Sensor failure, component failure	Erroneous P_2 pressure signal to the $P_1 < P_2$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS1 block circuit.	Annunciating, pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS1 becomes 2-out-of-2 coincident. The block logic becomes 1-out-of-2 coincident.	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	c. Fails on	Sensor failure, component failure	Erroneous high P_2 pressure signal to $P_1 < P_2$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS1 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Same as above	Same as above
3 Steam Generator 1 pressure sensor	a. Fails off	Sensor failure, open circuit, D/C power supply failure	Low P_1 pressure signal to $P_1 < P_2$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS1 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS1 becomes 2-out-of-2 coincident. Block logic becomes 1-out-of-2 coincident.	Same as above
	b. Fails as is	Sensor failure, component failure	Erroneous P_1 pressure signal to $P_2 < P_1$ differential pressure bistable during actual SG1 trip. Bistable changes logic state and initiates input to channel A AFAS2 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 2-out-of-2 coincident. Block logic becomes 1-out-of-2 coincident.	Same as above
	c. Fails on	Sensor failure, component failure	Erroneous high P_1 pressure signal to $P_2 < P_1$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS2 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Same as above	Same as above
4 Steam Generator 2 Pressure sensor	a. Fails off	Sensor failure, open circuit, D/C power supply failure	Low P_2 pressure signal to $P_2 < P_1$ differential pressure bistable. Bistable changes logic state and initiates input to Channel A AFAS2 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 2-out-of-2 coincident. Block logic becomes 1-out-of-2 coincident.	Same as above
	b. Fails as is	Sensor failure component failure	Erroneous P_2 pressure signal to $P_1 < P_2$ differential pressure bistable during actual SG2 trip. Bistable changes logic state and initiates input to channel A AFAS1 block circuit	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS1 becomes 2-out-of-2 coincident. Block logic becomes 1-out-of-2 coincident.	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	c. Fails on	Sensor failure, component failure	Erroneous high P_2 pressure signal to $P_1 < P_2$ differential pressure bistable. Bistable changes logic state and initiates input to channel A AFAS1 block circuit.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Same as above	Same as above
5 Steam Generator 1 low-level sensor	a. Fails off	Sensor failure, component failure	Low steam generator level signal to Lo LVL SG1 bistable Bistable changes logic state and initiates input to channel A AFAS1 block circuit and actuation logic.	Annunciating pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS1 becomes 1-out-of-2 coincident. No effect on block logic.	Same as above
	b. Fails on	Sensor failure, component failure	High steam generator level signal to Lo LVL SG1 bistable. Will not trip for actual lo level.	Periodic test 3-channel comparison.	3-channel redundancy (4th channel in bypass)	AFAS1 logic becomes 2-out-of-2 coincident	Same as above
6 Steam Generator 2 low-level sensor	a. Fails off	Sensor failure, component failure	Low steam generator level signal to Lo LVL SG2 bistable. Bistable changes logic state and initiates channel A AFAS2 block circuit/and actuation logic.	Annunciating, pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Actuation logic for AFAS2 becomes 1-out-of-2 coincident. No effect on block logic.	Same as above
	b. Fails on	Sensor failure, component failure	High steam generator level signal to Lo LVL SG2 bistable. Will not trip for actual Lo level.	Periodic test, 3-channel comparison	3-channel redundancy (4th channel In bypass)	AFAS2 logic becomes 2-out-of-2 coincident.	Same as above
				BISTABLES			
7 SG1 lo level bistable (Channel A Typical)	a. Setpoint power fails off	Component failure open circuit	SG1 level setpoint drops to zero. Bistable will not change state on valid Lo level signal.	Power supply annunciator	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 2-out-of-2 coincident.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel and then by pass the failed Channel function.

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	b. Trip set-point fails low	Component failure	Same as 7a.	Same as 7a.	Same as 7a.	Same as 7a.	Same as above
	c. Trip set-point fails high	Component failure	Bistable will trip at greater than desired SG1 level	Annunciation if bistable is tripped. Periodic test.	3-channel redun-dancy (4th channel in bypass)	AFAS1 actuation logic becomes 1-out-of-2 coin-cident.	Same as above
	d. Trip vol-tage com-parator fails off	Open circuit, component failure	Bistable relays will deenerg-ize resulting in half trips of the AB, AC and AD actuation logic matrices.	Annunciating	3-channel redun-dancy (4th channel in bypass)	AFAS1 actuation logic becomes 1-out-of-2 coin-cident.	Same as above
	e. Trip vol-tage com-parator fails on	Component failure, short circuit	Bistable relays will not de-energize for valid SG1 lo level signal.	Periodic test, 3-channel com-parison.	3-channel redun-dancy (4th channel in bypass)	AFAS1 actuation logic becomes 2-out-of-2 coinci-dent.	Same as above
	f. Pre-trip setpoint fails low or off	Component failure, open circuit	Pre-trip setpoint decreases Pre-trip relays will not de-energize when SG1 at desired pre-trip level.	Periodic test, 3-channel com-parison	3-channel redun-dancy (4th channel in bypass)	No impact on AFAS1 actuation logic.	Same as above
	g. Pre-trip setpoint fails high	Component failure	Pre-trip relays will de-energize at higher than desired SG1 level.	Pre-trip alarm and test. 3-channel comparison	None required	Spurious pre-trip alarms. No impact on AFAS1 actuation logic.	Same as above
	h. Pre-trip voltage comparator fails off	Open circuit, component failure	Same as 7g.	Same as 7g.	Same as 7g.	Same as 7g.	Same as above
	i. Pre-trip voltage comparator fails on	Component failure	Pre-trip relays will not de-energize when SG1 level reaches pre-trip setpoint.	Periodic test, 3-channel com-parison	3-channel redun-dancy (4th channel in bypass)	No impact on AFAS1 actuation logic.	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	j. Pre-trip opto-isolator fails off	Open circuit, component failure	Pre-trip relay will de-energize	Annunciating pre-trip alarm	None required	No impact on AFAS1 actuation logic.	Same as above
	k. Pre-trip relay driver fails off	Open circuit, component failure	Same as 7j.	Same as 7j.	Same as 7j.	Same as 7j.	Same as above
	l. Pre-trip relay driver fails on	Emitter to collector short circuit	Same as 7i.	Same as 7i.	Same as 7i.	Same as 7i.	Same as above
	m. Pre-trip relay coil fails open	Mechanical failure	Same as 7j.	Same as 7j.	Same as 7j.	Same as 7j.	Same as above
	n. Pre-trip relay contact in annunciator circuit fails open	Mechanical damage, corrosion	Channel A pre-trip will not annunciate.	Periodic test, 3-channel comparison	Visual indicator not affected. 3-channel redundancy (4th channel in bypass).	No impact on AFAS1 actuation logic	Same as above
	o. Pre-trip relay contact in annunciator circuit fails closed	Contact arcing	Spurious pre-trip alarms	Annunciating	None required	AFAS1 actuation logic not affected	Same as above
	p. Pre-trip relay contact in indicator circuit fails open	Mechanical damage, corrosion	No visual indication of channel A pre-trip.	Periodic test	Annunciator not affected. 3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic not affected -	Same as above
	q. Pre-trip relay contact in indicator circuit fails closed	Contact arcing	Spurious pre-trip visual indications	Visual pre-trip indication	None required	AFAS1 actuation logic not affected	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	r. Trip opto-isolator fails off	Component failure, open circuit	Bistable relays will de-energize resulting in half trips of the AB, AC and AD actuation logic matrices.	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 1-out-of-2 coincident.	Same as above
	s. Trip opto-isolator fails on	Component failure, short circuit	Bistable relays will not de-energize on valid low level signal	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 2-out-of-2 coincident.	Same as above
	t. Trip relay driver fails off	Transistor failure, open circuit.	One bistable relay de-energizes resulting in spurious half trips in AB, AC or AD logic matrices or spurious trip indication	Annunciation indication	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 1-out-of-2 coincident.	Same as above
	u. Trip relay driver fails on	Emitter to collector short circuit	Affected relay will not de-energize for valid low level signal. One logic matrix (AB, AC or AD) will not de-energize	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 2-out-of-2 coincident.	Same as above
	v. Trip relay coil fails open	Mechanical failure	Same as 7t.	Same as 7t.	Same as 7t.	Same as 7t.	Same as above
	w. Trip relay form c contacts to SG1 Rupture identification circuit fails to N.C. pole	Contacts welded by arcing, fuse failure	Relay initiates input to the channel A block circuit.	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	No effect on AFAS1 actuation logic or on block logic.	Same as above
	x. Trip relay form c contacts to SG1 Rupture ID Circuit fails open	Open circuit	Channel A block circuit can not be activated.	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	No effect on AFAS1 actuation logic, block logic becomes 2-out-of-2 coincident.	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	y. Trip relay form c contact to AFAS1 fails to N.O. Pole	Contacts welded	Relay will not de-energize on actual Lo level signal.	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	AFAS1 logic becomes 2-out-of-2 coincident no effect on channel A block logic	Same as above
	z. Trip relay form c contact to AFAS1 fails to N.C. pole	Contacts welded	One relay will de-energize resulting in half trips of AB, AC or AD actuation logic matrix and initiating input to channel A block circuit.	Annunciating	3-channel redundancy (4th channel in bypass)	No effect on AFAS block logic. AFAS1 actuation logic becomes 1-out-of-2	Same as above
	aa. Trip relay form c contacts in trip annunciator circuit fails to N.O. Pole	Contacts welded	Annunciator will not signal relay coil or relay driver failure.	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic not affected	Same as above
	ab. Trip relay form c contacts in trip annunciation circuit fails to N.C. Pole	Contacts welded, fuse failure	Spurious relay coil or relay driver failure indications	Annunciating	None required	AFAS1 actuation logic not affected	Same as above
	ac. Pre-Trip Opto-Isolator fails on	Component Failure Short Circuit	Bistable relays will not de-energize on valid low level signal	Periodic test 3 channel comparison	None required	No impact on AFAS1 actuation logic	Same as above
	ad. Bistable Hysteresis voltage fails high	Component Failure	Bistable will reset at greater than desired SG1 level	Periodic test	3-channel redundancy (4th channel in Bypass)	AFAS1 reset logic becomes 1-out-of-2 coincident	Same as above
	ae. Bistable Hysteresis voltage fails low	Component Failure	Bistable will reset at less than desired SG1 level.	Periodic test	Same as 7ad	Same as 7ad	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	af. Bistable Hysteresis voltage analog switch fails open	Component Failure Open Circuit	Bistable will reset at less than desired SG1 level. For reset before actuation, reset level will equal trip level, resulting in relay cycling	Periodic test	Same as 7ad	Same as 7ad	Same as above
	ag. Bistable Hysteresis voltage analog switch fails closed	Component Failure Short Circuit	Bistable will trip at greater than desired SG1 level	Periodic test	Same as 7ad	AFAS 1 actuation logic becomes 1-out-of-2 coincident	Same as above
8 SG2 Lo level bistable			Failure modes and effects on AFAS2 actuation logic for lo steam generator level trips are equivalent to the failure modes and effects on AFAS1 actuation logic provided in line item 7, failure modes a through ag.				
9 Pressure SG1< SG2 bistable	a. Setpoint power fails off or low	Component failure, open circuit	Setpoint level goes to zero bistable relays de-energize for any $P_1<P_2$ signal resulting in input to channel A block circuit.	Anunciating	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic becomes 1-out-of-2 coincident	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel and then bypass the failed channel function.
	b. Setpoint power fails high	Component failure, short circuit	Bistable relays will not de-energize for valid Lo ΔP	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic for SG 1 ΔP becomes 2-out-of-2. Block logic for FWH ΔP not affected.	Same as above
	c. Trip setpoint fails low	Component failure	Same as 9a.	Same as 9a.	Same as 9a.	Same as 9a.	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	d. Trip set-point fails high	Component failure	Same as 9b.	Same as 9b.	Same as 9b.	Same as 9b.	Same as above
	e. Process "A" input buf-fer fails off or low	Component failure, open circuit	SG1 pressure signal goes to zero. Trip and pre-trip com-parators de-energize bistable relays and initiates input to channel A block circuit.	Same as 9a.	Same as 9a.	Same as 9a.	Same as above
	f. Process "A" input buf-fer fails high	Component failure,short circuit	SG1 pressure signal goes high. Bistable will not change logic state for valid pressure dif-ferential.	Periodic test	3-channel redun-dancy (4th channel in bypass)	AFAS 1 block logic for SG1ΔP becomes 2-out-of-2. Block logic for FWH ΔP not affected	Same as above
	g. Process "B" input buf-fer fails off or low	Component failure, open circuit	SG2 pressure goes negative. Bistable will not change logic state for valid signal	Periodic test	3-channel redun-dancy (4th channel in bypass)	AFAS 1 block logic for SGΔP becomes 2-out-of-2	Same as above
	h. Process "B" input buf-fer fails high	Component fai-lure, open circuit	SG2 pressure goes high. Bist-able relays de-energize result-ing in input to channel A block circuit	Annunciating	3-channel redun-dancy (4th channel in bypass)	AFAS 1 block logic becomes 1-out-of-2 coinci-dent	Same as above
	i. Pre-trip setpoint fails low or off	Component failure	Pre-trip setpoint increases pre-trip relays will not de-energize at desired pre-trip level	Periodic test	3-channel redun-dancy (4th channel in bypass)	No impact on AFAS1 block logic. Spur-ious pre-trip alarms	Same as above
	j. Pre-trip setpoint fails high	Component failure	Pre-trip relays will de-energize at higher than de-sired pressure differential	Pre-trip alarm and periodic test	None required	No impact on AFAS1 block logic. Spur-ious pre-trip alarms.	Same as above
	k. Pre-trip voltage comparat-or fails off	Component failure, open circuit	Pre-trip relays de-energize at higher than desired SG2A pre-trip pressure	Pre-trip alarm and test	None required	Spurious pre-trip alarms no impact on AFAS1 block logic	Same as above
	l. Pre-trip voltage comparat-or fails on	Component failure, short circuit	Pre-trip relays will not de-energize at desired pre-trip setpoint	Periodic test	3-channel redundancy (4th channel in bypass)	No impact on AFAS1 block logic.	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	m. Pre-trip opto-isolator fails off	Open circuit, component failure	Pre-trip relay will de-energize	Annunciating pre-trip alarm	None required	No impact on AFAS1 block logic.	Same as above
	n. Pre-trip relay driver fails off	Component failure, open circuit	Same as 9m.	Same as 9m.	Same as 9m.	Same as 9m.	Same as above
	o. Pre-trip relay driver fails on	Emitter to collector short circuit	Same as 9l.	Same as 9l.	Same as 9l.	Same as 9l.	Same as above
	P. Pre-trip relay coil fails open	Mechanical failure	Same as 9m.	Same as 9m.	Same as 9m.	Same as 9m.	Same as above
	q. Pre-trip relay contact in annunciator fails open	Mechanical damage, corrosion	Channel A pre-trip will not annunciate.	Periodic test	3-channel redundancy (4th channel in bypass) visual indicator not affected	No impact on AFAS 1 block logic.	Same as above
	r. Pre-trip relay contact in annunciator fails closed	Contact arcing	Spurious channel A pre-trip alarms	Annunciating	None required	AFAS1 block logic not affected.	Same as above
	s. Pre-trip relay contact in indicator circuit fails open	Mechanical damage, corrosion	No visual indication of channel A pre-trip	Periodic test	Annunciator not affected 3-channel redundancy (4th channel in bypass)	AFAS1 block logic not affected.	Same as above
	t. Pre-trip relay contact in indicator circuit fails closed	Contact arcing	Spurious channel A pre-trip indications	Visual pre-trip indication	None required	AFAS1 block logic not affected	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	u. Trip voltage comparator fails off	Open circuit, component failure	Bistable relays will de-energize resulting in input to AFAS1 block circuit	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic becomes 1-out-of-2 coincident	Same as above
	v. Trip voltage comparator fails on	Component failure	Bistable relays will not de-energize for valid pressure differential signal	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic for SGΔP becomes 2-out-of-2 coincident	Same as above
	w. Trip opto-isolator fails off	Component failure, open circuit	Bistable relays will de-energize resulting in input to channel A AFAS1 block circuit	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic becomes 1-out-of-2 coincident	Same as above
	x. Trip relay driver fails off	Transistor failure, open circuit	Bistable relay de-energizes resulting in input to channel A AFAS1 block circuit	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic becomes 1-out-of-2 coincident	Same as above
	y. Trip relay driver fails on	Emitter to collector short circuit	Affected relay will not be able to de-energize for valid signals	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS 1 block logic for SGΔP becomes 2-out-of-2 coincident	Same as above
	z. Trip relay coil fails open	Mechanical failure	Same as 9x.	Same as 9x.	Same as 9x.	Same as 9x.	Same as above
	aa. Trip relay form c contacts to SG1 Rupture identification circuit fails to N.C. pole	Contacts welded by arcing, fuse failure	Bistable relay de-energizes resulting in input to channel A AFAS1 block circuit	Periodic test	3-channel redundancy (4th channel in bypass)	No impact on AFAS1 actuation logic. Block logic becomes 1-out-of-2 coincident.	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	ab. Trip relay form c contacts to SGI Rupture identi-fication circuit fails to N.O. pole	Contacts welded	Relay cannot activate channel A, block circuit	Periodic test	3-channel redundancy (4th channel in bypass)	No effect on AFAS1 block logic	Same as above
	ac. Trip annuncia-tor relay form c contacts fail to N.O. pole	Contacts welded	Annunciator will not signal relay coil or relay driver failure	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	No effect on AFAS1 block logic	Same as above
	ad. Trip annuncia-tor relay form c contacts fail to N.C. pole	Contacts welded, fuse failure	Spurious relay coil or relay driver failure indications	Annunciating	None required	AFAS1 block logic not affected	Same as above
10 Pressure SG2<SG1 Bistable			Failure modes and effects on AFAS2 block logic for pressure SG2<SG1 trips are equivalent to the failure modes and effects on AFAS1 block logic provided in line item 9, failure modes a through ad.				
11 Pressure FWH1<FWH2 Bistable			Failure modes and effects for pressure FWH1<FWH2 trips are equivalent to the failure modes and effects provided in line item 9, failure modes a through ad.				
12 Pressure FWH2<FWH1 bistable			Failure modes and effects on AFAS2 block logic for pressure FWH2<FWH1 trips are equivalent to the failure modes and effects on AFAS1 block logic provided in line item 9, failure modes a through ad.				
13 AFAS1 bistable card	a. One trip relay driver fails off	Transistor failure, open circuit	One bistable relay de-energ-izes resulting in half trip of AB, AC or AD logic matrix.	Indication in affected logic matrix	3-channel redundancy (4th Channel In bypass)	AFAS1 actuation logic remains 2-out-of-3 coinci-dence, with 1-out-of-2 selective coincidence between unaffected channels	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	b. One trip relay driver fails on	Emitter to collector short circuit	Affected relay will not de-energize for valid signal	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS actuation logic becomes 2-out-of-2 coincident	Same as above
	c. One trip relay coil fails	Mechanical failure	Same as 13a	Same as 13a	Same as 13a	Same as 13a	Same as above
	d. One trip relay form c contact to 2/4 logic matrix fails to N.C. pole	Contacts welded, component failure	Channel A AFAS 1 test coils will de-energize resulting in half trips of the AB, AC and AD logic matrices	Visual indication	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 1-out-of-2 coincident	Same as above
	e. One trip relay form c contact to 2/4 logic matrix fails to N.O. pole	Contacts welded	Channel A AFAS 1 test coils will not de-energize for valid signal	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic becomes 2-out-of-2 coincident	Same as above
	f. One trip relay form c con tact to trip annuncia-tor circuit fails to N.O. pole	Contacts welded	Annunciator will not signal relay coil or relay driver failure	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS1 actuation logic not affected	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	g.One trip form c contact to trip annun. circuit falls to N.O. pole	Contacts welded	Spurious relay coil or relay driver failure indications	Annunciating	None required	AFAS1 not affected	Same as above
14 AFAS2 bistable card			Failure modes and effects on AFAS2 actuation logic for AFAS2 bistable trips are equivalent to the failure modes and effects on AFAS 1 actuation logic provided in line item 13. Failure modes a through g.				
			LOGIC MATRICES - AB TYPICAL				
15 Logic matrix relay driver	a. Fails off	Transistor failure, open circuit	One matrix relay de-energizes inducing a trip via the time Delay circuitry in one of four AFAS trip paths	Visual indicator	A minimum of two trip paths must be de-energized to produce a trip	AFAS actuation logic remains 2-out-of-3 coincident	Same as 9a
	b. Fails On	Emitter to collector short circuit	One logic matrix relay will not de-energize on a valid signal coincidence	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS actuation logic remains 2-out-of-3 coinci-dent. Affected logic matrix can still generate a trip to other three circuits	Same as above
16 Logic matrix relay coil	a. Fails open	Open circuit	One matrix relay de-energizes inducing a trip via the time delay circuitry in one AFAS 1 trip path	Visual indication	A minimum of two trip paths must be de-energized to produce a trip	AFAS actuation logic remains 2-out-of-3 coincident	Same as above
	b. Short-ed	Hot Short	Affected matrix relay will not de-energize on valid signal	Periodic test	3-channel redundancy (4th channel in bypass)	Same as above	Same as above
17 One Logic matrix relay contact in trip path	a. Fails open	Open circuit mechanical damage corrosion	One matrix relay de-energizes inducing a trip via the time delay circuitry in one of four trip paths	Visual indication	A minimum of two trip paths must be de-energized to produce a trip	AFAS actuation logic remains 2-out-of-3 coincident	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	b. Fails closed	Contact weld	One matrix relay will not de-energize on a valid signal coincidence	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS actuation logic remains 2-out-of-3 coincident. Affected logic matrix can still generate a trip with other relays	Same as above
18 One logic matrix indicator lamp	a. Fails off	Broken filament	Spurious indication that one matrix relay is de-energized	Annunciating visual indication	None required	No effect on AFAS trip logic	Same as above
	b. Fails on	Hot short	No indication of matrix relay failure or de-energization.	Periodic test	None required	Same as above	Same as above
19 one matrix power supply	a. Fails off or low	Component failure, open circuit	Loss of one power supply	Annunciating visual indication	Second power supply provides power to logic matrix relays	No effect on AFAS trip logic.	Same as above
	b. Fails high	Component failure	Possible overstress of 2-out-of-4 logic matrix relays. Relays may fail open and logic matrix may become half-tripped	Visual indication if matrix fails open	Same as above	Same as above	Same as above
20 Logic matrix power supply diode	a. Fails open	Overstress, mechanical damage	Loss of one of two matrix power supplies	Power supply trouble alarm, visual indication	Same as above	Same as above	Same as above
	b. Shorted	Overstress	No impact during normal operation, loss of isolation for power supplies	Periodic test	Redundant power supplies	No impact on AFAS trip logic	Same as above
21 Logic matrix power supply fuses	Fail open	Overstress mechanical damage	Loss of one of two matrix power supplies	Power supply trouble alarm, visual indication	Redundant power supplies	AFAS actuation logic remains 2-out-of-3 coincident	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
22 Logic matrix power supply indicator lamp	Fails off	Open filament	Spurious visual indication of failure of one logic matrix power supply	Visual indication, no alarm	None required	No impact on AFAS trip logic	Same as above
23 Logic matrix power supply trouble annunciator relay	Fails open	Overstress, mechanical damage open circuit	Spurious logic matrix power supply alarms	Annunciating	None required	No impact on AFAS trip logic	Same as above
24 Logic matrix power supply trouble annunc. relay contact	a. Fails open	Mechanical damage, open circuit, corrosion	Same as above	Same as above	Same as above	Same as above	Same as above
	b. Fails closed	Contact weld	Power supply trouble alarm will not sound if power supply fails	None, if power supply fails then visual indication no alarm	Visual power supply operabi-lity indication	No impact on AFAS trip logic	Same as above
			INITIATION CIRCUIT - CHANNEL A TYPICAL				
25 Remote manual pushbutton	a. Fails open	Mechanical damage, open circuit	Initiation relays for one AFAS will de-energize and initiate input to the AFAS	Visual indication and annunciation actuation circuit.	A minimum of two trip paths must be de-energized in actuation circuit to Produce a trip	AFAS for one leg will become 1-out-of-3 selective In actuation circuit to pro-duce a trip.	Same as 9a
	b. Fails closed	Contact weld short circuit	Unable to de-energize channel A initiation relays for one AFAS by using pushbutton	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS for one leg becomes 2-out-of-3 selective	Same as above
26 Initiation relay	Fails open	Open circuit	One initiation relay de-energizes and initiates input to one leg of actuation circuit.	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS remains 2-out-of-3 coincident initiation logic becomes 1-out-of-3 selective	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
27 Initiation relay contacts in actuation circuit	a. Fails open	Open circuit corrosion, mechanical damage	One train of AFAS will open	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS remains 2-out-of-3 coincident with initiation logic becoming 1-out-of-3 selective	Same as above
	b. Fails closed	Contact weld, short circuit	AFAS1-A actuation relay will not de-energize to actuate AFAS1-A equipment.	Periodic test	Parallel redundancy in channel.	AFAS remains 2-out-of-3 coincident with initiation logic becoming 2-out-of-3 selective	Same as above
ACTUATION CIRCUIT - CHANNEL A TYPICAL							
28 Actuation power supply	a. Fails off or low	Component failure, open circuit	Loss of power from one power supply for one set of actuation relays and bistables	Annunciating and visual indication	Power to each bistables and actuation circuits of each channel is provided by two auctioneered supplies. If one fails the other will meet requirements	No effect on AFAS logic	Same as 9a
	b. Fails high	Component failure	Loss of power from one power supply for one set of actuation relays and bistables	Annunciating if relays fail and visual indication	Automatic overvoltage protection, redundant power supply unaffected	No effect on AFAS logic	Same as above
29 Actuation power supply diode	a. Fails open	Overstress, mechanical damage	Loss of one of two power supplies for one set of actuation relays	Power supply trouble alarm, visual indications	Redundant power supply	No effect on AFAS logic	Same as above
	b. Shorted	Overstress	No impact in normal operation loss of isolation for one power supply	Periodic test	Redundant power supply	No effect on AFAS logic	Same as above
30 Auctioneering diode	a. Fails open	Overstress, mechanical damage	Loss of power from one power supply to one set of actuation relays	Annunciating visual indication	Redundant power supply	No effect on AFAS logic	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	b. Shorted	Overstress	Loss of isolation between power supplies possible short of both power supplies which initiates actuation of equipment associated with channel A AFAS.	Periodic test, visual indication	Will not force delivery of aux. feedwater or inhibit delivery of aux. feedwater due to actuation of equipment.	No effect on AFAS logic	Same as above
31 Actuation circuit indicator lamp	Fails off	Burnt filament mechanical damage	Spurious visual indication that one leg of actuation circuit has opened	Visual indication	None required	No effect on AFAS logic	Same as above
32 Local Manual Actuation Switch	a. Fails open	Mechanical damage. Open Circuit	AFAS1-A actuation	Annunciating	AFAS1 not fully actuated Only channel MA components	AFAS1-A actuated AFAS2 unaffected	Same as above
	b. Fails closed	Contact weld, mechanical damage	Manual actuation will not open one leg of actuation circuit	Periodic test	Automatic actuation not affected	No manual actuation of one leg of AFAS	Same as above
33 Lockout reset push button	a. Fails open	Mechanical damage	No impact in normal operation. Unable to reset channel MA actuation Relays after test or actuation.	Periodic test	Automatic actuation and manual initiation not affected r l	No effect on AFAS logic	Same as above
	b. Fails closed	Contact weld mechanical damage	No impact in normal operation, automatic reset of channel MA Activation relays.	Periodic test	Automatic actuation and manual initiation not affected	AFAS logic not affected.	Same as above
34 Lockout relay coil	a. Fails open	Open circuit, overstress, mechanical damage	One actuation leg opens	Annunciating	Opposite actuation leg will provide power to actuation relays	A No effect on AFAS o logic	Same as above
	b. Shorted	Mechanical damage. Open Circuit	AFAS1-A actuation A	Annunciating	AFAS1 not fully actuated Only channel MA components t	AFAS1-A actuated AFAS2 unaffected d	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
35 Lockout relay N.O. contact	a. Fails open	Open circuit, mechanical damage	One actuation leg opens	Annunciating	Opposite actuation leg provides power to actuation relays	ANo effect on oAFAS logic	Same as above
	b. Fails closed	Contact weld, mechanical damage	Equipment will cycle with relays	Periodic test	Automatic actuation and manual initiation not affected	AFAS logic not affected	Same as above
36 Lockout indication lamp	Fails off	Burnt filament, mechanical damage	Spurious visual indication that one lockout relay is de-energized	Visual indication	None required	No effect on AFAS logic	Same as above
37 Actuation relay coil	a. Fails open	Mechanical damage. Open Circuit	AFAS1-A actuation a A	Annunciating	AFAS1 not fully actuated Only channel MA components a	AFAS1-A actuated AFAS2 unaffected r 3 c	Same as above
	b. Shorted	Mechanical short	Actuation relay will not hold contacts, one pump or one valve will be actuated in one AFAS train	Visual indication	Same as above	Same as above	Same as above
38 Actuation relay indicator N.C. contacts	a. Fail closed	Contact weld, mechanical damage	Unable to test actuation of one pump or valve in one AFAS train	Periodic test	None required	No effect on AFAS logic	Same as above
	b. Fails open	Mechanical damage	One valve or one pump will be actuated in one AFAS train	Visual indication	One component will be actuated full train will not be actuated by failure of one actuation relay	AFAS actuation remains 2-out-of-3 coincidence	Same as above
39 Actuation relay indicator N.O. contacts	a. Fail closed	Contact weld mechanical damage	Spurious indication of failed actuation relay	Visual indication	None required	No impact of AFAS logic	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	b. Fails open	Mechanical damage open circuit	No indication of actuation relay failure	Periodic test	None required	No impact on AFAS logic	Same as above
40 Time Delay Circuitry	a. Timer fails fails off or slow	Component Failure	Timer will not deenergize initiation relays if it fails off. Time delay will be increased if timer fails slow	Periodic test.	3-channel redundancy (4th channel in bypass)	AFAS 1 remains 2-out-of-3 coincident with initiation logic becoming 2-out-of-3 selective	Same as above
	b. Timer Fails fast	Component Failure	Timer will deenergize initiation relays before desired delay	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS 1 remains 2-out-of-3 coincident with initiation logic becoming 1-out-of-3 selective after timer has timed out	Same as above
	c. Time delay relay driver fails off	Transistor failure, open circuit	Time delay relay will de-energize resulting in the de-energization of the associated initiation relays	Visual inspection	A minimum of 2 trip paths must be deenergized to produce a trip	AFAS 1 remains 2-out-of-3 coincident with initiation logic becoming 1-out-of-3 selective	Same as above
	d. Time delay relay driver fails on	Emitter to collector short circuit	Affected relay will not de-energize for valid signal	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 40a	Same as above
	e. Time delay coil fails open	Mechanical Failure	Same as 40c	Same as 40c	Same as 40c	Same as 40c	Same as above
	f. Time delay relay contact to initiation circuit fails to N.O. pole	Contacts welded, component failure	Initiation relays in affected trip path will not be deenergized on valid signal	Periodic test	Same as 40a	Same as 40a	Same as above
	g. Time delay relay contact to initiation circuit fails to N.C. pole	Component failure	Initiation relays will be de-energized	Visual Indication	Same as 40c	Same as 40c	Same as above

* SG2A is SG1
SG2B is SG2

** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

TABLE 7.3-12 (Cont'd)

Name*	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method ** Of Detection	Inherent Compensating Provision	Effect Upon AFAS	Remarks And Other Effects
	h. Opto-Isolator between timer and analog fails off	Component failure Open circuit	Analog switch in normally open state providing continuous hysteresis voltage to bistable comparator, associated bistable will trip at greater than desired SG1 level	Periodic test	Same as 40a	AFAS 1 actuation logic becomes 1-out-of-2 coincident	Same as above
	I. Opto-isolator between time and analog switch fails on	Component failure, short circuit	Timer timing-out will not change state of analog switch. Associated bistable will reset at less than desired SG1 level	Periodic test	Same as 40a	AFAS 1 reset logic becomes 1-out-of-2 coincident	Same as above
	j. Time delay analog switch fails closed	Component failure, short circuit	Associated bistable will trip at greater than desired SG1 level	Periodic test	Same as 40a	Same as 40i	Same as above
	k. Time delay analog switch fails high	Component failure, open circuit	Associated bistable will reset at lower than desired SG1 level	Periodic test	Same as 40a	Same as 40h	Same as above
	l. Time delay hysteresis voltage fails high	Component failure	Same as 40j	Periodic test	Same as 40a	Same as 40i	Same as above
	m. Time delay hysteresis voltage fails low	Component failure	Same as 40k	Periodic test	Same as 40a	Same as 40h	Same as above
	n. Hysteresis voltage summer output fails high	Component failure	Same as 40j	Periodic test	Same as 40a	Same as 40i	Same as above
	o. Hysteresis voltage summer output fails low	Component failure	Same as 40k	Periodic test	Same as 40a	Same as 40h	Same as above

* SG2A is SG1
SG2B is SG2
** Pre-trip & trip annunciation consists of local light indication & sequence of events printout.

Refer to Drawings
2998-3956 and 2998-3957

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BLOCK DIAGRAM -
ENGINEERED SAFEGUARDS
LOGIC SYSTEM
FIGURE 7.3-1

Refer to Drawing
2998-B-327 SH 372

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

CONTROL WIRING DIAGRAM
PRESSURIZER PRESSURE P-1102A
MEASUREMENT LOOP
FIGURE 7.3-2

DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-3

DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-4

DELETED

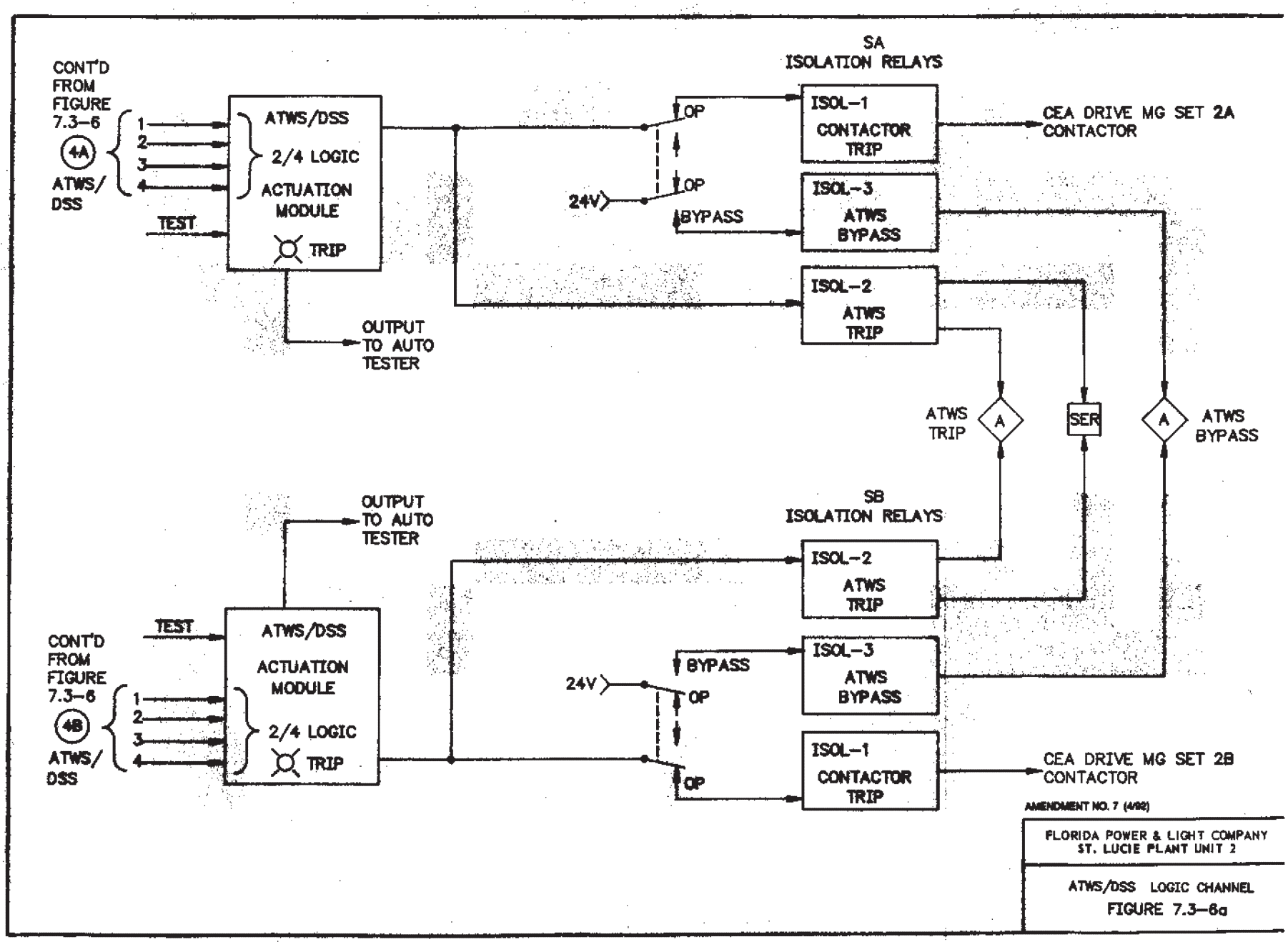
FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-5

DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-6



AMENDMENT NO. 7 (4/92)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ATWS/DSS LOGIC CHANNEL
FIGURE 7.3-6a

DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-7

DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.3-8

Deleted

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

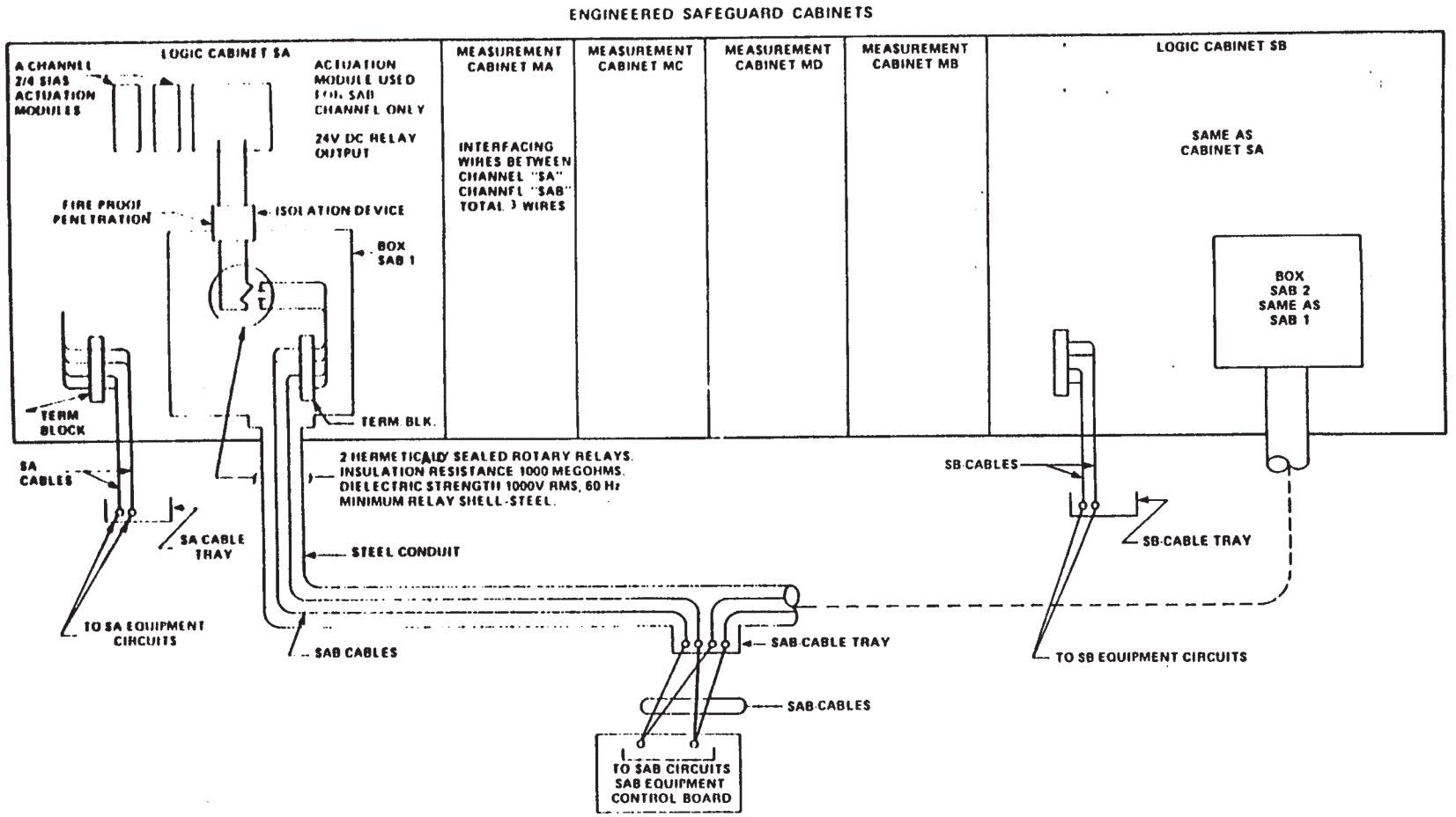
FIGURE 7.3-9

Refer to Drawing
2998-4311

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BLOCK DIAGRAM
POWER DISTRIBUTION
FOR ENGINERED SAFEGUARDS
LOGIC SYSTEM

FIGURE 7.3-10



AMENDMENT NO. 13 (05/00)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ESFAS INTERCONNECTION FOR AB SHARED SYSTEM EQUIPMENT

FIGURE 7.3-11

REF DWG: SK 2998 145 SHEET 5

REFER TO DRAWING 2998-12613

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

AUXILIARY FEEDWATER ACTUATION SYSTEM SIMPLIFIED FUNCTIONAL DIAGRAM
FIGURE 7.3-12

SEE DRAWING 2998-12614

FLORIDA POWER & LIGHT COMPANY **ST. LUCIE PLANT UNIT 2**
AUXILIARY FEEDWATER ACTUATION SYSTEM TESTING SYSTEM DIAGRAM **FIGURE 7.3-13**

Refer to Drawing
2998-15003

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

AFW ACTUATION
SYSTEM SIGNAL LOGIC DIAGRAM

FIGURE 7.3-14

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

This section describes the instrumentation and control systems that are required to establish and maintain a safe shutdown condition for the reactor. "Safe Shutdown" is defined depending on plant operating conditions as hot standby, hot shutdown or cold shutdown conditions. "Capability for safe shutdown," in all cases, is defined as maintaining the capability to reach cold shutdown conditions even though cold shutdown may not be required for maintaining the plant in a safe condition. In most cases these instrumentation and control systems are utilized in the performance of both normal and emergency plant operations. Shutdown conditions addressed in this section include both hot shutdown and cold shutdown. Hot shutdown and cold shutdown modes are defined in the plant Technical Specification.

7.4.1 DESCRIPTION

Controls and instrumentation are provided to enable the operator to monitor operations and actuate controls of systems and components necessary to bring the unit from full power operation to cold shutdown. A tabulation of the control room instruments and readouts used to monitor shutdown is shown in Table 7.4-1.

The normal shutdown procedure includes the following operations:

a. Maintenance of hot standby conditions which requires:

    1. Actuation and operation of the Auxiliary Feedwater System

    2. Actuation and control of the Steam Dump and Bypass System

    3. Monitoring of Reactor Coolant System pressurizer temperature, pressure and water level

    4. Monitoring of steam generator pressure and water level

b. Boration of Reactor Coolant System which requires:

    1. Actuation and control of boron addition and charging subsystem of the Chemical and Volume Control System (CVCS)

    2. Monitoring of Reactor Coolant System boron concentration

c. Reactor Coolant System cooldown to 325°F which requires:

    1. Operation and control of Auxiliary Feedwater System

    2. Control of Steam Dump and Bypass System

    3. Monitoring of Reactor Coolant System temperature, pressurizer pressure and water level

    4. Monitoring of steam generator pressure and water level

d. Reactor Coolant System cooldown to cold shutdown which requires:

1. Actuation and control of Shutdown Cooling System

2. Control of Component Cooling Water System

3. Control of Intake Cooling Water System

4. Operation and control of boron addition and charging subsystem of CVCS

5. Monitoring of Reactor Coolant System pressurizer temperature, pressure and water level

6. Availability of auxiliary spray flow, as further described in Subsection 5.4.7.5 (item A.2). However, RCS depressurization during cooldown can be accomplished without auxiliary spray flow (see Subsection 5.4.7.5 (Item A.2) and Subsection 9.3.4.3.1.3.4).

For off-normal shutdowns (e.g., loss of offsite power, loss of condenser cooling), the atmospheric dump valves are utilized for heat removal until shutdown cooling is initiated. The Onsite Power System (Section 8.3) provides power upon a loss of offsite power. For all shutdown conditions the capability exists for emergency actions (see Subsections 7.4.1.5 and DBD-FP-1 (Reference 1)) outside of the control room. EC282743

Based on the above, the following is the minimum equipment required to be operable for safe shutdown:

a. Auxiliary Feedwater System

b. Chemical and Volume Control System (Boron addition and charging portions only)

c. Shutdown Cooling System

d. Atmospheric Dump Valves (or Steam Dump and Bypass System)

e. Control Room

f. Instrumentation listed in Table 7.4-1.

The following support systems are also required to be operable for safe shutdown, including shutdown with a concurrent loss of offsite power:

a. Onsite Power System

b. Diesel Fuel Oil Storage and Transfer System

c. Intake Cooling Water System

d. Component Cooling Water System

e. Heating, Ventilating, and Air Conditioning (HVAC) Systems for areas containing systems and equipment required for safe shutdown

The instrumentation and control systems required for safe shutdown of the reactor are in the subsections which follow.

The instrumentation and control systems required for safe shutdown are not protective systems as defined by IEEE 279-1971, and therefore the Design Basis (Section 3) of IEEE 279-1971 does not apply. Nevertheless, the instrumentation and control systems conform to many of the requirements of IEEE 279-1971 as described in Subsection 7.4.2.

7.4.1.1 Auxiliary Feedwater System Instrumentation and Control

The Auxiliary Feedwater (AFW) System design is more fully described in Subsection 10.4.9. The system P&ID is shown on Figures 10.1-1a and 10.1-2b and locations of system components are shown on the reactor Auxiliary Building (RAB) general arrangement drawings in Section 1.2. The system instrumentation and controls utilized to achieve plant shutdown are as follows:

a. Controls

Two full capacity motor driven (2A, 2B) and one full capacity turbine driven (2C) auxiliary feedwater pumps are actuated automatically upon low steam generator level. Controls are provided for opening and closing the steam inlet valves for starting and stopping the turbine driven auxiliary feedwater pump 2C (Valves MV-08-12 and 13) and for starting and stopping the motor driven auxiliary feedwater pumps 2A and 2B. Steam for turbine driven pump is supplied from either one of the steam generators. Power for the steam inlet valve motors MV-08-12 and 13 and their controls is supplied from the 125 Volt dc bus A and B, respectively. The motor driven AFW pump 2A and 2B are powered from separate 4.16 kV buses 2A3 and 2B3, respectively. Auxiliary feedwater pump 2C inlet valve MV-08-3 is normally open and does not require power during auxiliary feedwater pump 2C operation.

Auxiliary feedwater required for each steam generator during shutdown is supplied by throttling the appropriate feedwater pump discharge valves until the desired flow is reached. Flow indicators (reference Table 7.4-1) and valve control switches are provided in the control room. The water level in each steam generator is adjusted by controlling the inlet valves thereby increasing or decreasing the auxiliary feedwater flow rate. The level in steam generator 2A is adjusted by opening valve SE-09-2 and throttling valves MV-09-9 and/or MV-09-11 using flow indicators FI-09-2A and/or FI-09-2C. The level in steam generator 2B is adjusted by opening valve SE-09-3 and throttling valves MV-09-10 and/or MV-09-12 using flow indicators FI-09-2B and/or FI-09-2C. The motor operated valves fail "as is" and the solenoid valves fail closed on loss of ac power. In the event of loss of ac power, auxiliary feedwater is supplied from the turbine driven auxiliary feedwater pump 2C through dc operated valves MV-09-11 and 12. Flow from auxiliary feedwater pump 2C to the steam generator is controlled by opening dc operated valves SE-09-3 and SE-09-4 and throttling dc operated MV-09-11 and 12.

When the Auxiliary Feedwater System is operated from outside the control room, resetting of the automatic Auxiliary Feedwater Initiation signal is not required.

The individual transfer switches enable the operator to take control of the system from outside the control room.

Control room process indication, alarm and status instrumentation is provided to enable the operator to evaluate system performance and detect malfunctions. The condensate storage tank water level is provided with redundant control room indicators and with redundant low, low-low water alarms. Separate processing instrumentation is provided for each of the auxiliary feedwater pumps. Pump discharge pressure and flow are indicated and low pump suction pressure is alarmed. Steam generator water level and pressure instrumentation is provided as shown in Table 7.5-1. Further discussion of the control room display instrumentation is presented in Section 7.5.

b. Bypasses, Interlocks and Sequencing

Upon a loss of offsite power, the motor driven pumps are automatically restarted and powered from the emergency diesel generators if they were previously running due to an AFAS. Sequencing is shown in Table 8.3-2.

The turbine driven pump requires no ac or dc power for its operation.

c. Redundancy and Diversity

The two motor driven pumps and their respective discharge valves MV-09-9 and 10 to the steam generators are redundant to the turbine driven pump and its discharge valves MV-09-11 and 12 to each steam generator. Separate and independent circuitry, logic and controls are provided for the redundant components.

125V dc power for the turbine driven pump and associated valves is available from the 125V dc A and B buses (see Subsection 8.3.2).

Auxiliary Feedwater System diversity is provided by virtue of the diverse pump drivers, motor driven versus steam turbine driven, and the associated ac-powered versus dc- powered motor operated valves. Additionally, there are manual operators (handwheels) on the flow control valves to the steam generators.

7.4.1.2 Chemical and Volume Control System (Boron Addition and Charging Portions)

The boron concentration in the reactor coolant is increased to the cold shutdown value, during the cooldown of the plant; to assure sufficient shutdown margin throughout the cooldown period.

The boron addition and charging subsystems are portions of the Chemical and Volume Control System (CVCS) which are used in the shutdown process. The Chemical and Volume Control System is discussed in Subsection 9.3.4. The system P&ID is shown on Figure 9.3-5(a-c). Location of major system components is shown on the RAB general arrangement drawings in Section 1.2. The system instrumentation and controls utilized to achieve plant shutdown are discussed as follows:

a. Initiating Circuits and Logic

To help achieve a safe shutdown and cooldown, the system component actuation steps required are:

1. coordinated control of the charging pumps, letdown control valves, and letdown backpressure valves to adjust and maintain the correct pressurizer water level

2. periodic sampling and adjustment of the boron concentration to compensate for the temperature decrease and other variables until shutdown concentration is reached.

Control board mounted instrumentation tabulated in Table 7.4-1, is provided to enable the operator to evaluate system performance and to control system operation.

b. Interlocks, Sequencing and Bypasses

System operation is achieved by the coordinated operation of the charging pump and boric acid makeup pump control circuits. The charging pump control circuit sequences charging pump operation in response to pressurizer water level control circuit requirements as discussed in Subsection 7.7.1.1.3. The boric acid makeup pump control circuit sequences the boric acid makeup pump and valve operation to achieve the desired boric acid concentration.

Manual control of any portion of these systems can be achieved while allowing the remainder to continue functioning in automatic. The receipt of a safety injection actuation signal (SIAS) (discussed in Subsection 7.3.1) overrides any control mode condition so that full boron addition and charging capabilities are achieved. No instrument bypasses exist which could degrade this response.

c. Redundancy and Diversity

Two separate and distinct modes of boron addition are available through the use of the boric acid makeup pumps or the gravity feed lines. Either of these methods can be used to transfer concentrated boric acid from each of the boric acid makeup tanks to either the volume control tank or directly to the reactor coolant system. Charging system redundancy is achieved by having separate charging pumps (with diverse injection paths) and supporting instrumentation powered from separate electrical buses.

7.4.1.3 Shutdown Cooling System I&C

The Shutdown Cooling System (SDCS) is more fully described in Subsection 5.4.7. The SDCS P&ID is shown on Figure 6.3-1(a-c) and the location of major components are shown on the RAB general arrangement drawings in Section 1.2. The SDCS instrumentation and controls necessary to initiate and achieve safe shutdown are described below.

As described in Subsection 5.4.7, the SDCS utilizes the low pressure safety injection (LPSI) pumps, which are aligned for the Emergency Core Cooling System (ECCS) mode of operation when the Reactor Coolant System temperature is above 325°F. Alignment from the ECCS to the SDCS mode is described in Subsection 5.4.7.2.

a. Initiating Circuits, Logics and Controls

   The Shutdown Cooling System is manually initiated when the Reactor Coolant System temperature and pressure are reduced to about 325°F and about 276 psia. Subsequent to the valve switchovers from ECCS to SDCS mode, actions are performed in the control room to initiate shutdown cooling as outlined in Subsection 5.4.7.2.6.

   The process instrumentation and controls for the SDCS including the LPSI pumps are delineated in Table 7.4-1.

b. Bypasses and Interlocks

   The Shutdown Cooling System instrumentation has no bypass features. Interlocks, key locked switches and administratively locked valves are provided to prevent the possibility of overpressurization of the lines, which are designed for low pressure operation. These interlocks are described in Subsection 7.6.1.1. Also see discussions provided in Subsection 5.4.7.2.

   Following certain postulated accidents (e.g., feedwater line break, small break LOCA, steamline break) or loss of offsite power, it may become necessary to initiate shutdown cooling with Reactor Coolant System hot leg conditions which exceed the normal shutdown cooling initiation temperature. However, shutdown cooling is not initiated at conditions which exceed the design temperature of the SDCS components.

c. Redundancy and Diversity

   Initiation of shutdown cooling with the most limiting single failure (loss of one shutdown cooling train) is accomplished using the procedures under plant cooldown for the operable train (i.e., operating the valves with (A) for train A, or the valves without (A) for train B). The power supplies to the isolation valves are so arranged that the following objectives are met assuming a single failure.

   1. Both redundant lines are closed at least by one valve when the pressure is above the set value, thus protecting the low pressure part of the line, Valves V3481 and V3664 in train A and V3652 in train B are powered from SA power. Valves V3480 in line A and V3651 and V3665 in line B are powered from SB power.

2. Header A and B tie valve V3545 is powered from SAB power assuring that at least one header is available for shutdown,

In the unlikely event of a loss of power to one of the two SDCS trains, the SDCS suction line cross-connect valve (V3545) is utilized to provide at least one complete shutdown cooling train. The operator selects the system flow path with an active available power supply (emergency or normal) since the SDCS suction line cross-connect valve (V3545) is normally locked open, the SDC functions can continue.

7.4.1.4 Atmospheric Dump Valves (or Steam Dump and Bypass System)

During plant shutdown, the steam dump and bypass valves may be remote manually positioned to remove reactor decay heat, pump heat and Reactor Coolant System sensible heat to reduce the reactor coolant temperature at the design cooldown rate until shutdown cooling is initiated. See Subsection 10.4.4 for a discussion of the Steam Dump and Bypass System. For a discussion of the instrumentation and control for the Steam Dump and Bypass System, see Subsection 7.7.1.1.5.

For normal and off-normal shutdowns, the atmospheric dump valves (ADV) may be utilized for heat removal. Four 50 percent capacity ADVs each, are located outside the containment upstream of the main steam isolation valves, and are discussed in Subsection 10.3.3. The ADV P&ID is shown on Figure 10.1-1a and the location of the valves are shown on the RAB general arrangement drawings in Section 1.2.

In the event of loss of condenser cooling or offsite power the valves remove reactor decay heat by venting steam to the atmosphere. In this way the Reactor Coolant System is maintained at hot standby conditions or cooled down to SDCS initiation temperature and pressure. The instrumentation and control design features of these valves are as follows:

a. Initiating Circuits, Logic and Controls

   The valves are electrically operated, and are manually initiated and automatically or manually controlled with auto/hand indicating controllers either from the control room or from the hot shutdown panel. An electronic transmitter converts the steam line pressure to an electronic signal. When a high steam generator pressure signal is received by the controller, the opening of the valve is automatically modulated until the pressure is reduced. The operator maintains pressure automatically or reduces pressure by reducing the PIC setpoint or by manually operating the PICs.

b. Bypasses and Interlocks

   No bypasses or interlocks are provided for the atmospheric dump valves.

c. Redundancy and Diversity

   The atmospheric dump valves are sized such that the reactor can be brought to shutdown cooling initiation pressure and temperature assuming a loss of two out of four valves. Upon a loss of ac power, the atmospheric dump valves can be remote manually operated using battery power only. The cooldown of the reactor

to 350°F can also be accomplished through manual operation of the atmospheric dump valves. Each atmospheric dump valve has a hand wheel which can be operated locally to override the motor operator. Each atmospheric dump valve has a corresponding block valve operated from the opposite safety channel. This block valve is normally locked open, but can be closed so as to isolate its associated atmospheric dump valve.

7.4.1.5 Control Room (or Hot and Cold Shutdown Capability from outside the Control Room)

Emergency instrumentation and controls are provided outside the control room to enable the operator to shutdown and maintain the unit at hot standby or initiate a cool down as required by GDC 19.

The postulated control room conditions and/or event which would make it inaccessible and result in its evacuation remain undefined, with the exception of a plant fire in the control room or cable spreading room. Since no other failure mechanisms have been established or identified, a shutdown from outside the control room is not assumed to be accompanied by any DBA. EC282743

A shutdown from outside the control room due to a fire is discussed in the Fire Protection Design Basis Document (Reference 1) and the Unit 2 Nuclear Safety Capability Assessment (NSCA) (Reference 2). The Unit 2 Essential Equipment List (Reference 3) defines the instrumentation and controls for equipment required for the safe and stable plant operations from both inside and outside the control room to address a plant fire. The NSCA identifies which circuits require transfer switches so that shutdown can be achieved independent of the control room and/or cable spreading room. These transfer switches and other provisions (such as redundant fuses) are located throughout the plant to provide for electrical isolation of electrical faults which could occur in the control room and/or spreading room due to a fire. For both NFPA 805 and GDC 19 functions, transfer switches are also used to switch instrumentation and control functions from the control room to their remote location. EC282743 EC282743

Tables 7.4-1, 2, 3, 4, 5 & 6 are applicable to the GDC 19 requirements and do not include analysis which is applicable to NFPA 805. As discussed above, these requirements are included in the NSCA. Plant Procedures for a shutdown from outside the control room due to a fire are based on the NSCA. EC282743

Table 7.4-3 lists the locations of the transfer switches and alarm number that are initiated in the control room when any of the transfer switches are activated. This table also includes those transfer switches for equipment required for cold shutdown from outside the control room.

Table 7.4-4 lists equipment that can be actuated from outside the control room during reactor cooldown and shutdown without needing transfer switches actuation.

Table 7.4-5 lists the instrumentation available for reactor shutdown from outside the control room and indicates the location of the transfer switch and the alarm that actuates in the control room when the transfer switch is actuated. As indicated in this table, some instruments outside the control room do not require the actuation of transfer switches.

Controls and instrumentation for redundant equipment are mounted in separate sections of the hot shutdown panel (HSDP) such that no single failure can prevent the safe shutdown of the

reactor. A list of indicators, controllers, control switches and indicating lamps located on the HSDP is given in Table 7.4-2.

The HSDP design meets the separation requirement of R.G. 1.75 (R1) and the overall design criteria of IEEE 279-1971 for protection system.

To activate the HSDP, transfer switches and isolation switches have to be turned to "isolate" position. Transfer switches and isolation switches are located on transfer panel 2A, 2B, 2AB and various MCCs and switchgears are concentrated in the middle section of RAB at Elevation 43 and RAB at Elevation 19.5 to facilitate transfer from control room to Hot Shutdown Panel (HSDP). The transfer switches are safety class 1E. The transfer switches meet the separation requirements of R.G. 1.75 (R1) and the overall design criteria of IEEE 323-1971 for the protection system. HSDP is located in a room at the southwest corner of the RAB at Elevation 43. The seismic and environmental qualification is described in Sections 3.10 and 3.11.

Equipment that does not change operating status when transferred is controlled at the Hot Shutdown Panel or locally by spring return to "auto" or return to "normal" type switches. Equipment in this category have latched-in circuitry such as switchgear operated pumps and motor operated valves.

Equipment that does change operating status when transferred is controlled by maintained contact switches. These circuits drop out at interrupted power. Equipment such as solenoid valves and pumps actuated by motor starters have this type of circuitry.

In the event of a non-mechanistic evacuation of the control room, the operator trips the reactor before leaving the control room. Manual transfer switches are provided at appropriate locations outside the control room so that the required circuits for hot shutdown are isolated from, the circuits in the control room. A control room operator forced to leave the control room and proceed to the Shutdown Panel uses his security card key to exit the control room. He proceeds to the 45' elevation and again uses his key card to gain access to the cable spreading area where the Hot Shutdown Panel is located. The hot shutdown panel room is located within a security area and therefore, is not required to be locked, but may include security access control that does not inhibit the ability of the operator to gain access to the room during safe shutdown. The controls can be isolated from the control room and transferred to the Hot Shutdown Panel control shortly after leaving the control room. Refer to section 7.4.2.3 (R.G. 1.68). As described in the Emergency Procedures one operator is transferring the controls while the other operator is ready to take control as soon as the transfer takes place. Until a transfer is executed the automatic functions of the logic cabinets located in the control room are in full effect. (Example: Auxiliary Feedwater is automatically initiated if low-level is reached before the transfer takes place. After the transfer the operator can manually control Steam Generator level from the Hot Shutdown Panel).

Table 7.4-6 provides a list of the Hot Shutdown Panel switch positions with a justification for the chosen positions. After the completion of the required circuit transfers, the Hot Shutdown Panel becomes fully operational. An alarm is initiated in the control room whenever any one of the transfer switches are operated into the transfer position. Operability of controls for equipment required for shutdown are based on the assumption that they are not affected by the destruction of circuitry within the control room. Sufficient instrumentation and controls are provided outside the control room to:

a. Achieve prompt hot shutdown of the reactor

b. Maintain the unit in a safe condition during descent to hot shutdown

c. If required, monitor cooldown and achieve cold shutdown through the use of suitable procedures.

7.4.1.6 Supporting Systems for Safe shutdown

The supporting systems required for safe shutdown of the reactor listed below are described in the referenced sections:

a. Component Cooling Water System (Subsection 9.2.2)

b. Intake Cooling Water System (Subsection 9.2.1)

c. Onsite Power System, including diesel generator system (Section 8.3)

d. Diesel Fuel Oil Storage and Transfer System (Subsection 9.5.4)

e. Heating, Ventilating and Air Conditioning (HVAC) Systems as required for areas containing systems and equipment required for safe shutdown (Section 9.4).

7.4.1.7 System Drawings

Control wiring diagrams, block diagrams, final logic diagrams, and location layout drawings are listed and provided by reference in Section 1.7.

7.4.2 ANALYSIS

7.4.2.1 General Design Criteria (GDC)

For a discussion of GDCs, see Subsection 7.1.2.1.

7.4.2.2 Conformance to IEEE 279-1971

The shutdown systems, which are manually operated, are not protective systems as listed in the Scope (Section 1) of IEEE 279-1971 and therefore, the Design Bases (Section 3) of IEEE 279-1971 does not apply. Nevertheless, the systems conform to many of the requirements of Section 3 of IEEE 279-1971 as described below:

Bases 1, 6 7, 8 and 9

Not applicable. The safe shutdown system instruments are used for the indication of the safe shutdown system performances only.

Basis 2

The station variables which are monitored to provide information for the safe shutdown are listed in Table 7.4-1.

Basis 3

None of the station variables listed In Basis 2 for the safe shutdown have spatial dependence.

Bases 4, 5

Table 7.4-1 lists the instrumentation monitoring station variables of systems required for the safe shutdown.

In addition, the instrumentation and controls for safe shutdown meet the following design bases:

a. any single failure does not prevent safe plant shutdown.

b. channel independence is maintained by electrical and physical separation between redundant channels.

c. equipment, including electric cables, associated with redundant systems are uniquely identified as detailed in section 8.3.1.3.

d. the systems are designed to withstand safe shutdown earthquake loads without loss of their safety functions.

e. the systems can be tested with the plant shutdown.

f. equipment is provided in appropriate locations outside the control room to bring the plant to a hot standby condition with capability for subsequent cold shutdown.

Conformance with the applicable portions of IEEE 279, Section 4 is discussed below:

4.1, "General Functional Requirements"

Controls and instrumentation are provided to enable the operator to monitor operations and actuate controls of systems and components necessary to bring the unit from full power operation to safe shutdown. Instrument performance characteristics, response time, and accuracy are selected for compatibility with and adequacy for the particular function. Trip setpoints are established by analysis of the system parameters. Factors such as instrument inaccuracies, bistable trip times, valve travel time, and pump starting times are considered in establishing the margin between the trip setpoints and the safety limits.

4.2, "Single Failure Criterion"

The instrumentation and controls required for the maintenance of a hot shutdown condition are designed and arranged such that no single failure can prevent a safe shutdown. Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with the single failure criterion is accomplished by providing redundancy of power supplies and actuation circuits, and by

separating the redundant elements electrically and physically to achieve the required independence. Each of these provisions is discussed below:

a. Redundancy

Each of the systems required for safe shutdown consists of redundant subsystems and/or components for maximum system reliability. The emergency power system consists of two redundant emergency diesel generator sets. Each of the redundant components has automatic and/or manual actuation circuits which are separate from those provided for its redundant counterpart. Redundant instrumentation is provided to monitor Reactor Coolant System conditions. Each steam generator is provided with separate pressure and level monitoring instrumentation.

b. Electrical Separation

Electrical separation is achieved through the provision of independent power supplies and the elimination of electrical interconnection between redundant elements. Control power for redundant circuits is fed from separate 125V dc buses. Power for redundant pumps and valves is supplied from separate emergency diesel generators. Components designated A are part of electrical load group A and components designated B are part of electrical load group B. Third service components are part of electrical load group AB.

The provision of separate power supplies and elimination of electrical connections between redundant circuits ensures that loss of power or electrical faults on any circuit cannot affect the redundant circuit.

c. Physical Separation

Protection against the possibility of mechanical damage to both redundant portions of any instrumentation and control system required for safe shutdown is achieved by spatial separation and/or the provision of physical barriers between redundant elements.

Physical separation within control panels is achieved by providing at least six inches of spatial separation between redundant circuitry or by a metal barrier. This separation is provided between control switches, controllers, relays and wiring necessary to actuate and control redundant components.

Cable trays and conduit containing redundant wiring and cables necessary to actuate and control redundant components are physically separated as discussed in Subsection 8.3.1.

Redundant system pumps, piping and other components are physically separated to ensure that no single failure can cause damage to both redundant components. This separation afforded by component separation is maintained for redundant instrumentation which is mounted on the piping or components and which is utilized for safe shutdown.

The redundant wiring and circuitry of the instrumentation and control systems required for safe shutdown are marked and identified as described in Subsection 8.3.1.3.

4.3, "Quality Control of Components and Modules"

For a discussion of the Quality Assurance program, see Chapter 17.

4.4, "Equipment Qualification"

The instrumentation and controls necessary to achieve safe shutdown meets the equipment qualification requirements discussed in Sections 3.10 and 3.11.

4.5, "Channel Integrity"

The safe shutdown "Channel Integrity" is functionally identical to that described in Subsection 7.3.2.1.2.

4.6, "Channel Independence"

Safe shutdown system "Channel Independence" is functionally identical to that described in Subsection 7.3.2.1.2.

4.7, "Control and Protection System Interaction"

No portion of the safe shutdown system is used for both control and protection.

4.8, "Derivation of System Inputs"

The safe shutdown system monitoring signals are a direct measurement of the desired variables.

4.9, "Capability for Sensor Checks"

The safe shutdown system monitoring sensors are checked by comparing the monitored variables of redundant channels or by observing the effects of introducing and varying a substitute input to the sensor similar to the measured variable.

4.10, "Capability for Test and Calibration"

IEEE 338-1971 and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," 2/72 (R0) provides guidance for the development of procedures, equipment and documentation of periodic testing. The measurement signals required for safe shutdown have the capability of being tested and calibrated under the design requirements of the system.

4.11, "Channel Bypass or Removal from Operation"

Any one of the channels may be tested, calibrated, or repaired without detrimental effects on the other channels.

4.12, "Operating Bypasses"

There are no "Operating Bypasses" for the safe shutdown systems.

4.13, "Indication of Bypasses"

A discussion of bypass and inoperable status indication is provided in Subsection 7.5.1.6 and a listing of inoperable or bypassed components is contained in Table 7.3-10.

4.14, "Access to Means for Bypassing"

This section is not applicable.

4.15, "Multiple Setpoints"

This section is not applicable.

4.16, "Completion of Protective Action Once it is Initiated"

This section is not applicable.

4.17, "Manual Initiation"

The safe shutdown systems may be manually actuated.

4.18, "Access to Setpoint Adjustments, Calibration, and Test Points"

This section is not applicable.

4.19, "Identification of Protective Actions"

This section is not applicable.

4.20, " Information Readouts"

Safe shutdown system monitoring and control channels are indicated in the control room.

4.21, "System Repair"

The safe shutdown systems may be actuated manually; therefore, replacement or repair of components can be accomplished in reasonable time when the systems are not actuated. Outage of system components for replacement or repair are limited by the Technical Specifications.

4.22, "Identification"

Safety equipment and cables associated with the systems required for safe shutdown are uniquely identified.

7.4.2.3 Conformance to Applicable Regulatory Guides

Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions", 2/72 (R0)

The design conforms to the requirements of Regulatory Guide 1.22 (R0). These systems are periodically tested to verify proper functioning during normal plant operation. Actuation devices and actuated equipment are simultaneously operated during testing without any bypasses.

The HSDP instrumentation and control is periodically tested in accordance with technical specification requirements and plant procedures. By positioning the transfer/isolation switch to "ISOLATE", the instrumentation and controls on the Hot Shutdown Panel can be tested to assure their operability. This test is performed on a "not to disturb the normal operation" basis. There are a few other instruments on Hot Shutdown Panel (such as pressurizer pressure) which have their own dedicated detectors and do not require transfer action because they are continuously functioning.

Valves are actuated for full travel verification. The safeguards actuation system has an automatic test circuit to monitor trip setpoints. At 18 month intervals an integrated test of the ESF is performed. This test assures operation and response of all safeguards required equipment and circuits.

Testing of pumps and valves for safety and shutdown systems is done in accordance with the appropriate technical specifications.

Regulatory Guide 1.30, "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment," 8/72 (R0)

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," 5/73 (R0)

Refer to Subsection 7.5.2.7 for a discussion of bypassed and inoperable status indication.

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," 6/73 (R0)

These systems are designed so that any single failure within each system does not prevent proper action at the system level. No single failure defeats more than one of the two channels associated with any one system. The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, negates the intended function of the system. Signal conductors are protected and routed independently.

Compliance with the single failure criterion is accomplished by providing redundant channels and separating these redundant elements physically and electrically to achieve the required independence. The instrumentation and controls for these systems meet the requirements of IEEE 379-1972 and are consistent with the recommendations of Regulatory Guide 1.53 (R0).

Regulatory Guide 1.68, "Initial Test Programs for Water-Cooled Reactor Power Plants,", 11/73 (R0)

To meet the intent of Regulatory Guide 1.68 (R1) for reactor remote shutdown capability, the following are remote shutdown procedures under three different plant conditions.

The three plant conditions are:

1. Remote Hot Shutdown (No LOOP)
2. Remote Hot Shutdown (LOOP)
3. Remote Cooldown and Shutdown (with or without LOOP)

These shutdown procedures are based on the availability of three to four operational personnel.

1. Condition I: Remote Hot Shutdown (No Loop)

   Before leaving the control room, the operators assure the reactor and turbine have been tripped. One person will be sent to the turbine building ground floor (7 kV and 4 kV switchgear room) to trip the reactor coolant pumps, feed pumps, etc. Meanwhile, additional persons will have the responsibility to activate the transfer (isolate) devices. Most of these MCCs, switchgear and transfer panels are located in the Reactor Auxiliary Building, floor elevation 43 feet, on the west half of the floor. The 480 volt switchgear 2AB and 4 kV switchgear 2AB are located on the 19.6 feet floor elevation. Approximately 56 transfer switches have to be activated. It takes personnel approximately 10 minutes to complete the above transfer functions. The time from when the operators leave the control room to the moment the hot shutdown panel is fully operational, is approximately 15 to 20 minutes. Once the hot shutdown station is operational, a senior licensed operator is primarily stationed there to monitor and control the hot shutdown process, whereas the other operators are strategically stationed throughout the plant. Communication is maintained by way of sound power phones (head sets) at required stations.

2. Condition II: Remote Hot Shutdown (LOOP)

   If offsite power is not available (or lost), the Reactor Coolant Pumps and main FW pump are de- energized. Under LOOP conditions, the operators proceed to pre-designated stations including the diesel generator building.

   Some additional manual switchgear loading might be required in order to connect certain plant investment load onto the emergency buses. Upon completion of all the necessary transfer functions, the hot shutdown panel is manned continuously by a licensed operator, whereas the other operators are stationed throughout the plant, awaiting further instructions.

3. Condition III: Remote Cooldown and Shutdown (with or without (LOOP))

   For further plant cooldown and shutdown from the HSDP, several systems are required to be operated.

   They are identified as follows:

   a. Chemical & Volume Control System (CVCS) (See Subsection 9.3.4)

   b. Shutdown Cooling System (See Subsection 5.4.7)

   c. Reactor Coolant Sampling System (See Subsection 9.3.2)

   d. Other supporting Systems such as CCW, ICW System etc; that are needed for a), b), and c) above. For a list of ESF support systems and their associated subsections, see Subsection 7.4.1.6.

   From the Hot Shutdown Panel, the senior licensed operator directs the lineups of the above systems which requires manual valve operation, "locked closed"

and "locked open" valves, and coolant sampling to check proper reactivity. Additional operators are assigned to accomplish these tasks.

Regulatory Guide 1.75, "Physical Independence of Electric Systems", 1/75 (R1)

With respect to the instrumentation and controls for these systems, the method used for identifying power and signal cables and cable trays as safety related equipment, and the identification scheme used to distinguish between redundant cables, cable trays, and instrument panels are in accordance with the recommendations of Subsections 5.1.2 and 5.6.3 of Regulatory Guide 1.75 (R1). For further information see Subsections 7.1.2.2 and 8.3.1.2.

7.4.2.4 Loss of Instrument Air Systems

Pneumatically operated valves in systems required for safe shutdown upon loss of instrument air takes the position required for system operation in the plant shutdown mode. Valves which are in required flow paths open on loss of instrument air. Valves which isolate nonessential portions of the system from portions required for safe shutdown closes on a loss of air. Valve failure positions are identified on the system P&I diagrams.

The essential control and monitoring instrumentation is not pneumatic. Electric power for the instrumentation is capable of being supplied from the emergency power system.

The intake cooling outlet flow from the component cooling heat exchangers is pneumatically controlled. The valves fail open on loss of air. Flow modulation is not required for safe shutdown.

The pressurizer spray pneumatically controlled valves (PCV-1100E and PCV-1100F) fail closed on loss of instrument air. Pressurizer pressure is then controlled by operation of the electric pressurizer heaters and electrically operated auxiliary spray valves.

Therefore, the loss of instrument air does not prevent safe shutdown of the plant.

7.4.2.5 Loss of Cooling Water to Vital Equipment

None of the instrumentation and controls required for safe shutdown rely on cooling water for operation.

7.4.2.6 Plant Load Rejection, Turbine Trip and Loss of Offsite Power

In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the Onsite Power System. The description and analysis of the emergency power system are discussed more fully in Section 8.3. The emergency diesel generators provide power for operation of all necessary pumps and valves. The station dc system provides uninterrupted power for operation of control and instrumentation systems required to actuate and control essential components.

The emergency diesel generators automatically start and begin supplying power to components necessary to achieve safe shutdown. The station dc system maintains continuity of dc control power.

The emergency power system meets the single failure criterion and can withstand the most severe natural phenomena. Adequate onsite emergency power is available, in the event of loss-of-offsite power to safely shutdown the plant under postulated design basis accident conditions assuming a single failure.

REFERENCES EC282743

1. DBD-FP-1, Fire Protection Design Basis Document.

2. 2998-B-048, Unit 2 Nuclear Safety Capability Assessment (NSCA).

3. 2998-B-049, Unit 2 Essential Equipment List.

TABLE 7.4-1

INSTRUMENTS FOR MONITORING-SAFE SHUTDOWN

System Parameter & Location	Contr. Room Indication	Alarm	Tag Number	Inst.[1] Range	Normal[A] Operating Value
Shutdown Cooling System					
1) HX 2A Outlet Temperature	RTGB-206	----	TI-3303X		175 F
2) HX 2B Outlet Temperature	RTGB-206	----	TI-3303Y		175 F
3) HX 2A Inlet Pressure	RTGB-206	----	PI-3303X		450 psig
4) HX 2B Inlet Pressure	RTGB-206	----	PI-3303Y		450 psig
5) Low Press Safety Inject-tion Loop 2A2 Flow	RTGB-206	----	FI-3312		1800 gpm
6) Low Press Safety Injec-tion Loop 2A1 Flow	RTGB-206		FI-3322		1800 gpm
7) Low Press Safety Injec-tion Loop 2B1 Flow	RTGB-206	----	FI-3332		1800 gpm
8) Low Press Safety Injec-tion Loop 2B2 Flow	RTGB-206	----	FI-3342		1800 gpm
9) Shutdown Cooling Loop 2A Return Flow	RTGB-206	----	FR-3306		3500 gpm
10) Shutdown Cooling Loop 2B Return Flow	RTGB-206	----	FR-3301		3500 gpm
11) Low Press Safety Injec-tion Hdr A Press	RTGB-206	----	PI-3307		450 psig

[1] Instrument ranges are selected in accordance with standard engineering practices.

TABLE 7.4-1 (Cont'd)

System Parameter & Location	Contr. Room Indication	Alarm	Tag Number	Inst.[1] Range	Normal[A] Operating Value
12) Low Press Safety Injec-Tion Hdr B Pressure	RTGB-206	----	PI-3304		450 psig
13) LPSI Pump 2A Amp.	RTGB-206	----	AM/251		
14) LPSI Pump 2B Amp	RTGB-206	----	AM/252		
15) Shutdown HX 2A Inlet Temp	RTGB-206	----	TR-03-1		EC290696
16) Shutdown HX 2B Inlet Temp	RTGB-206	----	TR-03-2		EC290696
Atmospheric Dump System					
1) St Generator 2A Pressure	RTGB-202 PACB	----	PIC-08-1A PIC-08-3B		900 psig
2) St Generator 2B Pressure	RTGB-202 PACB	----	PIC-08-1B PIC-08-3A		900 psig
Auxiliary Feedwater System					
1) Aux Feedwater Pumps Disch Hdr Flow					
- 2A HDR	RTGB-202		FI-09-2A		250 gpm
- 2B HDR	RTGB-202	----	FI-09-2B		250 gpm
- 2C HDR	RTGB-202		FI-09-2C		500 gpm
2) Aux Feedwater Pumps Disch Hdr Press					
- 2A HDR	RTGB-202	----	PI-09-8A		1115 psig
- 2B HDR	RTGB-202	----	PI-09-8B		1115 psig
- 2C HDR	RTGB-202	----	PI-09-8C		1115 psig

[1] Instrument ranges are selected in accordance with standard engineering practices.

TABLE 7.4-1 (Cont'd)

System Parameter & Location	Contr. Room Indication	Alarm	Tag Number	Inst.[1] Range	Normal[A] Operating Value
3) Aux Feedwater Pump 2A Ammeter	RTGB-202	----	AM/629		47A
Aux Feedwater Pump 2B Ammeter	RTGB-202	----	AM/630		47A
4) Condensate Storage Tank Water Level	RTGB-202 RTGB-202	Lo/Lo-Lo Lo	LIS-12-11A LIS-12-11B		44 ft 44 ft
5) Steam Generator Level (Narrow Range)					
2A Level	RTGB-202	----	LIC-9013A, 9013B, 9013C, 9013D		65%
2B Level	RTGB-202	----	LIC-9023A, 9023B, 9023C, 9023D		65%
6) Steam Press to Steam Driven Aux Feed Pump	RTGB-202	----	PI-08-5		800 psig
Intake Cooling Water System					
1) Intake CW Hdr A & B Pressure	RTGB-202	Low	PIS-21-8A PIS-21-8B		90 psig
2) Intake CW Pump 2A Amp Intake CW Pump 2B Amp Intake CW Pump 2C Amp	RTGB-202 RTGB-202 RTGB-202	---- ---- ----	AM-832 AM-833 AM-834		
Component Cooling Water System					
1) CCW Press at HX Outlets					
HX 2A Outlet HX 2B Outlet	RTGB-206 RTGB-206	Low Low	PIS-14-8A PIS-14-8B		100 psig 100 psig

[1] Instrument ranges are selected in accordance with standard engineering practices.

TABLE 7.4-1 (Cont'd)

System Parameter & Location	Contr. Room Indication	Alarm	Tag Number	Inst.[1] Range	Normal[A] Operating Value
2) CCW Flow Hdrs					
HDR A	RTGB-206	High-Low	FIS-14-1A		8,500 gpm
HDR B	RTGB-206	High-Low	FIS-14-1B		8,500 gpm
3) CCW Flow at Shutdown Cooling HX outlet					
HX 2A Outlet	RTGB-206	High-Low	FIS-14-10A		4,820 gpm
HX 2B outlet	RTGB-206	High-Low	FIS-14-10B		4,820 gpm
4) Charging Pumps					
Charging Hdr Pressure	RTGB-205	Low	PIA-2212		2,377 psig
Charging Flow to RHX	RTGB-205	Low	FIA-2212		44 ea pump
Reactor and Primary Loop					
1) Pressurizer Pressure	RTGB-203	----	PI-1103, -1103D, -1104, 1105, -1105D, -1106		----
	RTGB-203	----	PI-11O2A,-1102B, -1102C,-1102D		2,250 psia
	RTGB-203	----	PI-1107-1,-1108-1.		2,250 psia
2) Pressurizer Water Level	RTGB-203	----	LI-1110X & LI-1110Y		50%
3) Reactor Cold Leg Temp	RTGB-203	----	TI-1115 & TI-1125		551F
4) Neutron Power Level	RTGB-204	----	JI-001A,-001B, -001C,-001D		100%
5) Neutron Power Wide Range	RTGB-204, PACB-2		RI-26-80A5 & 80B5 RR-26-80A & 80B		NA NA
6) Neutron Power Rate	RTGB-204		RI-26-80A3 & 80B3		NA

[1] Instrument ranges are selected in accordance with standard engineering practices.

TABLE 7.4-2

INSTRUMENTATION AND CONTROL - HOT SHUTDOWN PANEL
OUTSIDE THE CONTROL ROOM

Instruments Tag No.	Service	Safety Section	Scale[2] Range
LI-9113	Steam Generator 2A Water Level	SA	
PI-8113	Steam Generator 2A Pressure	SA	
*PIC-08-1A1, 3A1	SG 2A Atmospheric Steam Dump	SA	
PI-1108	Pressurizer Pressure	SA	
LI-1105	Pressurizer Water Level	SA	
TI-1115-1	Reactor Cold Leg Temperature	SA	
TI-3351Y	Shutdown Cooling Temperature	SA	
FI-3306	Shutdown Cooling Flow	SA	
VM/1606-1	Diesel Generator 2A Volts	SA	
WM/1606-1	Diesel Generator 2A Watts	SA	
FI-2212	Charging Flow	SA	
JI-001A-1	Neutron Power Level	MA	
JI-001B-1	Neutron Power Level	MB	
RI-26-80A1	Neutron Power - Wide Range	SA	
RI-26-80A2	Neutron Power - Source Range	SA	
RI-26-80B1	Neutron Power - Wide Range	SB	
RI-26-80B2	Neutron Power - Source Range	SB	
LI-9123	Steam Generator 2B Water Level	SB	
PI-8123	Steam Generator 2B Pressure	SB	
*PIC-08-1B1, 3B1	SG 2B Atmospheric Steam Dump	SB	
PI-1107	Pressurizer Pressure	SB	
PI-2212	Charging Pressure	SB	
LI-1104	Pressurizer Water Level	SB	
TI-1125-1	Reactor Cold Leg Temperature	SB	
TI-3352Y	Shutdown Cooling Temperature	SB	
FI-3301	Shutdown Cooling Flow	SB	
VM/1616-1	Diesel Generator 2B Volts	SB	
WM/1616-1	Diesel Generator 2B Watts	SB	
LI-9012	SG 2A Wide Range Level	None	
LI-9022	SG 2B Wide Range Level	None	
TI-2223	Letdown Heat Ex Outlet Temperature[1]	None	

Switches & Indicating Lamps Tag No.	Service	Safety Section	Scale[2] Range
CS-608-2	Auxiliary FW 2A Discharge MV-09-9	SA	
CS-629-2	Auxiliary FW Pump 2A	SA	
CS-189-1	Auxiliary Spray Valve SE-02-3	SA	

TABLE 7.4-2 (Cont'd)

Switches and Indicating Lamps Tag No.	Service	Safety Section	Scale[2] Range
CS-157-1	Letdown Contain Isol V2516	SA	
CS-194-2	Charging Line Isol V2523	SA	
CS-177	Charging Pump 2A and Position Indication for Recirculation Valve V2554	SA	
CS-176-1	Charging Line Valve SE-02-2	SA	
CS-246-3	SIAS "A" Block	SA	
CS-1625-2	Stm Gen 2A Atm Stm Dump Valve MV-08-19A	SB	
CS-1626-2	Stm Gen 2A Atm Stm Dump Valve MV-08-18A	SA	
CS-1628-2	Stm Gen 2B Atm Stm Dump Valve MV-08-18B	SA	
CS-1627-2	Stm Gen 2B Atm Stm Dump Valve MV-08-19B	SB	
CS-609-2	Auxiliary FW 2B Disch MV-09-10	SB	
CS-630-2	Auxiliary FW Pump 2B	SB	
CS-189-2	Auxiliary Spray Valve SE-02-4	SB	
CS-157-2	Letdown Stop Valve V2515	SB	
CS-194-1	Letdown Contain Isol V2522	SB	
CS-178	Charging Pump 2B and Position Indication for Recirculation Valve V2555	SB	
CS-176-2	Charging Line Valve SE-02-01	SB	
CS-248-3	SIAS "B" Block	SB	
CS-612-2	Auxiliary FW 2C to SC 2A MV-09-11	SB	
CS-1632-2	Auxiliary FW 2B Disch to SG 2B Valve SE-09-3	SE	
CS-1633-2	Auxiliary FW 2C Disch to SG 2A Valve SE-09-4	SB	
CS-179	Charging Pump 2C and Position Indication for Recirculation Valve V2553	SAB	
CS-652-2	Steam from SG 2A to Auxiliary FW 2C Turbine MV-08-13	SB	
CS-653-2	Steam from SG 2B to Auxiliary FW 2C Turbine MV-08-12	SA	
CS-632-2	Auxiliary FW Pump 2C Turbine	SAB	
CS-124	Pressurizer Back-up Heater Bank B-1	None	
CS-125	Pressurizer Back-up Heater Bank B-2	None	
CS-126	Pressurizer Back-up Heater Bank B-3	None	
CS-127	Pressurizer Back-up Heater Bank B-4	None	
CS-128	Pressurizer Back-up Heater Bank B-5	None	
CS-129	Pressurizer Back-up Heater Bank B-6	None	
CS-613-2	Auxiliary FW 2C to SG 2B MV-09-12	SA	
CS-1631-2	Auxiliary FW 2A to SG 2A SE-09-2	SA	
CS-1634-2	Auxiliary FW 2C to SC 2B SE-09-5	SA	

(1) Required for cold shutdown only.

(2) Instrument ranges are selected in accordance with standard engineering practices.

* This instrument includes an Auto/Manual switch located on the HSCP for operation of the Atmospheric Dump Valves.

TABLE 7.4-3

EMERGENCY REACTOR HOT SHUTDOWN/HOT STANDBY FROM OUTSIDE OF THE CONTROL ROOM CONTROL & TRANSFER SWITCH LIST

ITEM	CWD	EQUIPMENT	CLASS	TRANSFER SWITCH LOCATION	ALARM	HOT SHUTDOWN CONTROL SWITCH LOCATION	NOTES
1	177	Charging Pump 2A	1E	480 Swgr 2A2	M-46	HSP	(3)
2	178	Charging Pump 2B	1E	480 Swgr 2B2	M-47	HSP	(3)
3	179	Charging Pump 2C	1E	480 Swgr 2AB	M-48	HSP	(3)
4	124	Press Heater Bank B1	NS	Press Htr MCC 2A3	H-30	HSP	(4)
5	125	Press Heater Bank B2	NS	Press Htr MCC 2A3	H-30	HSP	(4)
6	126	Press Heater Bank B3	NS	Press Htr MCC 2A3	H-30	HSP	(4)
7	127	Press Heater Bank B4	NS	Press Htr MCC 2B3	H-30	HSP	(4)
8	128	Press Heater Bank B5	NS	Press Htr MCC 2B3	H-30	HSP	(4)
9	129	Press Heater Bank B6	NS	Press Htr MCC 2B3	H-30	HSP	(4)
10	189	AUX Spray Valve SE-02-3	1E	Transfer Panel 2A	H-12	HSP	(4)
11	189	AUX Spray Valve SE-02-4	1E	Transfer Panel 2B	H-12	HSP	(4)
12	176	Charging Line Valve SE-02-1	1E	Transfer Panel 2B	M-36	HSP	(4)
13	176	Charging Line Valve SE-02-2	1E	Transfer Panel 2A	M-36	HSP	(4)
14	194	Charging Line Isolation V2523	1E	Transfer Panel 2A	M- 6	HSP	(4)
15	629	AUX FW Pump 2A	1E	4 kV Swgr 2A3	G-44	HSP	(3)
16	630	AUX FW Pump 2B	1E	4 kV Swgr 2B3	G-45	HSP	(3)
17	631	AUX FW Pump 2C	1E	Transfer Panel 2AB	G-46	HSP	(3)
18	1631	AFW 2A Disch Valve SE-09-2	1E	480 MCC 2A5	G-12	HSP	(4)
19	1632	AFW 2B Disch Valve SE-09-3	1E	480 MCC 2B5	G-13	HSP	(4)
20	652	AFWP 2C Steam Valve MV-08-13	1E	480V MCC 2B5	G-14	HSP	(3)
21	653	AFWP 2C Steam Valve MV-08-12	1E	480V MCC 2A5	G-14	HSP	(3)
22	608	AFW 2A Disch Valve MV-09-9	1E	MCC 2A5	G-12	HSP	(3)
23	609	AFW 2B Disch Valve MV-09-10	1E	MCC 2B5	G-13	HSP	(3)
24	1633	AFW 2C Disch Valve SE-09-4	1E	Transfer Panel 2B	G-12	HSP	(4)
25	1634	AFW 2C Disch Valve SE-09-5	1E	Transfer Panel 2A	G-13	HSP	(4)
26	612	AFW 2C Disch Valve MV-09-11	1E	Transfer Panel 2B	G-12	HSP	(3)
27	613	AFW 2C Disch Valve MV-09-12	1E	Transfer Panel 2A	G-13	HSP	(3)
28	1625	SG 2A ATM STM Dump MV-08-19A	1E	DC Starter	LB-12	HSP	(3)
29	1626	SG 2A ATM STM DUMP MV-08-18A	1E	DC Starter	LA-12	HSP	(3)
30	1627	SG 2B ATM STM Dump MV-08-19B	1E	DC Starter	LB-12	HSP	(3)
31	1628	SG 2B ATM STM Dump MV-08-18B	1E	DC Starter	LA-12	HSP	(3)
32	201	Component CW Pump 2A	1E	4 kV Swgr 2A3	S-51	4 kV Swgr 2A3	(1)(3)
33	205	Component CW Pump 2B	1E	4 kV Swgr 2B3	S-52	4 kV Swgr 2A3	(1)(3)
34	209	Component CW Pump 2C	1E	4 kV Swgr 2AB	S-53	4 kV Swgr 2AB	(1)(3)
35	203	Component CW Valve MV-14-3	1E	MCC 2AB	S-56	Local PB	(1)(3)
36	204	Component CW Valve MV-14-1	1E	MCC 2AB	S-55	Local PB	(1)(3)
37	207	Component CW Valve MV-14-4	1E	MCC 2AB	S-56	Local PB	(1)(3)
38	208	Component CW Valve MV-14-2	1E	MCC 2AB	S-55	Local PB	(1)(3)
39	832	Intake CW Pump 2A	1E	4 kV Swgr 2A3	E-46	4 kV Swgr 2A3	(1)(3)
40	833	Intake CW Pump 2B	1E	4 kV Swgr 2B3	E-47	4 kV Swgr 2B3	(1)(3)
41	834	Intake CW Pump 2C	1E	4 kV Swgr 2AB	E-48	4 kV Swgr 2AB	(1)(3)

TABLE 7.4-3 (Cont'd)

ITEM	CWD	EQUIPMENT	CLASS	TRANSFER SWITCH LOCATION	ALARM	HOT SHUTDOWN CONTROL SWITCH LOCATION	NOTES
42	285	Containment Fan Cooler HVS-1A	1E	480V MCC 2A9	T-22	480 V MCC 2A9	(1)(3)
43	286	Containment Fan Cooler HVS-1B	1E	480V MCC 2A9	T-23	480 V MCC 2A9	(1)(3)
44	304	Containment Fan Cooler HVS-1C	1E	480V MCC 2B9	T-24	480 V MCC 2B9	(1)(3)
45	305	Containment Fan Cooler HVS-1D	1E	480V MCC 2B9	U-19	480 V MCC 2B9	(1)(3)
46	220	MV-14-9 CCW to and from Contain-	1E	MCC 2A5	T- 3	Local PB	(1)(3)
47	221	MV-14-10 ment Coolers	1E	MCC 2A5	T- 3	Local PB	(1)(3)
48	222	MV-14-11 CCW to and from Contain-	1E	MCC 2A5	T- 3	Local PB	(1)(3)
49	223	MV-14-12 ment Coolers	1E	MCC 2A5	T- 3	Local PB	(1)(3)
50	224	MV-14-13 CCW to and from Contain-	1E	MCC 2B5	T- 3	Local PB	(1)(3)
51	225	MV-14-14 ment Coolers	1E	MCC 2B5	T- 3	Local PB	(1)(3)
-	226	MV-14-15 CCW to and from Contain-	1E	MCC 2B5	T- 3	Local PB	(1)(3)
53	227	MV-14-16 ment Coolers	1E	MCC 2B5	T- 3	Local PB	(1)(3)
54	165	Boric Acid Grav. Feed V2508	1E	MCC 2B5	M-33	Local PB	(1)(3)
55	166	Boric Acid Grav. Feed V2509	1E	MCC 2B5	M-41	Local PB	(1)(3)
56	167	Make-Up By Pass to Ch. V2514	1E	MCC 2A5	M-42	Local PB	(1)(3)
57	174	Boric Acid Makeup Pump 2A	1E	MCC 2A6	N-47	Local Switch	(4)
58	175	Boric Acid Makeup Pump 2B	1E	MCC 2A6	N-48	Local Switch	(4)
59	906	4 kV Startup Transfer 2A2	NS	4 kV Swgr 2A2	B-51	4 kV Swgr 2A2	(3)
60	907	4 kV Startup Transfer 2B2	NS	4 kV Swgr 2B2	A-51	4 kV Swgr 2B2	(3)
61	934	4kV Bus Tie 2A2 to 2A3	NS	4 kV Swgr 2A2	B-52	4 kV Swgr 2A2	(3)
62	935	4 kV Bus Tie 2B2 to 2B3	NS	4 kV Swgr 2B2	A-52	4 kV Swgr 2B2	(3)
63	936	4 kV Bus Tie 2A3 to 2A2	1E	4 kV Swgr 2A3	B-52	4 kV Swgr 2A3	(3)
64	937	4 kV Bus Tie 2B3 to 2A2	1E	4 kV Swgr 2B3	A-52	4 kV Swgr 2B3	(3)
65	938	4 kV Bus Tie 2A3 to 2AB	1E	4 kV Swgr 2A3	B-54	4 kV Swgr 2A3	(3)
66	939	4 kV Bus Tie 2B3 to 2AB	1E	4 kV Swgr 2B3	A-54	4 kV Swgr 2B3	(3)
67	940	4 kV Bus Tie 2AB to 2A3	1E	4 kV Swgr 2AB	B-54	4 kV Swgr 2AB	(3)
68	941	4 kV Bus Tie 2AB to 2B3	1E	4 kV Swgr 2AB	A-54	4 kV Swgr 2AB	(3)
69	946	Sta Service Transf. 2A2	1E	4 kV Swgr 2A3	B-57	4 kV Swgr 2A3	(3)
70	948	Sta Service Transf. 2B2	1E	4 kV Swgr 2B3	A-57	4 kV Swgr 2B3	(3)
71	977	480V Swgr 2A2 Feeder	1E	480V Swgr 2A2	B-57	480V Swgr 2A2	(3)
72	980	480V Swgr 2B2 Feeder	1E	480V Swgr 2B2	A-57	480V Swgr 2B2	(3)
73	978	480V Swgr Tie 2A2 to 2AB	1E	480V Swgr 2A2	B-58	480V Swgr 2A2	(3)
74	981	480V Swgr Tie 2B2 to 2AB	1E	480V Swgr 2B2	A-58	480V Swgr 2B2	(3)
75	979	480V Swgr Tie 2AB to 2A2	1E	480V Swgr 2AB	B-58	480V Swgr 2AB	(3)
76	982	480V Swgr Tie 2AB to 2B2	1E	480V Swgr 2AB	A-58	480V Swgr 2AB	(3)
77	943	Pressurizer Heater Transf 2A	1E	4 kV Swgr 2A3	B-59	4 kV Swgr 2A3	(3)
78	944	Pressurizer Heater Transf 2B	1E	4 kV Swgr 2B3	A-59	4 kV Swgr 2B3	(3)
79	953	Diesel Gen Breaker 2A	1E	4 kV Swgr 2A3	B-56	4 kV Swgr 2A3	(3)
80	963	Diesel Gen Breaker 2B	1E	4 kV Swgr 2B3	A-56	4 kV Swgr 2B3	(3)
81	956	DG 2A Control	1E	DG 2A CP	B-26	DG 2A CP	(3)
82	958	DG 2A Governor Contr.	1E	DG 2A CP	B-26	DG 2A CP	(3)
83	1608	DG 2A Volt Regulator	1E	DG 2A CP	B-26	DG 2A CP	(3)
84	966	DG 2B Control	1E	DG 2B CP	A-26	DG 2B CP	(3)
85	968	DG 2B Governor Contr.	1E	DG 2B CP	A-26	DG 2B CP	(3)
86	1618	DG 2B Volt Regulator	1E	DG 2B CP	A-26	DG 2B CP	(3)

TABLE 7.4-3 (Cont'd)

ITEM	CWD	EQUIPMENT	CLASS	TRANSFER SWITCH LOCATION	ALARM	HOT SHUTDOWN CONTROL SWITCH LOCATION	NOTES
87	198	Charging Pump 2C Bypass V2553	1E	480V MCC 2AB	M-48	Hot Shutdown Panel (Valve Position Indication Only)	(3)
88	197	Charging Pump 2B Bypass V2554	1E	480V MCC 2B5	M-47	Hot Shutdown Panel (Valve Position Indication Only)	(3)
89	196	Charging Pump 2A Bypass V2555	1E	480V MCC 2A5	M-46	Hot Shutdown Panel (Valve Position Indication Only)	(3)
90	162	RWT to Charging Pumps V2504	NS	None	----	Local Manual Valve Control	
91	1126	DG Fuel Oil Transfer Pump 2A	1E	None	None	DG 2A Control Panel	(2)
92	1136	DG Fuel Oil Transfer Pump 2B	1E	None	None	DG 2B Control Panel	(2)
93	1126	DG Fuel Oil Transfer Shutoff Valve SE-59-1A1	1E	None	None	Auto Control - Local	(2)
94	1126	DG Fuel Oil Transfer Shutoff Valve SE-59-1A2	1E	None	None	Auto Control - Local	(2)
95	1136	DC Fuel Oil Transfer Shutoff Valve SE-59-1B1	1E	None	None	Auto Control - Local	(2) (2)
96	1136	DC Fuel Oil Transfer Shutoff Valve SE-59-1B2	1E	None	None	Auto Control - Local	
98	146	Boric Acid Heat Trace System A	1E	None	None	Local Auto Control	(2)
99	147	Boric Acid Heat Trace System B	1E	None	None	Local Auto Control	(2)
100	476	Elec Equipment RM Supply Fan (HVS-5A)	1E	480V MCC 2A5	None	Local Control	(2) PCM 99104
101	477	Elec Equipment RM Supply Fan (HVS-5B)	1E	None	None	Local Control	(2)
102	46B	Elec Equip RM Exhaust (HVE-11)	1E	480 MCC 2A6	X-6	Local Control	(4)
103	468	Elec Equip RM Exhaust (HVE-12)	1E	None	None	Local Control	
104	1169	Power Roof Vent (RV-3)	1E	None	None	Local Control	(2)
105	1169	Power Roof Vent (RV-4)	1E	None	None	Local Control	(2)
106	157	Letdown Isol Valve V2515	1E	Transfer PNL 2B	M-37	HSP	(1)(3)
107	157	Letdown Isol Valve V2516	1E	Transfer PNL 2A	M-44	HSP	(1)(3)
108	194	Letdown Isol Valve V2522	1E	Transfer PNL 2B	M-21	HSP	(1)(3)
109	1702	480V SWGR 2A5 FDR	1E	480V SWGR 2A5	B-57	480V SWR 2A5	(1)(3)
110	1712	480V SWGR 2B5 FDR	1E	480V SWGR 2B5	A-57	480V SWR 2B5	(1)(3)
111	503	Reactor Aux Bldg Emergency Exhaust Fan HVE-9A	1E	480V MCC 2A5	W-10	Local Control	(4)
112	1629	PORV V1474	1E	Local Box	H-40	None	(4)
113	1630	PORV V1475	1E	Local Box	H-40	None	(4)

Notes:

(1) - Required for Cold Shutdown
(2) - No Interaction with the control room
(3) - Equipment does not change operating status (remains as is) by switching transfer switch to "isolate" position.
(4) - Equipment changes status and assumes safe position required by the Hot Shutdown Panel or local control switch position. Procedures for reactor shutdown from outside the control room specify Hot Shutdown Panel/Local control switch position settings while the reactor is controlled from the control room.

TABLE 7.4-4

EMERGENCY REACTOR COOLDOWN & SHUTDOWN
FROM OUTSIDE OF THE CONTROL ROOM

ITEM	CWD	EQUIPMENT	CLASS	COLD SHUTDOWN CONTROL SWITCH	NOTES
1	246	Safety Injection Block CH-A	1E	HSP (Key Lock SW)	(1)
2	248	Safety Injection Block CH-B	1E	HSP (Key Lock SW)	(1)
3	269	SI Tank 2A1 Isol Valve V3624	1E	CS-Key Operated	
4	270	SI Tank 2A2 Isol Valve V3614	1E	Switch-Outside	
5	271	SI Tank 2B1 Isol Valve V3634	1E	Control Room & Outside	
6	272	SI Tank 2B2 Isol Valve V3644	1E	Containment	
7	249	Shutdown Isol Valve V3480	1E		
8	250	Shutdown Isol Valve V3481	1E	Pressurizer	
9	254	Shutdown Isol Valve V3652	1E	Pressure Interlocks	
10	253	Shutdown Isol Valve V3651	1E		
11	1501	Shutdown Isol Valve V3545	1E		
12	1502	Shutdown Isol Valve V3664	1E	CS-Key Operated Switch outside control room & containment	
13	1503	Shutdown Isol Valve V3665	1E		
14	251	LPSI Pump 2A	1E	4KV SWGR 2A3-2 CS CLOSE/TRIP & SS ISOL/NORM	(4)
15	252	LPSI Pump 2B	1E	4KV SWGR 2B3-6 CS CLOSE/TRIP & SS ISOL/NORM	(4)
16	1504	Shdn from HX 2A V3456	1E		
17	1505	Shdn from HX 2B V3457	1E	CS-Key Operated	
18	1506	Shdn to HX 2A V3517	1E	Switch	
19	1507	Shun to HX 2B V3658	1E	Local	
20	1510	Shdn Warm-up V3536	1E		
21	1511	Shdn Warm-up V3539	1E		
22	1514	Shdn Control HCV-3657	1E		
23	1515	Shdn Control HCV-3512	1E		
24	1516	LPSI Loop 2A Flow FCV-3306	1E	Key Operated	
25	1517	LPSI Loop 2B Flow FCV-3301	1E	Control Switch - Local	
26	257	LPSI Flow Contr. HCV-3615	1E		
27	260	LPSI Flow Contr. HCV-3625	1E	Local PB Sta	
28	263	LPSI Flow Contr. HCV-3635	1E		
29	266	LPSI Flow Contr. HCV-3645	1E		
30	244	Mini Flow V3659	1E		
31	245	Mini Flow V3660	1E	Key locked	
32	1520	Mini Flow V3495	1E	Local Contr. Sw's	
33	1520	Mini Flow V3496	1E		
34	247	SI Tank 2A2 Vent V3733	1E		
35	247	SI Tank 2A1 Vent V3735	1E		
36	247	SI Tank 2B2 Vent V3739	1E	Key Locked	
37	247	SI Tank 2B1 Vent V3737	1E	Local Control Sw's	
38	275	SI Tank 2A2 Vent V3734	1E	Located Outside	
39	275	SI Tank 2A1 Vert V3736	1E	Containment & Outside	
40	275	SI Tank 2B2 Vent V3740	1E	Control Room	
41	275	SI Tank 2B1 Vent V3738	1E		

EC283597

TABLE 7.4-4 (Cont'd)

ITEM	CWD	EQUIPMENT	CLASS	COLD SHUTDOWN CONTROL SWITCH	NOTES	
42	578	Primary Coolant Sample V5200	1E	Cable Spreading Room		
43	578	Primary Coolant Sample V5203	1E	Outside N. Wall of PASS Room		
44	579	Pressurizer Surge Sample V5201	1E	Cable Spreading Room		
45	579	Pressurizer Surge Sample V5204	1E	Pipe Penetration Room		
46	580	Pressurizer Steam Sample V5202	1E	Cable Spreading Room		
47	580	Pressurizer Steam Sample V5205	1E	Pipe Penetration Room		
48	1531	LPSI Pump 2A Suction V3444	1E	Key Locked -		
49	1532	LPSI Pump 2B Suction V3432	1E	Local Control Sw's		
50	1529	Containment Spray Hdr. 2A MV-07-3	1E			
51	1530	Containment Spray Hdr. 2B MV-07-4	1E			
52	211	CCW From HX 2A HCV-14-3A	1E	None – Local Manual Operation Required	(4)	
53	211	CCW From HX 2B HCV-14-3B	1E			
54	505	ECCS Area Supply HVS-4A	1E	Local PB Sta		
55	506	ECCS Area Supply HVS-4B	1E	Local PB Sta		
56	503	ECCS Area Exhaust HVE-9A	1E	Local PB Sta		
57	504	ECCS Area Exhaust HVE-9B	1E	Local PB Sta		
58	465	ECCS Area Dampers	1E	Automatic Control by HVE-9A, -9B		
61	237	HPSI Pump 2A	1E	4KV SWGR 2A3-1 CS & SS ISOL/NORM	(2)	(3)
63	238	HPSI Pump 2B	1E	4KV SWGR 2B3-5 CS & SS ISOL/NORM	(2)	(3)
63	287	Containment Spray Pump 2A	1E	4KV SWGR 2A3-3 CS & SS ISOL/NORM	(2)	(3)
64	290	Containment Spray Pump 2B	1E	4KV SWGR 2B3-7 CS & SS ISOL/NORM	(2)	(3)

EC283597

NOTES:

(1) - SIAS cannot be blocked unless pressurizer pressure is less than the “block permissive” allowed by Technical Specifications.
(2) - Transfer Switch Deactivated by Jumpering SW Contacts to Permit Automatic Start by ESFAS. ESFAS Cabinets are Located in the Control Room.
(3) - Not Required for Hot or Cold Shutdown.
(4) - Required for cold shutdown only.

TABLE 7.4-5

EMERGENCY REACTOR SHUTDOWN FROM OUTSIDE OF THE CONTROL ROOM - INSTRUMENTATION

ITEM	CWD	EQUIPMENT	CLASS	TRANSFER SWITCH LOCATION	ALARM	COLD SHUTDOWN INSTR SWITCH	NOTES
1	369	Steam Gen 2A Level LI-9113	1E	Not Required	None	HSP	(2)
2	369	Steam Gen 2B Level LI-9123	1E	Not Required	None	HSP	(2)
3	136	Reactor Cold Leg Temp TI-1115-1	1E	Not Required	None	HSP	(2)
4	137	Reactor Cold Leg Temp TI-1125-1	1E	Not Required	None	HSP	(2)
5	370	Pressurizer Press PI-1108	1E	Not Required	None	HSP	(2)
6	370	Pressurizer Press PI-1107	1E	Not Required	None	HSP	(2)
7	370	Pressurizer Level LI-1105	1E	Not Required	None	HSP	(2)
8	370	Pressurizer Level LI-1104	1E	Not Required	None	HSP	(2)
9	369	Stm Gen 2A Press PI-8113	1E	Not Required	None	HSP	(2)
10	369	Stm Gen 2B Press PI-8123	1E	Not Required	None	HSP	(2)
11	955	DG 2A - Ammeter	1E	Not Required	None	DG 2A Control Panel	(2)
12	965	DG 2B - Ammeter	1E	Not Required	None	DG 2B Control Panel	(2)
13	1606	DG 2A Voltmeter	1E	Transfer Panel 2A	B-26	HSP	(3)
14	1606	DG 2A Wattmeter	1E	Transfer Panel 2A	B-26	HSP	(3)
15	1616	DG 2B Voltmeter	1E	Transfer Panel 2B	A-26	HSP	(3)
16	1616	DG 2B Wattmeter	1E	Transfer Panel 2B	A-26	HSP	(3)
17	603	Atmos Stm Dump Control PIC-08-1A1	1E	Transfer Panel 2A	G-41	RSP	(4)
18	603	Atmos Stm Dump Control PIC-08-1B1	1E	Transfer Panel 2B	G-41	HSP	(4)
19	654	Atmos Stm Dump Control PIC-08-3A1	1E	Transfer Panel 2A	G-41	HSP	(4)
20	654	Atmos Stm Dump Control PIC-08-3B1	1E	Transfer Panel 2B	G-41	HSP	(4)
21	1528	Shutdn Cooling Flow FI-3301	1E	None	None	HSP	(1)
22	1528	Shutdn Cooling Flow FI-3306	1E	None	None	HSP	(1)
23	1525	Shutdn Cooling Temp TI-3351Y	1E	None	None	HSP	(2)(1)
24	1525	Shutdn Cooling Temp TI-3352Y	1E	None	None	HSP	(2)(1)
25	50	Neutron Power J1-001A-1	1E	None	None	HSP	(1)
26	50	Neutron Power J1-001B-1	1E	None	None	HSP	(1)
27	150	Charging Flow FI-2212	1E	None	None	HSP	(2)
28	150	Charging Pressure PI-2212	1E	None	None	HSP	(2)
29	627	SG 2A Level Wide Range LI-9012	NS	Local Box	None	HSP	
30	627	SG 2B Level Wide Range LI-9022	NS	None	None	HSP	
31	58	Neutron Power RI-26-80A1	1E	None	None	HSP	(2)
32	59	Neutron Power RI-26-80B1	1E	None	None	HSP	(2)
33	151	Letdown HT EX Outlet Temp TI-2223	NS	None	None	HSP	(1)

NOTES:

(1) - Required for Cold Shutdown only
(2) - No interaction with the Control Room
(3) - Equipment does not change operating status (remains as is) by switching transfer switch to "isolate" position.
(4) - Equipment changes status and assumes safe position required by the Hot Shutdown Panel or Local control switch position. Procedures for reactor shutdown from outside the control room specify Hot Shutdown Panel/Local control switch position settings while the reactor is controlled from the control room.

TABLE 7.4-6

HOT SHUTDOWN PANEL SWITCH POSITIONS

ITEM # TABLE 7.4-3	EQUIPMENT	SWITCH POSITION ON THE HSP	REMARKS
4	Pressurizer Heater B1 (Back-up Heater)	Off	During normal operation the pressurizer pressure is maintained via the “Proportional Heaters”. The “Back-up Heaters” are normally off and placing them in the “Off” position on the HSP maintains the plant as is in the control room if offsite power loss is not postulated. With a loss of offsite power all heaters are off. With all heaters off the operator has a minimum of four hours to establish pressurizer pressure control. This is done outside the control room by manually loading the appropriate number of heaters on the emergency power source and turning heater switches to the “On” position on the HSP.
5	Pressurizer Heater B2 (Back-up Heater)	Off	
6	Pressurizer Heater B3 (Back-up Heater)	Off	
7	Pressurizer Heater B4 (Back-up Heater)	Off	
8	Pressurizer Heater B5 (Back-up Heater)	Off	
9	Pressurizer Heater B6 (Back-up Heater)	Off	
10	Auxiliary Spray Valve SE-02-3	Close	These valves are normally closed fail closed valves. Auxiliary spray is utilized during cooldown to reduce pressurizer pressure on a pre-determined curve. If auxilary spraying is interrupted, pressurizer pressure is maintained until spraying is resumed.
11	Auxiliary Spray Valve SE-02-4	Close	
12	Charging Line Valve SE-02-1	Open	These valves are normally open fail open valves and are closed only when the auxiliary spray is used during cooldown. Closing of the auxiliary spray valves (Items 10 and 11) and reopening of these valves during the transfer will maintain the pressurizer pressure until auxiliary spraying is resumed.
13	Charging Line Valve SE-02-2	Open	
14	Charging Line Isolation V2523	Open	This valve is a fail open locked open valve and it should not be closed during operation or shutdown.
18	AFW 2A Discharge Valve SE-09-2	Open	These valves are normally closed fail closed valves however, the Emergency Procedure will require placing these valves in the open position on the HSP. This position will ensure that water flow to the Steam Generators will not he terminated if it bas been automatically initiated before the transfer occurs. Steam Generator high-level isolation is manually accomplished from the HSP.
19	AFW 2B Discharge Valve SE-09-3	Open	
24	AFW 2C Discharge Valve SE-09-4	Open	
25	AFW 2C Discharge Valve SE-09-5	Open	

TABLE 7.4-6 (Cont'd)

ITEM # TABLE 7.4-3	EQUIPMENT	SWITCH POSITION ON THE HSP	REMARKS
106	Letdown Isolation Valve V2515	Close	These valves are normally-open, fail-closed valves. V2515 closes on SIAS, V2522 closes on CIS, and V2516 closes on SIAS or CIS. The analysis for shutdown from outside the control room for a fire assumes pressurizer level is maintained by isolation of letdown and by use of a charging system pump and valves. Plant procedures for a shutdown from outside the control room due to a fire require closing these valves in the control room to isolate letdown prior to the transfer of control to the HSP. The switch position of close on the HSP maintains the isolation of letdown. Loss of air closes these valves regardless of switch position.
107	Letdown Isolation Valve V2516	Close	
108	Letdown Isolation Valve V2522	Close	

HSP CONTROL

ITEM # TABLE 7.4-5	EQUIPMENT	POSITION	SETPOINT	REMARKS
17	Atmos Stm Dump Control PIC-08-1A1	Manual	Closed	During normal operation the control room controller for the ADVs are in the manual mode with a setpoint to maintain the valves closed. Similarly, the controller positions on the Hot Shutdown Panel is "Manual" set for fully closed valves. The closed position of the ADVs minimizes the possibility of a steam generator dryout event and thus promotes an orderly cooldown. These ADVs are backed-up by the safety relief valves if the pressure builds up during the transfer. After the transfer the operator has full manual control of the ADVs at the Hot Shutdown Panel.
18	Atmos Stm Dump Control PIC-08-1B1	Manual	Closed	
19	Atmos Stm Dump Control PIC-08-3A1	Manual	Closed	
20	Atmos Stm Dump Control PIC-08-3B1	Manual	Closed	

Note:

(#) Switch is not located on HSCP.

7.5 SAFETY RELATED DISPLAY INSTRUMENTATION

(INCLUDES NON-SAFETY RELATED DISPLAY INSTRUMENTATION)

This section describes non-safety and safety related display instrumentation. The safety related (Class 1E) display instrumentation provides timely information to the operator so that he may initiate appropriate safety actions if and when required. Non-safety instrumentation is used for normal operation and although not required may be available for operator information. Table 7.5-1 lists the safety display instrumentation.

7.5.1 DESCRIPTION

The safety related display instrumentation provides monitoring of the automatic or manually actuated systems associated with the operation of the plant during normal or accident conditions. The following displays are included:

- ESFAS Input Parameters/ESF Systems Monitoring (1E)
- ESF Support Systems Monitoring (1E)
- Reactor Protective System Monitoring (1E)
- CEA Position Indication System (non 1E)
- Control Boards (1E) and Annunciators (1E and non 1E)
- Bypass and Inoperable Status Indication (non 1E)
- Control Room Habitability Instrumentation (1E)
- Post Accident Monitoring Instrumentation (1E)
- Shutdown Cooling System Instrumentation (1E)

7.5.1.1 ESFAS Input Parameters/ESF System Monitoring

The Engineered Safety Features Actuation System (ESFAS) continuously monitors and feeds into the actuation logic the ESFAS input parameters in order to initiate the safeguards when parameters reach their trip setpoints. The ESFAS is described in Section 7.3. After the ESF systems are automatically actuated, they continue to function without operator action. Table 7.5-1 lists the ESFAS input parameters safety related display instrumentation.

Information is made available for monitoring the status of each ESF system. Sufficient information is provided to the operator in the control room to monitor ESF systems during normal operating and post accident conditions. Based on this information the operator can take any anticipatory action that is required. The available information consists of valve position indication, pump operating status, and indication of process parameters. Table 7.5-1 also lists ESF safety related display instrumentation.

The ESF valves have red and green indicating lights in the control room where a red light indicates open valve position and a green light indicates closed valve position. The lights are

powered from the same power source as the valve actuating circuit and are located above the control switch, except for valves supplied with valve position indicators; in this case, the valve position indicator is located above the control switch lights located on the vertical section of the board.

Refer to Table 7.5-4 for a list of valves which have position indicators and indicating lights in the control room.

7.5.1.2 ESF Support Systems Monitoring

ESF support systems are those systems which are required to function when the ESF systems are operating (Subsection 7.3.1.1.6). The instrumentation provided enables the operator to monitor the process variables for these systems in order to take appropriate action when required. The ESF support systems are as follows:

- Component Cooling Water System
- Intake Cooling Water System
- Onsite Power System, including Diesel Generator System
- HVAC Systems for Areas Containing ESF Systems
- Diesel Fuel Oil Storage and Transfer System

The safety related display instrumentation for the ESF support systems are also listed in Table 7.5-1.

7.5.1.3 Reactor Protective System (RPS) Monitoring

The RPS has automatic monitoring of the safety parameters and does not require operator action. Sufficient information is provided to the operator in the control room to confirm that a limiting setpoint has been reached and that a reactor trip has taken place. This information includes: pretrip reactor trip indication, warning lights, audible alarms, control element assembly (CEA) position indication (Subsection 7.5.1.4) and trip switchgear circuit breaker position indication. Subsequently, the operator has full verification that the reactor has tripped and that the CEAs are fully inserted into the core by monitoring the CEA position and neutron level information that is provided in the control room. The display instrumentation together with the system components for the RPS are described in Section 7.2. The display instrumentation in the control room for the RPS is listed in Table 7.5-1.

7.5.1.4 CEA Position Indication System

a. Pulse Counting CEA Position Indication System

The pulse counting CEA position indication system infers each CEA position by maintaining a record of the "up" and "down" control power pulses received from the Control Element Drive Mechanism Control System (CEDMCS). Each "up" or "down" pulse represents 0.75 inches of CEA motion. The CEA position value associated with each CEA is reset to zero whenever the rod dropped contact (located within the reed switch position transmitter housing) is closed. This

permits the pulse counting system to automatically reset the position to zero whenever a reactor trip occurs or whenever a CEA is dropped into the core. This system is incorporated in the DCS which transmits digital information to an output printer. CEA position information is periodically printed out by the printer and also upon operator demand, for a permanent record. The DCS also provides deviation information to the reactor operator. If the deviation in position between the highest and lowest CEA in any group exceeds either of two preset amounts (for predeviation or deviation), an alarm is annunciated. This alarm condition is documented on the DCS printer. The DCS also provides alarm information when an out-of-sequence condition occurs for the regulating groups or power and pre-power dependent insertion limits are being exceeded.

b. Reed Switch CEA Position Indication System

The reed switch CEA position indication system utilizes a series of magnetically actuated reed switches, spaced at 1-1/2 inch intervals along the CEDM housing and arranged with precision resistors in a voltage divider network. These reed switches are employed on each CEA to provide an analog voltage signal that is proportional to the CEA position. This voltage signal is continuously output by its reed switch position transmitter to the Analog Display System (ADS) (refer to Subsection 7.7.1.1.6). The reed switch position transmitter signals are displayed in a bar graph format by the ADS display on the control board. In addition reactor power signals from the Reactor Protective System received through isolation in accordance with IEEE 279-1971, are used to determine the prepower dependent insertion limit and power dependent insertion limit for each CEA regulating group. Both insertion limits are displayed on the display to assist the operator in ensuring a correct control rod pattern. A backup numerical display is employed to readout an individual CEA position selected by the operator. This backup numerical display is completely independent of the ADS logic and displays. This feature can be used to cross-check the display.

c. CEA Limits Indication System

The Control Element Drive Mechanism Control System (CEDMCS) receives indication of a fully withdrawn or fully inserted CEA position from distinct contact closure signals from the reed switch position transmitter assembly. The reed switch position transmitter assembly, on each CEA, transmits an upper electrical limit signal, if the CEA is fully withdrawn or transmits a lower electrical limit signal, if the CEA is fully inserted. The CEDMCS control panel provides indication of CEA travel limits to the reactor operator when an upper or lower limit signal is received for a CEA. The CEA limits indication system is separate from the reed switch CEA position indication system discussed in Subsection 7.5.1.4.b. The CEA Limits Indication System is powered by battery backed supply to provide indication in the control room under LOOP or SBO conditions.

d. Core Mimic CEA Limit Indication

A light display, arranged in the shape of the CEA configuration in the core, is provided in the control room to indicate the dropped rod status of each CEA. The

detection of a dropped CEA is received, through the CEDMCS, from the dropped rod contact on the reed switch position transmitter assembly for each CEA. The Core Mimic CEA Limit Indication is powered from battery backed supply to provide indication in the control room under LOOP or SBO conditions.

e. NSSS Process Display Instrumentation

Table 7.5-1 lists the safety related process instrumentation that is provided to inform the operator of the status of the NSSS. This information, which is used for the startup, operation and shutdown of the plant, is provided on the reactor turbine generator board (RTGB) and other control panels in the control room. Indicating and control instrumentation is provided at local panels and the hot shutdown panel outside of the control room to allow reactor shutdown and maintenance of the reactor in a safe condition during either hot shutdown or cold shutdown.

7.5.1.5 Control Boards and Annunciators

a. Control Boards

The reactor-turbine generator board (RTGB) is a free standing benchboard type board with control switches primarily arranged on the lower bench portion, indicating and recording display instrumentation primarily on the lower vertical section, and annunciator windows on the upper vertical section. The RTGB consists of six separate control panels as follows:

- 201 Turbine Generator Control Panel
- 202 Feedwater and Cooling Water Systems
- 203 Reactor Coolant System
- 204 Reactivity Control
- 205 Waste Management and Chemical and Volume Control System
- 206 Engineered Safety Features Systems

The heating ventilating control board (HVCB) and plant auxiliary boards are free standing vertical boards with control switches, indicating and recording display or flat panel display driven by Distributed Control System (DCS) instrumentation on the front of the boards. For a discussion of plant heating, ventilating and air conditioning systems see Section 9.4.

Plant Auxiliary Control Board 1, PACB-1, is one panel section of Heating-Ventilating and Plant Auxiliaries Control Board. On the safety sections of the board (SA and SB section), two safety-related redundant annunciator panels LA and LB and atmospheric steam dump controls are located. The atmospheric steam dump controls are duplicated here as a backup to the controls located on RTG board 202 and the Hot Shutdown panel. The safety section is separated from the non-safety section of the plant auxiliary control board in accordance with Regulatory Guide 1.75 (R1) (refer to Table 7.5-1).

Plant Auxiliary Control Board 2, PACB-2, is located next to the Safety Related Radiation Monitoring Panels. The panel has several safety-related instruments including, but not limited to, Containment Sump Water Level recorder, Containment Pressure recorder, Neutron Power Wide Range recorders, and PORV and SRV position indication. See Table 7.5-1 for Safety Related Instruments located on the two Plant Auxiliary Control Boards.

The hot shutdown panel is a free standing vertical board with control switches and indicating display instrumentation on the front of the board. For a discussion of emergency shutdown from outside the control room see Subsection 7.4.1.5.

The display instruments, switches and indicating lights are functionally grouped on the boards and identified with nameplates for each component. The safety related display instrumentation located on each of the above mentioned boards are listed in Table 7.5-1.

b. Annunciators

The annunciator windows are located on the upper vertical portion of the RTGB and HVCB and are functionally grouped and form nonsafety display units.

The annunciator windows on each board are associated with the systems having instrumentation and/or controls on that same board. The annunciator initiating circuits, generated by the Class 1E devices are connected to the annunciator logic through isolation devices.

Safety related annunciator window display units are provided on the plant auxiliary board with 16 windows for channel SA and 16 windows for channel SB. Table 7.5-3 lists the safety related windows.

Audible alarms, together with visual displays, alert the operator of departures from normal operating conditions, such as trips, bypasses, overrides of safety signals or equipment faults. The arrangement of annunciator windows is shown on figures listed in Table 1.7-1.

7.5.1.6 Bypass and Inoperable Status Indication

Bypass and inoperable status indication for ESF and ESF support systems are located on the 206 RTGB. The bypass and inoperable status system is actuated through logics within the annunciator cabinets, which processes safety related systems status information and drives indicating lights on the bypass and inoperable status module.

The light, indicating bypass or inoperable status, stays until the bypass is removed or the inoperable condition is rectified. St. Lucie Bypass Indication System is basically actuated automatically. The effectiveness of this automatic indicating system is further enhanced by including a manual actuation capability. The manual capability of the bypass indication system is endorsed by the Regulatory Guide 1.47 position C4, (R0).

The grouping of the windows on the status module indicates bypass and inoperable conditions on a system and channel level.

The listing of inoperable or bypass condition of the individual components is shown in Table 7.3-10. Description of bypass and inoperable status indication of the RPS and the ESF systems is discussed in Sections 7.2 and 7.3 respectively.

7.5.1.7 Control Room Habitability Instrumentation

The design for the control room habitability system is discussed in Section 6.4. The Control Room Air Conditioning System is discussed in Subsection 9.4.1. The system flow and P & I diagrams are shown on Figures 9.4-1 and 9.4-2, respectively.

System component status indicating lights, system failure alarms and control room and outside air intake monitoring are provided in the control room to enable the operator to evaluate habitability conditions. Instrumentation for this system is listed in Tables 9.4-4 and 12.3-3 (Control Room outside air monitors).

7.5.1.8 Post Accident Monitoring Instrumentation

The post accident monitoring is designed to monitor plant variables during and following an accident; and conform to the requirements of Branch Technical Position EICSB Number 23, "Qualification of Safety Related Display Instrumentation for Post-Accident Condition Monitoring and Safe Shutdown," and Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Rev. 3. For more information see Subsection 7.5.2.9. EC286245

The wide range of information furnished to the operator by the extensive instrumentation and control systems depicted in Table 7.5-1 provides him with the long-term monitoring and surveillance capabilities of post accident conditions. For a complete list of Post Accident Monitoring Instrumentation see Subsection 7.5.2.9.

7.5.1.9 Shutdown Cooling System Instrumentation

A description of Shutdown Cooling System instrumentation is discussed in Subsection 7.4.1.3. Instrumentation utilized to monitor safe shutdown is listed in Table 7.4-1.

7.5.2 ANALYSIS

7.5.2.1 ESFAS Input Parameters/ESF Systems Monitoring

The following design criteria are used in the selection of ESF system monitored parameters:

a. Provide display of system conditions requiring operator attention or testing during routine plant operation.

b. Provide annunciation for automatic or manual initiation of any of the ESF systems including annunciation for malfunctions after system was initiated.

c. Provide information to determine if manual action is required to aid in proper system operation after automatic initiation, including input/output parameter indication for verification that proper functions have been established.

d. Provide indication for manually blocked or bypassed safeguard equipment.

e. Provide redundancy of indication.

The information which is displayed for the operators' use is listed in Table 7.5-1 consistent with the above criteria.

7.5.2.2 ESF Support Systems Monitoring

Information generated by the ESF support systems monitoring instrumentation is available to the operator to allow him to take appropriate action. The requirements are the same as for the ESF system. The following design criteria are used in the selection of monitoring instrumentation:

a. Provide a continuous display of various process parameters that are essential for proper support of the ESF systems in normal and in emergency modes.

b. Provide alarm for system conditions requiring operators' attention or action.

c. Provide redundancy of instrumentation, for reliability.

d. Provide visual verification of parameter function and accuracy during periodic testing of equipment.

Using these criteria the operator has sufficient instrumentation at his disposal, to assess properly the situation during various modes of operation in order to take corrective action if required. This instrumentation is shown in Table 7.5-1.

7.5.2.3 Reactor Protective System Monitoring

Sufficient information is provided for the operator to confirm that a trip has occurred.

CEA insertion information after a trip can be determined by the operator from the Analog Display System bar chart display and the Core Mimic CEA limit light indication (see Subsection 7.5.1.4).

Indication of neutron faux levels in the reactor core, as well as other reactor and RCS information, are provided for the operator.

The following design criteria were used in the selection of information that is provided to the operator:

a. System conditions requiring operator attention during routine plant operations and at the time of reactor trip are displayed in the control room.

b. Indication in the control room of all operations performed at the RPS cabinet affecting the function of the system.

c. Indication of all selected plant variables that are manually bypassed.

d. Indication of automatic removal of a bypass.

7.5.2.4 CEA Position Indication Systems

CEA position indication is provided to give the operator information to easily determine the CEA positions and perform any related operations that are required. The following design criteria are used in selection of the CEA position indication systems:

a. Provide a redundant and diverse means of indicating CEA position;

b. Provide a permanent record of any or all of the CEAs for which trend information is useful;

c. Provide a continuous display of all CEA positions and readout of any selected CEA;

d. Provide redundant means of displaying to the operator CEA deviation within a control group, improper group sequencing or overlap, and CEA group inserted below power dependent insertion limits; and

e. Provide separate fully inserted and fully withdrawn indications for each CEA.

7.5.2.5 NSSS Process Display Instrumentation

NSSS process display instrumentation gives the operator information to monitor conditions in the plant and to perform necessary operations. In addition, the information allows the operator to cross check protective system measurement channels to ensure operational availability of these channels as discussed in Sections 7.2 and 7.3. The following design criteria are used in the selection of the NSSS process instrumentation:

a. Provide continuous monitoring of process parameters required by the operator.

b. Provide reliable and comprehensible information to the operator.

c. Provide information display that adequately monitors the parameter over the range required for various conditions.

d. Provide a permanent record of those parameters for which trend information is useful.

e. Provide four channels of indication for RPS and ESFAS process parameters to allow cross checking of channels.

f. Ensure that failure of a single indicator or one channel does not adversely affect operators' action.

Sufficient information is provided for the operator to accurately assess the conditions within the plant systems, to perform those appropriate actions in a timely manner, and to maintain the reactor systems within the conditions assumed by the safety analyses in Chapter 15.

7.5.2.6 Control Panels and Annunciators

The control boards and annunciators are arranged in functional groupings to allow the operator to assess quickly the operating conditions of the various plant systems over the full range of normal operating and accident conditions.

Safety related parameters in the Reactor Protective System, ESFAS and systems required for safe shutdown are indicated and/or annunciated. This monitoring instrumentation also provides the means for determining malfunctions in safety related systems.

Control boards containing more than one set of redundant components are subdivided into compartments separated by a barrier. None of the compartments contain wiring or other components from redundant safety systems. Cables, entering the boards from redundant

components, are run in separate fully enclosed steel raceways. Wiring within the board mounted equipment is carried in separate enclosed raceways.

Electrical and physical separation in the panels is maintained between the following:

a. redundant safety related channels SA, SB, and SAB

b. redundant safety related measurement channels MA, MB, MC, and MD

c. redundant safety related (SA, SB AND SAB) channels and safety related (MA, MB, MC, and MD) measurement channels

d. Class 1E and non-Class 1E circuits

Identification of redundant cable and components is as described in Subsection 8.3.1.3.

7.5.2.7 Bypass and Inoperable Status Indication

Bypass or inoperable equipment conditions are governed by administrative procedures. These administrative procedures are supplemented by bypass and inoperable status indication of selected equipment in the control room.

The following design criteria are used in the selection of the status indication:

a. Provide indication windows for a bypass and inoperable condition on a system and channel level.

b. Determine the significance of the function of the equipment with regard to the safety of the plant.

c. Testing capability by activating each indicator manually.

Conformance with the Regulatory Guide 1.47 Position (R0) C2 is as follows:

The Bypass Indicating System is automatically activated by the bypassing or deliberately induced inoperability on the supporting systems. Table 7.3-10 reflects these requirements (e.g., LP Safety injection "A1" automatically activated by the diesel generator and/or pump motor breaker unavailability).

The operator has sufficient information about the important safety related systems which are removed from service, tested or being repaired, or disabled to allow him to take the proper course of action.

The bypass and inoperable status indication windows are listed in Table 7.3-10. Figure 7.5-8 shows the interaction of the diesel generator and the bypass and inoperable status indication board.

7.5.2.8 Control Room Habitability Instrumentation

During normal operation of the plant, the control room envelope is air conditioned by one or two of three air conditioning units. The air inside the control room is mixed with fresh air taken in from the north or the south side of the Reactor Auxiliary Building in order to maintain a positive

pressure differential. During an emergency condition the control room is isolated by closing the fresh air intakes, and the emergency air filtration is started. Indication is provided in the control room for the fresh air intakes, for the differential pressure and for the emergency air filtration. The instrumentation is shown in Tables 9.4-4 and 12.3-3 (Control Room outside air monitors).

7.5.2.9 Post Accident Monitoring Instrumentation

The post accident monitoring instrumentation, which is identified (as "Required Post Accident") in Table 7.5-1, is provided for monitoring post accident conditions within the RCS, the steam generating system and the containment.

The extensive instrumentation, as shown in the tables, provide the operator with required monitoring and surveillance capabilities to obtain information of post accident conditions. Accident environments and times required for equipment to operate post accident are referenced in Section 3.11.

The post accident monitoring (PAM) instrumentation design conforms to the requirements of Branch Technical Position EICSB Number 23 and Regulatory Guide (RG) 1.97, R3 through the following: EC286245

a. the PAM instrumentation is redundant, with indication in the control room and with at least one channel continuously recorded when required by RG 1.97 (R3). EC286245

b. the PAM instrumentation is energized from the onsite emergency power supplies.

c. the PAM instrumentation is qualified for operation in the environmental and seismic conditions specified in Sections 3.10 and 3.11. Recorders function with their required accuracy immediately after the SSE ground motion subsides without requiring any maintenance.

d. for the safety-related PAM instrumentation the intent of IEEE 279-1971 is applied as discussed below.

The requirements of IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Station," are not completely applicable to the design of the post accident monitoring instrumentation because this instrumentation is not a part of a protection system. However, the intent of the design criteria contained therein has been applied, in the design of those systems used for post accident monitoring conditions, to the following extent:

4.1 "General Functional Requirement"

The safety related display instrumentation is designed to provide monitoring of the automatic or manually actuated systems associated with the operation of the plant during normal or accident conditions. The instrument performance characteristics, response times, and accuracy are selected for compatibility with the design goal of providing the operator with longterm monitoring and surveillance capabilities after the plant has reached a stable condition.

4.2 "Single Failure Criterion"

The safety related display instrumentation "Single Failure Criterion" is functionally identical to that described in Subsection 7.3.2.1.2.

4.3 "Quality Control of Components and Modules"

For a discussion of the Quality Assurance program see Chapter 17.

4.4 "Equipment Qualification"

The post accident monitoring instrumentation meets the environmental and seismic qualification requirements discussed in Sections 3.10 and 3.11.

4.5 "Channel Integrity"

The safety related display instrumentation "Channel Integrity" is functionally identical to that described in Subsection 7.3.2.1.2.

4.6 "Channel Independence"

The safety related display instrumentation "Channel Independence" is functionally identical to that described in Subsection 7.3.2.1.2. Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with Regulatory Guide 1.75, Revision 3.

4.7 "Control and Protection Systems Interaction"

No control and protective interaction occurs in any portion of the post accident monitoring instrumentation.

4.8 "Derivation of System Inputs"

All system inputs are derived from signals that are direct measures of the desired variables.

4.9 "Capability for Sensor Checks"

The safety related display instrumentation sensors are checked by comparing the monitored variables of redundant channels or by observing the effects of introducing and varying a substitute input to the sensor similar to the measured variable.

4.10 "Capability for Test and Calibration"

IEEE 338-1971 and Regulatory Guide 1.22 "Periodic Testing of Protection System Actuation Functions" 2/72 (R0) provides guidance for the development of procedures, equipment and documentation of periodic testing. The measurement signals for post accident monitoring that are also signals of the RPS, ESF, ESF support or systems required for plant shutdown have the capability of being tested and calibrated under the design requirements of that respective system.

4.11 "Channel Bypass or Removal from Operation"

Any one of the channels may be tested, calibrated, or repaired without detrimental effects on the other channels. A limitation is provided in the Technical Specification for continued operation with one channel out of service.

4.12 through 4.17

These sections are not applicable.

4.18 "Access to Setpoint Adjustments, Calibration and Test Points"

Administrative controls are provided for access to calibration points.

4.19 "Identification of Protective Action"

This section is not applicable.

4.20 "Information Readout"

The post accident monitoring instrumentation contains indication of the required variable parameters for each of the redundant channels. At least one redundant channel of each analog variable is continuously recorded by a seismic Category I digital recorder in the control room.

4.21 "System Repair"

A defective component can be detected by testing. Replacement or repair of components within one channel does not affect the other channels.

4.22 "Identification"

The safety related display instrumentation equipment, including panels, meters, recorders, and cables associated with the system are uniquely identified. Interconnecting cables are color coded on channel basis (see Subsection 8.3.1.3).

Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"

The requirements of RG 1.97, R3 are defined and implemented as described below:

Variable Type Definitions

Type A - Those variables that provide primary information so that operators can take the specified manual actions for which there are no automatic actions so that safety systems can accomplish their safety function for DBE. This does not include those variables required for contingency actions.

Type B - Those variables that indicate that safety functions are being accomplished.

Type C - Those variables that indicate a breach or potential to breach of barriers to fission product release. (Fuel cladding, RCS pressure boundary, containment)

Type D - Those variables that indicate the operation of individual safety systems and other systems important to safety.

Type E - Those variables that indicate the magnitude of radioactive releases and for assessing such releases.

Design and Qualification Criteria

Category 1

a. Provide the most stringent requirements for key variables.

b. Qualified to RG 1.89 (R0)

c. Seismically qualified to RG 1.100 (R1). Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with Regulatory Guide 1.100 (R2).

d. The instrumentation systems are single failure proof.

e. A minimum, of two channels are provided with additional backup instruments (same or diverse) to verify correct channel in the event of a "mid-scale" instrument failure.

f. Redundant or diverse channels are independent and physically separated in accordance with RG 1.75 (R1). Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with Regulatory Guide 1.75 (R3).

g. The instrumentation is powered from Standby Power per RG 1.32 (R0) and backed up by battery where momentary interruption of power is not tolerable.

h. The instrumentation is available prior to an accident.

i. The proper QA requirements apply.

j. Continuous indication is provided (may be a recorder).

k. Where variable trending is required for operator information, dedicated recorders or continuously updated and stored in computer memory and displayed on demand information are provided.

l. These variables are considered PAM instrumentation or part of effluent monitoring instrumentation.

m. Types A, B, and C are identified on the control boards for easy recognition by the operator.

Category 2

a. Less stringent requirements than Category 1 and applies to variables which indicate system operating status.

b. Qualified to RG 1.89 (R0).

c. Seismic qualification to RG 1.100, (R1) if the device is part of a safety related system. Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with Regulatory Guide 1.100 (R2).

d. Instrumentation is powered from a high reliability power source.

e. Technical Specification out of service requirements for the system the process variable covers, apply also to the process variable components.

f. The proper QA requirements apply.

g. The signal way be displayed on an individual instrument or CRT (demand display).

h. The display may be dial, digital, CRT or stripchart recorder.

i. Where variable trending is required for operator information, a dedicated recorder or continuously updated, stored in computer memory and displayed on demand information is provided.

j. These variables are considered PAM instrumentation or part of effluent monitoring instrumentation.

k. Types A, B and C are identified on the control boards for easy recognition by the operator.

Category 3

a. Provides requirements for high qualified off-the-shelf instrumentation and applies to backup and diagnostic variables.

b. Provides the requirements for equipment where state-of-the art cannot meet Category 1 and 2 levels.

c. High quality commercial grade and capable of operating in the specified service environment.

d. Display may be dial, digital, CRT or stripchart recorder.

e. Where variable trending is required for operator information, a dedicated recorder or continuously updated, stored in computer memory and displayed on demand information is provided.

Implementation

Type A, B, C, D and E variables per reference 5 were identified to the NRC.

Environmental Qualification

Environmental qualification of RG 1.97, (R3) equipment is covered in Section 3.11.

Wide Range Steam Generator Level Instrumentation

In response to RG 1.97 concerning the issue of wide range level instrumentation, FPL committed to upgrade the environmental qualification of existing transmitters to meet post-accident containment conditions, and add a redundant measurement channel for each steam generator. The upgrade was completed under PC/M 138-293. Additionally, PC/M 068-294 added redundant instrumentation to the single instrument tap shared between the two channels.

Based on FPL letter to the NRC, L-92-28, dated February 10, 1992, the NRC agreed to an exception for redundant instrument taps until the steam generators are replaced.

Redundant Instrument Taps were provided with the replacement of the steam generators in fall 2007 and implementation of PC/M No. 05136M, “Steam Generator 2A & 2B Water Level modifications for the Unit 2 Component Replacement Projects.”

7.5.2.10 Shutdown Cooling System Instrumentation

The Shutdown Cooling System (SDCS) utilizes low pressure safety injection pumps, which are aligned for the Emergency Core Cooling System, (ECCS) mode of operation when the Reactor Coolant System temperature is above 325°F. Alignment from the ECCS to the SDCS mode is described in Subsection 5.4.7. For a discussion of the SDCS initiating circuits, logic, bypasses, interlocks and redundancy, see Subsection 7.4.1.3.

7.5.2.11 System Drawings

Applicable safety related display instrumentation system schematics, functional block diagrams, wiring diagrams and layouts are provided by reference in Section 1.7.

7.5.3 TMI RELATED ADDITIONAL ACCIDENT MONITORING INSTRUMENTATION

7.5.3.1 TMI Containment Pressure Monitors

In compliance with NUREG-0737 permanently installed wide range containment pressure monitors are provided for post accident monitoring of containment pressure.

7.5.3.1.1 Design Bases

a. Measurement and indication capability is provided over a range of -5 psig to four times the containment design pressure (175 psig).

b. Safety related redundant instrumentation channels are provided to meet the single failure criteria.

c. The redundant containment pressure monitoring instrumentation channels are energized from independent Class 1E power sources, and are physically separated in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems," January 1975 (R1).

d. The containment pressure monitoring instrumentation is qualified in accordance with IEEE 323-1974 for the design bases accident environment in which they operate.

e. The containment pressure monitors are designed seismic Category I and qualified per the IEEE 344-1975 criteria.

f. Continuous indication and recording of containment pressure is provided in the control room.

g. Each instrument covers the entire pressure range.

h. The monitoring instrumentation inputs are from sensors that directly measure containment pressure and provide input only to the containment pressure monitors.

i. An instrumentation channel is available during normal operation prior to an accident as specified in plant technical specification.

j. Testing and calibration requirements are specified in plant technical specification.

k. The instruments are specifically identified on the control panels so that the operator can easily discern that they are intended for use under accident conditions.

7.5.3.1.2 Design Description

The containment pressure detectors are electronic transmitters mounted outside the Reactor Containment Building. The detectors utilize independent sensing lines which penetrate the containment. A normally open fail closed solenoid valve with remote manual control operated from the control room is provided for containment isolation for each loop. The redundant containment pressure monitoring channels are provided with indicators in the control room and one of the channels is recorded in the control room. Instrument loop accuracy is addressed in Table 7.5-1.

7.5.3.1.3 Safety Evaluation

The TMI containment pressure monitors are designated seismic Category I and designed to the Quality Group B standard. Two more channels of containment pressure monitoring instrumentations are provided as post accident monitors (refer to Table 7.5-1). Hence in the unlikely event when the two redundant TMI containment pressure monitor displays disagree the operator has available to his disposition these other monitoring channels for verification purposes. Channel calibration and channel check are performed periodically.

7.5.3.2 TMI Containment Water Level Monitors

In compliance with NUREG-0737, permanently installed narrow and wide range containment water level monitors are provided for post accident monitoring. The narrow range instrument covers the range from the bottom to the top of the reactor cavity sump. The wide range instruments cover the range from the bottom of the containment to the elevation equivalent to 600,000 gallon capacity.

7.5.3.2.1 Design Bases

a. Safety related, redundant wide range water level monitors are provided to meet the single failure criteria. The wide range monitors are designed to seismic Category I requirements.

b. The redundant wide range water level instrumentation channels are energized from independent Class 1E power sources and are physically separated in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems," January 1975 (R1).

c. One narrow range containment water level monitor is provided.

d. Both the narrow and wide range containment water level monitoring channels are qualified to IEEE 323-1974 for post accident environment in which they operate seismic qualification per IEEE 344-1975 is also provided.

e. Continuous indication and recording of containment water level is provided in the control room.

f. Adequate overlapping of the ranges of narrow and wide range monitors are provided.

g. Signals from the associated sensors are only used for monitoring the containment water level.

h. The availability requirement of the wide range containment water level monitors is specified in plant technical specification.

i. Testing and calibration requirements are specified in plant technical specification.

j. The instruments are specifically identified on the control panels so that the operator can easily discern that they are intended for use under accident conditions.

7.5.3.2.2 Design Description

The wide and narrow range containment level detectors are located inside the containment. The narrow range monitor measures discrete level points from the bottom of the reactor cavity sump (elevation -7 ft.) to the top of the sump (elevation 0 ft.). The wide range monitors measure discrete level points from elevation -1 ft. to elevation 26 ft. of the containment. The electronics portion of each of the sensors are located outside the containment and converts the discrete point measurement to a continuous level indication in the control rooms. The two channels of wide range level monitors are recorded in the control room. The narrow range level monitoring channel is recorded also in the control room.

7.5.3.2.3 Safety Evaluation

The redundant wide range water level monitors are safety related and designated seismic Category I. They are qualified for the design basis accident environment in which they operate per IEEE 323-1974, seismic qualification is per IEEE 344-1975. These monitors are provided strictly for monitoring purpose.

The narrow range water level instrument is primarily used during normal operation and does not serve any safety related function post accident.

7.5.4 INSTRUMENTATION FOR DETECTION OF INADEQUATE CORE COOLING

This subsection responds to the requirements in Section II.F.2 of NUREG-0737 (Reference 1), for the development of CE instrumentation or detection of Inadequate Core Cooling (ICC).

Results of initial studies by the CE Owners Group are documented in reports CEN-117 (Reference 2) and CEN-125 (Reference 3).

7.5.4.1 Description of Inadequate Core Cooling (ICC)

7.5.4.1.1 Definition of ICC

The definition of ICC and the functional requirements for the ICC Detection System have been established within the bounds of the following core conditions:

a. The reactor is tripped so only decay power is considered.

b. The coolant level falls below the top of the core, which can occur only with a loss of coolant mass from the Reactor Coolant System (RCS).

c. The event proceeds slowly enough so that the operator has time to observe and to make use of the instrument displays.

The condition at which ICC is considered to occur is at a fuel clad temperature of 2200°F (which is the licensing limit for design basis events using approved analytical methods).

7.5.4.1.2 Description of Event Progression

Events considered have the potential for progressing toward and returning from ICC. Events which might progress to core uncovery and heatup or which might appear as such events include LOCA, loss-of-feedwater, and rapid cooldown events including steamline breaks. These events all have in common a progression through some or all of three distinct sets of thermal and hydraulic conditions during the approach to ICC, and they follow a reversal of that progression through the same thermal and hydraulic conditions during the recovery from ICC. The three sets of conditions and the ICC variables which are displayed to indicate each condition are as follows:

Condition 1: The reduction in subcooling until the primary system reaches saturation. Saturation Margin is the ICC variable.

Condition 2: The loss of coolant inventory from the reactor vessel until the two-phase level falls to the top of the active core. Collapsed level above the core is the ICC variable.

Condition 3: The rising core temperatures as the two-phase level falls below the top of the active fuel. Core exit superheat and steam temperature are the ICC variables.

The following subsections describe the sensors used in an ICC detection system during the above event progression

7.5.4.1.3 Description of Sensors

7.5.4.1.3.1 Saturation Margin Monitor

The Saturation Margin Monitor (SMM), using input from existing Resistance Temperature Detectors (RTD) in the hot and cold legs and from the pressurizer pressure sensors, detects the initial occurrence of saturation during LOCA events and during loss of heat sink events.

Fluid temperature measurements from the Heated Junction Thermocouples (HJTC) and the signals from core exit thermocouples are input to calculate and display degrees superheat (up to about 1800°F) in addition to degrees subcooling. The signals from the HJTC temperature measurements provide information about possible local differences in temperature between the

reactor vessel upper head/upper plenum (location of the HJTC) and the hot or cold legs (location of the RTDs). The core exit thermocouples respond to the coolant temperature at the core exit and their signal indicates superheat after the coolant level drops below the top of the core and, thus, provide an approximate indication of the depth of core uncovery.

The SMM can be used for detection of the approach to ICC, namely Condition 1 (loss of subcooling), and Condition 3 (core uncovery). The SMM is not capable of indicating the existence of Condition 2 when the coolant is at saturation conditions and the level is between the top of the vessel and the top of the core.

7.5.4.1.3.2 Resistance Temperature Detectors (RTD)

The RTDs sense the initial occurrence of saturation. However, the RTD range is not adequate for ICC indications during core uncovery since, as the uncovery proceeds, the superheated steam temperature may quickly exceed the upper limit of the RTD range. The core exit thermocouples and the unheated thermocouples in the HJTC are then used.

7.5.4.1.3.3 Heated Junction Thermocouples (HJTC)

The HJTC show the liquid inventory of the mixture of liquid and vapor coolant above the core. These are the instruments which show the approach to ICC in Condition 2, namely the period from the initial occurrence of saturation conditions until the start of core uncovery.

The installed instruments are also referred to as Liquid Level Probes (LLP), and the two terms may be used interchangeably.

7.5.4.1.3.4 Core Exit Thermocouples (CET)

The core exit thermocouples show the approach to ICC after core uncovery for the event analyzed. As mentioned above, the core exit thermocouples respond to the coolant temperature at the core exit and indicate superheat after the core is no longer completely covered by coolant. Except for a time delay of about 200 to 400 seconds, depending on event, the trend of the change in superheat corresponds to the trend of core uncovery as well as to the accompanying trend of the change in cladding temperature.

7.5.4.2 System Functional Description

In the following subsections a functional description of the instruments of the ICC Detection System is given and the function of the instruments is related to the ICC conditions which are described in Subsection 7.5.4.1.

7.5.4.2.1 Subcooling and Saturation

The parameters measured to detect subcooling and saturation are the RCS coolant temperature and the pressurizer pressure. Temperature is measured in the hot legs for typical LOCA type events and is measured in the vessel upper head region for cooldown events. The measurement range extends from the shutdown cooling conditions up to saturation conditions at the pressurizer safety valve setpoint. The response time is such that the operator obtains adequate information during those events which proceed slowly enough for him to observe and to act upon the information from the instrument display.

The information which is derived from the reactor vessel temperature and pressure measurements is the amount of subcooling during the initial approach to saturation conditions and the occurrence of saturation during Condition 1. Following core recovery, the reestablishment of subcooled conditions is obtained. During Condition 3, core uncovery, coolant superheat is measured.

7.5.4.2.2 Coolant Level Measurement in Reactor Vessel

The Reactor Coolant System is at saturation conditions until sufficient coolant is lost to lower the two-phase level to the top of the active core. A Reactor Vessel Level Monitoring System provides a direct measurement during this period. The parameter which is measured is the collapsed liquid level above the fuel alignment plate. The collapsed level represents the amount of liquid mass which is in the reactor vessel above the core. Measurement of the collapsed water level is selected because it is a direct indication of the water inventory.

The collapsed level is obtained over the same temperature and pressure range as the saturation measurements, thereby encompassing all operating and accident conditions where it must function. Also, it functions during the recovery interval. Therefore, it is designed to survive the high steam temperature which may occur during the preceeding core uncovery interval.

The level range extends from the top of the vessel down to the top of the fuel alignment plate. The response time is short enough to track the level during small break LOCA events. The resolution is sufficient to show the initial level drop, the key locations near the hot leg elevation and the lowest levels just above the alignment plate. This provides the operator with adequate indication to track the progression during Condition 2 and core recovery and to detect the consequences of his mitigating actions or the functionability of automatic equipment.

7.5.4.2.2.1 Alternate Reactor Vessel Level Monitoring

Technical Specifications required that an alternate method of determining reactor vessel level be implemented when both channels of RVLMS are out-of-service. The alternate methods are:

1. Mismatch between charging and letdown with incorrect response of pressurizer level to pressurizer spray or charging;

2. CET indicated temperature in the superheat region;

3. Unheated junction thermocouples indicating superheat.

PWR operators have been trained on these methods as part of the Mitigating Core Damage courses required following TMI.

7.5.4.2.2.2 Mismatch between Charging and Letdown with Incorrect Response of Pressurizer Level to Pressurizer Spray or Charging

This process to identify voids was incorporated into St. Lucie procedures following the Natural Circulation Cooldown event on Unit 1. A void developed in the reactor head due to incomplete cooling of the upper head region. The void was identified by the mismatch in charging and letdown and a response opposite to the normal response to pressurizer sprays. With voids present in the reactor vessel head, increasing pressurizer sprays causes pressurizer level to rise. A reduction in sprays and increased charging would cause pressurizer level to decrease. Both of

these indications are abnormal and opposite to what is expected for a subcooled RCS. Post event evaluations confirmed the creation and collapse of a reactor head void.

7.5.4.2.2.3 CET Indicating Temperatures in the Superheat Region

Events where RCS inventory is reduced to the top of the core can be determined by use of the CETs. Once the core becomes uncovered, the steam rising from the core would become superheated as it passes over the top of the uncovered fuel assemblies. The CETs can be used to monitor this condition by providing a temperature that indicates the steam has entered the superheat region. Pressurizer pressure and steam tables would have to be used in conjunction with the indicated temperature to determine that the steam is being superheated. The CETs can be read directly on QSPDS.

7.5.4.2.2.4 Unheated Junction Thermocouples Indicating Superheat

As discussed above, thermocouples can be used to determine if superheated conditions exist in the reactor core. The RVLMS uses both heated and unheated thermocouples to determine reactor vessel level. If the unheated thermocouples are available, they can be used and temperatures read from QSPDS.

7.5.4.2.3 Fuel Cladding Heatup

The overall intent of ICC detection is to detect the potential for fission product release from the reactor fuel. The parameter which is most directly related to the potential for fission product release is the cladding temperature rather than the uncovery of the core by coolant.

Since clad temperature is not directly measured, a parameter to which cladding temperature may be related is measured. This parameter is the fluid temperature at the core exit. After the core becomes uncovered, the fluid leaving the core is superheated steam and the amount of superheat is related to the fuel length exposed and to the cladding temperature.

The amount of superheat of the steam leaving the core is measured by the core exit thermocouples. The time behavior of the superheat temperature is, with the exception of an acceptably small time delay, similar to the time behavior of the cladding temperature. Thus, from the observation of the steam superheat, the behavior of the cladding temperature can be inferred. Observation of the cladding temperature trends during an accident is considered to be of more value to the operator than information on the absolute value of the cladding temperature.

The core exit steam temperature is measured with the thermocouples included in the Incore Instrument (ICI) string. They are located inside the ICI support tube above the fuel alignment plate. Calculations for representative uncovery events show that the thermocouples respond sufficiently fast to the increasing steam temperature.

The required temperature range of the thermocouples extends from the lowest saturation temperature at which uncovery may occur up to the maximum core average exit temperature which occurs when the peak clad temperature reaches 2200°F. The actual thermocouple range encompasses the required range, which extends from 32°F to about 1800°F. Thermocouples function with reduced accuracy at even higher temperatures, so the range for processing the thermocouple output extends to about 2300°F.

7.5.4.3 System Design Description

The following sensors have been selected as the basic instruments to meet the functional requirements described tn Subsection 7.5.4.2,

a. The Saturation Margin Monitoring (SMM) system (Reference 1)

b. The Heated Junction Thermocouple (HJTC) system (Reference 2) and

c. The Core Exit Thermocouple (CET) system.

The conceptual design of each ICC Instrument is described In this section which addresses:

a. Sensors design

b. Signal processing and display design

Figures 7.5-1a and 7.5-1b are the functional diagrams for the ICC instrument systems. Each instrument system consists of two safety grade channels from sensors through signal processing equipment. The outputs of processing equipment systems feeding the primary display (i.e., SAS/DCS) are isolated to separate safety grade and non-safety grade systems. Channelized safety grade backup displays are included for each instrument system. The following sections present details of the design.

7.5.4.3.1 Sensors Design

7.5.4.3.1.1 Saturation Margin Monitoring System (SMMS)

The SMM includes the RCS temperature and pressure inputs plus the maximum unheated junction thermocouple temperature (UHJTC) described in Subsection 7.5.4.3.1.2 and the representative core exit thermocouple (CET) temperature (Subsection 7.5.4.3.1.3). The UHJTC and CET inputs come from the outputs of the HJTC and CET processing units. In summary, the sensor inputs to the SMMS are:

Input	Range
Pressurizer Pressure	0-3000 psia
Cold Leg Temperature	50-750°F
Hot Leg Temperature	50-750°F
Maximum UHJTC Temperature (from HJTC processing)	32-2300°F
Representative CET Temperature (from CET processing)	32-2300°F

7.5.4.3.1.2 Heated Junction Thermocouple (HJTC) System

The HJTC system measures reactor coolant liquid inventory with discrete HJTC sensors located at different levels within a separator tube ranging from the top of the core to the reactor vessel head. The basic principle of system operation is the detection of a temperature difference between adjacent heated and unheated thermocouples.

The HJTC sensor consists of a Chromel-Alumel thermocouple surrounded by a resistance wire heater (or heated junction) and another Chromel-Alumel thermocouple (or unheated junction) positioned 4 1/2 inches above the heater. In a fluid with relatively good heat transfer properties, the temperature difference between the adjacent thermocouples is very small. In a fluid with relatively poor heat transfer properties, the temperature difference between the thermocouples is large.

Two design features ensure proper operation under all thermal-hydraulic conditions. First, each HJTC is shielded to avoid overcooling due to direct water contact during two-phase fluid conditions. The HJTC with the splash shield is referred to as the HJTC sensor (see Figure 7.5-2). Second, each string of HJTC sensors is enclosed in a separator tube that separates them from the turbulent liquid and vapor phases that surround the HJTC during a reactor coolant inventory transient.

The separator tube creates a collapsed liquid level that the HJTC sensors measure. This collapsed liquid level is directly related to the average liquid fraction of the fluid in the reactor head volume above the fuel alignment plate. This mode of direct in-vessel sensing reduces spurious fluid effects due to pressure, fluid properties, and non-homogeneities of the fluid medium. The string of HJTC sensors and the separator tube is referred to as the HJTC instrument.

The HJTC System is composed of two channels of HJTC instruments. Each HJTC instrument is manufactured into a probe assembly. The probe assembly includes eight HJTC sensors, a seal plug, and electrical connector (Figure 7.5-3). The eight HJTC sensors are located at eight levels from the reactor vessel head to the fuel alignment plate.

The volume above the core in the St. Lucie Unit 2 reactor vessel is hydraulically separated into two regions (Figure 7.5-5). The region between the Fuel Alignment Plate (FAP) and Upper Guide Structure Support Plate (UGSSP) is the upper plenum. The second region, between the UGSSP and the top of the vessel head, is the upper head. The HJTC probe assembly is located outside of a CEA shroud and extends through both these regions.

The HJTC probe assembly for St. Lucie Unit 2 is designed to measure the collapsed water level in the upper head independently from the collapsed water level in the upper plenum. This is accomplished by the use of a "split" probe assembly (Figure 7.5-6). Functionally, the probe is divided into an upper separator tube in the upper head region and a lower separator tube in the upper plenum region. A divider disk inside the probe located at the UGSSP elevation isolates the upper and lower tubes hydraulically. Holes at the top and bottom of each separator tube allow the collapsed water level in each region to be formed and measured inside the separator tubes.

The HJTC sensors are located axially in the probe assembly so that the collapsed water level in each region can be measured. The location of the eight sensors available in each of two probe assemblies are shown on Figure 7.5-6. A sensor is placed as high as possible in the upper head and upper plenum to provide an early indication of voiding in each region. A sensor just above the UGSSP indicates when the upper head is completely empty. A sensor placed midway between these sensors provides increased resolution for the level measurement in the upper head.

In the lower separator tube, sensors are placed at the top, centerline, and bottom of the hot leg. These sensors tell the operator when the collapsed water level passes through the hot leg

elevation. The final sensor is placed as close as possible to the FAP. This sensor provides an indication that the water inventory above the core in the upper plenum has been depleted and thus, gives an advanced warning of the impending core uncovery.

7.5.4.3.1.3 Core Exit Thermocouple (CET) System

St. Lucie Unit 2 is equipped with a Type K (Chromel-Alumel) thermocouple within each of the 56 (maximum) core exit thermocouples (CETs). The CETs are arranged so that 14 CETs are distributed as uniformly as possible in each of the four core quadrants. Each of the two Qualified Safety Parameter Display System (QSPDS) channels receives input from 28 CETS. The input of all valid CETs to each of the QSPDS channels will be used to determine the representative core exit temperature.

An Evaluation was made of the minimum number of valid CETs necessary for ICC detection. The evaluation determined the reduced complement of CETs that adequately detect initial core uncovery and trend the ensuing core heatup. The evaluation account for core nonuniformities including in-core effects of the radial decay power distribution; and ex-core effects of condensate runback in the hot legs and nonuniform inlet temperatures. Based on these evaluations adequate ICC detection is assured with two valid CETs per quadrant. Therefore, the full core complement of CETs to be installed is more than adequate for use In ICC detection, and provides an additional degree of operational flexibility.

The junction of each thermocouple is located a few inches above the fuel assembly inside a structure which supports and shields the ICI detector assembly string from flow forces in the outlet plenum region. These core exit thermocouples (CET) monitor the temperature of the reactor coolant as it exits the fuel assemblies. Figure 7.5-7A depicts a typical ICI detector assembly, showing the CET. The cure locations of the ICI detector assemblies are shown on Figure 7.5-7B.

The CETs have a usable temperature range from 32°F up to 2300°F (Reference 4) although accuracy is reduced at temperatures above 1800°F.

7.5.4.3.2 Signal Processing and Display Equipment Design

The processing and display hardware is divided into two major hardware groups - the Qualified Safety Parameter Display System (QSPDS) and the Safety Assessment System (SAS)/Distributed Control System (DCS). The equipment groups process and display the ICC detection sensor inputs as well as sensor inputs to meet other NRC requirements. The QSPDS provides the safety grade processing and display for the ICC detection instruments. The SAS is the non-safety grade primary display system which has full human factors engineering display capabilities. The design objectives for the equipment is to address the NUREG-0737 criteria, including the criteria for Attachment 1 to II.F.2 and Appendix B.

7.5.4.3.2.1 Qualified Safety Parameter Display System (QSPDS)

The QSPDS is a two-channel system which displays the ICC instrument (Saturation Margin Monitor, HJTC and CET System) outputs to the control room. The QSPDS uses a microprocessor-based design for the signal processing equipment in conjunction with an alphanumeric display for each of the two channels. Each channel accepts and processes ICC input signals and transmits its output to the SAS.

The two QSPDS channels are powered by Channel A & B station vital busses. Each QSPDS is electrically independent and physically separated according to the Regulatory Guide 1.75 (R1). The QSPDS Is designed to meet Class 1E isolation requirements. Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with Regulatory Guide 1.75 (R3).

The QSPDS is qualified environmentally in accordance with IEEE 323-1974 and seismically qualified according to IEEE STD 344-1975. Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with IEEE 323-1983 and seismic qualified according to IEEE 344-1987. The QSPDS consists of two redundant channels to avoid interruptions of display due to a single failure. This two safety grade channel configuration provides QSPDS availability greater than 99 percent. If in the remote chance that one complete QSPDS channel fails, the operator has:

a. Additional channels of ICC sensor inputs for cold leg temperature, hot leg temperature, and pressurizer pressure on the control board separate from the QSPDS.

b. The HJTCS and CET have multiple sensors in each channel for the operator to correlate and check inputs.

c. The HJTCS sensor output may be tested by adjusting the heater power.

The QSPDS is available during normal operation and availability is addressed in the Technical Specifications.

The QSPDS has two functions:

a. Sensor input processing

b. Display of safety parameters

The sensor input processing consists of:

a. Checking that the sensor inputs are within range

b. Converting sensor inputs into display units

c. Calculating parameters from the sensor inputs (if required)

d. Alarming when a parameter exceeds setpoint

The QSPDS processing equipment includes operator interfaces for equipment testing, setup, and maintenance. The processing for the ICC instrumentation will have surveillance testing and diagnostic capabilities. Automatic on-line surveillance tests continuously check for specified hardware and software malfunctions. The on-line automatic surveillance tests as a minimum, indicate inputs that are out of range and computer hardware malfunctions. The malfunctions are indicated through the operator interface. A manual on-line diagnostic capability is incorporated to aid the operator in locating the source of these malfunctions.

The QSPDS displays present the most reliable basic information for each of the ICC instrument systems. The QSPDS displays are designed:

a. To give primary instrument indications in the remote chance that the SAS display becomes inoperable.

b. To provide confirmatory indications to the SAS display.

c. To aid in surveillance tests and diagnostics.

The QSPDS displays (located in the control room) also incorporate human factors engineering. The two channels of QSPDS display present direct and continuous safety grade indication of the ICC detection parameters. The QSPDS displays the following types of information:

a. Safety parameters according to safety function.

b. Additional Safety parameter information on other pages (such as sensor inputs needed to calculate safety parameters).

c. Alarm indication.

7.5.4.3.2.2 Saturation Margin Monitoring System

The SMM processing equipment performs the following functions:

a. Calculates the saturation margin.

   The saturation temperature is calculated from the minimum pressure input and the saturation pressure is calculated from the maximum temperature input (see Subsection 7.5.4.3.1). The temperature saturation margin is the difference between saturation temperature and the maximum temperature input. The pressure saturation margin is the difference between saturation pressure and the minimum pressure input.

b. Processes all outputs for display.

c. Provides an alarm output when saturation margin reaches a preselected setpoint.

The following information is presented on the QSPDS displays:

a. Pressure margin to saturation

b. Temperature margin to saturation for each temperature source (i.e., RTD, HJTC or CET)

c. Temperature inputs

d. Pressure inputs

7.5.4.3.2.3 Heated Junction Thermocouple (HJTC) System

The processing equipment for the HJTC performs the following functions:

a. Determine if liquid inventory exists at the HJTC positions.

   The heated and unheated thermocouples in the HJTC are connected in such a way that absolute and differential temperature signals are available. The exact value for the differential temperature (ΔT) and the unheated junction temperatures (T_R) setpoints are based on test results (including Phase III testing) and a setpoint calculation. The ΔT setpoint is 200F. It is selected to ensure covered and uncovered conditions can be distinguished from each other unambiguously. The unheated junction (T_R) setpoint is 700F. The T_R setpoint is used to ensure a continued indication of sensor uncovery in high temperature environments when the applied heated junction heater power is cut back to prevent overheating the HJTC.

b. Determine the maximum upper head fluid temperature from the top three unheated thermocouples for use as an input to the SMM.

c. Process all inputs and calculated outputs for display.

d. Provide an alarm output when any of the HJTC detects the absence of liquid level.

e. Provide control of heater power for proper HJTC output signal level.

The following information is displayed on the QSPDS displays:

a. Liquid inventory level above the upper guide support plate derived from top three discrete HJTC positions and the liquid inventory above the fuel alignment plate to the upper guide support plate (plenum level) derived from the bottom five discrete HJTC positions.

b. Unheated junction temperature at the eight positions

c. Heated junction temperature at the eight positions.

7.5.4.3.2.4 Core Exit Thermocouple System

The processing equipment for the CETs performs the following functions:

a. Processes all core exit thermocouple inputs for display. Half of the available CET inputs (28 maximum CET per channel) are processed in each channel.

b. Provides an alarm output when the temperature from any of the CETs exceeds a preselected setpoint.

c. Determines the CET temperature to be supplied to the SMM.

The representative core exit temperature is calculated as follows. During normal RCS conditions (saturation margin alarm not active), non-valid core exit thermocouples (CETs) is detected with

out-of-scale checks, tolerance checks, and statistical analysis. The representative core exit temperature is selected from the upper end of the temperature distribution of the remaining valid CETs. While a saturation margin alarm is active, indicating abnormal RCS conditions, the same method will be used to select the representative core exit temperature from among the valid CETs determined during prior normal operation. The out-of-scale failure checks are still performed.

The following information is displayed on the QSPDS displays:

a. All CET temperatures for each channel (or 28 maximum CET temperatures)

b. The representative CET temperature

7.5.4.4 System Qualification

The in-vessel sensors are designed to meet the NUREG-0737, Appendix B guide to install the best equipment available consistent with qualification and schedular requirements. Design of the equipment is consistent with the guidelines of Appendix B as well as the clarification and Attachment 1 to Item II.F.2 in NUREG-0737. Specifically, instrumentation meets appropriate stress criteria when subjected to normal and design basis accident loadings. Seismic qualification to safe shutdown conditions verifies function after being subjected to the seismic loadings.

The out-of-vessel instrumentation system, up to and not including the cabinets are environmentally qualified in accordance with IEEE 323-1974 as interpreted by CENPD-255 Rev.01. Plant-specific containment temperature and pressure design profiles are used where appropriate in these tests. This equipment is seismically qualified according to IEEE STD 344-1975. CENPD-182, "Seismic Qualification of CE Supplied Instrumentation Equipment, Combustion Engineering, Inc.," May 1977 describes the methods used to meet the criteria of this document. Safety related QSPDS electronic (cabinet) equipment has been qualified in accordance with IEEE 323-1983 and seismic qualified according to IEEE 344-1987.

FP&L has evaluated what is required to augment the out-of-vessel Class 1E instrumentation equipment qualification program to NUREG-0588. Consistent with Appendix B of NUREG-0737, the out-of-vessel equipment under procurement is the best available equipment. See Section 3.11 for more information.

The primary display (i.e., SAS/DCS) is not designed as a Class 1E system, but is designed for high reliability; thus it is not qualified environmentally or seismically to Class 1E requirements nor does it meet the single failure criteria of Appendix B, Item 2. Post-accident maintenance accessibility is included in the design. The quality assurance provisions of Appendix B, Item 5 do not apply to the primary display according to NUREG-0737. However, the computer driven primary display system is separated from the Class 1E sensors, processing and backup display equipment by means of an isolation device which is qualified to Class 1E criteria.

Verification and validation of the QSPDS software for the ICC display includes use of a designated test facility, integrated software testing, and static and dynamic tests which thoroughly test the software. The QSPDS verification testing procedures utilize the experience gained from previous CPCS software verification.

7.5.4.5 System Verification Testing

This section describes tests and operational experience with ICC instruments.

7.5.4.5.1 RTD and Pressurizer Pressure Sensors

The hot and cold leg RTD temperature sensors and the pressurizer pressure sensors are standard NSSS instruments which have well known responses. No special verification tests have been performed nor are planned for the future. These sensors along with UHJTC inputs provide basic, reliable temperature and pressure inputs which are considered adequate for use in the SMM and other additional display functions.

7.5.4.5.2 Core Exit Thermocouples

Testing at the Oak Ridge National Laboratory was performed to evaluate thermocouple performance under simulated accident conditions (Reference 4). These tests included long term exposure to elevated temperatures and repeated quenchings. In summary, these tests demonstrated that the Type K Chromel-Alumel thermocouples remain functional up to 2300°F.

7.5.4.5.3 HJTC System Sensors and Processing

The HJTC System is a new system. Extensive testing has been performed to assure that the HJTC System will operate to unambiguously indicate liquid inventory above the core.

The test program has been completed and the results submitted to the NRC in late 1982 in CEN-185-P, Supplement 3-P. The full prototype system, including the probe and associated microprocessor, heater controllers, and display were integrated into one test arrangement. The system as a whole was subjected to steady-state single and two phase conditions, top and bottom depressurizations, as well as repressurization.

7.5.5 POST ACCIDENT EXCORE NEUTRON FLUX MONITORING SYSTEM

The Excore Neutron Flux Monitoring System monitors neutron flux wide range and source range monitors with Class 1E independent displays in the Control Room and on the Hot Shutdown Panel. This system is designed to meet the NRC requirements necessary to support the NFPA 805 Nuclear Safety Capability Assessment and Regulatory Guide 1.97, Revision 3, Type B variable. EC282743

The Excore Neutron Flux Monitoring System consists of two redundant Class 1E channels each consisting of the following major components:

a. Fission chamber neutron detector assembly

b. Cable assemblies with qualified junction box

c. Containment triaxial cable penetration feedthrough modules

d. Amplifier assembly

e. Signal processing assembly

f. Control Room instrumentation (displays and trend recorder)

g. Hot shutdown panel instrumentation (displays)

The design basis of the Excore Neutron Flux Monitoring System is to provide neutron flux measurement from 5 x 10^{-2} nv (neutron/cm^2-sec) to 5 x 10^9 nv.

The basis for range required by Regulatory Guide 1.97 R3 is 1x10^{-6} to 100% power. The installed Excore Neutron Flux Monitoring System meets or exceeds these bases. Reference Table 7.5-1.

REFERENCES: SECTION 7.5

1. NUREG-0737, "Clarification of TMI Action Plan Requirements," U.S. Nuclear Regulatory Commission, November, 1980.

2. CEN-117, "Inadequate Core Cooling - A Response to NRC IE Bulletin 79-060, Item 5 for Combusiton Engineering Nuclear Steam Supply Systems," Combustion Engineering, October, 1979.

3. CEN-125, "Input for Response to NRC Lessons Learned Requirements for Combustion Engineering Nuclear Steam Supply Systems," Combustion Engineering, December, 1979.

4. Anderson, R. L., Banda, L.A., Cain, D. G., "Incore Thermocouple Performance Under Simulated Accident Conditions," IEEE Nuclear Science Symposium, Vol. 28, No. 1 page 773, Figure 81.

5. FP&L Letter L-85-417 from J. W. Williams (FPL) to Mr. E. J. Butcher (NRC) dated November 18, 1985.

6. Title 10 Code of Federal Regulations, Part 50.62.

7. NUREG-1394, “Emergency Response Data System (ERDS) Implementation,” Rev. 1.

8. PC/M No. 05136M, Steam Generator 2A & 2B Water Level Modification for the Unit 2 Component Replacement Projects.

TABLE 7.5-1

SAFETY-RELATED DISPLAY INSTRUMENTATION[1]

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
1. RTGB - 201									
Battery 2A-Volts	Indication	VM-1001				X			
Battery 2A-Amps	Indication	AM-1801				X			
4.16 KV Bus 2A3-Amps	Indication	AM-936				X			
4.16 KV Bus 2A3-Volts	Indication	VM-954				X			
D.G. #2A-Frequency	Indication	FM-1606				X			
D.G. #2A-Amps	Indication	AM-955D				X			
D.G #2A-Volts	Indication	VM-1606D				X			
4.16 KV Bus 2AB-Amps	Indication	AM-942				X			
4.16 KV Bus 2AB-Volts	Indication	VM-942				X			
D.G. #2B-Frequency	Indication	FM-1616				X			
D.G. #2B-Amps	Indication	AM-965D				X			
D.G. #2B-Volts	Indication	VM-1616D				X			
Battery 2B-Volts	Indication	VM-1002				X			
Battery 2B-Amps	Indication	AM-1802				X			
4.16 KV Bus 2B3-Amps	Indication	AM-937				X			
4.16 KV Bus 2B3-Volts	Indication	VM-964				X			
D.G #2A-MVARS	Indication	VARM-1606				X			
D.G #2B-MVARS	Indication	VARM-1616				X			
D.G #2A-Watts	Indication	REC/1606				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
1. RTGB - 201 (Cont'd)									
D.G #2B-Watts	Indication	REC/1616				X			
D.G #2A-Kilowatt Hour	Indication	WHM-955D				X			
D.G #2B-Kilowatt Hour	Indication	WHM-965D				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
II. RTGB - 202:									
S. Gen #2A-Level	Ind/Control	LIC-9013A		X	X		X	X[4]	
S. Gen #2A-Level	Ind/Control	LIC-9013B		X	X		X	X[4]	
S. Gen #2A-Level	Ind/Control	LIC-9013C		X	X		X	X[4]	
S. Gen #2A-Level	Ind/Control	LIC-9013D		X	X		X	X[4]	
S. Gen #2B-Level	Ind/Control	LIC-9023A		X	X		X	X[4]	
S. Gen #2B-Level	Ind/Control	LIC-9023B		X	X		X	X[4]	
S. Gen #2B-Level	Ind/Control	LIC-9023C		X	X		X	X[4]	
S. Gen #2B-Level	Ind/Control	LIC-9023D		X	X		X	X[4]	
S. Gen #2A Wide Range	Indication	DCS Flat Panel Display					X	X[4]	
(DCS Flat Panel Display is Not Nuclear Safety but has its transmitter qualified for post accident environment.)									
S.Gen #2B Wide Range	Indication	DCS Flat Panel Display					X	X[4]	
(DCS Flat Panel Display is Not Nuclear Safety but has its transmitter qualified for post accident environment.)									
S.Gen #2A Wide Range*	Recorder	DCS / Historian						X	
S.Gen #2B Wide Range*	Recorder	DCS / Historian						X	
Aux. FW Hdr. A-Flow/	Indication	FI-09-2A/			X		X	X	
Aux. FW Hdr. A-Press	Indication	PI-09-8A			X		X		
Aux. FW Hdr. B-Flow/	Indication	FI-09-2B/			X		X	X	
Aux. FW Hdr. B-Press	Indication	PI-09-8B			X		X		
Aux. FW Hdr. C-Flow/	Indication	FI-09-2C/			X		X	X	
Aux. FW Hdr. C-Press	Indication	PI-09-8C			X		X		
Intk. Clg. Wtr. Hdr. A-Press	Ind/Alarm	PIS-21-8A				X			
Intk. Clg. Wtr. Hdr. B-Press	Ind/Alarm	PIS-21-8B				X			
Cond. St. Tk-Level	Ind/Alarm	LIS-12-11A					X	X	
Cond. St. Tk-Level	Ind/Alarm	LIS-12-11B					X	X	
Stm. to Aux. FW Pump 2C-Press	Ind/Alarm	PI-08-5			X		X		

* Not Safety Related but transmitter is EQ qualified.

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
II. RTGB - 202:(Cont'd)									
Atm. Stm. Dump SG #2A-Press	Ind/Control	PIC-08-1A					X		
Atm. Stm. Dump SG #2B-Press	Ind/Control	PIC-08-1B					X		
Aux FW Hdr. B-Flow/ Hdr. C-Flow	Recorder	FR-09-2B/2C			X			X	
Feedwater Hdr. A Press	Indication	PI-09-9A			X				
Feedwater Hdr. A Press	Indication	PI-09-9B			X				
Feedwater Hdr. A Press	Indication	PI-09-9C			X				
Feedwater Hdr. A Press	Indication	PI-09-9D			X				
Feedwater Hdr. B Press	Indication	PI-09-10A			X				
Feedwater Hdr. B Press	Indication	PI-09-10B			X				
Feedwater Hdr. B Press	Indication	PI-09-10C			X				
Feedwater Hdr. B Press	Indication	PI-09-10D			X				
Aux. FW Hdr. A-Flow	Recorder	FR-09-2A			X			X	
Aux. FW Pump 2A-Amp	Indication	AM-629			X		X		
Aux. FW Pump 2B-Amp	Indication	AM-630			X		X		
Intake Pump 2A-Amp	Indication	AM-832				X			
Intake Pump 2C-Amp	Indication	AM-834				X			
Intake Pump 2B-Amp	Indication	AM-833				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
III. RTGB - 203:									
RCS Cold Leg 2A1-Temp	Indication	TI-1115					X	X	
RCS Cold Leg 2B1-Temp	Indication	TI-1125					X	X	
Pressurizer Water Level	Indication	LI-1110X					X	X	
Pressurizer Water Level	Indication	LI-1110Y					X	X	
Pressurizer-Press (Low Range)	Indication	PI-1103					X		
Pressurizer-Press (Low Range)	Indication	PI-1104					X		
Pressurizer-Press (Low Range)	Indication	PI-1105					X		
Pressurizer-Press (Low Range)	Indication	PI-1106					X		
Pressurizer-Press	Indication	PI-1102A		X	X		X		
Pressurizer-Press	Indication	PI-1102B		X	X		X		
Pressurizer-Press	Indication	PI-1102C		X	X		X		
Pressurizer-Press	Indication	PI-1102D		X	X		X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
III. RTGB - 203: (Cont'd)									
Thermal Margin-Lo Press Set Pt. (RPS)	Ind/Alarm	PIA-1102A		X					
Thermal Margin-Lo Press Set Pt. (RPS)	Ind/Alarm	PIA-1102B		X					
Thermal Margin-Lo Press Set Pt. (RPS)	Ind/Alarm	PIA-1102C		X					
Thermal Margin-Lo Press Set Pt. (RPS)	Ind/Alarm	PIA-1102D		X					
SG 2AΔP /SG 2BΔP/ Total Core Flow	Indication	PDI-1101A		X					
SG 2AΔP /SG 2BΔP/ Total Core Flow	Indication	PDI-1101B		X					
10 SG 2AΔP /SG 2BΔP/ Total Core Flow	Indication	PDI-1101C		X					
SG 2AΔP /SG 2BΔP/ Total Core Flow	Indication	PDI-1101D		X					
Coolant Loop-Temp TC/TH	Indication	TI-1102A		X					
Coolant Loop-Temp TC/TH	Indication	TI-1102B		X					
Coolant Loop-Temp TC/TH	Indication	TI-1102C		X					
Coolant Loop-Temp TC/TH	Indication	TI-1102D		X					
Hot/Cold Leg-Temp	Recorder	TR-1112 HA/CA						X	

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-Down	Post Accident	Loop Accuracy[2] (Percent)
III. RTGB - 203: (Cont'd)									
Hot/Cold Leg-Temp	Recorder	TR-1122 HB/CB						X	
Pressurizer-Level/Press	Recorder	LR-1110X/PR-1108						X	
Pressurizer Pressure	Indication	PI-1107-1					X	X	
Pressurizer Pressure	Indication	PI-1108-1					X	X	
IV. RTGB - 204:									
% of Power	Indication	JI-001A		X			X		
% of Power	Indication	JI-001B		X			X		
% of Power	Indication	JI-001C		X			X		
% of Power	Indication	JI-001D		X			X		
NIS Wide Range-Rate	Indication	JKI-001A		X					
NIS Wide Range-Rate	Indication	JKI-001B		X					
NIS Wide Range-Rate	Indication	JKI-001C		X					
NIS Wide Range-Rate	Indication	JKI-001D		X					
NIS Power Range Safety Power	Indication	JI-003A/ 004A		X					
NIS Power Range Safety Power	Indication	JI-003B/ 004B		X					
Neutron Power Wide Range	Indication	RI-26-80A5					X	X	
Neutron Power Wide Range	Indication	RI-26-80B5					X	X	
Neutron Power Rate of Change	Indication	RI-26-80A3					X		
Neutron Power Rate of Change	Indication	RI-26-80B3					X		
Neutron Power Source Range	Indication	RI-26-80A4					X		
Neutron Power Source Range	Indication	RI-26-80B4					X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
IV. RTGB - 204: (Cont'd)									
NIS Power Range Safety Power	Indication	JI-003C/ 004C		X					
NIS Power Range Safety Power	Indication	JI-003D/ 004D		X					
Flux Indicators	Indication	JI-005A/ 007A		X					
		JI-006A		X					
Flux Indicators	Indication	JI-005B/ 007B		X					
		JI-006B		X					
Flux Indicators	Indication	JI-005c/ 007C		X					
		JI-006C		X					
Flux Indicators	Indication	JI-005D/ 007D		X					
		JI-006D		X					
NIS Wide Range Log Power	Recorder	JR-001A		X					
NIS Wide Range Log Power	Recorder	JR-0018		X					
NIS Wide Range Log Power	Recorder	JR-001C		X					
NIS Wide Range Log Power	Recorder	JR-001D		X					
V. RTGB - 205:									
Charging Flow to RHX	Ind/Alarm	FIA-2212					X	X	
Charging Hdr. Press	Ind/Alarm	PIA-2212					X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)	Remarks
VI. RTGB - 206:										
CCW Hdr. 2A - Flow	Ind/Alarm	FIS-14-1A				X		X		
CCW Hdr. 2B - Flow	Ind/Alarm	FIS-14-1B				X		X		
CCW HX-2A Outlet Press	Ind/Alarm	PIS-14-8A				X				
CCW HX-2B Outlet Press	Ind/Alarm	PIS-14-8B				X				
CCW from Shutdown HX-2A Flow	Ind/Alarm	FIS-14-10A				X				
CCW from Shutdown HX-2B Flow	Ind/Alarm	FIS-14-10B				X				
CCW from Fuel Pool HX Flow	Ind/Alarm	FIS-14-2				X				Process Display
CCW from Letdown HX Flow	Ind/Alarm	FIS-14-6								(5)
CCW Pump 2A	Indication	AM-201				X				
CCW Pump 2B	Indication	AM-205				X				
CCW Pump 2C	Indication	AM-209				X				
C.S. Hdr. A Press	Ind/Alarm	PIS-07-3A			X					
C.S. Hdr. A Wtr. Flow	Indication	FI-07-1A			X			X		
C.S. Hdr. B Press	Ind/Alarm	PIS-07-3B			X					
C.S. Hdr. B Wtr. Flow	Indication	FI-07-1B			X			x		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VI. RTGB - 206 (Cont'd)									
Cont. Spray Pump 2A	Indication	AM-287			X				
Cont. Spray Pump 2B	Indication	AM-290			X				
Pressurizer Press	Ind/Alarm	PIA-1102ALL		X	X				
Pressurizer Press	Ind/Alarm	PIA-1102BLL		X	X				
Pressurizer Press	Ind/Alarm	PIA-1102CLL		X	X				
Pressurizer Press	Ind/Alarm	PIA-1102DLL		X	X				
Cont. Pressure	Ind/Alarm	PIS-07-2A		X	X				
Cont. Pressure	Ind/Alarm	PIS-07-2B		X	X				
Cont. Pressure	Ind/Alarm	PIS-07-2C		X	X				
Cont. Pressure	Ind/Alarm	PIS-07-2D		X	X				
RWT Water Level	Ind/Alarm	LIS-07-2A			X			X[4]	
RWT Water Level	Indication	LIS-07-2B			X			X[4]	
RWT Water Level	Ind/Alarm	LIS-07-2C			X			X[4]	
RWT Water Level	Ind/Alarm	LIS-07-2D			X			X[4]	
High Containment Rad "MA"	Ind/Alarm	RIS-26-3-2			X			X[3]	
High Containment Rad "MB"	Ind/Alarm	RIS-26-4-2			X				
High Containment Rad "MC"	Ind/Alarm	RIS-26-5-2			X				
High Containment Rad "MD"	Ind/Alarm	RIS-26-6-2			X				
S.G. #2A Press	Indication	PI-8013A		X	X			X[4]	
S.G. #2A Press	Indication	PI-8013B		X	X			X[4]	

TABLE 7.5-1 (Cont'd

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VI. RTGB - 206 (Cont'd)									
S.G. #2A Press	Indication	PI-8013C		X	X			X[4]	
S.G. #2A Press	Indication	PI-8013D		X	X			X[4]	
S.G. #2B Press	Indication	PI-8023A		X	X			X[4]	
S.G. #2B Press	Indication	PI-8023B		X	X			X[4]	
S.G. #2B Press	Indication	PI-8023C		X	X			X[4]	
S.G. #2B Press	Indication	PI-8023D		X	X			X[4]	
CCW from RCP	Ind/Control	FIS-14-15A		X					
CCW from RCP	Ind/Control	FIS-14-15B		X					
CCW from RCP	Ind/Control	FIS-14-15C		X					
CCW from RCP	Ind/Control	FIS-14-15D		X					
LPSI Loop 2A2 Flow	Indication	FI-3312			X		X	X	
LPSI Loop 2A1 Flow	Indication	FI-3322			X		X	X	
LPSI Loop 2B1 Flow	Indication	FI-3332			X		X	X	
LPSI Loop 2B2 Flow	Indication	FI-3342			X		X	X	
HPSI Loop 2A2 Flow	Indication	FI-3311			X			X	
HPSI Loop 2A1 Flow	Indication	FI-3321			X			X	
HPSI Loop 2B1 Flow	Indication	FI-3331			X			X	
HPSI Loop 2B2 Flow	Indication	FI-3341			X			X	
LPSI Hdr. A Press	Indication	PI-3307			X		X		
HPSI Hdr. A Press	Indication	PI-3308			X				

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VI. RTGB - 206 (Cont'd)									
All Containment Isolation Valves	**Position Indicator				X			X	
SIT Iso. Vlv. Pos	Indication	ZI-3614			X			X	
SIT Iso. Vlv. Pos	Indication	ZI-3624			X			X	
SIT Iso. Vlv. Pos	Indication	ZI-3634			X			X	
SIT Iso. Vlv. Pos	Indication	ZI-3644			X			X	

** All containment isolation valves are provided with valve position indication in the control room.

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VI. RTGB - 206 (Cont'd)									
LPSI Hdr B Press	Indication	PI-3304			X		X		
HPSI Hdr B Press	Indication	PI-3309			X				
HPSI to Hot Loop 2A Flow	Indication	FI-3315			X			X	
HPSI to Hot Loop 2B Flow	Indication	FI-3325			X			X	
Hydrazine Spray Flow	Indication	FI-07-2-1			X				
Cont. Temperature	Indication	TI-07-3A						X	
Cont. Sump Temp	Indication	TI-07-5A						X	
Cont. Press/Cont. Sump Press	Indication	PI-07-4A PI-07-5A						X X	
Hydrazine Tank Level	Ind/Alarm	LIS-07-9			X				
HPSI Pump 2A Amp	Indication	AM-237			X			X	
HPSI Pump 2B Amp	Indication	AM-238			X			X	
LPSI Pump 2A Amp	Indication	AM-251			X		X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)	
VI. RTGB - 206 (Cont'd)										
LPSI Pump 2B Amp	Indication	AM-252				X	X			
Shutdown Cooling Loop 2A Flow	Recorder	FR-3306					X	X		
Shutdown Cooling Loop 2B Flow	Recorder	FR-3301					X	X		
Shutdown HX 2A Inlet Temp/LPSI Hdr 2A Temp	Recorder	TR-03-1					X			EC 290696
C.S. Flow	Recorder	FR-07-1B			X			X		
Shutdown HX 2B Outlet Temp	Indicator Recorder	TI-3303Y TR-03-1					X X	X X		EC 290696
Shutdown HX 2B Inlet/ LPSI Hdr 2B Temp	Recorder	TR-03-2					X			EC 290696
C.S. Flow	Recorder	FR-07-1A			X			X		
Shutdown HX 2A Outlet Temp	Indicator Recorder	TI-3303X TR-03-2					X X	X X		EC 290696
HPSI to Hot Loop 2B Flow	Recorder	UR-03-1			X			X		EC 290696
HPSI Loop 2B1/2B2 Flow	Recorder	UR-03-1			X			X		EC 290696
HPSI Pump 2B Disch. Hdr Press	Recorder	UR-03-1			X					EC 290696
LPSI Hdr "B" Press	Recorder	PR-3302			X					
HPSI to Hot Loop 2A Flow	Recorder	UR-03-2			X			X		EC 290696

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)	
VI. RTGB - 206 (Cont'd)										
HPSI Loop 2A2/2A1 Flow	Recorder	UR-03-2			X			X		EC 290696
HPSI Pump 2A Disch. Hdr Press	Recorder	UR-03-2			X					EC 290696
LPSI Hdr "A" Press	Recorder	PR-3301			X					
Cont. Press/Cont. Sump Press	Recorder	UR-07-1B						X		
Cont. Temp/Cont. Sump Temp	Recorder	UR-07-1B						X		
Hydrazine Spray Flow	Recorder	FR-07-2-2			X					
RWT Level	Recorder	LR-07-2D			X			X		
S.G. 2A/2B Press	Recorder	UR-09-2						X		
S.G. 2A/2B Level	Recorder	UR-09-2						X		
Plant Auxiliary Control Boards										
Containment Sump Wtr Level (Narrow Range)	Recording	UR-07-2A						X		
Containment Wtr Level (Wide Range)	Recording	UR-07-2A						X		
Containment Wtr Level (Wide Range)	Recording	UR-07-2B						X		
Containment Pressure	Recording	UR-07-2A						X		
Containment Pressure	Recording	UR-07-2B						X		
Atm. Stm. Dump SG #2A-Press	Ind/Control	PIC-08-3B					X			
Atm. Stm. Dump SG #2B-Press	Ind/Control	PIC-08-3A					X			
Neutron Power Wide Range	Recorder	RR-26-80A					X	X		
Neutron Power Wide Range	Recorder	RR-26-80B					X	X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
Pressurizer Heater*	Indication	AM-943					X	X	
Pressurizer Heater*	Indication	AM-944					X	X	
Condensate Storage Tank	Recording	LR-12-11B						X	
PORV & SRV Position**	Indication and Alarm	FI-01-1						X	
PORV & SRV Position**	Indication and Alarm	FI-01-2						X	
PORV & SRV Position**	Indication and Alarm	FI-01-3						X	
PORV & SRV Position**	Indication and Alarm	FI-01-4						X	
PORV & SRV Position**	Indication and Alarm	FI-01-5						X	
Steam Generator #2A Wide Range	Indication	LI-9014					X	X[4]	
Steam Generator #2B Wide Range	Indication	LI-9024					X	X[4]	
VII. HVCB:									
Control Room to Outside Air Diff Pressure	Indicating/ Control	PDIC-25-23A1				X			
Control Room to Outside Air Diff Pressure	Indicating/ Control	PDIC-25-23B1				X			
Annulus to Outside P	Ind/Alarm	PDIS-25-7A				X			
Annulus to Outside P	Ind/Alarm	PDIS-25-7B				X			
Shield Building HEPA Filter ΔP	Ind/Alarm	PDIS-25-8A			X				

* Not Safety Related. Required by NUREG-0737 Item II.E.3.1.

** Not Safety Related but sensor is EQ Qualified. Required by NUREG-0737 Item II.D.3.

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII HVCB (Cont'd)									
Shield Bldg HEPA Filter ΔP	Ind/Alarm	PDIS-25-8B			X				
Shield Bldg Exhaust-Flow A	Ind/Alarm	FIS-25-20A1			X				
Shield Bldg Exhaust-Flow B	Ind/Alarm	FIS-25-20B1			X				
Containment to Annulus ΔP	Ind/Cont	PDIS-25-1A				X			
Containment to Annulus ΔP	Ind/Cont	PDIS-25-1B				X			
Containment to Annulus ΔP	Indication	PDI-25-15A				X			
Containment to Annulus ΔP	Indication	PDI-25-15B				X			
Fuel Pool Area to Outside ΔP	Ind/Alarm	PDIS-25-17A				X			
Fuel Pool Area to Outside ΔP	Ind/Alarm	PDIS-25-17B				X			
ECCS Pump Room to Outside ΔP	Ind/Alarm	PDIS-25-16A				X			
ECCS Pump Room to Outside ΔP	Ind/Alarm	PDIS-25-16B				X			
ECCS Area Exhaust RAB HEPA Filter "A" ΔP	Ind/Alarm	PDIS-25-5A				X			
ECCS Area Exhaust RAB HEPA Filter "B" ΔP	Ind/Alarm	PDIS-25-5B				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII HVCB (Cont'd)									
ECCS Area Exhaust Flow	Indication	FI-25-21A1				X			
ECCS Area Exhaust Flow	Indication	FI-25-21B1				X			
Control Room Emerg Filter ΔP HEPA Filter	Ind/Alarm	PDIS-25-9A				X			
Control Room Emerg Filter ΔP HEPA Filter	Ind/Alarm	PDIS-25-9B				X			
Control Room Emerg Filter Fan Discharge Flow	Indication	FI-25-19A1				X			
Control Room Emerg Filter Fan Discharge Flow	Indication	FI-25-19B1				X			
Control Room to Outside ΔP	Ind/Alarm	PDIS-25-23A				X			
Control Room to Outside ΔP	Ind/Alarm	PDIS-25-23B				X			
Control Room (North) Intake-Flow	Indication	FI-25-18A				X			
Control Room (South) Intake-Flow	Indication	FI-25-18B				X			
Shield Bldg Vent-Flow Train A	Ind/Control	FIC-25-20A1			X				
ECCS Area Exhaust-Flow Train A	Ind/Control	FIC-25-21A1				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII HVCB (Cont'd)									
Shield Bldg Vent-Flow Train B	Ind/Control	FIC-25-20B1			X				
ECCS Area Exhaust-Flow Train B	Ind/Control	FIC-25-21B1				X			
Control Room South Iso. Valve Position	Indication	ZI-25-17	-			X			-
Control Room North Iso. Valve Position	Indication	ZI-25-14	-			X			-
Cont Room Emerg Filtration Sytem Train A Disch-Flow	Recorder	FR-25-1A				X			
Shield Bldg Vent System Train A Discharge-Flow	Recorder	FR-25-1A			X				

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII HVCB (Cont'd)									
Auxiliary Building and ECCS Vent System Train A Discharge-Flow	Recorder	FR-25-1A				X			
Control Room A/C Emerg Filter System Train B Discharge-Flow	Recorder	FR-25-1B				X			
Shield Bldg Vent System Train B Discharge-Flow	Recorder	FR-25-1B			X				
Auxiliary Building and ECCS Vent System Train B Discharge-Flow	Recorder	FR-25-1B				X			
Containment Cooling Fan HVS-1A Cooling Coil Inlet - Temperature	Recorder	TR-25-1A			X			X	
Containment Cooling Fan HVS-1A Cooling Coil Outlet-Temperature	Recorder	TR-25-1A			X			X	
Containment Cooling Fan HVS-1B Cooling Coil Inlet-Temperature	Recorder	TR-25-1A			X			X	

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII. HVCB (Cont'd)									
Containment Cooling Fan HVS-1B Cooling Coil Outlet - Temperature	Recorder	TR-25-1A			X			X	

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII. HVCB(Cont'd)									
Containment Cooling Fan HVS-1C Cooling Coil Inlet Temperature	Recorder	TR-25-1B			X			X	
Containment Cooling Fan HVS-1C Cooling Coil Outlet Temperature	Recorder	TR-25-1B			X			X	

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)	Remarks
VII. HVCB: (Cont'd)										
Containment Cooling Fan HVS-1D Cooling Coil Inlet Temperature	Recorder	TR-25-1B			X			X		
Containment Cooling Fan HVS-1D Cooling Coil Outlet Temperature	Recorder	TR-25-1B			X			X		
Control Room Train B Pre HEPA Filter diff Pressure	Recorder	PR-25-1B				X				
Control Room Train B Charcoal Filter diff Pressure	Recorder	PR-25-1B				X				
Control Room Train B After HEPA Filter Diff Pressure	Recorder	PR-25-1B				X				
Control Room Train B Diff Pressure	Recorder	PR-25-1B				X				
Aux Build and ECCS Vent System Train B HEPA Filter Diff Pressure	Recorder	PR-25-1B				X				
Aux Build and ECCS Vent System Train B Charcoal Filter Diff Pressure	Recorder	PR-25-1B				X				
Aux Build and ECCS Vent System Train B Diff Pressure	Recorder	PR-25-1B				X				

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII. HVCB: (Cont'd)									
Shield Build Vent System Train B Pre HEPA Filter Diff Press	Recorder	PR-25-1B			X				
Shield Build Vent System Train B Charcoal Filter Diff Press	Recorder	PR-25-1B			X				
Shield Build Vent System Train B Diff Press	Recorder	PR-25-1B			X				
Shield Build Vent System Train B After HEPA Filter Diff Press	Recorder	PR-25-1B			X				
Control Room Train A Pre HEPA Filter Diff Press	Recorder	PR-25-1A				X			
Control Room Train A Charcoal Filter Diff Press	Recorder	PR-25-1A				X			
Control Room Train A After HEPA Filter Diff Press	Recorder	PR-25-1A				X			
Control Room Train A Diff Press	Recorder	PR-25-1A				X			
Aux Build and ECCS Vent System Train A HEPA Filter Diff Press	Recorder	PR-25-1A				X			

TABLE 7.5-1 (Cont'd)

Parameters Associated With The System	Function	Tag No.	Instrument[2] Range	REQUIRED FOR RPS	ESF	ESF/Shutdown Support	Shut-down	Post Accident	Loop Accuracy[2] (Percent)
VII. HVCB: (Cont'd)									
Aux Build and ECCS Vent System Train A Charcoal Filter Diff Press	Recorder	PR-25-1A				X			
Aux Build and ECCS Vent System Train A Diff Press	Recorder	PR-25-1A				X			
Shield Build Vent System Train A Pre HEPA Filter Diff Press	Recorder	PR-25-1A			X				
Shield Build Vent System Train A Charcoal Filter Diff Press	Recorder	PR-25-1A			X				
Shield Build Vent System Train A Diff Press	Recorder	PR-25-1A			X				
Shield Build Vent System Train A After HEPA Filter Diff Press	Recorder	PR-25-1A			X				
VIII. HSDP (Hot Shutdown Panel)									
Pressurizer Pressure	Indication	PI-1107					X		
Pressurizer Pressure	Indication	PI-1108					X		
Pressurizer Level	Indication	LI-1104					X		
Pressurizer Level	Indication	LI-1105					X		
Neutron Power Wide Range	Indication	RI-26-80A1					X		
Neutron Power Wide Range	Indication	RI-26-80B1					X		
Neutron Power Source Range	Indication	RI-26-80A2					X		
Neutron Power Source Range	Indication	RI-26-80B2					X		

TABLE 7.5-1 (Cont'd)

Parameters Associated With the System	Function	Tag No.	Instrument[2] Range	REQUIRED					Loop Accuracy [2] (Percent)
				RPS	ESF	ESF/Shutdown Support	Shutdown	Post Accident	
VIII. HSDP: (Cont'd) (Hot Shutdown Panel)									
Steam Gen 2A Pressure	Indication	PI-8113					X		
Steam Gen 2A Level	Indication	LI-9113					X		
Steam Gen 2B Pressure	Indication	PI-8123					X		
Steam Gen 2B Level	Indication	LI-9123					X		
Reactor Cold Leg 2A Temp	Indication	TI-1115-1					X		
Reactor Cold Leg 2B Temp	Indication	TI-1125-1					X		
Shutdown Cooling Temp	Indication	TI-3351Y					X		
Shutdown Cooling Temp	Indication	TI-3352Y					X		
Shutdown Cooling Flow	Indication	FI-3306					X		
Shutdown Cooling Flow	Indication	FI-3301					X		
Diesel Gen 2A Volts	Indication	VM-1606-1					X		
Diesel Gen 2B Volts	Indication	VM-1616-1					X		
Diesel Gen 2A Watts	Indication	WM-1606-1					X		
Diesel Gen 2B Watts	Indication	WM-1616-1					X		
Neutron Power Level	Indication	JI-001A-1					X		
Neutron Power Level	Indication	JI-001B-1					X		
SG 2A ADV	Ind/Control	PIC-08-1A1, -3B1					X		
SG 2B ADV	Ind/Control	PIC-08-1B1,-3A1					X		
Charging Pump Discharge-Pressure	Indication	PI-2212					X		
Charging Pump Discharge-Flow	Indication	FI-2212					X		

(1) Instrument setpoints and accuracies are referenced in the Technical Specifications.
(2) Instrument ranges are selected in accordance with standard engineering practices. Instrument accuracies are selected such that existing instrument loop performance and safety analysis assumptions remain valid. Where applicable, instrument accuracies are also evaluated for their impact on setpoints in accordance with the FPL Setpoint Methodology.
(3) Post-LOCA monitoring is provided on the radiation Monitoring Panel.
(4) Available Reg. Guide 1.97 Instrumentation; see Technical Specification for minimum channels required.
(5) This instrument does not provide a safety related display function; however, it is electrically “associated” with a safety channel. As such, it is Class 1E and meets the requirements of RG 1.75.

Table 7.5-2
This table has been deleted.

TABLE 7.5-3

SAFETY RELATED ANNUNCIATOR WINDOWS

Window No.		Actuating Device
LA-1	INTAKE WATER LEVEL LOW	LS-21-5A
LA-2	B SAFEGUARDS PUMP ROOM SUMP LEVEL HIGH-HIGH	LS-06-41
LA-3	2A DIESEL OIL STORAGE TANK LEVEL LOW	LS-17-10A
LA-4	3A1/3A2 LUBE WATER SUPPLY STRAINER Δ/P HIGH [1]	PDIS-21-25-1A1 PDIS-21-25-1A2
LA-5	PZR CHANNEL X LEVEL HIGH	LA-1110X-1
LA-6	ADV ISOL MV-08-15/ MV-08-17 OVRLD/CLOSED	(74,33)1621 (74,33)1623
LA-7	CST LEVEL LOW-LOW	LIS-12-11A
LA-8	A SAFEGUARDS PUMP ROOM SUMP LEVEL HIGH / HIGH-HIGH	LS-06-1A
LA-9	2A1/2A2 DIESEL OIL DAY TANK LEVEL LOW-LOW	LS-59-009A/014A
LA-10	CCW SURGE TANK COMPARTMENT A LEVEL LOW	LS-14-1A
LA-11	PZR CHANNEL X LEVEL LOW-LOW	LC-1110X
LA-12	ADV MV-08-18A/MV-08-18B OVRLD/SS ISOL	(74)1626,SS-1626-3 (74)1628,SS-1628-3
LA-13	CST LEVEL LOW	LIS-12-11A
LA-14	FUEL POOL TEMP HIGH/ LEVEL HIGH/LOW	LS-4420,TA-4420
LA-15	VALVES SE-07-5A/5C/5E CLOSE	SE-07-5A,-5C,-5E
LB-1	INTAKE WATER LEVEL LOW	LS-21-5B
LB-2	A SAFEGUARDS PUMP ROOM SUMP LEVEL HIGH-HIGH	LS-06-40
LB-3	2B DIESEL OIL STORAGE TANK LEVEL LOW	LS-17-10B
LB-4	3B1/3B2 LUBE WATER SUPPLY STRAINER Δ/P HIGH [1]	PDIS-21-25-1B1 PDIS-21-25-1B2
LB-5	PZR CHANNEL Y LEVEL HIGH	LA-1110Y-1
LB-6	ADV ISOL MV-08-14/ MV-08-16 OVRLD/CLOSED	(74,33)1622 (74,33)1624
LB-7	CST LEVEL LOW-LOW	LS-12-8
LB-8	B SAFEGUARDS PUMP ROOM SUMP LEVEL HIGH / HIGH-HIGH	LS-06-1B
LB-9	2B1/2B2 DIESEL OIL DAY TANK LEVEL LOW-LOW	LS-59-021B/028B
LB-10	CCW SURGE TANK LEVEL HIGH/ COMPARTMENT B LEVEL LOW	LS-14-1B,LS-14-5
LB-11	PZR CHANNEL Y LEVEL LOW-LOW	LC-1110Y
LB-12	ADV MV-08-19A/ MV-08-19B OVRLD/SS ISOL	(74)1625,SS-1625-3 (74)1627,SS-1627-3
LB-13	CST LEVEL LOW	LIS-12-11B
LB-14	FUEL POOL TEMP HIGH/ LEVEL HIGH/LOW	LS-4421,TA-4421
LB-15	VALVES SE-07-5B/5D/5F CLOSE	SE-07-5B,-5D,-5F

[1] System is no longer Safety Related; however, annunciation circuit remains with Safety Related components.

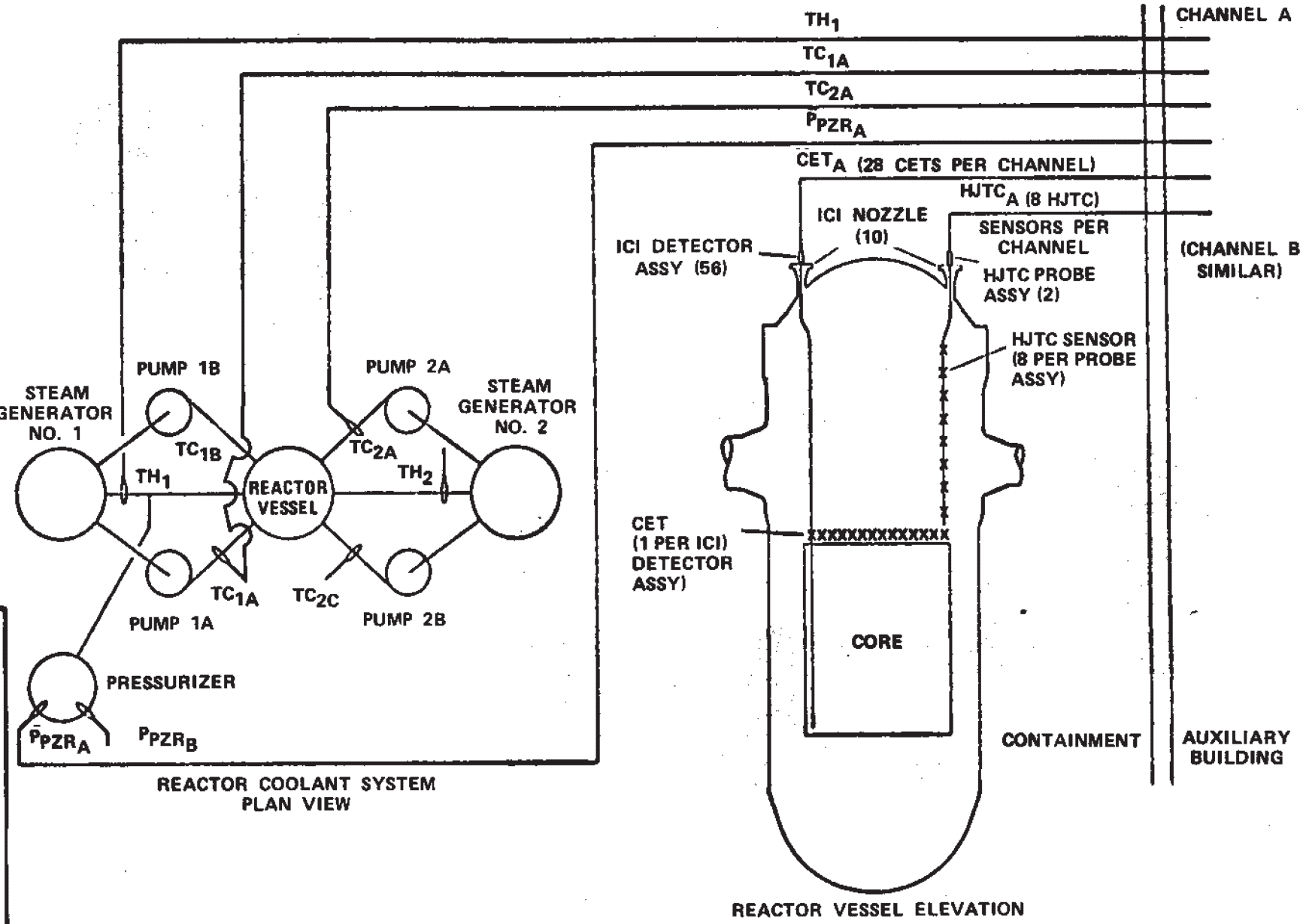
TABLE 7.5-4

ESF SYSTEM VALVE INDICATORS

Valve Tag	Valve Description	Position Type	Indication Power
V3614	SIT 2A2 Isolation Valve	Analog	Separate from control power
V3624	SIT 2A1 Isolation Valve	Analog	Separate from control power
V3634	SIT 2B1 Isolation Valve	Analog	Separate from control power
V3644	SIT 2B2 Isolation Valve	Analog	Separate from control power
HCV-3615	LPSI Flow Control Valve	Lights	Same as control
HCV-3625	LPSI Flow Control Valve	Lights	Same as control
HCV-3635	LPSI Flow Control Valve	Lights	Same as control
HCV-3645	LPSI Flow Control Valve	Lights	Same as control
HCV-3616	HPSI Flow Control Valve	Lights	Same as control
HCV-3626	HPSI Flow Control Valve	Lights	Same as control
HCV-3636	HPSI Flow Control Valve	Lights	Same as control
HCV-3646	HPSI Flow Control Valve	Lights	Same as control
HCV-3617	HPSI Flow Control Valve	Lights	Same as control
HCV-3627	HPSI Flow Control Valve	Lights	Same as control
HCV-3637	HPSI Flow Control Valve	Lights	Same as control
HCV-3647	HPSI Flow Control Valve	Lights	Same as control
V3540	HPSI to Bot Leg 2A Valve	Lights	Same as control
V3523	HPSI to Hot Leg 2B Valve	Lights	Same as control
FCV-3306	Shutdown Cooling Bypass Valve	Lights	Same as control
FCV-3301	Shutdown Cooling Bypass Valve	Lights	Same as control
V3545	Shutdown Cooling Return Crosstie Valve	Lights	Same as control

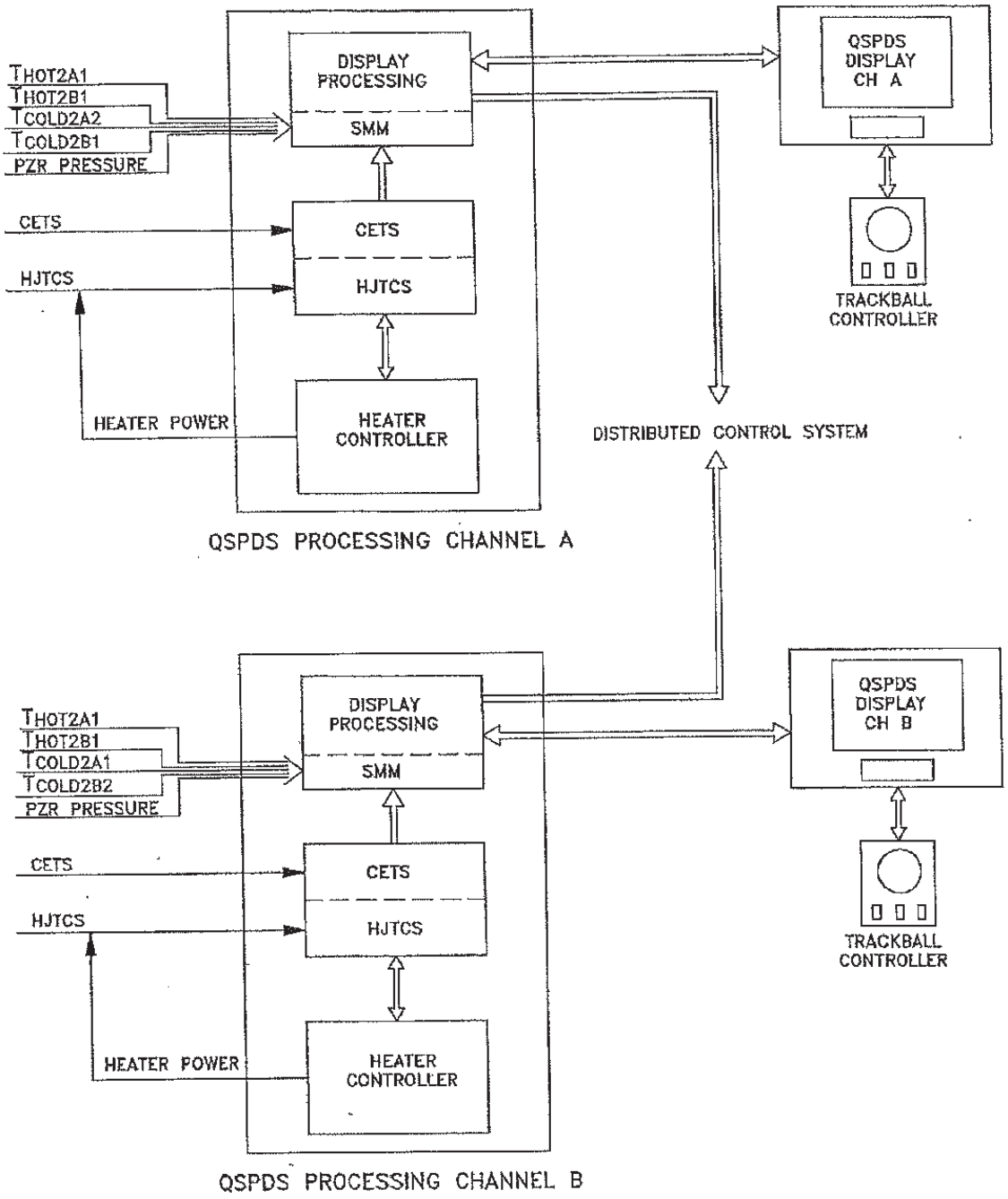
TABLE 7.5-4 (Cont'd)

Valve Tag	Valve Description	Position Type	Indication Power
HCV-3657	Shutdown Cooling Control Valve	Lights	Same as control
HCV-3512	Shutdown Cooling Control Valve	Lights	Same as control
V3536	Shutdown Clg Line 2A Warm-up Valve	Lights	Same as control
V3539	Shutdown Clg Line 2B Warm-up Valve	Lights	Same as control
V1474	Pressurizer Power Oper. Relief (PORV)	Acoustical - Lights	Separate
V1475	Pressurizer Power Oper. Relief (PORV)	Acoustical - Lights	Separate
V1200	Pressurizer Relief Valve	Acoustical - Lights	Separate
V1201	Pressurizer Relief Valve	Acoustical - Lights	Separate
V1202	Pressurizer Relief Valve	Acoustical - Lights	Separate



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ICC DETECTION INSTRUMENTATION
FIGURE 7.5-1a

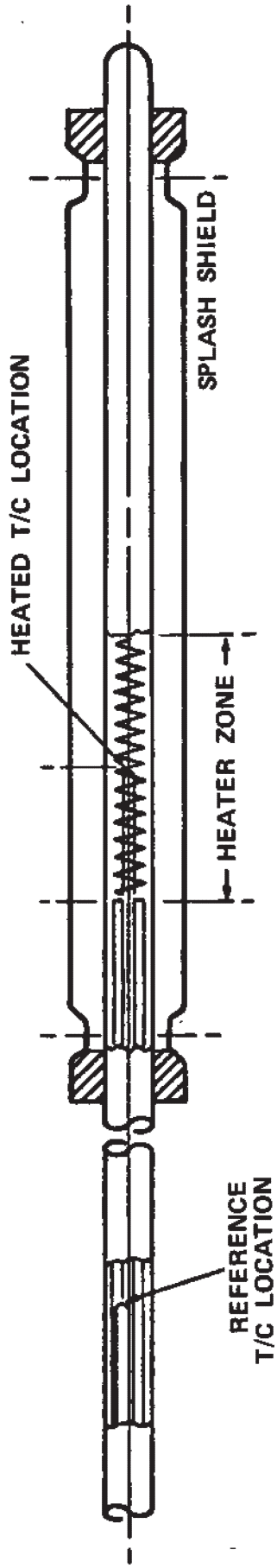


Amendment No. 20 (05/11)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

QUALIFIED SAFETY PARAMETER DISPLAY SYSTEM

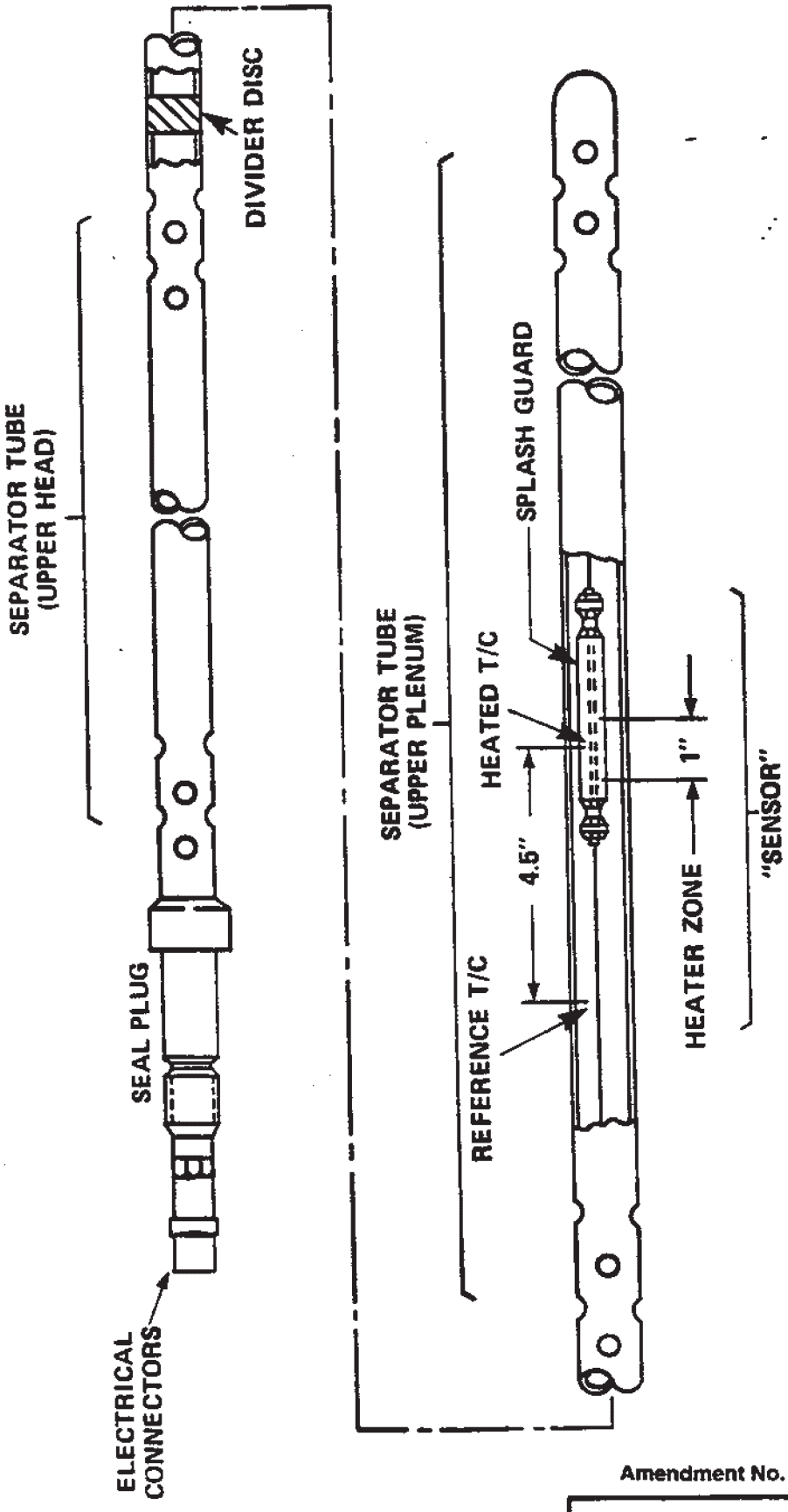
FIGURE 7.5-1b



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

HJTC SENSOR – HJTC/SPLASH SHIELD

FIGURE 7.5-2



Amendment No. 11, (5/97)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

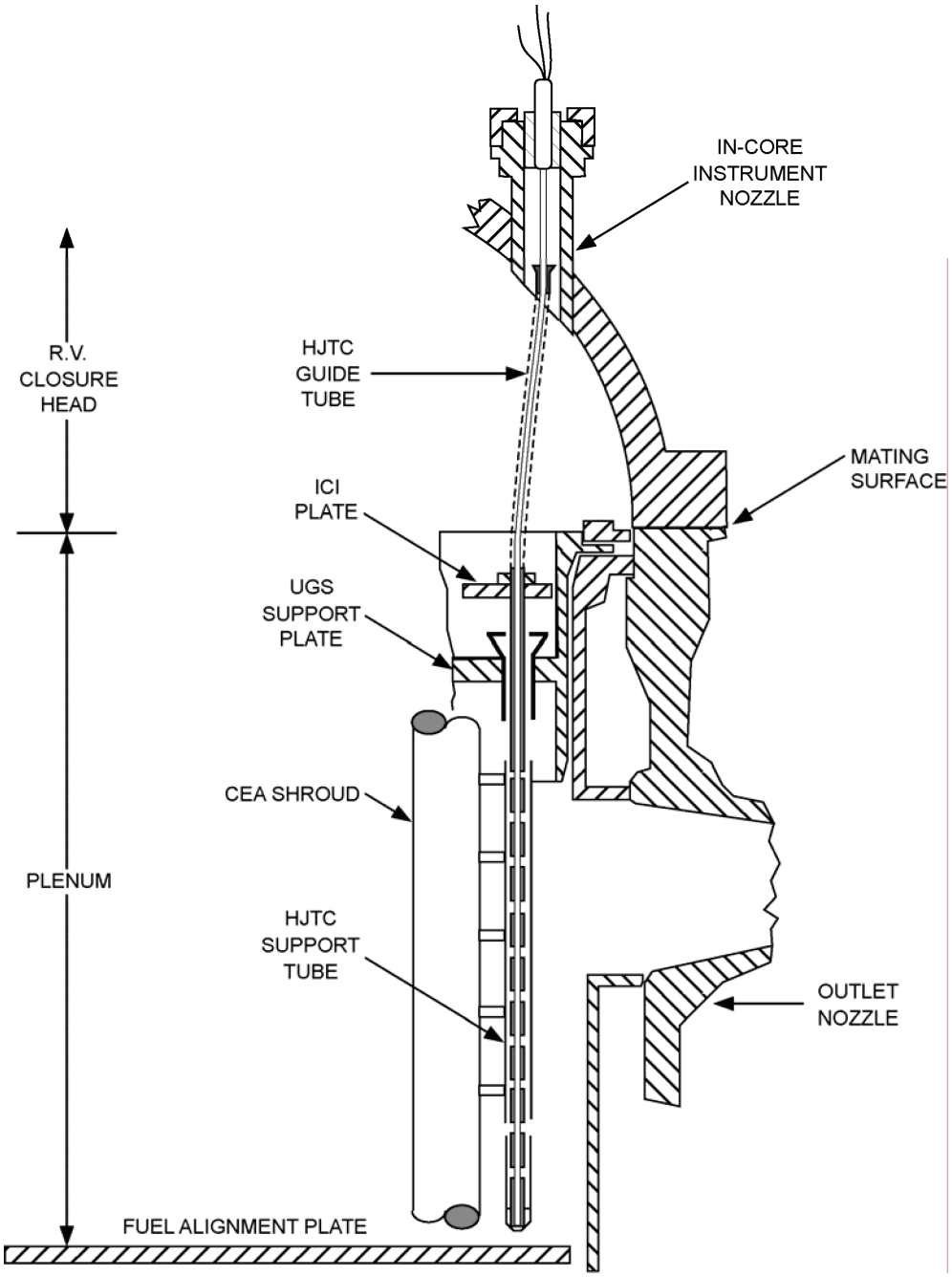
HEATED JUNCTION THERMOCOUPLE
PROBE ASSEMBLY

FIGURE 7.5-3

THIS FIGURE DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.5-4

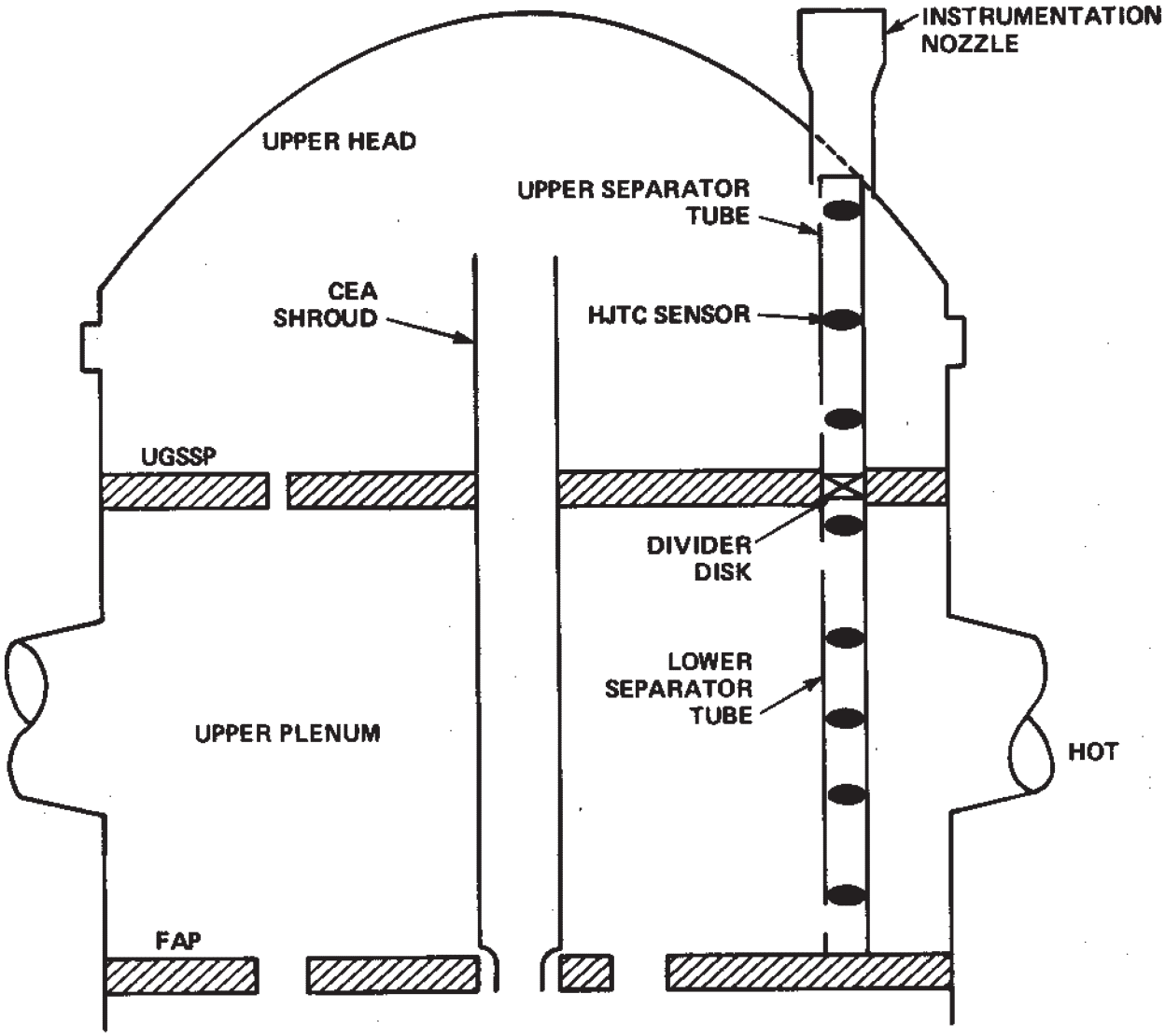


FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

HJTC PROBE INSTALLATION

FIGURE 7.5-5

Amendment No. 18 (01/08)



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

HJTC SENSOR LOCATIONS
FIGURE 7.5-6

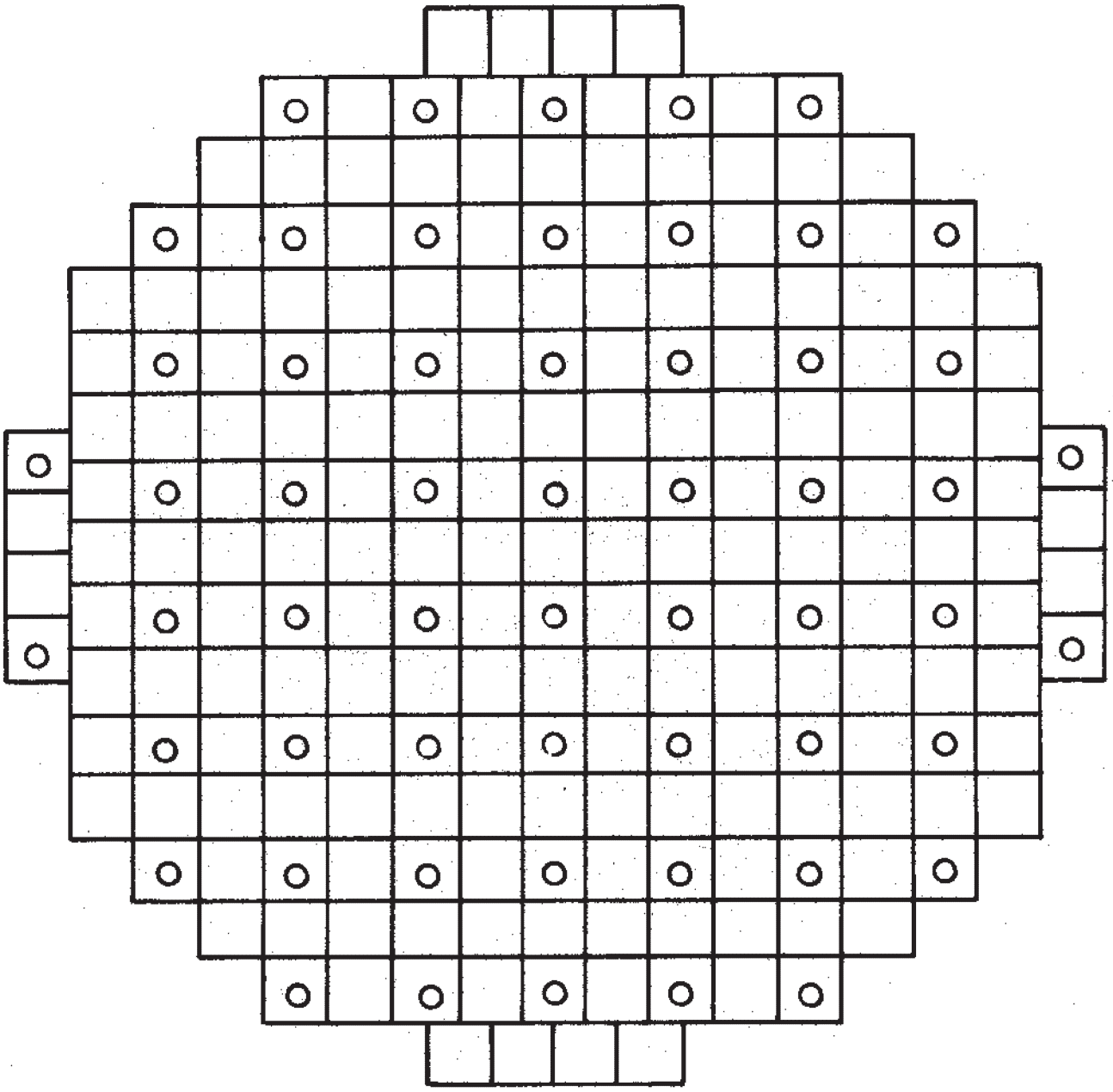
Refer to Dwg.
2998-19729

Amendment No. 11, (5/97)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

IN-CORE INSTRUMENT ASSEMBLY

FIGURE 7.5-7a



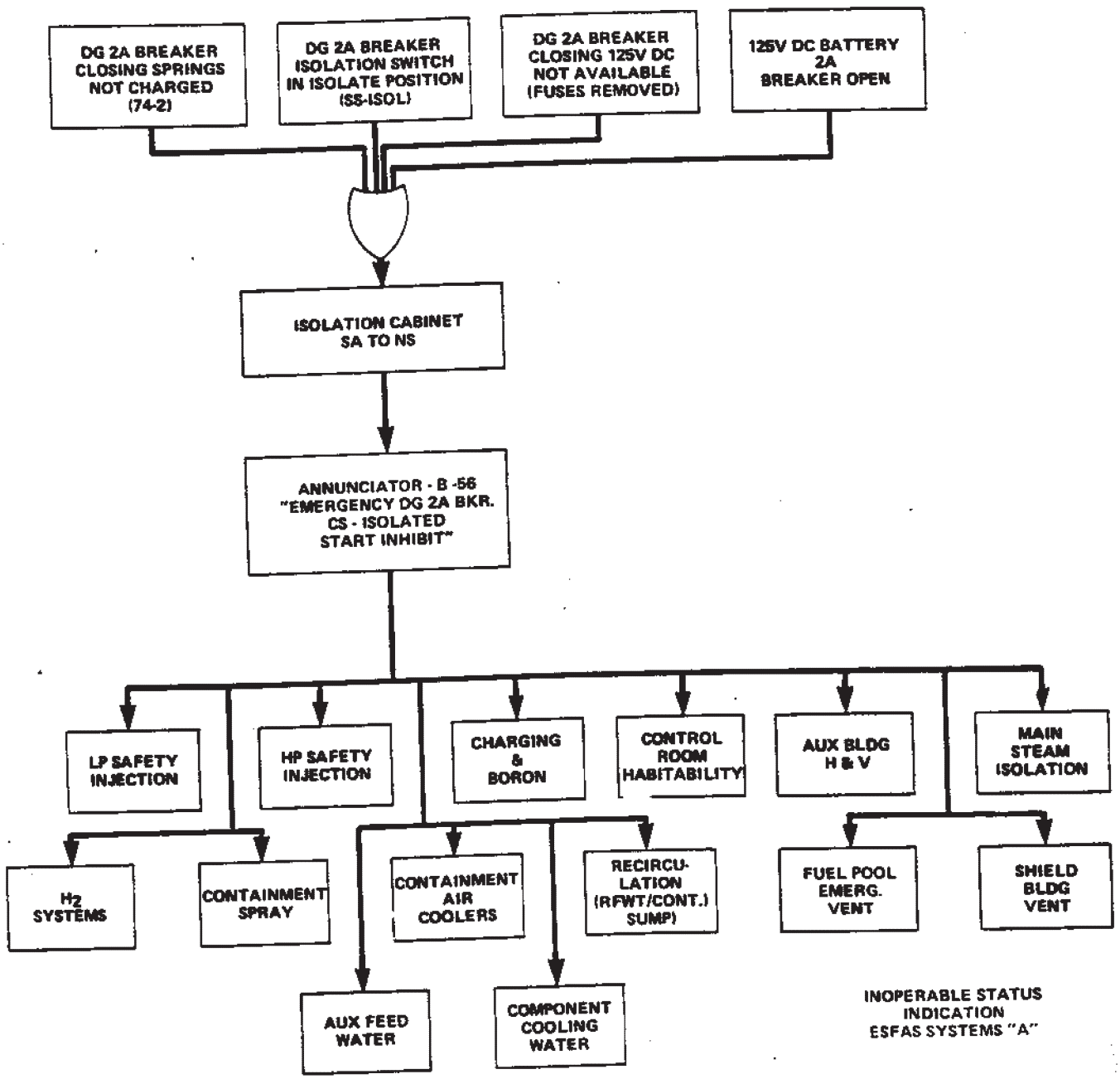
LEGEND

ICI DETECTOR ASSEMBLY/CORE EXIT THERMOCOUPLE LOCATION

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ICI DETECTOR ASSEMBLIES/CORE EXIT THERMOCOUPLES CORE LOCATIONS

FIGURE 7.5-7b



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

INTERACTION OF THE DG AND THE INOPERABLE STATUS BOARD

FIGURE 7.5-8

APPENDIX 7.5A

SAFETY ASSESSMENT SYSTEM/

EMERGENCY RESPONSE DATA ACQUISITION AND DISPLAY SYSTEM

APPENDIX 7.5A

SAFETY ASSESSMENT SYSTEM/

EMERGENCY RESPONSE DATA ACQUISITION AND DISPLAY SYSTEM

7.5A.1 DESCRIPTION

The Safety Assessment System (SAS)/The Emergency Response Data Acquisition And Display System (ERDADS) provides necessary data to the Safety Parameter Display System (SPDS) plus other Emergency Response Functions data required in the control room. SAS/ERDADS also provides the Technical Support Center (TSC) and Emergency Operations Facility (EOF) and the NRC Operations Center through the PI servers. This report describes that portion of the SAS which meets the SPDS requirements of NUREG-0696, "Functional Criteria for Emergency Response Facilities," dated February 1981 and NUREG-1394, “Emergency Response Data System (ERDS) Implementation.” It provides a centralized, flexible, computer-base data and display system to assist control room personnel in evaluating the safety status of the plant. This assistance is accomplished by providing the operators, the Emergency Response Facilities (ERFs) and the NRC with high-level graphical displays containing a minimum set of key plant parameters representative of the plant safety status.

The displays of the SAS have been evaluated against human factors design criteria. The concepts used in the SAS design were verified using data recorded from a PWR Power Plant Simulator.

The Distributed Control System (DCS) was expanded to include the SAS/ERDADS System. This ERDADS subsystem to the DCS is referred to as ERDADS/DCS or just DCS.

The SAS is operable during normal and abnormal plant operating conditions. The SAS is available during all SPDS required modes of plant operation. The normal operation mode encompasses all plant conditions at or above normal operating pressure and temperature. When the Reactor Coolant System is intentionally cooled below normal operating values, the operator selects the
Heatup-Cooldown mode which alters the limit checking algorithm for the key parameters. There are also modes of operation which address the Hot Shutdown and Cold Shutdown statuses of the plant.

The SAS equipment is composed of the:

1. Field inputs to the SAS isolation cabinets to the ERDADS/DCS.

2. Hardware and software necessary to communicate with other associated computers via high-speed serial links to the DLS services computers for the General Atomics Radiation Monitoring Systems, and the Meteorological System.

3. Man Machine Interface (MMI) display stations are provided in the Unit 1 Control Room, the Unit 2 Control Room, the Technical Support Center (TSC), and in the Emergency Offsite Facility (EOF) through the PI servers.

The SPDS portion of the SAS is implemented on a FPD which is seismically mounted in an area of the Control Room visible to the control room operator and the senior reactor operator. This

FPD contains the high-level display from which the overall safety status of the plant may be assessed. A dedicated function keyboard allows the operator to select any of the high level displays and various supporting displays at any time.

The SAS is designed such that control room personnel can utilize its features without requiring additional operations personnel.

The SPDS display consists of bar graphs of selected parameter values, digital status indicators for important safety system parameters and digital values. The parameters indicated by bar graphs and digital values include: RCS pressure, RCS temperature, pressurizer level, steam generator levels and steam generator pressures. Status indicators are provided for containment environment and secondary system radiation. Reactor vessel level core exit temperature, amount of subcooling and containment radiation are indicated by digital values.

In addition, there is a message area for an appropriate secondary display providing information related to off-normal value or event detection.

The bar graphs indicate wide-range values and if a parameter is outside its normal range the bar color will change.

During normal operation, the message area is used to display average power, reactor core average temperature, data, time, and unit time. These messages may be displayed by high priority messages as required.

Trend graph groups of selected related parameters are available.

The SAS/ERDADS hardware system utilizes a redundant component configuration to insure high availability. The ERDADS/DCS receive the available variables specified in Regulatory Guide 1.97 Rev. 3. EC286245

The system specified by the U.S. Nuclear Regulatory Commission to fulfill the data collection needs of the NRC is the Emergency Response Data System (ERDS). The ERDS data link provides a direct near real time transfer of parametric reactor data of specified data points from the DCS through the PI servers to the NRC Operations Center. The ERDS data link is used only during emergencies and is activated by the licensee during declared emergencies of ALERT or a higher level classification. Specified data parameter points include (1) core and coolant system conditions, (2) conditions inside containment, (3) radioactivity release rates and (4) Meteorological Tower data. This information allows the NRC information with which to assess the potential or actual impact on public safety.

The interface between the SAS and the input variables derived from safety-related systems are isolated in accordance with the safety system criteria to preserve channel independence and Integrity of the safety systems in the case of SAS malfunction. Also design provisions are included in the Interface between the SAS and non-safety systems to ensure the integrity of the SAS upon failure of non-safety systems.

7.5A.2 HUMAN FACTORS CONSIDERATIONS

Human factors engineering and industrial design techniques have been effectively combined in accordance with established man-machine interface design requirements to maximize system effectiveness, reduce training and skill demands, and minimize operator error.

The FPD color graphic formats and functional keyboard designs have been developed through an interdisciplinary team of senior operational, human factors, industrial design and computer interface personnel.

Minimum use of color, combined with simplified format throughout the FPD presentation, have been key design features to provide both normal and off-normal pattern recognition. The operator, who is the end user, has been directly involved from the conception to insure that man-machine interface goals of SAS have been satisfied. The human factor engineering standards and testing verification methods which have been used are consistent with accepted practices.

7.5A.3 VERIFICATION AND VALIDATION

The SAS is implemented on a digital computer system. The display software that controls the sensor data, key parameter construction and display formats has been developed under strict verification and validation.

Verification and validation is addressed and designed into the DCS software to provide a highly reliable product and a mechanism for identifying and controlling future changes.

THIS FIGURE
HAS BEEN DELETED

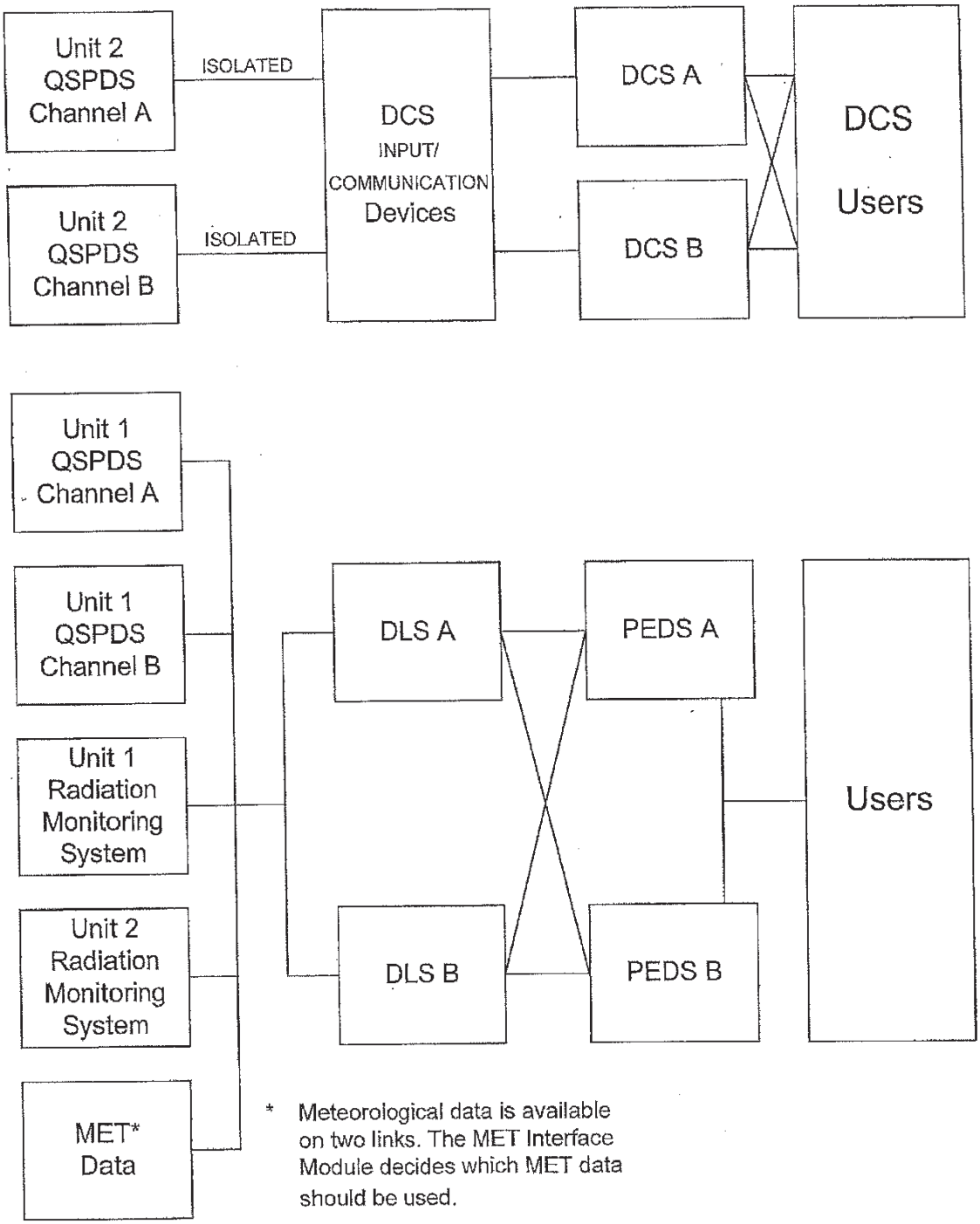
FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.5A-1

THIS FIGURE
HAS BEEN DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.5A-2



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

Data Link System Configuration

FIGURE 7.5A-3

Amendment No. 20 (05/11)

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

7.6.1 DESCRIPTION

This section includes a description of those systems which are required for safety which have not been discussed in Sections 7.2 through 7.5.

7.6.1.1 Shutdown Cooling System Suction Line Valve Interlocks

The Shutdown Cooling System (SDCS) discussed in Subsection 5.4.7 is used to remove decay heat from the Reactor Coolant System.

To preclude overpressurization of the SDCS there are redundant, motor driven isolation valves on each suction line. Interlocks prevent these valves from being opened if RCS pressure has not decreased below the value shown in Table 7.6-1. If the SDCS is operating, and RCS pressure increases above the setpoint shown in Table 7.6-1, the interlock automatically closes the isolation valves. The RCS pressure signals used are provided by the pressurizer pressure 0-750 psia safety channels.

These interlocks are redundant so that any single failure does not cause the SDCS to be subjected to pressures greater than design pressure. The interlock cannot be overridden so that operator action cannot inadvertently subject the SDCS to RCS pressure. In addition, no single failure can prevent the operator from aligning the valves, on at least one suction line, for shutdown cooling after RCS pressure requirements are satisfied. They are powered from safety related buses.

7.6.1.2 Safety Injection Tank Isolation Valve Interlocks

The Safety Injection System (SIS) is discussed in Section 6.3. The safety injection tanks (SIT) inject borated water if system pressure drops below their internal pressure.

The SIT interlocks permit the operator to close the tank isolation valves to prevent the SITs from inadvertently pressurizing the SDCS during shutdown. The SIT isolation valves are also closed to prevent introduction of nitrogen into the RCS. The isolation valves may be manually closed or the SITs partially depressurized when RCS pressure drops below the value shown in Table 7.6-1 so that the SITs cannot cause overpressurization of the SDCS and also so that the SITs can be maintained at some pressure above atmospheric. As RCS pressure increases, the valves automatically reopen at the pressure indicated in Table 7.6-1. The SIAS over-rides the interlock or any manual signal. These interlocks are powered from safety related buses. Following License Amendment no. 100, the SITs are not required to be operable (isolation valves may be closed) when the RCS temperature is below Mode 3 temperature.

7.6.1.3 Design Bases

7.6.1.3.1 Shutdown Cooling System Suction line Valve Interlocks

The SDCS interlocks conform to the following design criteria:

a. The isolation valves have interlocks to prevent opening the isolation valves while the RCS pressure is above the allowable SDCS pressure;

b. The interlocks keep the SDCS line isolated even after a single failure;

c. The interlocks do not prevent achieving cold shutdown after a single failure (Section 5.4.7.2.6 and 5.4.7.5);

d. Pressurizer pressure is used to provide the interlock functions;

e. Two pair of physically independent sensors, located on separate pressurizer sensing nozzles, are provided; and

f. The interlocks do not fail so as to preclude opening of at least one SDCS path (if RCS pressure permits), or closing of both suction paths after a LOCA.

7.6.1.3.2 Safety Injection Tank Isolation Valve Interlocks

The SIT isolation valve interlocks are designed consistent with the balance of the SIS. Because the SIS is an ESF system, the ESF criteria takes precedence over any other criteria applied to the interlocks. The SIT interlocks meet the following criteria:

a. The SITs cannot be isolated from the RCS when RCS pressure exceeds a preset value; the interlocks automatically open the isolation valves when RCS pressure exceeds a preset value;

b. Pressurizer pressure provides the input to interlocks; and

c. Two pair of physically independent sensors, located on separate pressurizer sensing nozzles, are provided.

7.6.1.4 Final System Drawings

For schematic diagrams see Section 1.7 for a list of drawings.

7.6.2 ANALYSIS

7.6.2.1 Design Criteria

7.6.2.1.1 Shutdown Cooling System Suction Line Valve Interlocks

a. The isolation valve interlocks are redundant in that there are two trains; mechanical train A has two valves, one receiving its electrical signal from one pressure sensor and the second valve receives its signal from another sensor; mechanical train B also has two valves but using two different pressure sensors. Each electrical path to each pair of valves is physically independent and separate from the others. With this degree of redundancy, and independence, the interlocks can sustain a single failure and still isolate both heat exchangers or make one available when required (see Figure 7.6-1).

b. The method for identifying power, signal and control cables and cable trays dedicated to the instrumentation, control and electrical equipment associated with the isolation valves is discussed in Subsection 8.3.1 and meets the intent of Regulatory Guide 1.75, "Physical Independence of Electric Systems," 1/75 (R1) as discussed in Subsections 7.1.2.2 and 8.3.1.2.

c. The instrumentation, control and electrical equipment associated with SDCS interlocks are seismically and environmentally qualified in accordance with the requirements stated in Sections 3.10 and 3.11.

7.6.2.1.2 Safety Injection Tank Isolation Valve Interlocks

The SIS is an ESF system and the requirements of the General Design Criteria, Regulatory Guides, and IEEE standards appropriate for ESF systems are used for the instrumentation and controls associated with SIS. The interlocks design is consistent with the balance of the system and its requirements. Refer to Section 6.3 for a discussion of the SIS and Section 7.3 for a discussion of the ESFAS.

7.6.2.2 Equipment Design Criteria

7.6.2.2.1 Shutdown Cooling System Suction Line Valve Interlocks

This description is only of the interlocks. The valves and piping are discussed in Subsection 5.4.7. The requirements of IEEE 279-1971 are written expressly for protection systems and as such are not directly applicable to these interlocks. However, a discussion of the extent to which these interlocks comply with Section 4 of this standard is provided below:

4.1 "General Function Requirement"

The interlocks are designed to operate during normal shutdown, refueling and accident conditions.

4.2 "Single Failure Criterion"

Any single failure leading to loss of one channel does not result in opening of all of the isolation valves installed in series in one SDCS suction line.

4.3 "Quality Control of Components"

The sensors and other instrumentation associated with these interlocks meet the same quality requirements imposed on the protection system sensors.

4.4 "Equipment Qualification"

Type tests are performed on the instrumentation to ensure that it meets its performance requirements.

4.5 "Channel Integrity"

The interlocks are designed to maintain functional capability during accident environments. Failure of one interlock does not preclude opening a path or closing both paths of the SDCS.

4.6 "Channel Independence"

The pressure transmitters are located on separate pressurizer nozzles. Separation is maintained between channels.

4.7 "Control and Protection System Interaction"

There is no control and protection system interaction.

4.8 "Derivation of System Inputs"

Pressurizer pressure is the sensed parameter.

4.9 "Capability for Sensor Check"

The operational availability of the four pressure sensing channels can be determined by comparing their outputs once pressurizer pressure has come within the range of the sensors.

4.10 "Capability for Test and Calibration"

Testing is performed during normal plant shutdown periods using standard test devices and approved procedures.

4.11 "Capability for Bypass or Removal from Operation"

Removal of one channel for test does not compromise system reliability. Failure of one of the remaining channels during a test outage does not create an unacceptable situation, since administrative controls (key locks) preclude inadvertent opening of the valves by the operator.

4.12 through 4.14 "Bypassing"

There are no bypasses.

4.15 "Multiple Setpoints"

This requirement is not applicable.

4.16 "Completion of Protective Action Once it is Initiated"

This requirement is not applicable.

4.17 "Manual Initiation"

The controllers are permissive controls which permit the operator to open the valves below a certain pressure. The controllers also close the valve above a certain pressure. The key lock required to open the valves does not override the controllers.

4.18 "Access to Setpoint Adjustments, Calibration and Test Points"

Access is controlled by administrative procedures.

4.19 "Identification of the Protective Action"

This requirement is not applicable.

4.20 "Information Readout"

The readout consists of an annunciator alarm and position indication lights for each valve. This provides the operator with clear and concise information.

4.21 "System Repair"

Components are accessible for repair. One channel can be placed out of service for maintenance without jeopardizing the isolation of the SDCS.

4.22 "Identification"

The method for identifying power, signal and control cables and cable trays dedicated to the instrumentation, control and electrical equipment associated with the isolation valves is discussed in Subsection 8.3.1.3 and meets the intent of Regulatory Guide 1.75 (R1) as discussed in Subsections 7.1.2.2 and 8.3.1.2.

7.6.2.2.2 Safety Injection Tank Isolation Valve Interlocks

The SIS design requirements are discussed in Section 6.3. The requirements of IEEE 279-1971 are written expressly for protection systems, and as such, they are not directly applicable to these interlocks. The following discussions refer to the requirements set forth in the respective items of Section 4 of IEEE 279-1971 as they relate to the SIT isolation valve interlocks:

4.1 "General Function Requirement"

The interlocks are designed to operate during normal shutdown, refueling and accident.

4.2 "Single Failure Criterion"

No single failure of an interlock channel can prevent system operation when it is required.

4.3 "Quality Control of Components"

The instrumentation for these interlocks meet the same quality requirements imposed on the protection system sensors.

4.4 "Equipment Qualification"

Type tests are performed on the instrumentation to ensure that it meets its performance requirements.

4.5 "Channel Integrity"

The interlocks are designed to maintain their functional capability when exposed to accident environments. They do not preclude safety injection during accident conditions.

4.6 "Channel Independence"

The pressure transmitters are located on separate pressurizer nozzles. Separation is maintained between channels.

4.7 "Control and Protection System Interaction"

There is no control and protection system interaction.

4.8."Derivation of System Inputs"

Pressurizer pressure is the sensed parameter.

4.9."Capability for Sensor Checks"

The operational availability of the four pressure sensing channels can be determined by comparing their outputs once pressurizer pressure has come within the range of the sensors.

4.10 "Capability for Test and Calibration"

Testing is performed during normal plant shutdown periods using standard test devices and approved procedures.

4.11 "Capability for Bypass or Removal from Operation"

Removal of one channel for test does not compromise system reliability. Failure of one of the remaining channels during a test outage does not create an unacceptable situation since administrative controls (key locks) preclude inadvertent closing of the valves by the operator.

4.12 through 4.14 "Bypassing"

There are no bypasses.

4.15 "Multiple Setpoints"

This requirement is not applicable.

4.16 "Completion of Protective Action Once Initiated"

This requirement is not applicable.

4.17 "Manual Initiation"

The valves are locked open during normal operation. The controllers are permissive controls which permit the operator to close the valves below a certain pressure. The controllers also open the valves above a certain pressure. The keylock required to close the valves does not override the controllers.

4.18 "Access to Setpoint Adjustments, Calibration and Test Points"

Access is controlled by administrative procedures.

4.19 "Identification of the Protective Action"

This requirement is not applicable.

4.20 "Information Readout"

The readout consists of pressure indicators, and position indicators and position indication lights for each valve. This provides the operator with clear and concise information.

4.21 "System Repair"

The components are accessible for repair. One channel can be placed out of service without jeopardizing the availability of the SITs.

4.22 "Identification"

The cables associated with SIT isolation valve interlocks are uniquely identified. The instrumentation cables associated with SIT level and pressure indication are not uniquely identified. The channels are identified to distinguish between channels of safety related equipment (see Subsection 7.1.2).

7.6.3 ADDITIONAL SYSTEMS REQUIRED FOR SAFETY

7.6.3.1 Refueling Interlocks

Refueling interlocks are described in Subsection 9.1.4.

7.6.3.2 Fuel Pool Cooling and Purification System

The fuel pool instrumentation system is described in Subsection 9.1.3.2.4. A tabulation of the instrument channels and Class 1E instrumentation is included in Table 9.1-7.

All Class 1E instrumentation identified in Table 9.1-7 is qualified to IEEE 323-1974 and 344-1975.

7.6.3.3 Reactor Coolant Leak Detection System

Reactor coolant leakage detection is described in Subsection 5.2.5.

7.6.3.4 Process and Effluent Radiological Monitoring and Sampling System

The radiation monitoring system is composed of process, effluent, area, and in-plant airborne monitors. Tabulations of these monitors are given in Tables 11.5-1, 12.3-2, and 12.3-3. The Class 1E effluent monitors are the plant stack, as described in Subsection 11.5.2.2.8, and the ECCS exhaust monitors, as described in Subsection 11.5.2.2.10. The Class 1E area monitors include the four CIAS and six spent fuel pool monitors, as well as two post-accident containment monitors. All these monitors are described in Subsection 12.3.4.1.4. The Class 1E in-plant monitors include the containment atmosphere monitors, as described in Subsection 12.3.4.2.3.1, the control room air intake monitors, as described in Subsection 12.3.4.2.3.2 and the ECCS exhaust monitors, as described in Subsection 12.3.4.2.3.3.

The component cooling water radiation monitors are Class 1E and are provided with Class 1E power supply (see Table 11.5-1).

All Class 1E monitors are qualified to IEEE 323-1974 and IEEE 344-1975.

7.6.3.5 Containment Vacuum Relief System

The instrumentation provided for this system is in accordance with Figure 9.4-9.

The containment to annulus differential pressure instrumentation that is used for automatic control of the containment vacuum relief valves is Class 1E. The associated differential pressure transmitters are qualified to IEEE 344-1975 and IEEE 323-1974 for the environment in which they operate. The remote mounted indicators and bistables are mounted on the seismically qualified HVCB in the control room.

7.6.3.6 Overpressurization Protection

Overpressurization protection is described in Subsection 5.2.2.

7.6.3.7 Shield Building Ventilation System (SBVS) Switchover from Fuel Handling Building (FHB)

The Shield Building Ventilation System is an ESF System and is listed in Section 7.3. The SBVS switchover from Fuel Handling Building is the only portion of this system listed in Section 7.6. The SBVS is described in Subsection 6.2.3.2.

The instrumentation requirements are provided in Subsection 6.2.3.5 and Table 6.2-51.

Instrumentation and controls discussed above for SBVS system are Class 1E. Alarms are annunciated on non-safety annunciation windows through proper isolation devices.

All controls and instrumentations for SBVS is qualified to IEEE 323-1974 and IEEE 344-1975. The remote mounted indicators and bistables are mounted on the seismically qualified HVCB in the control room.

7.6.3.8 IEEE 279-1971 Compliance

The four containment area radiation monitors which input into the CIAS and the SBVS conform to IEEE 279-1971 similar to the ESFAS described in Subsection 7.3.1.2.

The requirements of IEEE 279-1971 for the other systems required for safety are not completely applicable because this instrumentation is not part of a protection system. However, the intent of the design criteria contained therein has been applied in the design of these systems to the following extent:

4.1 - "General Functional Requirements"

The safety-related instrumentation for the above systems is designed to provide monitoring and actuation as applicable during normal or accident conditions. The instrument performance characteristics, response times and accuracy are selected for compatibility for the particular function.

4.2 - "Single Failure Criterion"

This is functionally identical to that described in Subsection 7.4.2.2.

4.3 - "Quality Control of Components and Module"

See Chapter 17.

4.4 - "Equipment Qualification"

The instrumentation and controls for these systems meet the equipment qualification requirements discussed in Sections 3.10 and 3.11.

4.5 - "Channel Integrity"

The "Channel Integrity" is functionally identical to that described in Subsection 7.3.2.1.2.

4.6 - "Channel Independence"

The Channel independence is functionally identical to that described in Subsection 7.3.2.1.2.

4.7 - "Control and Protection System Interaction"

No portion of these systems is used for both control and protection.

4.8 - "Derivation of System Inputs"

The monitoring signals for the above systems are a direct measurement of the desired variables.

4.9 - "Capability for Sensor Checks"

The monitoring sensors are checked by comparing the monitored variables of redundant channels or by observing the effects of introducing and varying a substitute input to the sensor similar to the measured variable.

4.10 - "Capability for Test and Calibration"

IEEE 338-1971 and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" 2/72 (R0) provides guidance for the development of procedures, equipment and documentation of periodic testing. The measurement signals required for the above systems have the capability of being tested and calibrated under the design requirements of the system.

4.11 - "Channel Bypass or Removal from Operation"

Any one of the channels may be tested, calibrated, or repaired without detrimental effects on the other channels.

4.12 - "Operating Bypasses"

There are no "Operating Bypasses" for these systems.

4.13 - "Indication of Bypasses"

A discussion of bypass and inoperable status indication is provided in Subsection 7.5.1 and a listing of inoperable or bypassed components is contained in Table 7.3-10.

4.14 - "Access to Means for Bypassing"

This section is not applicable.

4.15 - "Multiple Setpoints"

This section is not applicable.

4.16 - "Completion of Protective Action Once it is Initiated"

This section is not applicable.

4.17 - "Manual Initiation"

Manual initiation of the components in these systems is available.

4.18 - "Access to Setpoint Adjustments, Calibration, and Test Points"

This section is not applicable.

4.19 - "Identification of Protective Actions"

This section is not applicable.

4.20 - "Information Readouts"

The monitoring and control channels for these systems are indicated in the control room with the following exceptions:

Remote fuel pool temperature and water level indication is not provided. However, fuel pool temperature and water level alarms are annunciated in the control room.

4.21 - "System Repair"

Replacement or repair of components can be accomplished in reasonable time when the systems are not actuated. Outage of system components for replacement or repair are limited by the Technical Specifications.

4.22 - "Identification"

Safety equipment and cables associated with these systems are uniquely identified.

7.6.3.9 IEEE 308-1971 Compliance

The St. Lucie Unit 2 UFSAR is committed to Regulatory Guide 1.32 Rev. 0 which addresses IEEE 308-1971. For a further discussion of IEEE 308-1971 refer to Subsection 8.3.1.2. All Class 1E electrical components are electrically and physically separated in accordance with Regulatory Guide 1.75 (R1) as discussed in Subsection 8.3.1.2. Electrically redundant and physically independent power supplies to the above systems, electrical components, and to the safety-related power panels that provide power to control and instrumentation devices are provided.

All Class 1E electrical system components are uniquely identified in accordance with Subsection 8.3.1.3.

The fuel pool purification pump is a non-safety pump and as such is physically independent and electrically separated from Class 1E components.

7.6.3.10 Direct Position Indication of Relief And Safety Valves TMI Item II.D.3

Acoustic valve flow monitors are used to provide direct position indication of pressurizer safety valves (SRVs) and power operated relief valves (PORVs).

7.6.3.10.1 Design Basis

a. Valve positions are monitored acoustically and indicators and alarms are provided in the control room.

b. Acoustic Flow monitors are powered from a vital instrument bus and are designed as seismic Category I.

c. The acoustic flow monitors are qualified for the appropriate environment (any transient or accident which causes the relief or safety valve to open).

7.6.3.10.2 Description

The means of detecting pressurizer safety relief and power operated relief valve position is by continuously and automatically detecting acoustical signals generated by flow noise levels through the valve.

This is accomplished by utilizing accelerometers mounted on the discharge pipe. The accelerometer converts acoustical acceleration into an electrical charge which is converted to a voltage by the charge converter. This proportional voltage is then processed and a relative flow indication is obtained.

Five valve position monitors are provided, one for each of the three pressurizer safety relief valves and the two PORVs. A common audio-visual alarm alerts the operators when flow through any of the five valves exceeds a pre-established setpoint. These setpoints can be adjusted from the control room.

The system is powered from a 120V ac 60 Hz uninterruptible power supply (UPS). An alarm is initiated upon loss of instrument power. The indicator modules are located in the Control Room Plant Auxiliary Control Board No. 2 (PAC B-2). The system is qualified in accordance with IEEE 323-1974 and 344-1975. The accelerometers and charge converters are located inside the containment and are subjected to the containment environment during and following a small break LOCA. These components are designed and tested to withstand and remain operable following the postulated accident. Various components of the acoustic valve flow monitors are identified in Table 7.6-2.

7.6.3.11 Anticipated Transient Without Scram (ATWS)

On July 26, 1984, The Code of Federal Regulations was amended to include Section 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," (also known as

the ATWS Rule). The ATWS Rule requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the likelihood of a failure to shut down the reactor following anticipated transients, and to mitigate the consequences of anticipated transients which occur without a shutdown. The occurrence of an anticipated transient in conjunction with a failure of the Reactor Protective System (RPS) to produce a reactor trip is defined as an ATWS event.

The combination of an RPS failure and an anticipated transient is outside the present plant design basis and was analyzed by Combustion Engineering (CE) via CENPD-158.

It was determined that a complete loss of feedwater combined with a failure of the reactor to trip would result in a primary coolant system pressure excursion well above reactor vessel service level C limits, and therefore, potentially challenge the integrity of the reactor coolant pressure boundary.

For Combustion Engineering plants, the regulations require the implementation of two methodologies for ensuring that an excessive primary coolant pressure excursion does not occur. These methodologies are called "prevention" and "mitigation." Prevention takes form as a Diverse Scram System (DSS) whose purpose is to initiate a shutdown of the reactor by control rod insertion upon conditions indicative of an anticipated transient, independently and diversely from the RPS. Mitigation is accomplished by tripping the turbine and initiating Auxiliary Feedwater to conserve steam generator inventory and to ensure that a primary coolant heat sink is available. As required by the rule, both the turbine trip (DTT) and the auxiliary feedwater (DAFAS) initiation were also required to be diverse from the RPS. Through these diverse means of prevention and mitigation, peak reactor coolant system pressure will remain within acceptable values.

The requirements of 10 CFR 50.62 for prevention and mitigation were incorporated into the Diverse Scram System (DSS), Diverse Turbine Trip (DTT), and Diverse Auxiliary Feedwater Actuation System (DAFAS). Their design has been specifically approved in the USNRC Safety Evaluation of Compliance with ATWS Rule 10 CFR 50.62 dated September 6, 1989.

7.6.3.11.1 Diverse Scram System (DSS)

The Diverse Scram System (DSS) is a safety-related system that utilizes existing pressurizer pressure instruments and signal converters and takes as inputs, signals from secondary current loops in RTGB-206 (Figure 7.6-2). These signals are wired to the Engineered Safety Features Actuation System (ESFAS) cabinets where they are processed by DSS bistable and logic components to provide reactor trip signals. The trip signals are used to open the non-safety related control element assembly drive (CEA Drive) motor generator (MG) set output load contactors located between the CEA drive MG set output breakers and the Reactor Trip Switchgear. The consequential loss of voltage on the Reactor Trip Switchgear buses causes the reactor to shut down.

The DSS utilizes the four pressurizer pressure transmitters and their respective current loops for the source of the DSS input signals. These transmitters are also used for the RPS and ESFAS as discussed in Sections 7.2 and 7.3. Two E/I (voltage-to-current) converters in each instrument loop isolate the RPS and DSS inputs from each other.

The following table is provided to list the major components for the DSS inputs.

INST NUMBER	SAFETY CHANNEL	INSTRUMENT CABINET	RPS E/I CONV	DSS E/I CONV	ESFAS CHANNEL
PT-1102A	A	PY-1102A	PY-1102A-1	PY1102A-2	MA
PT-1102B	B	PY-1102B	PY-1102B-1	PY1102B-2	MB
PT-1102C	C	PY-1102C	PY-1102C-1	PY1102C-2	MC
PT-1102D	D	PY-1102D	PY-1102D-1	PY-1102D-2	MD

Pressurizer pressure input signals are wired into the ESFAS cabinets where they are routed to four bistable modules, one in each measurement cabinet. Digital outputs (ON) are produced from the DSS bistable modules when the pressurizer pressure reaches 2450 psia. This is the DSS actuation setpoint recommended by Combustion Engineering in CEOG report CE NPSD-354. Each of the four bistable modules produces an output for two digital isolators, an SA and an SB, located in the same measurement cabinets as their associated bistable modules. The outputs of the four SA isolators are routed to ESFAS cabinet ESC-SA while the four SB isolator outputs go to ESFAS cabinet ESC-SB. In each safety cabinet (SA and SB), there is an actuation module which accepts the four isolated digital signals and applies two-out-of-four (2/4) logic to produce a digital output. Each 2/4 actuation module sends its output through an isolator to a CEA drive MG set load contactor, the SER, and to an annunciator window. Both actuation modules must function and trip both load contactors to produce a reactor trip in a 2/2 output logic.

There are two bypass switches, one each located on safety channel cabinets SA and SB. Both switches have two positions, NORMAL and BYPASS, and are controlled by keys removable only in the NORMAL position. When in the NORMAL position, the DSS operates as designed and sends actuation signals to the MG set load contactors to trip the reactor. In the BYPASS position, however, the DSS actuation signals are blocked to allow operators to test and maintain the DSS with the plant at power without the potential for reactor trip. Complete testing overlap, from the sensors to the trip coils may be accomplished with the plant shut down. There are also four bistable bypass switches, one for each bistable device. Their function is to bypass bistable devices individually to test or maintain them without causing bistable output signals to be sent to the 2/4 actuation modules.

Since the logic of the DSS is integrated into the ESFAS, the existing ESFAS cabinet automatic testing instrument (ATI) is utilized to check the functions of the DSS components from the bistable devices through the 2/4 actuation modules by using pulses from an auto-test generator. ATI operates continuously as long as ESFAS circuits are energized.

An annunciator window is used to indicate when a DSS actuation signal is obtained from either 2/4 actuation module. A second annunicator window is used to indicate when either of the two safety channel bypass switches is placed in the BYPASS position. Local indicating lights on the ESFAS cabinets perform the same functions.

Diversity of the DSS from sensor output to, and including, the device that interrupts control rod power is required. This diversity to the RPS and its trip bypass is achieved by utilizing different manufacturers or circuit designs for the bistables, comparators, relay logic and relay actuation

outputs. Finally, the final actuation devices (contactors vs. breakers) are diverse and are operated independent of the RPS or its trip paths.

Although the electrical power supply system which serves RPS and DSS is the same, analysis has shown that the design of their inverter system is such that it minimizes common cause failures or will annunciate the condition before an unacceptable degradation occurs, which, could affect both the DSS and RPS. In addition, the DSS will remain operable upon loss of offsite power.

End to end testing of the DSS (DSS actuation to breaker opening) is performed each refueling outage.

This system, diverse and independent from the RPS except at the instrument loops, satisfies the ATWS Rule requirements for prevention.

7.6.3.11.2 Diverse Turbine Trip (DTT)

The Diverse Turbine Trip (DTT) is inherent in the design of the DSS and it utilizes the DSS bistable and logic functions. Tripping of the load contactors for both MG sets will initiate a Diverse Turbine Trip. When the DSS actuates during an ATWS event, the load contactors will open and de-energize the reactor trip switchgear buses. The loss of voltage on the reactor trip switchgear will be sensed by four undervoltage relays, which, in turn will operate one auxiliary relay each. The contacts on the four auxiliary relays are arranged in two-out-of-four logic to provide turbine trip signals to the emergency trip solenoids. If the emergency trip solenoids are operated, hydraulic oil will be dumped from the turbine control oil system and turbine trip will occur. Reference Section 10.2.2 for further description of the turbine trip system.

The undervoltage relays, auxiliary relays, and solenoids used in the DTT are diverse from the components used in the Reactor Protection System and its trip paths. The DTT, therefore, satisfies the ATWS Rule requirements for mitigation.

7.6.3.11.3 Diverse Auxiliary Feedwater Actuation System (DAFAS)

The Auxiliary Feedwater Actuation System is described in Section 7.3.1.1.8. Diversity of the DAFAS from sensor output up to, but not including, the final actuating devices is required. This diversity to the RPS is achieved by utilizing different manufacturers or circuit designs for the bistables, comparators, matrix relays and initiation relays. Finally, the commonality of the electrical power system has been shown to be acceptable based on an analysis of common mode failure mechanisms as discussed above for the DSS. The DAFAS, therefore, satisfies the ATWS Rule requirements for mitigation.

TABLE 7.6-1

SHUTDOWN COOLING SYSTEM AND SAFETY INJECTION TANK INTERLOCKS

System	(Pressurizer Pressure) Setpoint	Function
Shutdown Cooling System		
Suction Line Isolation Valves (V3480,3481,3651,3652)	≤276 psia	Permits valves to be opened by operator.
	≥515 psia **	Valves are automatically closed.
Safety Injection Tank		
Isolation Valves	≥515 psia **	Valves are automatically opened.
(V3614,3624,3634,3644)	≤276 psia *	Permits valves to be closed by operator.
	SIAS *	Automatically opens the valves, if the valves are closed. Sends an open signal if valves are open that overrides a closing signal.

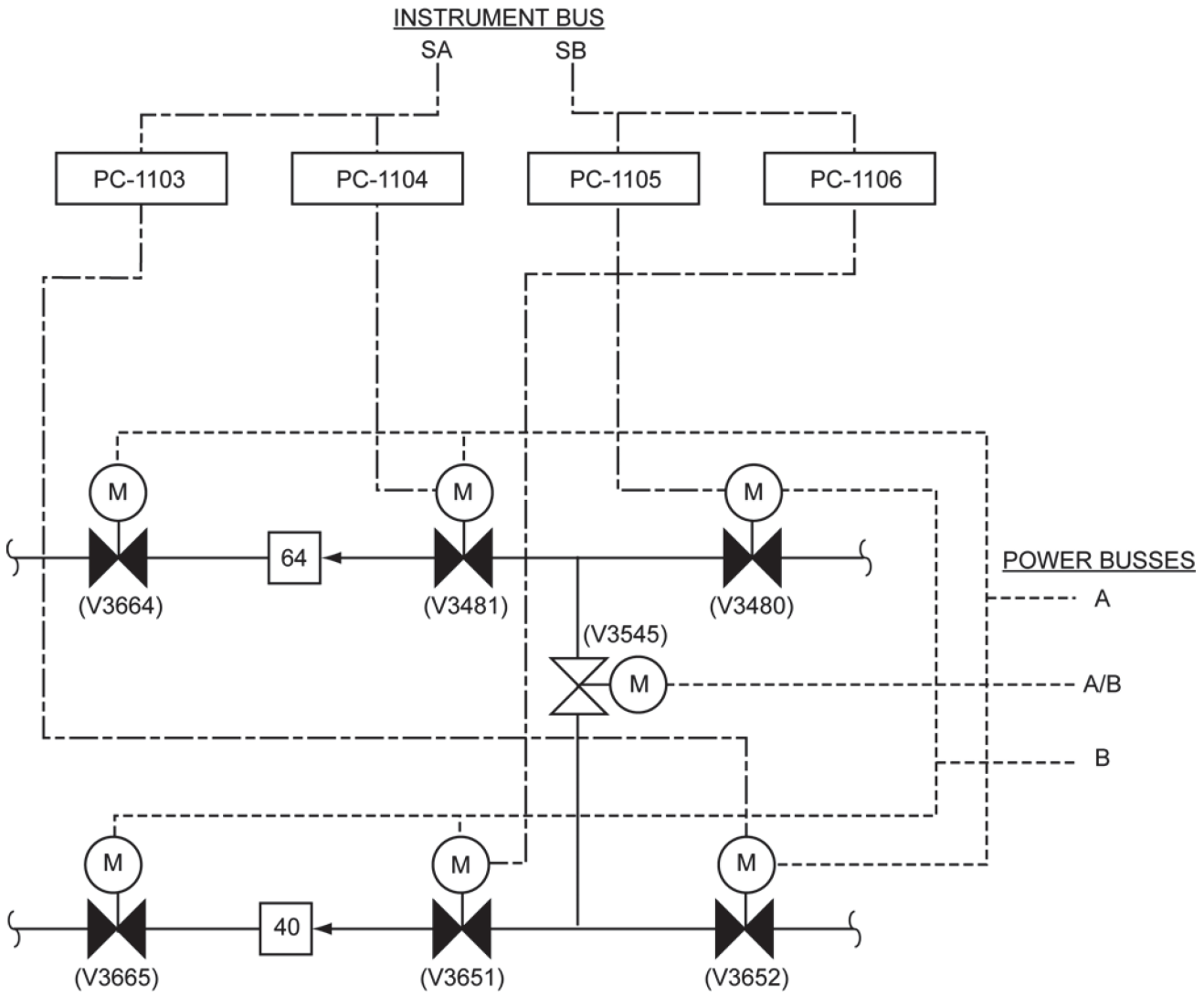
* Following License Amendment no. 100, the SITs are not required to be operable (isolation valves may be closed) when the RCS temperature is below Mode 3 temperature.

** Prior to an actual or simulated pressurizer pressure signal exceeding 515 psia.

TABLE 7.6-2

ACOUSTIC VALVE FLOW MONITOR COMPONENTS

Acoustical Sensors	Total number 5 Tested and qualified to IEEE 344 and 323 for the containment environment.
Charge Converters	Total number 5 Tested and qualified to IEEE 344 and 323 for the containment environment.
Indicator Modules	Total number 5 Tested and qualified to IEEE 344 and 323 for the control room environment.
Alarm Module	Total number 1 Tested and qualified to IEEE 344 and 323 for the control room environment.
Cable	Furnished as Class 1E. 50 feet of low noise, high temperature cable connects each valve sensor to its charge converter.



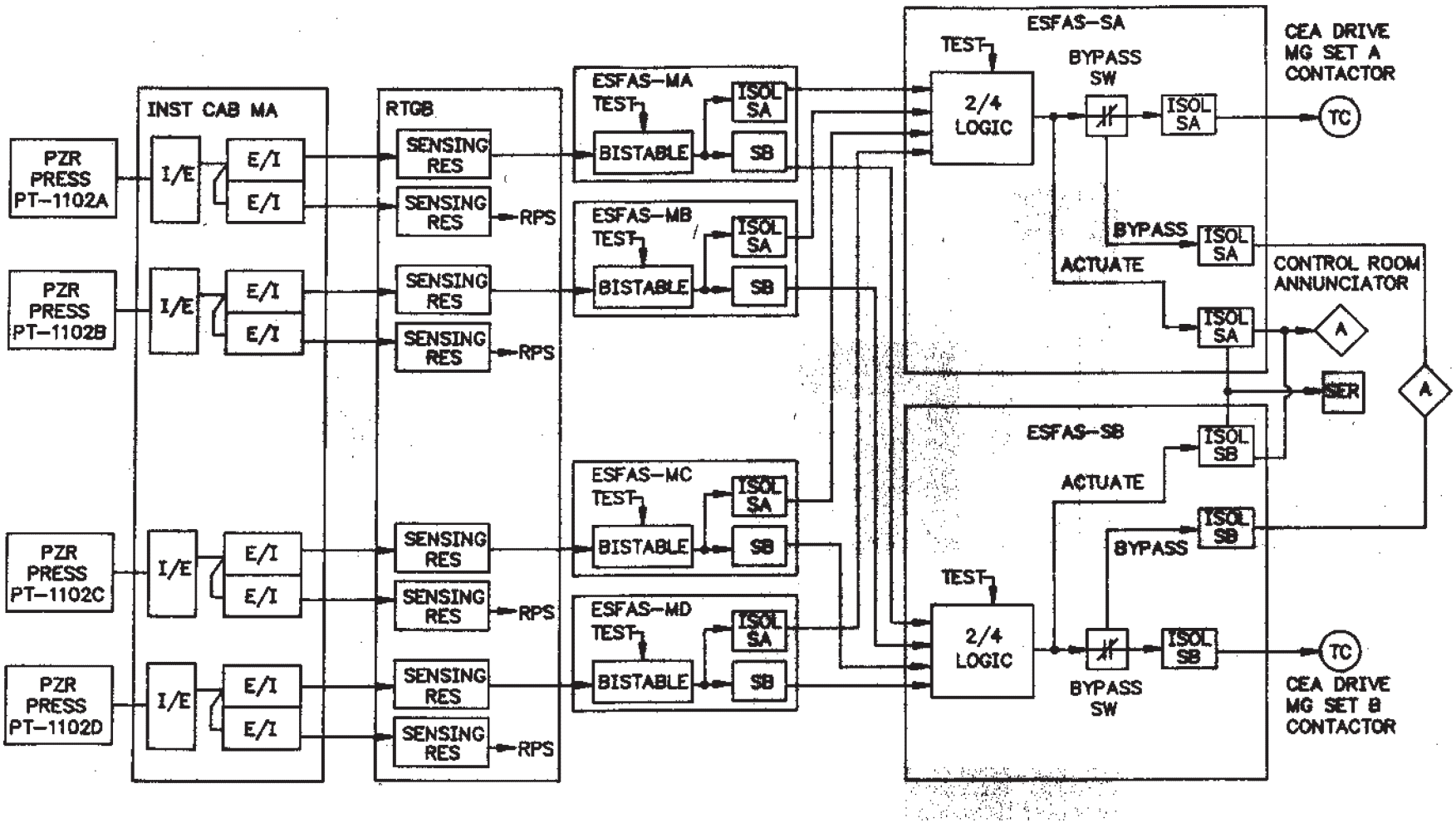
FLORIDA POWER & LIGHT COMPANY

ST. LUCIE PLANT UNIT 2

SHUTDOWN COOLING SUCTION VALVES POWER & CONTROL

FIGURE 7.6-1

Amendment No. 18 (01/08)



AMENDMENT NO. 7 (4/92)

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ATWS BLOCK DIAGRAM

FIGURE 7.6-2

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

7.7.1 DESCRIPTION

The control and instrumentation systems, whose functions are not essential for the safety of the plant, include plant instrumentation and control equipment not addressed in Sections 7.2 through 7.6. The general description given below permits an understanding of the reactor coolant and pertinent subsystem control methodology.

The designed reactivity feedback properties of the Nuclear Steam Supply System (NSSS) inherently cause reactor power to match the total NSSS load. The resulting reactor coolant temperature at which this occurs is a controlled parameter and is adjusted by changes in total reactivity as implemented through CEA position changes or through boric acid concentration changes in the reactor coolant.

The ability of the NSSS to follow turbine load changes is dependent on the ability of the automatic control systems or operator to adjust reactivity, feedwater flow, bypass steam flow, reactor coolant inventory, and energy content of the pressurizer such that NSSS conditions remain within normal operating limits.

Except as limited by xenon conditions, the major control systems described below provide the capability to automatically follow limited load changes.

7.7.1.1 Control Systems

7.7.1.1.1 Reactivity Control Systems

Reactivity is controlled by adjustments of control element assemblies (CEAs) for rapid reactivity changes or by adjustment of boric acid concentration for slow reactivity changes. The boric acid is used to compensate for slow load changes and for such long term effects as fuel burnup and changes in fission product concentration. Since these long term changes occur slowly, operator action is suitable for boric acid concentration control. The CEAs are controlled to maintain the programmed reactor coolant temperature and power level during boric acid concentration changes, within the limits of CEA travel.

The Reactor Regulating System (RRS) adjusts reactor power and reactor coolant temperature to follow turbine load transients within established limits. The RRS receives a turbine load index signal (HP turbine inlet pressure linear indication of load) and reactor coolant temperature signals (see Figure 7.7-1). The turbine load index is supplied to a reference temperature (T_{REF}) program which establishes the desired average temperature. The hot leg and cold leg temperature signals are averaged (T_{AVG}) in the RRS. The T_{REF} signal is then subtracted from the T_{AVG} signal to provide a temperature error signal. The turbine load index is subtracted from the power range neutron flux to provide a power error signal. A derivative network is used to provide a power error compensation signal that is proportional to the rate of change of the power error. The temperature error and power error compensation signals are then combined.

This resulting error signal is fed to a CEA rate program, to determine whether the CEAs are to be moved at a high or low rate, and to a CEA status program which determines if the CEAs are to be withdrawn, inserted or held. The outputs of the rate and status programs are sent to the Control Element Drive Mechanism Control System (CEDMCS). The automatic withdrawal signal

is presently disabled at the CEDMCS cabinet. CEA withdrawal is accomplished manually only. Consequently, the following discussion on Automatic Withdraw Prohibit (AWP) is maintained for completeness of system capability description only and is not relevant while automatic withdrawal is disabled.

If the temperature error signal is very high, that is T_{AVG} is much higher than T_{REF}, an Automatic Withdrawal Prohibit (AWP) signal is sent to the CEDMCS. Since the withdrawal of CEAs causes T_{AVG} to increase, prohibiting a withdrawal prevents an increase in the error signal.

The design of the AWP is functionally identical to St. Lucie Unit 1. Receipt of an AWP signal, which is a contact closure interface, energizes the AWP relay. The energized AWP relay opens the contact interfacing the AWP signal to the control AWP raise/lower logic. When the logic power is removed from the AWP input, the circuitry cannot generate a control group raise signal which is necessary for CEA motion.

Indications of AWP initiation are as follows:

1. At the CEDMCS supervisory panel
2. Plant Annunciator

The following is a functional description of the AWP:

a. The AWP prohibits the withdrawal of all regulating CEAs in the automatic sequential mode of control.

    1. The AWP interlock does not prohibit CEA motion in any other mode of control except automatic sequential.
    2. The AWP interlock does not prohibit CEA insertion.

b. An AWP interlock is generated by the CEDMCS whenever any of the following conditions occur:

    1. Reactor Coolant Loop Cold Leg Temperature (T_{cold}) exceeding a setpoint as indicated by a contact closing from either one or both of two channels of (T_{cold}) instrumentation.
    2. Mismatch between average reactor coolant temperature (T_{AVG}) and the programmed temperature (T_{REF}) exceeding a setpoint as indicated by a contact closure from the Reactor Regulating System.
    3. Turbine bypass demand as indicated by a contact closing from the Steam Bypass Control System.
    4. A dropped rod condition, as indicated by a contact closure from a Reed Switch Position Transmitter Dropped Rod Contact.

The CEDMCS accepts automatic CEA insertion* demand signals from the Reactor Regulating System, or manual motion demand signals from the CEDMCS operator s module and converts these signals to direct current pulses that are transmitted to the CEDM coil to cause CEA motion.

Further, the CEDMCS receives CEA motion inhibit signals from the Analog Display System (refer to Subsection 7.7.1.1.6) for certain abnormal CEA configurations.

The Reactor Protective System (RPS) generates a CEA withdrawal prohibit upon pre-trip conditions to the CEDMCS (refer to Section 7.2.2.1) to enhance plant availability.

The CEA withdraw prohibit (CWP) signal from the RPS is interfaced to the CEDMCS via a normally closed contact. A CWP condition opens the contact de-energizing the CWP relay in the CEDMCS Common Logic Relay Interface. This removes a logic "1" input to the individual CEA enable logic which prevents a "withdraw CEA" signal from being generated to the CEDM coil timing logic. The withdraw signal is necessary for CEA motion.

The following is a functional description of the CWP signal:

a. It prohibits the withdrawal of all CEAs in all modes of control regardless of any demand for motion.

b. It is generated by the CEDMCS upon a contact opening signal from the Reactor Protection System (RPS). This signal is initiated by a 2 of 4 pre-trip actuation in any one of the following.

    1. Local Power Density

    2. High Startup Rate

    3. Thermal Margin/Low Pressure

    4. High Power

c. Local indication and a contact opening output for remote annunciation of the interlock are provided.

d. The interlock may be overridden from the CEDMCS Control Panel by depressing both the Bypass Enable and Bypass Pusbbuttons. The bypass pushbutton must be held depressed while demanding CEA motion. The override allows all CEA motion in all modes of control.

The CWP function is not required by the Safety Analysis to prevent exceeding core safety limits. The CWP bypass is maintained under strict administrative control via plant operating procedures.

---

*Currently, the automatic CEA insertion feature of the RRS is not used to avoid any spurious CEA insertion (administratively disabled)

The Steam Dump and Bypass Control System (SBCS) sends an Automatic Withdrawal Prohibit (AWP) signal to the CEDMCS upon initiation of steam being bypassed (refer to Subsection 7.7.1.1.5).

A reactor trip initiated by the RPS causes the input motive power to be removed from the CEDMCS by the trip switchgear, which in turn causes all CEAs to be inserted by gravity (see Figure 7.7-2). The CEDMCS is thus not required for safety.

There are four different modes of CEA movement; sequential group movement in manual and automatic modes, manual group movement and manual individual CEA movement modes. Sequential group movement functions such that, when the moving group reaches a programmed low (high) position, the next group begins insertion (withdrawal), thus providing for overlapping motion of the regulating groups. The initial group stops after reaching its lower (upper) limit. Applied successively to all regulating groups, the procedure allows a smooth continuous rate of change of reactivity. The regulating group sequencing signals, called sequential permissives, are supplied to CEDMCS by the Distributed Control System (DCS). The DCS derives these signals based on current CEA positions as indicated by the CEDMCS supplied CEA up-down pulses. The shutdown CEAs are moved in the manual control mode only, with either individual or group movement. A selector switch permits withdrawal of no more than one shutdown group at any time.

During plant startup and shutdown, and all cases where power is below 15 percent, manual control is used. Automatic control of the regulating CEAs by the RRS may be selected by the operator only when above the RRS low power automatic motion prohibit interlock setpoint of approximately 15 percent power. Manual control may be used to override automatic control at any time.

The CEDMCS prohibits the withdrawal of regulating CEAs unless all shutdown CEAs are at their respective upper electrical limits. This interlock however, can be bypassed. An interlock bypass is provided, which enables the withdrawal of the Regulating Group of CEAs if any of the shutdown group rods are not at their upper electrical limit. This bypass is accomplished by a pushbutton. Further, insertion of shutdown CEAs is prohibited unless all regulating CEAs are at their lower electrical limits.

7.7.1.1.2 Reactor Coolant Pressure Control System

The Reactor Coolant Pressure Control System maintains system pressure within specified limits by the use of pressurizer heaters and spray valves. The control and alarm setpoints are shown on Figure 5.4-12. The system interconnection wiring diagram is provided by reference in Section 1.7 (see Table 1.7-2).

During normal steady state power operation, a small group of heaters (300 KW) is proportionally controlled to maintain operating pressure. If the pressure falls below the proportional band, all of the heaters are energized. Above the normal operating pressure range, the spray valves are proportionally opened to increase the spray flow rate as pressure rises. A small, continuous spray flow is maintained through the spray lines at all times to keep the lines warm and thereby reduce thermal shock when the control valves open, and to ensure that the boric acid concentration in the reactor coolant loops and pressurizer is in equilibrium.

7.7.1.1.3 Pressurizer Level Control System

The Pressurizer Level Control System minimizes changes in Reactor Coolant System water inventory by the use of charging pumps and letdown control valves in the Chemical and Volume Control System described in Subsection 9.3.4.

During normal steady state power operation, the pressurizer water level is calculated as a function of T_{AVG}. The control and alarm setpoints are shown on Figure 5.4-11. The level controller compares the measured and programmed water level signals and generates a proportional signal for regulating the letdown control valves. In addition, the level controller functions to start or stop an additional charging pump at low or high level setpoints. The system interconnection wiring diagram is provided by reference in Section 1.7 (see Table 1.7-2).

Two channels of control are provided and the controlling channel is selected by a switch on the control board. Automatic control is normally used during operation but manual control may be utilized at any time.

Both channels provide pressurizer water level signals for two additional functions:

a. A low water level signal from either channel de-energizes all heaters;

b. A high water level signal from the controlling channel energizes the backup heaters.

7.7.1.1.4 Feedwater Regulating System

The Feedwater Regulating System which is a subsystem of the Distributed Control System (DCS) maintains steam generator water level within acceptable limits by positioning the main feedwater regulating valves (FCV-9011 and 9021) which control the feedwater to each steam generator. These valves have a backup air supply to assure their proper operation and are designed to fail as-is upon low instrument air pressure. These valves have the capability for local manual operation and this can be accomplished by pinning the valve stem to the manual jacking mechanism. Local manual operation is controlled by plant operating procedures. The functional block diagram of the system is shown on Figure 7.7-5.

The two steam generators are operated in parallel. Each Feedwater Regulating System uses a three-element control system with inputs of feedwater flow, steam flow and steam generator water level for automatic water level control above 15 to 20 percent power. The output of DCS provides a signal to position the respective feedwater regulating valve.

When an abnormally high steam generator water level is sensed in either steam generator, a signal is sent to close the associated feedwater regulating valve. This signal can be removed by use of a manual override. (see Steam Generator Overfill discussion on next page.)

In the event of a reactor or turbine trip, the feedwater regulating valves are closed and feedwater control is transferred to the Low Power Feedwater Control System which is a subsystem of the DCS that controls steam generator level via the bypass valves (LCV 9005 and 9006). In order to reduce the frequency of reactor trips encountered during start-up due to the thermal shrink and swell characteristics of the steam generator, the Low Power Feedwater Control System (LPFCS) has been designed to provide automatic control of the feedwater by-pass valves and maintain steam generator level at setpoint value during unit start-up in the range of approximately 2 to 25% load. This provides the flow required for decay heat removal at

normal reactor coolant operating temperatures and allows the operator sufficient time before manual control of level is required.

The LPFCS monitors conditions in both the primary and secondary loops of the NSSS for control of feedwater flow into each steam generator. The LPFCS averages steam generator level signals, LT-9005 and LT-9011 for SG 2A and LT-9006 and LT-9021 for SG 2B, to maintain the level setpoint.

The LPFCS also utilizes a feedforward signal based on wide range steam generator water level deviation from its zero power value. This difference generates a reference feedwater flow demand that is proportional to changes in steam flow. The LPFCS uses feedwater temperature downstream of the high pressure heaters to compensate for the effect of feedwater temperature on the steam generator level characteristics.

Manual control of the Feedwater Regulating System may be selected at any power level. When in manual control, the operator in the control room can:

a. Position each feedwater regulating control valve (FCV-9011, FCV-9021)

b. Open or close each feedwater stop valve

c. Position each feedwater control bypass regulating valve (LCV-9005, LCV-9006)

d. Control operation of feedwater pumps

The DCS was expanded to include the feedwater regulating system and the Low Power Feedwater Control System. A more detailed discussion of the DCS can be found in Subsection 7.5.1.4a. To integrate the feedwater regulating and the low power feedwater subsystems into the DCS, equipment in addition to the equipment discussed in Subsection 7.5.1.4a was installed. Two touch screen Manual/Auto stations (FIC-9011/LIC-9005 and FIC-9021/LIC-9006) are used to control the valves, while two flat panel displays provide indication, alarms and control capabilities. This equipment is located on RTGB-202.

The operator can at any time control operation of two electrically driven auxiliary feedwater pumps and/or the turbine driven auxiliary feedwater pump described in Subsection 10.4.9 and position the associated auxiliary feedwater regulating valves. Remote manual control of auxiliary feedwater is provided in the control room and outside of the control room. Automatic auxiliary feedwater control is described in Sections 7.3 and 7.4.

<u>Steam Generator Overfill Protection Features: (Generic Letter 89-19)</u>

A review of the feedwater control system was performed in conjunction with Generic Letter 89-19, "Resolution of Unresolved Safety Issue A-47 (Safety Implication of Control Systems in LWR Nuclear Power Plants)." This generic letter required, in part, that all CE plants provide automatic steam generator overfill protection and that these features be sufficiently separate of the existing feedwater control system to mitigate main feedwater (MFW) overfill events. The desired degree of separation was such that it would not be powered from the same power source, not located in the same cabinet, and not routed so that a fire may affect both systems. Periodic testing of these added features, to verify functionality, was also required. (References: Engineering Evaluation JPN-PSL-SEIJ-90-007 and NRC SER, "Steam Generator Overfill Protection Response to Generic Letter 89-19," dated 4/4/94.)

The Steam Generator Overfill Protection features utilize the same safety grade steam generator level transmitters signals that provide input to the Reactor Protection System. High and High- High level trip settings provide logic outputs, which are isolated before passing to the non-class 1E Steam Generator Overfill Protection logic. Feedwater isolation functions are then performed under a 2-out-of-4 coincidence. Diverse and redundant equipment is actuated by these High and High-High signals. First, after the initiating event, high level protection closes the respective steam generator feedwater control valve(s) through the feedwater regulation system, as shown on Figure 7.7-5. Second, if the high level protection should fail, a High-High level protection will trip the turbine, stop the main feedwater pumps and close the main feedwater pump discharge valves. Separate sources of power are provided for the feedwater control system and High-High Steam Generator Overfill Protection circuits to insure availability of one of these systems should an overfill event occur. Furthermore, the design of the feedwater control system requires the feedwater regulating valve to fail closed on a loss of power such that even in the unlikely event of a total power failure to both systems, feedwater flow will still be isolated for the affected train.

Plant procedures are provided to periodically verify operability of Steam Generator Overfill Protection features during power operation and to functionally test the system during refueling.

7.7.1.1.5 Steam Dump and Bypass Control System

The Steam Dump and Bypass Control System is a subsystem of the DCS, is described in Subsection 10.4.4 and is designed to provide a means of manually controlling reactor coolant temperature during plant startup and for removing NSSS stored energy, decay heat, and pump energy during shutdown cooling. The original system design flow capacity of 45% was restored as part of the Extended Power Uprate. The system is designed to mitigate challenges to the pressurizer and steam generator safety valves during large load rejections.

The system is composed of five valves, with a combined capacity of greater than 45%, two reactor turbine generator (RTGB) board mounted manual-automatic controllers, and one flat panel display.

The system input variables of main steam header pressure, steam flow, reactor coolant average temperature, turbine load demand, and reactor trip enter into the computation in order to produce individual valve modulation signals or, if conditions warrant, individual "quick-opening" signals to the dump valves. Initiation of a steam dump action initiates an interlock in the CEDMCS which prevents automatic CEA withdrawal thereby ensuring timely termination of the transient.

7.7.1.1.6 Analog Display System (ADS)

The neutron flux and distribution is controlled, in part, through insertion and/or withdrawal of CEAs. The Analog Display System (Figure 7.7-6) utilizes the signals from the reed switch position transmitters to display the CEA positions on a display for the operator (refer to Subsection 7.5.1.4). Reactor power signals, derived from the Reactor Protection System through isolation in accordance with IEEE 279-1971 are utilized with the CEA position signals in the ADS to provide alarm and motion inhibit signals for specific improper CEA movements.

The ADS contains logic which detects certain abnormal CEA configurations such as: CEA deviation within a control group; CEA inserted to or below the power dependent insertion limit; improper CEA group sequencing or overlap; regulating CEA groups withdrawing before all

shutdown CEAs are fully withdrawn and shutdown CEA groups inserting before all regulating CEAs are fully inserted. Upon detection, the ADS initiates CEA motion inhibit (CMI) signals to the CEDMCS and alarm signals to the annunciation system display. The CMI signals are generated to prevent the specific improper CEA movement from continuing.

7.7.1.1.7 Boron Control System

The RCS boron control is accomplished by dilution and boration. Refer to Subsection 9.3.4 for a discussion of the Chemical and Volume Control System. To allow the operator to maintain the required boron concentration in the reactor coolant, the volume control tank contents are maintained at a prescribed boron concentration either manually or automatically. To assist the operator in maintaining the proper boric acid concentration in the Reactor Coolant System, recorders indicate reactor makeup water flow and boric acid makeup flow, which can be used to determine whether boration or dilution is occurring.

Sampling of the reactor coolant is used to determine boron concentration.

At a given power level, the boron concentration and CEA position determines reactor coolant temperature. Because of the long time required to change the boron concentration, boron is used to compensate for slow change of power. By adjusting the boron concentration, the CEAs can be withdrawn to provide an adequate shutdown margin.

7.7.1.1.8 Incore Instrumentation System

The Incore Instrumentation System monitors neutron flux distribution within the reactor core.

There are maximum of 56 incore instrument assemblies with four self powered rhodium detectors in each assembly. The assemblies are uniformally distributed in the reactor core. The four detectors in each assembly are axially distributed along the height of the core at 20, 40, 60 and 80 percent of core height. This permits representative three dimensional mapping of the neutron flux in the core. The rhodium detectors produce a delayed beta current proportional to the neutron flux in the detector region.

The current signal from each detector is individually converted to a proportional flux level and logged by the Distributed Control System (DCS). The DCS also compares each of these neutron flux levels with alarm setpoints indicative of high neutron flux conditions and prints a message when each of these conditions occurs.

In addition to the fixed system described above, the original design included a Movable Incore Detector System (MICDS) as a backup to the fixed system, which has subsequently been deleted. The MICDS consisted of two movable detectors and associated hardware to position either probe at any location within a dry calibration tube of the 56 fixed incore instrument assemblies. The MICDS was controlled by the DCS and provided a neutron flux map independent of the fixed detector system.

The incore instrumentation system is designed to perform the following functions:

a. To provide data sufficient to determine the gross power distribution in the core during different operating conditions from 20 percent to 100 percent power;

b. To provide data to estimate fuel burn up in each fuel assembly; and

c. To provide data for the evaluation of thermal margins in the core.

The incore detectors can be used to assist in the calibration of the excore detectors by providing azimuthal and axial power distribution information.

The fixed incore detectors will be used to periodically calibrate the excore axial flux offset detection system, monitor the azimuthal power tilt, calibrate the power level neutron flux channels and monitor the linear heat rate. The incore instrumentation system, when used to perform the functions listed above must consist of the operability requirements outlined in Section 13.7. These requirements were amended in the facility technical specifications, Amendment 75, and relocated to the UFSAR.

7.7.1.1.9 Startup and Control Excore Neutron Flux Monitoring System

The Startup and Control Excore Neutron Flux Monitoring System includes neutron detectors located around the reactor core and signal conditioning equipment located in the control room.

Two startup channels provide source level neutron flux information to the reactor operator for use during extended shutdown periods, initial reactor startup and startups after extended periods of reactor shutdown, such as core refueling operations. Each channel consists of one BF_3 detector, a preamplifier, a signal processing drawer containing power supplies, a logarithmic amplifier and test circuitry located in the control room. High voltage power to the proportional counters is automatically terminated on the increase in nuclear power, above 10,000 cps, to extend the detector's life. Annunciation is provided if this automatic feature fails to operate. High voltage from the startup detectors can be removed manually by the operators. These startup channels provide readout and audio count rate information, but have no direct control or protective functions.

Two control channels provide neutron flux information, in the power operating range of 1 percent to 200 percent, to the Reactor Regulating System for use during automatic turbine load - following operation (see Subsection 7.7.1). Each control channel consists of a dual section uncompensated ionization chamber detector and a signal conditioning drawer containing power supplies, a linear amplifier, and test circuitry.

The detector is operated in current mode only. These channels are completely independent of the safety channels.

7.7.1.1.10 Turbine Control System

The Turbine Control System has automatic control and trip devices necessary for operation and protection of the turbine-generator. Means are also provided for the operator to override some of the automatic controls when he finds it necessary. An automatic trip is provided to prevent any damage to the turbine-generator. The unit trips upon occurrence of conditions which are potentially hazardous to the turbine-generator or to other associated plant equipment.

7.7.1.1.10.1 System Design

The Turbine Control System is a digital electronic hydraulic (DEH) system which controls the turbine automatically using a process control computer, servo-mechanism and hydraulic valve actuators. The computer represents the digital portion of the system, the servo-hardware

represents the electrical portion of the system and the valve actuators represent the hydraulic part of the system.

The Turbine Control System is designed to:

a. Control automatically the turbine-generator output power during all phases of normal operation.

b. Trip the turbine to guard the equipment from exposure to hazardous conditions.

c. Provide an automatic reactor trip signal when the turbine is tripped.

During automatic operation the DEH control system, digital computer output signals are received by the servo system which in turn positions the hydraulic valve actuators to control turbine speed or load.

7.7.1.1.10.2 Turbine Trip Signals

The following conditions cause a turbine trip:

a. Reactor trip

b. Turbine overspeed

c. Low condenser vacuum *

d. DELETED

e. Generator lockout relay

f. Exhaust hood high temperature (two out of three high temperature on either exhaust hood) *

g. Turbine low bearing oil pressure

h. Manual trip

i. DEH control power failure

j. Hi-hi water level in either steam generator

Any turbine trip causes the hydraulic trip fluid header pressure to decrease and close steam to the turbine. Four redundant pressure switches are also provided on emergency trip fluid line common header, to serve as the loss of load, turbine trip input to the Reactor Protective System logic matrices. Actuation of any two of the pressure switches on low hydraulic oil pressure causes a reactor trip. The pressure switches and circuitry are electrically and physically separated and serve an equipment protection function rather than a reactor safety function, as described in Section 7.2.

7.7.1.1.10.3 Turbine Runback

The turbine runback feature has been deleted.

---

*Bypassed at low power conditions

7.7.1.1.11 Boron Dilution Alarm System

Reactivity control in the reactor core is affected, in part, by soluble boron in the reactor coolant system. The Boron Dilution Alarm System (Figure 7.7-8a) utilizes the start-up channel nuclear instrumentation signals to detect a possible inadvertent boron dilution event while in Modes 3-6. There are two redundant and independent channels in the Boron Dilution Alarm System (BDAS) to ensure detection and alarming of the event.

The Boron Dilution Alarm System is an on-line microcomputer based system which receives and monitors two (2) neutron flux signals (one per BDAS channel) processed from the startup channel signal processing nuclear instrumentation.

The BDAS alarm logic is designed to follow the decreasing neutron flux signal after a reactor shutdown occurs, including when the neutron flux signal levels out at that core's configuration steady state level. A functional diagram is presented on Figure 7.7-8a. If the neutron flux signal increases, the current alarm setpoint is equal to the previous alarm setpoint before the neutron flux signal increased (see Figure 7.7-8b).

A Boron Dilution Event is detected when the current inputted neutron flux signal is equal to or greater than the alarm setpoint. Each BDAS channel initiates an alarm signal to the Plant Annunciation System upon detection of a Boron Dilution Event thus providing two separate alarm signals to the Plant Annunciation System upon determination of a boron dilution event.

The BDAS has the capability for the operator to input, from the panel, a reset signal to the system. This reset capability allows the BDAS alarm to be acknowledged and alarm detection to be reset to the current core configuration.

The BDAS is powered from an offsite power source with an onsite backup power source.

7.7.1.1.12 Distributed Control System (DCS)

The Distributed Control System (DCS) consists of operator and engineering workstations, displays, printers and racks for the control processors. The DCS is connected into the Plant Data Network (PDN) a system of network switches, fiber optic cables and other components that integrate the DCS functions. The functions of the DDPS were integrated into the DCS.

The DCS provides the following functions (previously performed by the DDPS):

- Calculation of Calorimetric Power - results are displayed on RTGB 204 and on a line printer on a periodic basis.

- Monitoring of Incore Detectors and Input to the Beacon Core Monitor - status of the incore detectors is monitored and displayed periodically. Alarms are provided should a detector exceed a preset operating range.

- CEA Position Indication and Limit Checking - positions of CEAs and CEA groups are calculated from demand pulses from the CEDMCS. Alarms are provided should limits be exceeded. Contact outputs are provided to CEDMCS to sequence CEA regulating group insertion and withdrawal.

- Power Dependent and Pre-Power Dependent Insertion Limits - regulating group CEA insertion limits based on thermal power are calculated on a set frequency. Early warning alarms are provided if these insertion limits are approached.

- Xenon and Iodine Concentration Calculations - reactivity worth is calculated on a set frequency for subsequent use to estimate reactor critical conditions during startup operations.

- The difference between the feedwater venturi indicated flow and the LEFM is calculated and alarmed if a preset limit is exceeded.

- Average Tcold temperature and reactor power are calculated and displayed on RTGB-204.

- Provides "All Rods In"/"All Rods Not In" input signal to ERDADS as required by Reg. Guide 1.97.

The DCS provides printed records, both periodic and on demand, of all monitored activities via two printers provided in the Unit 2 Control Room. Two operator work stations consisting of keyboards and touch screen flat panel displays are installed on the Operators Console to provide historical, trending or current status of the system inputs. A small flat panel display is installed on RTGB 204 to display Qpower and Tcold. An engineering workstation is provided in the Southeast corner of the Unit 2 Control Room. This workstation is used to make configuration changes to the DCS, change alarm setpoints, and modify displays. This location, inside the Control Room but outside the Operators Work Area, allows for Operations supervision of configuration changes without the need for the additional security measures and communications necessary to make such changes from a remote location.

The DCS is designed with expansion capabilities so that additional instrumentation and control systems can be added in the future, which will utilize the same graphical user interface, storage and printing capability. The system architecture, types and locations of components has incorporated to the extent practical, reliability, redundancy and diversity. The power supplies have been selected so that any panel, inverter, battery or AC power feed can be removed from service without impact to the PDN, assuming a coincident loss of offsite power.

The DCS will also provide an additional capability. Sequence of Events (SER) records are provided by monitoring the opening and closing of contacts for various pieces of equipment. These reports are utilized to reconstruct events following plant trips or other transients.

7.7.1.2 Design Comparison

The design differences between the control systems in the St. Lucie Unit 2 design scope and the control systems provided for the reference plant are discussed in this section.

7.7.1.2.1 Reactivity Control Systems

The RRS is functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

The CEDMCS combines the Control Element Drive System (CEDS) and the coil power programmers (CPP) into one integrated system thus reducing the interfacing required between

the previous two separate subsystems. The CEDMCS is functionally identical to the CEDS/CPP of St. Lucie Unit 1 with the following changes:

The CEAs are controlled in subgroups typically consisting of four CEAs located symmetrically about the core;

CEDM timing functions within the CEDMCS are performed using digital techniques to increase the accuracy and flexibility of the integrated system;

The CEA withdrawal prohibit (CWP) is effective in all modes, and CWP can be bypassed at the operator's module;

To bypass the CEA withdraw prohibit (CWP) signal, at the CEDMCS control panel the operator must:

a. Depress the bypass enable switch.

b. Depress and maintain the CWP bypass switch.

   Control room annunciation is provided to indicate a CWP condition. Feedback signals from the CEDMCS illuminate the bypass pushbuttons on the CEDMCS control panel to indicate operation of the override. The CWP bypass is maintained under strict administrative control via plant operating procedures.

While the CEDMCS is in the automatic sequential mode, motion of individual CEAs is not possible;

While in the automatic sequential mode, the CEA motion inhibit (CMI) cannot by bypassed.

The CEDMCS can handle up to 91 CEAs.

7.7.1.2.2 Reactor Coolant Pressure Control System

The reactor coolant pressure control system is functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

7.7.1.2.3 Pressurizer Level Control System

The Pressurizer Level Control System is functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

7.7.1.2.4 Feedwater Regulating System

The Feedwater Regulating System is functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

7.7.1.2.5 Steam Dump and Bypass Control System

The Steam Dump and Bypass Control System is functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

7.7.1.2.6 Analog Display System

The Analog Display System is functionally identical to the metrascope originally supplied for St. Lucie Unit 1 (NRC Docket 50-335). The metroscope was subsequently replaced with the CEA Position Display System (CEAPDS), which is similar to the Analog Display System.

7.7.1.2.7 Boron Control System

The boron control system is functionally identifical to that supplied for St. Lucie Unit 1 (Docket 50-335).

7.7.1.2.8 Incore Instrumentation

The Incore Instrumentation System is similar to that supplied for Arkansas Nuclear One-Unit 2 (NRC Docket 50-368). The difference being 44 detector assemblies vs 56 (maximum) on St. Lucie Unit 2.

7.7.1.2.9 Excore Neutron Flux Monitoring System

The startup and control channels of the Excore Neutron Flux Monitoring System are functionally identical to that supplied on System 80 (NRC Docket STN-50470F), except for the addition of subchannel deviation circuitry. The safety channels are of a new design, but based on System 80 circuitry.

7.7.1.2.10 Turbine Control System

The Turbine Control System is Functionally identical to that supplied for St. Lucie Unit 1 (NRC Docket 50-335).

7.7.1.2.11 Boron Dilution Alarm System

The Boron Dilution Alarm System is an addition to the St. Lucie Unit 2 design.

7.7.1.2.12 Distributed Control System (DCS)

The Distributed Control System (DCS) provides identical functions as those provided by the St. Lucie Unit 1 Distributed Control System (DCS).

7.7.2 ANALYSIS

The plant control systems and equipment are designed to provide high reliability during steady state operation and anticipated transient conditions. The RPS analysis of Subsection 7.2.2 encompasses the failure modes of these control systems and demonstrates that these systems are not required for safety. Separation of control and protection systems is maintained throughout.

The safety analyses of Chapter 15 do not require these systems to remain functional.

7.7.3 SYSTEM EVALUATION - HUMAN FACTORS ENGINEERING

7.7.3.1 HFE Program

In response to the requirement of NUREG-0737, Clarification item I.D.1, "Control Room Design Review,", and supplement 1 to NUREG-0737, FPL established and maintains a Human Factors Engineering program to review the design of the control room and remote shutdown capabilities in order to identify and correct design deficiencies. The design review was performed following the guidelines of NUREG-0700, "Guidelines for Control Room Design Review," and NUREG-0801, "Evaluation Criteria for Detail Control Room Design Review." The continuing Human Factors Engineering program provides for a review of plant changes associated with the Control Room or the Remote Shutdown Facilities to ensure compliance with the guidance provided in NUREG-0700.

7.7.3.2 Detail Control Room Design Review Implementation

A summary report which outlined the activities performed for the implementation of the Detailed Control Room Design Review was issued on November 1, 1983. This report was prepared following the outline recommended in Section 5.2 of NUREG-0700. This report discusses:

a. The Detailed Control Room Design Review phases.

b. The technical activities.

c. Method of assessment of discrepancies.

d. Method of identification and selection of enhancement and design solutions.

e. Review results of Human Engineering Discrepancies, Human Engineering DiscrepancyAssessment, and the selected enhancement and design solutions.

f. Improvements to be made.

g. Schedule of implementation.

An overview of the major activities and methods utilized in the Detail Control Room Design Review (DCRDR) is presented below:

<u>Technical Approach</u>

The technical approach utilized in the DCRDR included those activities listed below. A detailed discussion of the methodologies and a discussion of the finding, of each of the surveys is included in Section 2. 0 of the DCRDR report.

- Review of operating experience
- Assembly of control room documentation
- Review of system functions and task analysis
- Surveys

  - noise

- lighting
- control room environment
- design conventions
- controls and displays
- computers
- emergency garments
- labeling
- annunciators
- anthropometrics
- force/torque
- communications
- maintainability

- Verification of task performance capability
- Validation of control room functions
- Assessment of discrepancies.

Each survey report addresses:

- Task Objectives - The type of data to be collected or human performance variables under analysis.
- Review Team - The personnel required to conduct the task.
- Criteria - Generally, the review guidelines appropriate to the evaluation being conducted.
- Task Definition - Steps or procedures followed in the conduct of the task.
- Outputs and Results - Task results. These are Human Engineering Discrepancies which may be drawn upon by subsequent tasks (e.g., Task Analysis).

Assessment

The surveys identified Human Engineering Discrepancies (HEDs). These HEDs were assessed for error inducing potential and the system consequences of the potential error. The means of resolving the HEDs were also reviewed.

The basic assessment process was divided into four steps as follows:

- Assess extent of deviation from NUREG-0700 guidelines
- Assess Human Engineering Discrepancy impact on error occurrence
- Assess potential consequences of error occurrence
- Assign Human Engineering Discrepancy scheduling priority.

Based on the assessment of the HEDs probability of inducing errors, a priority for correction was assigned. The HED priority was utilized in the establishment of a backlit schedule.

Implementation

The backlit schedule program for the correction of the HEDs was established based on the following functions:

- Human engineering discrepancy priority
- Engineering and procurement lead time requirements and constraints
- Overall plant outage schedules.

The following design solutions and/or enhancements selected for the correction of the HEDs were based on the recommendations of NUREG-0700:

- Analysis of correction by enhancement
- Analysis of correction by design alternatives
- Assess extent of correction.

As part of the correction of HEDs several backlit activities, plant change modifications, were implemented. The objectives of these activities were to reduce the potential for human errors and correct identified HEDs. Examples of these activities are: RTGB Demarcation Update which has provided enhanced demarcation and labeling for the RTG Boards; MSIV Test Panel Upgrade which split controls from the local test panel and the control panel to prevent erroneous information in the control room during testing; modification and upgrade of software for QSPD System providing enhanced display and a "user-friendly" environment; correction of Nuisance Alarms Program which eliminated nuisance alarms, provided logic enhancements, corrected setpoints and deleted non-applicable alarms; Remote Reactor Vessel Level Indicator Modification which has added instrumentation in the control room to provide true level indication during reactor refueling; replacement of Metrascope to provide high resolution and enhanced

software for indication of rod position; modifications to the circuitry of motor operated valves to provide enhanced annunciation in the control room during testing.

Operating procedures have been reviewed and changed to a new format that will reduce the potential for human error. In the new format, procedures are required to be written to the entry-level person, and have less print per page, one action per step, and cautions and warnings before, rather than after the applicable steps. A review also has been made of maintenance procedures, health physics, and chemistry procedures, etc, with the intention of making them "user-friendly".

Other examples of plant change modifications which reduce the potential of human errors include the modifications in Control Room equipment to upgrade the Emergency Response Data Acquisition and Display Systems (ERDADS), which is also known as the Safety Assessment System (SAS) and includes Safety Parameter Display System (SPDS) equipment. These modifications improve the performance and display capabilities of the existing system and include installation of new display, keyboards and a trackball.

A Human Factors Engineering evaluation of the ERDADS has been performed on the SPDS and non-SPDS portions. The SPDS portion consisted of a Human Factors Engineering Review and a SPDS verification. The Human Factors Engineering review involved the evaluation of SPDS displays, hardware, design and layout in accordance with the guidelines specified in Section 5 & 6 of NUREG-0800, Section 18.2, Appendix A, NRC Standard Review Plan and applicable guidelines specified in Section 5 and 6 of NUREG-0700, "Guidelines for Control Room Design Review." The SPDS review was performed using survey and table-top evaluation methods to obtain information regarding job compatibility, understandability, usability, and completeness. A table top evaluation was performed in conjunction with the SPDS survey on the SPDS portion of ERDADS. The results of the survey and table-top evaluation were analyzed to identify Human Engineering Discrepancies (HEDs). The SPDS Parameter Selection Verification consisted of comparing SPDS parameter displays against the design bases requirements and Emergency Operating Procedures (EOPs) for safety status. SPDS displayed alarms were also compared against current EOPs and SPDS design documents, and minimum displayed parameters were reviewed to determine their consistency with operators' needs.

The non-SPDS portion of the ERDADS HFE review consisted of the evaluation of the St. Lucie Unit 1 Critical Safety Function Monitoring (CSFM) displays, hardware evaluation, design, layout, and man-machine interface in accordance with the guidelines specified in NUREG-0700, "Guidelines for Control Room Design Review." The non-SPDS review was performed by a survey evaluation method. The results of the survey were analyzed and all HEDs were resolved.

7.7.3.3 DCRDR Implementation Evaluation

The St. Lucie Detailed Control Room Design Review (DCRDR) Program Plan was submitted to the NRC on June 30, 1983. The program plan utilized Supplement 1 to NUREG-0737, NUREG-0700, and NUREG-0801 as the bases for the program development. The St. Lucie Unit 1 DCRDR Summary Report was then submitted on November 1, 1983.

The NRC reviewed these reports and provided FPL with a draft Safety Evaluation and Technical Report of the St. Lucie DCRDR on February 2, 1984. This report indicated that a pre-implementation audit would be necessary to resolve the open or confirmatory items identified in the Safety Evaluation. The NRC then conducted the pre-implementation audit of the DCRDR program on April 2 through 6, 1984. The results of the NRC audit identified the

resolved items and those items requiring additional information. The NRC stated that a meeting would be appropriate to discuss FPL plans, methods, and schedules for submittal of a supplement to the St. Lucie DCRDR Summary Report.

FPL reviewed the requirements of NUREG-0737, Supplement 1 and the operating experience review problems identified. Programs were established to review and resolve the open or confirmatory items. The Supplemental Summary Report, issued on April 1, 1986 describes the review process. The ten items contained in the supplementary summary report are listed below:

1. Operating Experience Review Problems.
2. LER Review.
3. Task Analysis.
4. HFE Review of Post Control Room Changes.
5. Additional HED Justification.
6. Reverification of Control Room Changes.
7. Reverification of Control Room Changes to Ensure No New HEDS.
8. Future Control Room Changes.
9. Supplemental Summary Report.
10. Integration Into Other Programs.

The methodology utilized in the review and resolution of the open or confirmatory items is contained in the DCRDR Supplemental Summary Report.

All retrofit packages for St. Lucie Unit 2 are being implemented per the FPL quality program for Human Factors Engineering. This program ensures that all aspects of design are in compliance with the guidance provided in NUREG-0700 and that Human Factors engineering principles are followed for plant changes associated with the Control Room or the Remote Shutdown Facilities.

7.7.4 LEADING EDGE FLOW METER (LEFM)

The PSL Unit 2 Extended Power Uprate (EPU) raised the licensed maximum power level to 3020 MWt. The EPU change to the maximum rated thermal power (RTP) included a 1.7% Measurement Uncertainty Recapture (MUR). Modifications required for the MUR portion of the EPU included installation of the Cameron Leading Edge Flow Meter (LEFM) CheckPlus system. The use of LEFM for determination of feedwater temperature and feedwater mass flow, results in an overall calorimetric uncertainty of 0.3%. The MUR uprate of 1.7% results from the difference between the original 2% power determination uncertainty (required by 10CFR50 Appendix K) and the LEFM based calorimetric uncertainty of 0.3%. The MUR portion of the EPU license amendment request was based on the following Cameron Topical Reports:

1. ER-80P, Improving Thermal Power Accuracy and Plant Safety While Increasing Operating Power Level Using the LEFM Check System, dated March 1997 (NRC SER dated March 8, 1999)

2. ER-160P, Supplement to Topical Report ER-80P: Basis for a Power Uprate with the LEFM Check System, dated May 2000 (NRC SER, dated January 19, 2001)

3. ER-157P, Supplement to Topical Report ER-80P: Basis for a Power Uprate with the LEFM Check or CheckPlus System, dated October 2001 (NRC SER, dated December 20, 2001)

The LEFM feedwater flow measurement system is an ultrasonic 8-path transit time flowmeter. The LEFM CheckPlus system consists of one flow element (spool piece) installed in each of the two FW flow headers. Each individual LEFM CheckPlus system flow element (spool piece) has been calibrated in a site-specific model test at Alden Research Laboratories with traceability to National Standards. The LEFM flow elements (meters) are installed at specified locations upstream from the existing FW venturi nozzles. The resulting piping configurations were explicitly modeled as part of the LEFM meter factor and accuracy assessment testing performed at Alden Research Laboratories. Test data and results for the flow elements are documented in Cameron Engineering Report ER-736, Meter Factor Calculation and Accuracy Assessment for St. Lucie Unit 2. The calibration factor (also known as the meter factor) and the uncertainty in the calibration factor for the LEFM CheckPlus system are also based on this Cameron engineering report.

The LEFM CheckPlus system is used for continuous calorimetric power determination by providing FW mass flow and FW temperature input data to the distributed control system (DCS), which is the computer system used for automated performance of the calorimetric power calculations. The LEFM system communicates with the DCS via redundant digital communication links. The LEFM based mass flow rate and FW temperature data is integrated into appropriate DCS calorimetric display screens to facilitate side-by-side comparison with data based on conventional instruments. Hard-wired alarms from LEFM to main control room annunciator panels provide redundant operator notification of degraded system performance or outright system failure. The LEFM CheckPlus system incorporates self-verification features to ensure that hydraulic profile and signal processing requirements are met within the site-specific design basis uncertainty analysis contained in Cameron Report ER-740, Bounding Uncertainty Analysis for Thermal Power Determination at St. Lucie Units 1 & 2 using the LEFM CheckPlus System. Critical performance parameters are continually monitored for every individual meter path and alarm setpoints are established to ensure corresponding assumptions in the uncertainty analysis remain bounding.

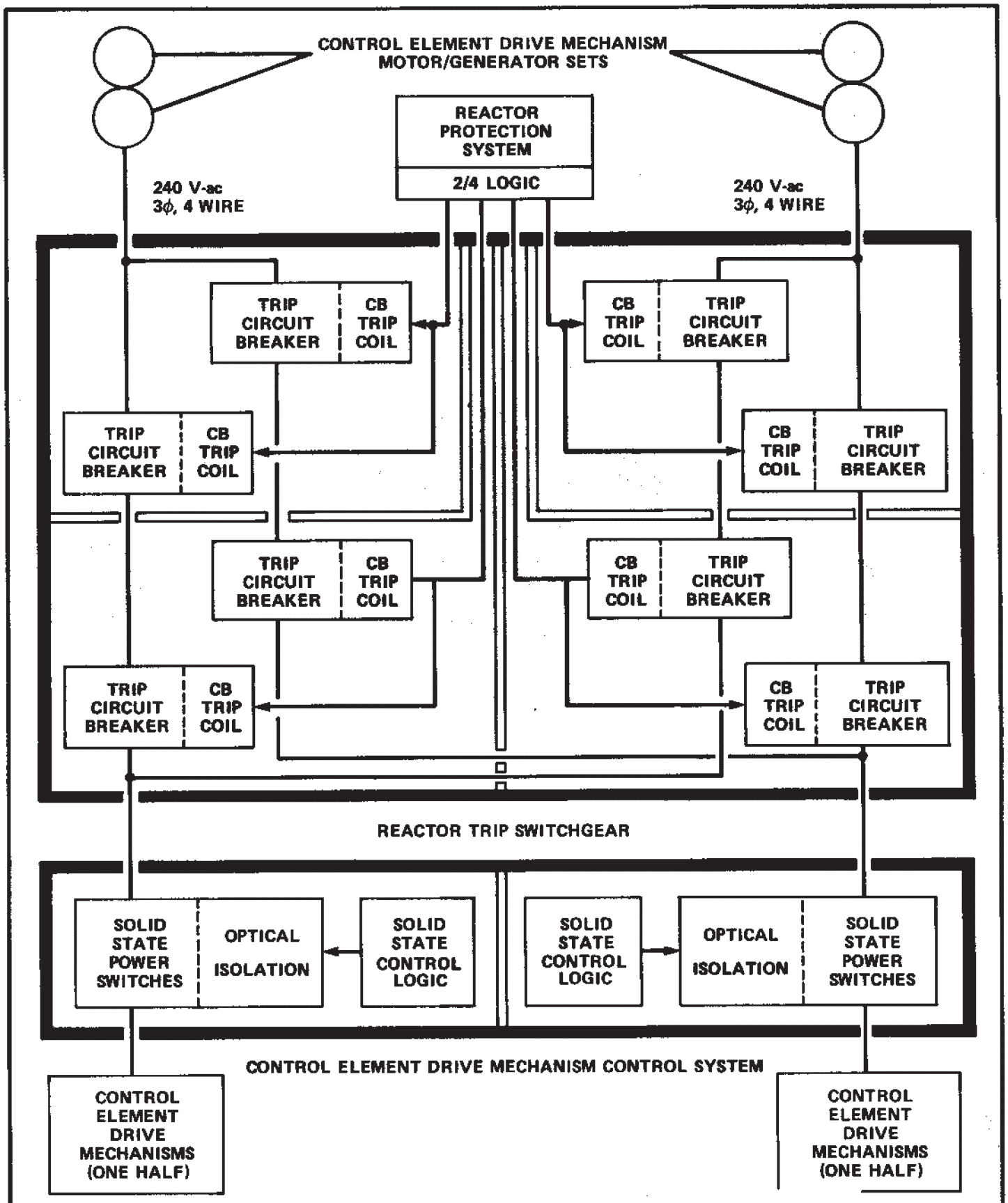
Operability of the LEFM instrumentation is required to support an overall calorimetric uncertainty of 0.3%. Operability requirements and associated action statements are identified in UFSAR Section 13.7. Various LEFM system failure modes and resulting action statements are considered based on the use of independent LEFM instrumentation for feedwater headers A & B, and also based on redundancy within each LEFM sub-system. Original feedwater flow (Venturis) and temperature (RTD) instrumentation were retained and are used as backup calorimetric instrumentation if needed.

Refer to Dwg
2998-3054

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

REACTOR REGULATING SYSTEM
BLOCK DIAGRAM

FIGURE 7.7-1



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

CEDMCS – RPS INTERFACE
BLOCK DIAGRAM
FIGURE 7.7–2

THIS FIGURE DELETED

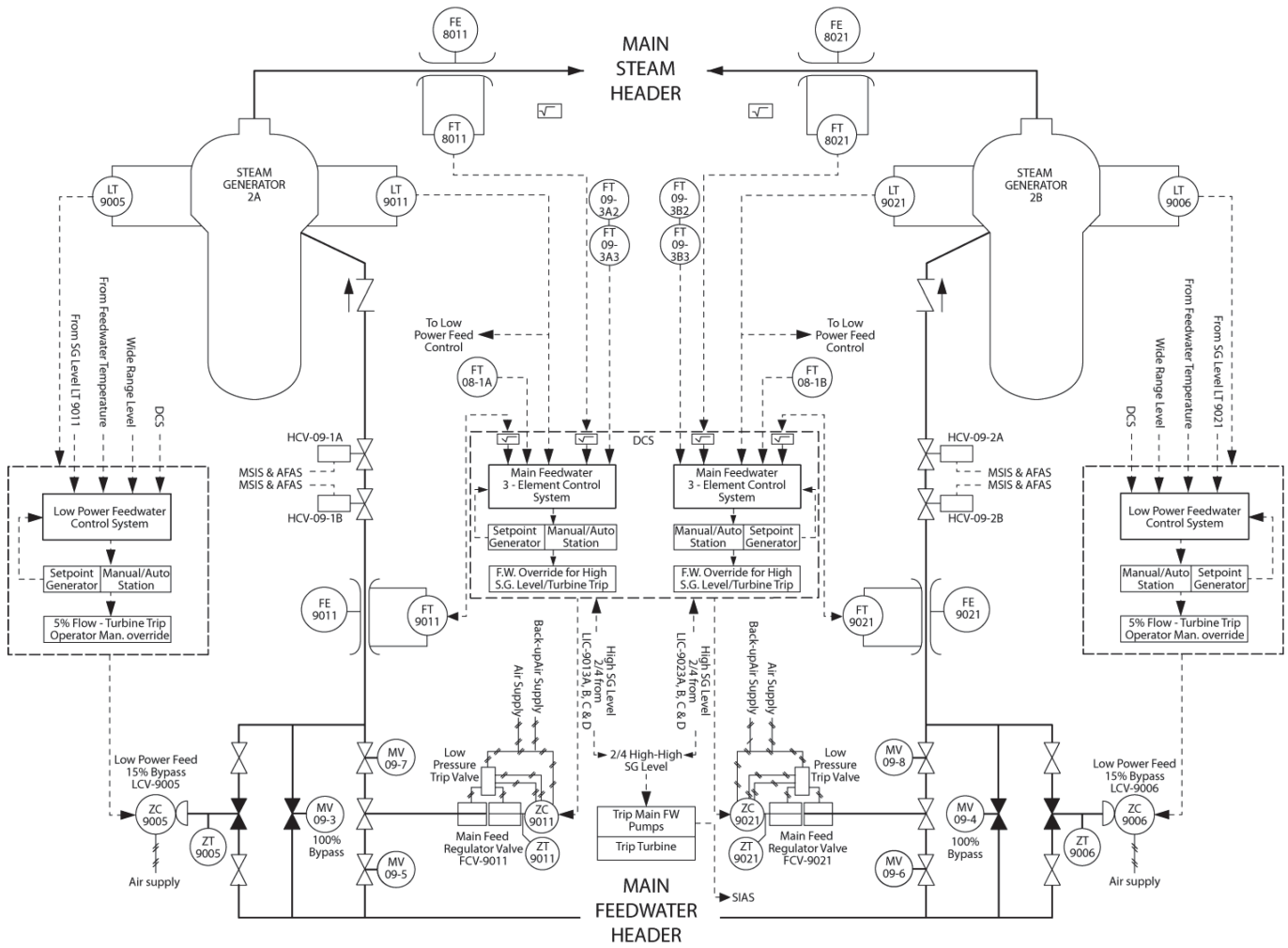
FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.7-3

THIS FIGURE DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

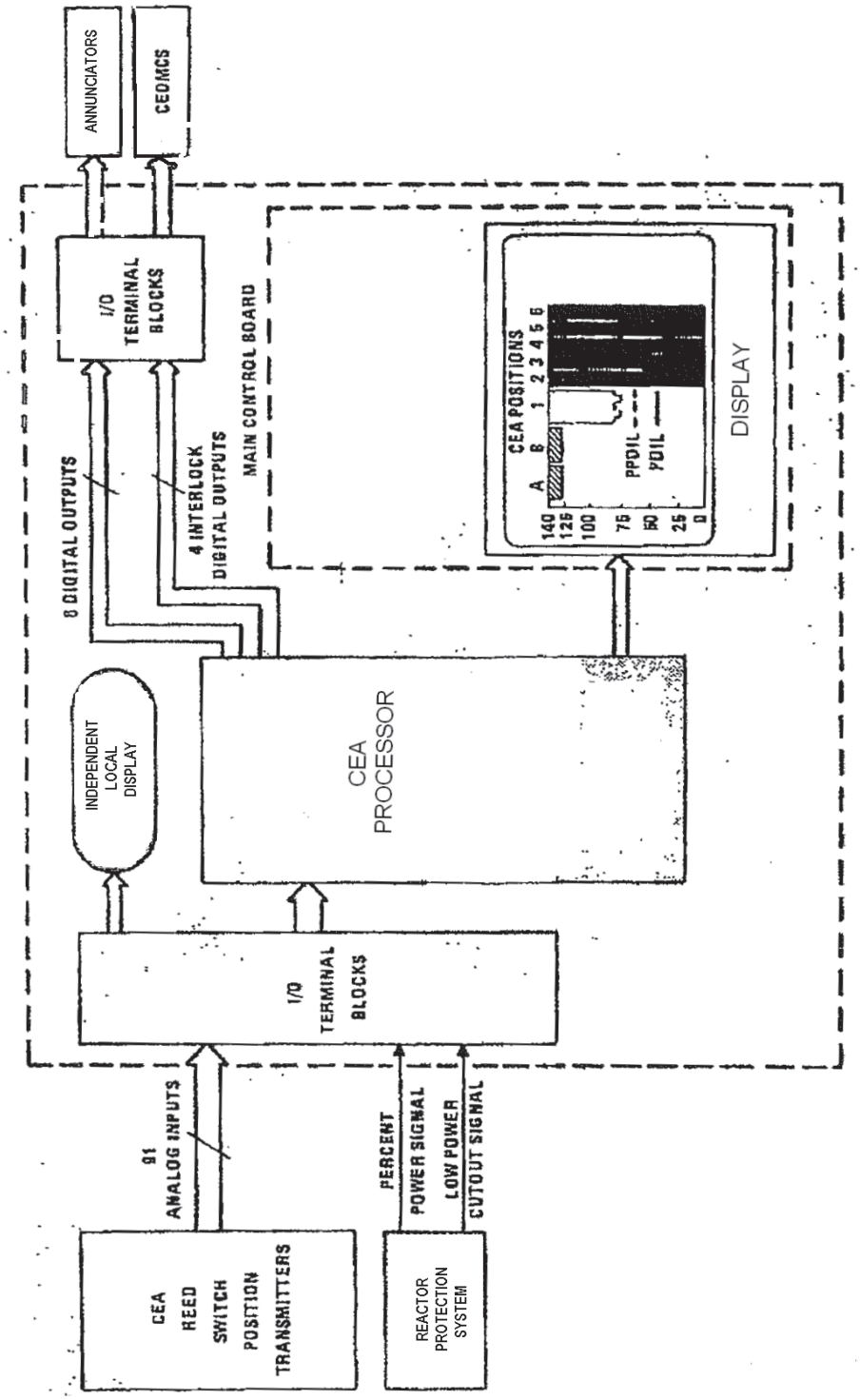
FIGURE 7.7-4



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FEEDWATER CONTROL SYSTEM BLOCK DIAGRAM

FIGURE 7.7-5



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

ANALOG DISPLAY SYSTEM
SIMPLIFIED – BLOCK DIAGRAM

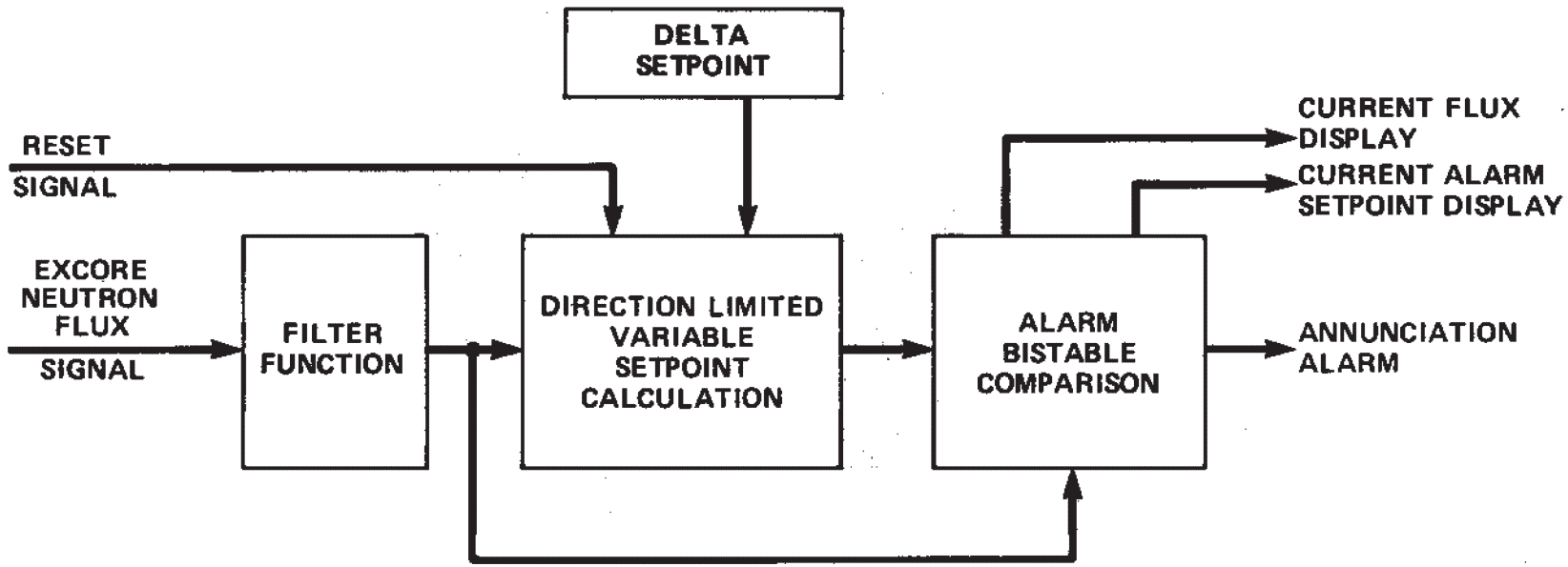
FIGURE 7.7-6

THIS FIGURE DELETED

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

FIGURE 7.7-7

FUNCTIONAL DIAGRAM

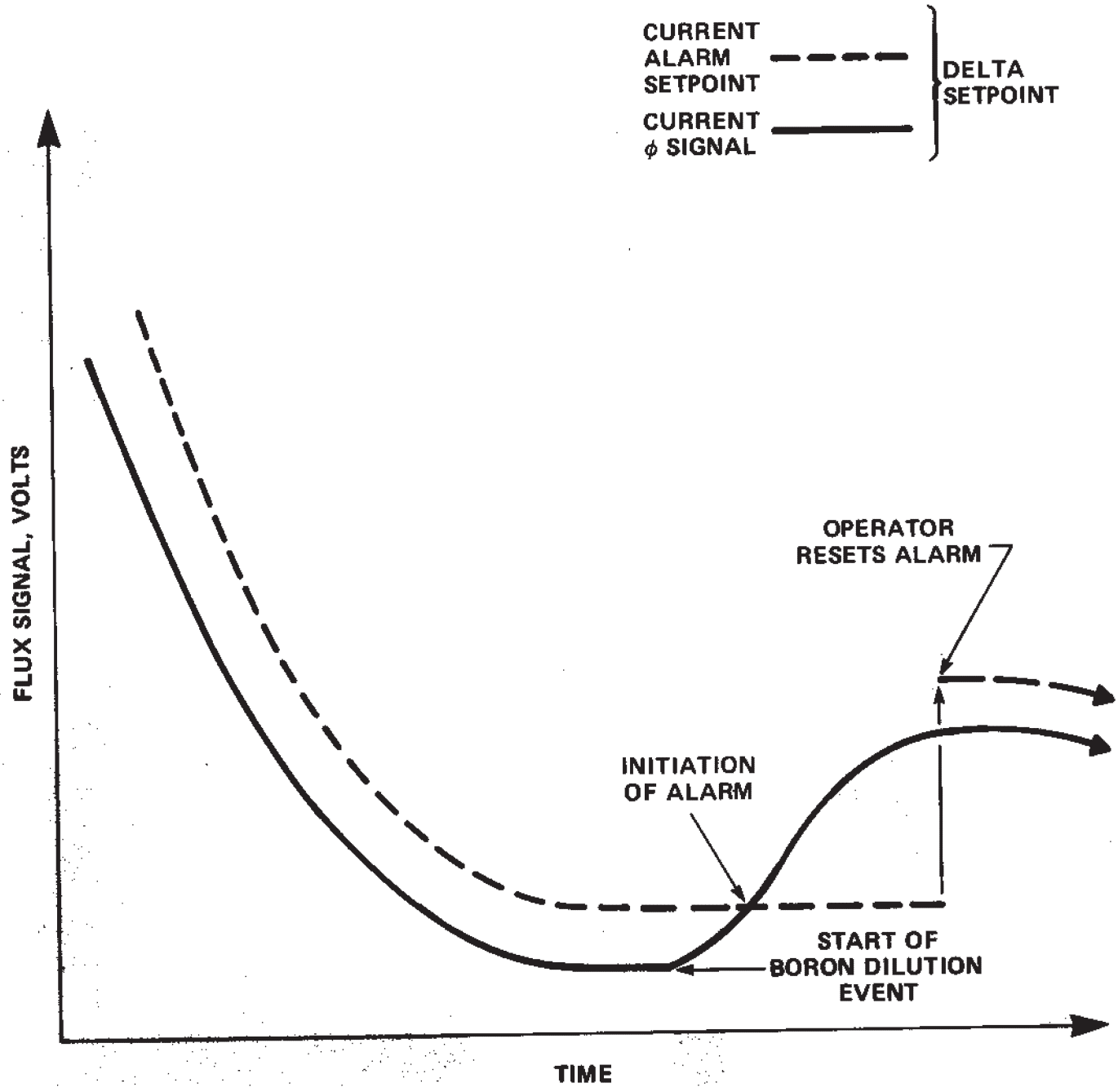


NOTE: ONLY ONE OF TWO IDENTICAL SYSTEMS IS SHOWN

FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BORON DILUTION ALARM SYSTEM
FUNCTIONAL DIAGRAM

FIGURE 7.7-8a



FLORIDA POWER & LIGHT COMPANY
ST. LUCIE PLANT UNIT 2

BORON DILUTION ALARM SYSTEM
NEUTRON FLUX AND SETPOINT

FIGURE 7.7-8b