7.0 INSTRUMENTATION AND CONTROLS
TABLE OF CONTENTS

7.0 INSTRUMENTATION AND CONTROLS
TABLE OF CONTENTS

7.0 INSTRUMENTATION AND CONTROLS
TABLE OF CONTENTS

7.0 INSTRUMENTATION AND CONTROLS
TABLE OF CONTENTS

7.0 INSTRUMENTATION AND CONTROLS
LIST OF TABLES

Table

7.0 INSTRUMENTATION AND CONTROLS
LIST OF FIGURES

Figure

7.0 INSTRUMENTATION AND CONTROLS
LIST OF FIGURES

Figure

DRAWINGS CITED IN THIS CHAPTER*

* The listed drawings are included as "General References" only; i.e., refer to the drawings to obtain additional detail or to obtain background information. These drawings are not part of the UFSAR. They are controlled by the Controlled Documents Program.

DRAWING*	SUBJECT
M-26	Diagram of Nuclear Boiler and Reactor Recirculation Piping Unit 2
M-34	Diagram of Control Rod Drive Hydraulic Piping Unit 2
M-357	Diagram of Nuclear Boiler and Reactor Recirculation Piping Unit 3
M-365	Diagram of Control Rod Drive Hydraulic Piping Unit 3

7.0 INSTRUMENTATION AND CONTROLS

This chapter presents various plant instrumentation and control systems including functions, design bases, system descriptions, design evaluations, and tests and inspections. The information provided in this chapter emphasizes instruments and associated equipment which constitute reactor protection and regulation systems. Particular attention is given to the instrumentation aspects of process systems, with the mechanical and nuclear design bases presented in the chapters or sections which address the respective process system. Chapter 7 includes a discussion of the instrumentation and controls for systems of major safety significance and those that provide reactor and turbine control. Discussions of instrumentation and controls for other systems are contained within the sections that address those systems.

7.1 INTRODUCTION

The equipment and evaluations presented in this chapter are applicable to either unit. Instrumentation and controls are provided to perform protective and regulating functions.

Protective systems, consisting of the reactor protective circuitry and the instrumentation and controls for engineered safety features (ESFs), normally perform the most important of the instrumentation and control safety functions.

The regulating instrumentation and controls provide the ability to regulate the unit from shutdown to full power and to monitor and maintain key unit variables, such as reactor power, flow, pressure, level, temperature, and radioactivity levels, within predetermined limits during both steady-state operation and normal unit transients.

The inputs to the protective and regulating controls are provided by a diversity of instruments. The following sections in this chapter provide descriptions of instrumentation and major components, evaluations of the instrumentation input adequacy, and analyses from both functional and reliability viewpoints.

Analytical Limits are those values assumed in calculations and evaluations, which show that plant operation is safe during postulated transients and accidents. These values are found in calculations of record and design/license basis evaluations.

Allowable Values are selected to be conservative to the Analytical Limits due to the effects on the instrumentation from the accident or transient conditions, which are not present during instrument calibration. Allowable Values are specified in the Technical Specifications and apply to the applicable instrument function.

Protective and regulating function trip setpoints are specified in setpoint calculations. The setpoints and their associated tolerances are selected to ensure that with a high degree of probability the setpoint does not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the setpoint, but within the Allowable Value is acceptable. An instrument CHANNEL is inoperable when its actual trip setpoint is not within its Allowable Value.

Some Technical Specifications delineate Allowable Values associated with Reactor Water Level. These Allowable Values are referenced to Instrument Zero. Instrument Zero is 503 inches above Vessel Zero, or 143 inches above Top of Active Fuel (TAF). Top of Active Fuel (TAF) is 360 inches above Vessel Zero.

7.1.1 Identification of Systems

Section 3.2 discusses the identification of safety-related instrumentation and control systems and equipment. The engineered safety features for Dresden are identified in Section 6.0.

7.1.1.1 Protective Systems

Protective systems include electrical and mechanical devices and circuitry required to initiate shutdown of the reactor and mitigate the consequences of accidents when required. These systems include:

A. The reactor protection system (RPS) which acts to trip the reactor when parameters exceed preset limits (RPS is described in Section 7.2);

B. The anticipated transient without scram (ATWS) system which trips the recirculation pumps and provides an alternate method to insert control rods in the unlikely event that the RPS fails to do so (ATWS mitigation is described in Section 7.8); and

C. ESF instrumentation and controls for emergency core cooling and containment isolation functions which are addressed in Section 7.3 (other ESF systems are discussed in Section 6.0):

   1. Emergency core cooling systems:

      a. Core spray,

      b. Low pressure coolant injection (LPCI),

      c. High pressure coolant injection (HPCI), and

      d. Automatic depressurization system (ADS).

   2. Containment isolation systems:

      a. Primary containment isolation system (PCIS) and

      b. Secondary containment isolation.

   3. Isolation condenser.

7.1.1.2 Safe Shutdown

Section 7.4 includes a discussion of the containment cooling mode of LPCI and reactor shutdown from outside the control room.

7.1.1.3 Display Instrumentation

Display instrumentation provides information used by the operator for normal operation and safe shutdown of the unit, including monitoring of post-accident conditions. Compliance with Regulatory Guide 1.97, the safety parameter display system (SPDS), and the process computer are discussed in Section 7.5. A summary of the detailed control room design review (DCRDR) is also provided in Section 7.5.

7.1.1.4 Core and Vessel Instrumentation

Section 7.6 describes additional instrumentation which provides both safety and nonsafety functions and which includes nuclear instrumentation and reactor vessel instrumentation.

7.1.1.5 Other Instrumentation

Reactor and turbine generator instrumentation and controls not essential to the safety of the plant are discussed in Section 7.7.

7.1.2 Identification of Safety Criteria

The design bases for the instrumentation and control systems include the safety criteria pertinent to each of the systems described. The design basis for each of the systems is presented in the section which discusses the system. The technical basis for the various protective functions is provided with the description of the protective system. A general discussion of Regulatory Guide compliance is provided in Section 1.8.

General Electric Company has reviewed the plant design to determine if the safety systems conform to IEEE 279-1968. IEEE 279-1968 was the proposed industry criteria for nuclear power plant protection systems, published August 1968. Specific compliance with IEEE 279-1968 is addressed with the system description.

7.1.2.1 Single-Failure Criteria

The compliance of the reactor protection and emergency core cooling systems with and the justification for all exceptions to IEEE 279-1968, Proposed Criteria for Nuclear Power Plant Protection Systems, are contained in NEDO-10139, "Compliance of Protection Systems to Industry Criteria: General Electric BWR Nuclear Steam Supply System." Compliance of the protection systems is presented in the sections providing the system details. These systems typically employ logic systems to accommodate single failures without jeopardizing functionality, such as one-out-of-two-twice.

7.1.2.2 Separation Requirements

The Dresden Plant Design predates the issuance of Regulatory Guide 1.75 and IEEE 384. Therefore, the original design does not fully conform to that guidance. However, as modifications are incorporated into the plant design, whenever practical, separation between 1E and non-1E loads will be provided in accordance with the current philosophy as stated in Regulatory Guide 1.75. One way to fulfill this requirement is to use two breakers in series between nonsafety loads and safety-related power supplies. When new systems are installed they are in accordance with current standards (e.g., IEEE 384) where practical. A discussion of Regulatory Guide 1.97 Category A variable separation is in Section 7.5. Additional description of separation requirements is contained in Section 8.3.1

7.1.2.3 Qualification

The qualification of instrumentation and controls is further described in Sections 3.10 and 3.11. Additional discussion of display instrumentation qualification for Regulatory Guide 1.97 Category 1 variables is in Section 7.5.

7.1.3 Other Control and Instrumentation

Controls and instrumentation for the following auxiliary and emergency systems are described in the sections that describe the systems:

	System	Section
A.	Reactor building heating, ventilation, and cooling system	9.4.5
B.	Reactor water cleanup system	5.4.8
C.	Fire protection system	9.5.1
D.	Service water system	9.2.2
E.	Demineralized water makeup system	9.2.4
F.	Service and instrument air systems	9.3.1
G.	Communications systems	9.5.2
H.	Spent fuel pool cooling and cleanup system	9.1.3
I.	Reactor shutdown cooling system	5.4.7
J.	Standby liquid control system	9.3.5
K.	Fuel handling system	9.1.4
L.	High radiation sampling system	9.3.2

7.2 REACTOR PROTECTION TRIP SYSTEM

This section describes the reactor protection system (RPS), provides the bases for all scram functions, and compares the design of the system with IEEE 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems." The first part of this section is a general system description. References to IEEE 279 criteria are indicated where appropriate. The applicable IEEE 279-1968 paragraphs have been noted where the discussion concerns this standard, although conformance was not required.

7.2.1 Design Bases

The reactor protection system is designed to:

A. Prevent, in conjunction with the containment and containment isolation system, the release of radioactive materials in excess of the limits of 10 CFR 100 or 10 CFR 50.67 as applicable as a consequence of any of the design basis accidents (Chapter 15);

B. Prevent fuel damage following any single equipment malfunction or single operator error;

C. Function independently of other plant controls and instrumentation; and

D. Function safely following any single component malfunction.

In order to meet its design requirements, the RPS, under various conditions, initiates a reactor scram.

7.2.2 System Description

The RPS in use on Dresden Units 2 and 3 is sometimes referred to as a dual logic system and has been utilized on previous General Electric reactor plants. The system is made up of two independent logic channels, each having two trip channels. Thus, the system has a total of four independent trip channels. Each trip channel has an input from at least one independent sensor monitoring each of the critical parameters.

7.2.2.1 System Logic

The complexity of the control and instrumentation systems necessitates the use of the definitions below. These definitions are most appropriate to safety-related systems. Figure 7.2-1 illustrates the use of the defined terms.

A. Trip system - A trip system is an interconnected arrangement of components making use of instrument channel outputs, trip logics, and trip actuators to accomplish a trip function when appropriate logic is satisfied.

B. Trip - A trip is the change of state of a bistable device from one state to another. A trip is generated by a trip channel, trip logic, or trip system, and represents recognition of an abnormal condition.

C. Trip channel - A trip channel is an arrangement of components required to originate a single signal. The channel includes the sensor and wiring up to the point where the trip signal is generated. A channel loses its identity where channel trip signals are combined.

D. Trip logic - A trip logic is an arrangement of components designed to recognize specific combinations of signals from trip channels. A trip logic generates a trip signal by actuating a trip actuator.

E. Trip actuator - A trip actuator is the mechanism that carries out the final action of a trip logic.

F. Trip actuator logic - A trip actuator logic is an arrangement of components designed to recognize specific combinations of signals from trip logics. This term is needed to clearly define portions of a complex trip system having more than one trip logic. Because trip actuators are the mechanism by which trip logics generate trip signals, the use of the term trip actuator logic is appropriate. When tripped, a trip actuator logic carries out the function of the trip system.

The reactor protection system is arranged as two separately powered trip systems. Each trip system has three trip logics, two of which are used to produce automatic trip signals. The remaining trip logic is used for a manual trip signal. Each of the two trip logics used for automatic trip signals receives input signals from at least one trip channel for each monitored variable.

The outputs of two trip channels are combined in a one-out-of-two logic; that is, an input signal on either or both of the independent trip channels produces a logic channel trip. The outputs of the remaining two trip channels are combined in another one-out-of-two logic, independent of the first logic channel. The outputs of the two logic channels are combined such that they must be in agreement to initiate a scram. This combination of logics is commonly known as one-out-of-two-twice logic. An off-limit signal, initiated by at least one of the independent sensors in one logic channel, must be confirmed by an off-limit signal in the other logic channel to initiate a scram.

During normal operation, all vital sensor and trip contacts are closed, and all sensor relays are energized. There are two scram pilot valves and two scram valves for each control rod, arranged functionally as shown in Figure 7.2-2. The pilot scram valve solenoids are energized, and instrument air pressure is applied to all scram valves. The backup scram valve solenoids are normally deenergized. Alternating current power is supplied to the system by two M-G sets. Direct current power is supplied from the battery chargers or the station batteries. Electrical power supplies are discussed in Section 8.3.

Figure 7.2-2 shows the relay and contact arrangements which make up single trip logic. When a trip point is reached in any of the monitored parameters, a contact opens to deenergize a relay which controls a contact in one of the two trip channels. The opening of a trip channel contact deenergizes a scram relay which opens a contact in the power supply to the pilot scram valve solenoids supplied by the affected logic channel. To this point, only one-half of the events required to produce a reactor scram have occurred. Unless the pilot scram valve solenoids supplied by the other logic channel are deenergized, instrument air pressure will continue to act on the scram valves through the piping arrangement shown on Figure 7.2-2. If a trip point is reached in any of the monitored parameters in the other logic channel, then instrument air pressure will be cut off from the scram valves for each control rod. The scram valves will be vented, allows them to open, and thereby initiating a scram of every control rod.

A reactor scram is initiated when one or both trip channels of both trip systems indicate that a critical parameter exceeds a predetermined limit or upon loss of power to at least one channel in each trip system. Trip system A is powered from one motor-generator (M-G) set, and trip system B is powered from another M-G set.

The system may be tripped manually in order to initiate a scram (this meets IEEE 279-1968 criteria, 4.17 - Manual Actuation). There are two manual scram buttons, one for reactor protection logic channel A and one for channel B. Depressing the scram button on channel A, as shown on Figure 7.2-2, opens the contacts which deenergize relays labeled MS1 and MS2. The MS relays in turn open contacts labeled MS1 and MS2. Since these contacts are in series with the contacts from the subchannel scram relays, a single channel trip proceeds exactly as before. Subsequently depressing the scram button in channel B causes a channel B trip which, combined with the channel A trip, completes a full reactor scram. The two manual scram buttons are located such that one operator can depress both buttons concurrently and initiate a full scram. However, by purposely operating only one scram button at a time, followed by a reset of the trip logic, the scram circuit may be thoroughly tested while the reactor is operating. (This meets IEEE 279-1968 criteria 4.10 - Capability for Test and Calibration for manual scram capability.)

Once a single channel trip or a full scram is initiated, contacts (also labeled MS1 and MS2) in the scram relay circuits open and keep the circuit deenergized until it is reset. A reset is possible only if all of the reactor protection system inputs are within limits. (This meets criteria 4.16 of IEEE 279-1968. For conditions describing reset of the RPS following a manual scram, see Section 7.2.5.16. Conditions which initiate a reactor scram are shown on Figure 7.2-3. Typical Analytical limits for scrams are listed in Table 7.2-1.

Analytical Limits are those values assumed in calculations and evaluations, which show that plant operation is safe during postulated transients and accidents. These values are found in calculations of record and design/license basis evaluations.

Allowable Values are selected to be conservative to the Analytical Limits due to the effects on the instrumentation from the accident or transient conditions, which are not present during instrument calibration. Allowable Values are specified in the Technical Specifications and apply to the applicable instrument function.

Protective and regulating function trip setpoints are specified in setpoint calculations. The setpoints and their associated tolerances are selected to ensure that with a high degree of probability the setpoint does not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the setpoint, but within the Allowable Value is acceptable. An instrument CHANNEL is inoperable when its actual trip setpoint is not within its Allowable Value.

Some Technical Specifications delineate Allowable Values associated with Reactor Water Level. These Allowable Values are referenced to Instrument Zero. Instrument Zero is 503 inches above Vessel Zero, or 143 inches above Top of Active Fuel (TAF). Top of Active Fuel (TAF) is 360 inches above Vessel Zero.

7.2.2.2 General Functional Requirements

The protective functions provided by RPS are described in the following list (these are the general functional requirements as described in IEEE 279, Paragraph 4.1):

A. High neutron flux - To prevent fuel damage resulting from bulk power increases, high neutron flux initiates a scram. The neutron flux scram, combined with safety valve actuation, provides vessel overpressure protection. The nuclear instrumentation (Section 7.6) provides high neutron flux trip signals. Four intermediate range monitor (IRM) channels and three average power range monitor (APRM) channels are connected to each of the dual logic channels for a total of 8 IRMs and 6 APRMs. The four source range monitors (SRMs) are combined with the IRMs and APRMs in the manual scram logic to provide non-coincidence high flux scram protection. This function is bypassed during normal operation by installation of shorting links. If the reactor mode switch (described later in this section) is in the RUN position and the APRM channels are not downscale, the IRM scrams are automatically bypassed.

During refueling the primary neutron monitoring system (NMS) indication of neutron flux level is provided by the Source Range Monitors (SRM). The NMS (including the SRMs) provide input to the RPS manual scram logic. However, the shorting links are normally installed such that tripping any combination of SRM channels does not cause a trip of a RPS channel. Performance of Shutdown Margin Demonstrations (multiple control rods withdrawn) with the vessel head removed or de-tensioned requires removal of these shorting links to provide additional protection above what the IRMs provide against a reactivity excursion. Removing these shorting links enables the SRM scram function.

B. High reactor pressure - An increase in reactor vessel pressure while the plant is operating tends to compress the steam voids and results in a positive reactivity effect, increased nuclear activity with subsequent heat generation, and further pressure increases. This threatens the integrity of the reactor vessel, which is an important barrier to the uncontrolled release of fission products. The high pressure scram reduces the heat generation to terminate the pressure rise. This scram is a backup to the high flux scram and the main steam isolation valve (MSIV) closure scram.

C. High drywell pressure - Abnormal pressure could indicate a rupture of, or excessive leakage from, the reactor coolant system into the drywell structure. This scram minimizes the energy which must be accommodated during a loss-of-coolant accident and prevents the reactor from going critical following the accident.

D. Low reactor water level - This scram signal assures that the reactor is not operated without sufficient water above the reactor core.

E. Control rod drive system scram discharge volume (SDV) high level - This scram signal assures that the reactor is operated with sufficient free volume in the scram discharge system to receive the discharge from the control rod drives if a scram is required.

F. Main condenser low vacuum - This scram signal anticipates the turbine stop valve closure scram and therefore reduces the pressure transient, neutron flux increase, and the fuel surface heat flux which occur when the condenser is isolated to protect the condenser from overpressure.

G. Deleted

H. Loss of ac power to the protection system - All electronic trips, logic relays, and scram solenoid valves will actuate on loss of power as the RPS M-G sets coast down and output breakers trip following a loss of ac power.

I. Partial closure of main steam line isolation valves - This scram signal assures that the reactor is not operated without a path to the main heat sink (condenser), since the resulting reactor vessel pressure increase could cause a fuel-damaging power transient. There are four main steam lines with two valves per line. The logic is arranged such that the partial closure of either the inboard or the outboard valve in any three steam lines will initiate a scram.

J. Manual scram - The manual scram provides a means for rapid, manual rod insertion during all modes of operation. A separate scram pushbutton is provided for each logic channel. To initiate a reactor scram, the pushbuttons for both logic channels must be pushed.

K. Generator load rejection - A loss of generator load will cause the turbine-generator to speed up. The turbine speed governor will react by closing the turbine control valves. The reduction of steam flow will cause the reactor vessel pressure to rise, and the pressure regulator will open the turbine bypass valves in an attempt to maintain constant reactor pressure. (Analysis of this event was performed assuming that the bypass valves do not open.) If the load reduction is sudden and of a greater magnitude than bypass valve capacity, the reactor pressure will rise, resulting in the transient described in Item B. To prevent possible fuel damage and the lifting of reactor safety valves, a sudden rejection of generator load causes a scram anticipatory to the high reactor pressure scram. The condition is sensed by comparing high-pressure turbine exhaust pressure (between high-pressure and low-pressure turbines) to generator stator current. A high pressure signal coincident with low generator electrical output causes a turbine control valve fast closure via the fast-acting solenoids. Operation of the fast-acting solenoids will cause a scram. This rate-sensitive power/load unbalance trip circuit is also designed to protect the turbine upon a rapid mismatch of the generator power and turbine steam flow. In order for an RPS trip to occur upon control valve fast closure, both of the following conditions must occur:

1. Greater than 40% mismatch between high pressure turbine exhaust (crossover) pressure and generator stator amps; and

2. A simultaneous loss of generator amps in less than 35 milliseconds.

L. Turbine stop valve closure- In order to protect the turbine, generator, output transformer, and main condenser, the four turbine stop valves are automatically closed upon certain conditions described in Section 7.7. The sudden closure of the turbine stop valves reduces the steam flow from the reactor and causes the reactor vessel pressure to rise. The pressure regulator responds to the pressure rise by opening the turbine bypass valves, unless opening the bypass valves would overpressurize the condenser. If the reduction in reactor steam flow is of greater magnitude than bypass valve capacity or if the bypass valves are not allowed to open (Section 7.7), the reactor vessel pressure rise causes a positive reactivity insertion which could lead to fuel damage. In order to prevent fuel damage resulting from a reactor pressure rise due to turbine stop valve closure, the four turbine stop valves are equipped with valve stem position switches which introduce reactor protection system logic

channel trips when the valves start to close. The logic is arranged so that the partial closure of three of the four stop valves initiates a reactor scram.

M. Deleted

N. Core power oscillations – BWR cores have been shown to exhibit thermal-hydraulic reactor instabilities when reactor power is above 25% of rated reactor power and recirculation flow is less than 60% of rated core flow. These instabilities, if allowed to propagate, could exceed the minimum critical power ratio (MCPR) and lead to fuel damage and the release of radioactive material. In order to avoid fuel damage, OPRMs are designed to utilize signals from the existing LPRMs to determine if core power oscillations are taking place. If an OPRM detects oscillations, and is fully armed, then it suppresses the oscillations by initiating a reactor scrams.

7.2.2.3 Reactor Mode Switch

A reactor mode switch is manually positioned to select scram functions appropriate to the plant operating status.

A. SHUTDOWN	This initiates a full reactor scram.
B. REFUEL	IRM scram functions are in operation;.
C. STARTUP/HOT STANDBY	IRM scram functions are in operation. Scrams on main condenser vacuum and main steam isolation valve closure, while reactor pressure is low are bypassed.
D. RUN	APRM scram functions in operation. IRM scrams are bypassed if APRM not downscale. All other scram functions are in operation.

7.2.2.4 Channel Bypasses

To provide for operational requirements, such as draining of the scram discharge volume or the repair of redundant electronic instruments, RPS design provides for

the following scram bypasses (see Section 7.2.5.12 for a comparison with IEEE 279, Paragraph 4.12):

A. Main condenser vacuum and main steam line isolation valve closure scrams are bypassed with the reactor mode switch in any position other than Run;

B. Trips from the scram discharge volume high level can be bypassed to allow for scram reset and draining of the discharge volume;

C. One of the four IRMs associated with each protection channel may be bypassed by the operator using a one-at-a-time selector switch (see Section 7.6.1.4);

D. One of the three APRMs associated with each protection channel may be bypassed by the operator using a one-at-a-time selector switch (see Section 7.6.1.5.2);

E. One of the four OPRMs associated with each protection channel may be bypassed by the operator using a one-at-a-time selector switch (see Section 7.6.1.5.6); and

F. Generator load rejection scram and turbine stop valve closure scram are automatically bypassed on low-first stage turbine pressure.

7.2.2.5 Sensing Instrumentation

Instrumentation providing inputs to the reactor protection system is separate from that used for process system control and indication; thus, control system instrumentation failures do not jeopardize the protection system. The RPS instrumentation is described below:

A. Containment pressure inputs to the protective system are from non-indicating pressure switches. Two switches sensing drywell pressure are located on each of the two instrument racks outside the drywell. The switches are arranged so that a single event cannot jeopardize the ability of the protective system to initiate a scram.

B. Scram discharge volume water level inputs to the RPS use two different types of level sensors. Unit 2 uses dP type level transmitters with electronic trip units for one of the inputs and thermal type level switches for the diverse means of initiation. Unit 3 uses two different dP type transmitter models with two different level switch manufacture's trip units for the diverse means of initiation. The switches are arranged so that a single event cannot jeopardize the ability of the RPS to scram.

C. Condenser vacuum inputs to the RPS are from four non-indicating vacuum switches mounted locally. These vacuum switches are arranged so that a single event cannot jeopardize the ability of the RPS to scram.

D. Main steam line valve closure scram inputs to the RPS are from valve stem position limit switches on the eight isolation valves. Each switch provides an independent signal to the RPS. The partial closure of either the inboard or outboard isolation valves in any three main steam lines would produce a trip in both logic channels, resulting in a reactor scram.

E. The turbine control valve fast closure inputs to the RPS are from pressure switches on each of the four fast-acting solenoid valves which initiate fast closure of the control valve.

F. Turbine stop valve closure inputs to the protection system are from valve stem position switches located on each of the four turbine stop valves. A position switch and two independent contacts are associated with each stop valve. One of the two contacts provides input to RPS trip system A; the other, to RPS trip system B. Thus, each RPS trip system receives an input from four Turbine Stop Valve-Closure channels, each consisting of one position switch (which is common to a channel in the other RPS trip system) and a switch contact. The logic is such that partial closure of any three stop valves initiates a scram.

G. Sensors which monitor reactor pressure vessel parameters are discussed in Section 7.6.

H. Nuclear instrumentation is described in Section 7.6. Nuclear instrumentation channel assignments to RPS automatic trip logic subchannels are as follows:

1. A1 - IRM 11, 13; APRM 1, 3; OPRM 1, 3
2. A2 - IRM 12, 14; APRM 2, 3; OPRM 2, 7
3. B1 - IRM 15, 17; APRM 4, 5; OPRM 8, 5
4. B2 - IRM 16, 18; APRM 4, 6; OPRM 4, 6

In addition, the following channel groupings provide coincident and non-coincident trip functions in the manual scram logic for each RPS channel when shorting links are removed:

1. SRM 21; IRM 11, 13; APRM 1, 3
2. SRM 22; IRM 12, 14; APRM 2, 3
3. SRM 23; IRM 15, 17; APRM 4, 5
4. SRM 24; IRM 16, 18; APRM 4, 6

I. Deleted.

7.2.3 Design Evaluation

In terms of protection system nomenclature, the dual logic channel reactor protection system is a one-out-of-two-twice system. Theoretically, its reliability is slightly lower than a one-out-of-two system. However, since the reliability differences are slight, they can be neglected. The advantage of the dual logic channel reactor protection system is that it can be tested completely during full-power operation. This capability for a thorough testing program, which contributes significantly to increasing reliability, is not possible on a one-out-of-two system. Topical Report APED-5179[1] presents a full discussion of the reliability of the dual logic channel system.

A failure of any one RPS input or component produces a trip in just one subchannel of one logic channel, a condition insufficient to produce a reactor scram. This resistance to spurious scrams contributes to plant safety since unnecessary cycling of the reactor through its operating modes would increase the probability of error or actual failure. The circuits are isolated to preclude a fault in one circuit from propagating to another and to reduce the likelihood that severe environmental influence, which might adversely affect reliability, will affect more than one circuit. The sensors are dispersed; both sensors in one logic channel are not allowed to occupy the same general region or to be connected to a common header or point. The wiring is dispersed so that a single fire or accident would probably not affect more than one input to the protection system. The relays associated with the

contacts feeding one subchannel scram relay are isolated from corresponding circuits in the other scram relay subchannel.

Since each control rod is scrammed as an independent unit, the failure of any one rod to scram does not affect the ability of the other rods to scram.

Additional scram reliability is provided by the backup scram valves, which energize from dc power when both logic channels are tripped. The backup scram valves relieve instrument air pressure from the scram valves when the solenoids are energized, resulting in a scram.

The response of the RPS is sufficiently rapid to prevent the release of radioactive material in excess of the limitations of 10 CFR 100 or 10 CFR 50.67 as applicable following the design basis accidents. The system response times from the opening of the sensor contacts up to and including the opening of the trip actuator contacts shall not exceed 50 milliseconds.

The RPS response to single component malfunctions or single operator errors is sufficient to prevent fuel damage. Single component malfunctions have been evaluated in Section 7.2.5.2.

The primary sensors for subchannels A1 and B1 share the same set of sensing lines. Those for subchannels A2 and B2 share a different set of sensing lines. The two sets of sensing lines servicing the two trip systems are geometrically separated by approximately 180° in azimuth and pass through drywell penetrations that are greater than 50 feet apart and are in separate rooms, in accordance with the separation criterion.

The wiring to the independent sensors for trip system A run in different conduits or trays from those of trip system B. The system is connected such that the channels of each trip system are electrically isolated from each other so that a failure of one channel cannot prevent a valid trip of the second channel of the trip system. The system thus meets the single-failure criterion and channel separation criterion. The highest quality materials and components were used in the design of the system.

The RPS meets IEEE 279 in that single failures in the system do not prevent the system from producing valid scrams, while the system design provides for maximum system availability by preventing or reducing the number of spurious scrams. The system is arranged to provide for physical separation of components and electrical isolation.

The design of the dual logic channel RPS facilitates maintenance and troubleshooting. Most faults annunciate themselves, and those that do not are easily located, without ambiguity, by testing.

The component parts used in the dual logic channel reactor protection system have been used in volume for many years in critical industrial applications. The parts are suitably derated to prolong life and increase the margin of safety.

The power supply for the RPS consists of two independent electrical buses (Figure 7.2-4). The components, wiring, and relays are seismically qualified as Class 1E at the interface of the power supply and the RPS.

The RPS bus breakers are equipped with mechanical interlocks to prevent both an M-G set and the reserve power source from simultaneously supplying power to an RPS bus. The normal feed for RPS bus A (M-G set B) is MCC 28-2(38-3). The normal feed for RPS bus B (M-G set A) is MCC 29-2(39-2). Either bus may be fed from the reserve feed from MCC 25-2(35-2).

A key interlock system, consisting of two locking devices on the reserve power supply breakers that require the same key, prevents reserve power from supplying more than one RPS bus at a time. It prevents cross-connecting the independent buses and overloading the reserve power instrument transformer.

During a power loss to the M-G set, the high-inertia flywheel is designed to maintain generator output within 5% of rated values for at least one second to keep the RPS bus energized. The non-Class 1E RPS M-G sets are provided with relaying to trip on undervoltage and underfrequency conditions.

In addition, two Class 1E electrical protection assemblies (EPAs) are in series between each RPS power supply and its RPS bus breaker (see Figure 7.2-4). The EPAs protect the Class 1E components powered by the RPS buses from abnormal voltage and frequency conditions resulting from failures of the non-Class 1E power supplies (RPS M-G sets or reserve power supply). Each EPA includes a breaker and associated monitoring module consisting of overvoltage, undervoltage, and underfrequency relays which trip the EPA breaker.

7.2.4 Surveillance and Testing

The trip circuitry is arranged to facilitate testing. A test signal can be applied to one input at a time. If the test signal exceeds the limit, a single logic channel trip occurs. Switches are installed in series with each pilot scram valve solenoid to facilitate scramming a single rod so that rod travel time can be measured. A single rod scram proves that each rod tested can be inserted by means of the scram valves within the time specified for rod travel.

Pressure switches are on/off devices. The signal used to test these devices is an actual pressure. Other on/off devices are tested similarly with basic signals.

Analog devices, notably the flux monitoring channels, are tested in two phases. First, the device must show reasonable agreement with similar devices and must respond normally to power level changes and control rod movements. Second, a dummy electrical signal may be introduced using the amplifier already tested. This dummy signal is adjusted until the setpoint limit is exceeded in order to initiate a single logic channel trip.

The reactor protection system is designed to fail safe. In every case a failure is annunciated so that the location of the failure can be ascertained without ambiguity.

A routine testing schedule is arranged to assure that a system failure can be identified and corrected. The testing prevents system degradation over time. Surveillance frequency is specified in Technical Specifications.

7.2.5 Analysis

The RPS was originally designed by the nuclear steam supply systems (NSSS) vendor (General Electric). In Topical Report NEDO-10139,[2] GE identified the means by which the RPS design conformed to IEEE 279-1968 and justified any exceptions. The remainder of this section summarizes the comparison of the RPS at Dresden Station with the criteria in IEEE 279-1968. Parenthetical references are to paragraph numbers in IEEE 279-1968.

7.2.5.1 General Functional Requirement

Section 7.2.2. describes each input parameter monitored and provides a basis for each parameter selection. (4.1) Table 7.2-1 lists the specific setpoint for each parameter.

7.2.5.2 Single-Failure Criterion

The design and installation of the RPS has generally followed practices which are intended and expected to make it invulnerable to any single failure in sensory equipment or electrical wiring. (4.2) These practices are summarized below:

A. Sensors are divided into four or more channels, and their channel division is carried through to the protection system relay panels, which consist of four separate panel sections having end closures of steel;

B. All protection system wiring is run in rigid metallic conduit or solid trays with covers;

C. Cables through drywell penetrations are grouped such that failure of all cables in a single penetration cannot prevent a scram;

D. Routing of cables is such that damage to any single tray cannot disable the protective function;

E. Sensors are arranged so that no single sensor failure or process sensing line failure in any mode can disable the scram function; and

F. Wiring to scram solenoids are grouped so that no failure within a single metallic enclosure can affect more than one of the four groups of control rods.

The designated outputs from the RPS to other systems are designed so that no single failure in any portion of the RPS, including these output networks, can prevent proper protection system operation when it is required.

It is not necessary that the output networks meet the single-failure criterion in terms of their purpose, but it is essential that the outputs not compromise the single-failure performance of the RPS in terms of its protective function. This latter objective has been accomplished in the design of these output functions.

The use of an independent trip channel for each trip logic allows the system to sustain any trip channel failure without preventing other sensors monitoring the same variable from initiating a scram. A single sensor or trip channel failure will cause a single trip system trip and actuate alarms that identify the trip. The failure of two or more sensors or trip channels would cause either a single trip system trip, if the failures were confined to one trip system or a reactor scram, if the failures occurred in different trip systems. Any intentional bypass, maintenance operation, calibration operation, or test - all of which result in a single trip system trip - leaves at least two trip channels per monitored variable capable of initiating a scram by causing a trip of the remaining trip system. The resistance to spurious scrams contributes to plant safety, because unnecessary cycling of the reactor through its operating modes would increase the probability of error or actual failure.

Each control rod is controlled as an individual unit. A failure of the controls for one rod would not affect other rods. The backup scram valves provide a second method of venting the air pressure from the scram valves, even if either scram pilot valve solenoid for any control rod fails to deenergize when a scram is required.

Failure of either RPS M-G set would result, at worst, in a single trip system trip (the deenergization of one of the two scram valve pilot solenoids on each CRD). Alternate power is available to the RPS buses. A complete, sustained loss of electrical power to both buses would result in a scram, delayed by the M-G set flywheel inertia.

7.2.5.3 Quality of Component and Modules

The sensors and trip channel components are described in the appropriate design and purchasing documentation. Proven components were chosen in the design stage and manufacturing, quality control, and field personnel assured proper vigilance during the production and installation cycles. The RPS components and modules are specified to withstand the transient and steady state conditions of the environment (e.g., temperatures, humidity, pressure and vibration). The Master Equipment List identifies the classification of components. The equipment for the following functions apply to the requirements of IEEE 279-1968, Quality of Components and Modules (4.3), in that they were chosen to meet the requirements of their intended functions:

Neutron monitoring system scram trip;

Reactor vessel high-pressure scram trip;

Reactor vessel low water level scram trip;

Turbine stop valve closure scram trip;

Turbine control valve fast closure scram trip;

Main steam line isolation valve closure scram trip;

Scram discharge volume high water level scram trip;

Primary containment high-pressure scram trip;

Manual scram pushbuttons;

Reactor mode switch;

Reactor protection system reset switch;

Turbine stop valve closure and turbine control valve fast closure trip bypass;

Neutron monitoring system trip bypass;

Scram discharge volume high water level trip bypass; and

Main steam line isolation valve closure trip bypass.

IEEE 279-1968 applies to the remaining RPS equipment as indicated:

A. Reactor protection system M-G sets and power distribution - Cabling used within the RPS panels has been selected to be appropriate for RPS use. The RPS M-G sets have been chosen to provide low maintenance.

B. Reactor protection system trip logic, actuators, and trip actuator logic - The RPS trip logic consists of series-connected relay contacts from the trip channel output relays. The RPS trip actuator logic consists of relay contacts connected in a specific arrangement from the trip actuators. Within the RPS panels in the control room, electrical circuits are fused. Individual control rod drive scram solenoids are fused at the scram solenoid fuse panels.

C. Reactor protection system outputs to other systems - At the RPS interface with the output networks, isolated contacts of various RPS relays have been used to provide the signal source. These contacts are classified as being a portion of the RPS component. The load device driven by these contact outputs is not included in the RPS scope. The use of isolated contact outputs from the RPS provides a large measure of isolation and independence for this interface relative to the protective action portions of the RPS.

7.2.5.4 Equipment Qualification

For each of the RPS functions, the original equipment was required to be certified by the vendor to meet the requirements listed in the purchase order and for the intended application described for that function. These certifications, in conjunction with applicable field experience for those components in their particular applications, qualified the components. In this way, the functions meet the requirements of IEEE 279-1968, Equipment Qualification. (4.4)

In addition to the vendor qualification, qualification tests of the relay panels were conducted to confirm their adequacy for this application.

For RPS outputs to other systems, the RPS contact outputs from the designated relays were qualified during the relay and panel tests. Qualification testing beyond this interface was not considered.

This design requirement is not applicable to the trip logic test switch function.

Vendor certification that the component will perform as required on the purchase specification is required for all components which perform a safety function. This certification, in conjunction with field experience with these components suffices to qualify these parts. In situ testing was performed during the preoperational test phase.

For information on the current seismic and environmental qualification programs, refer to Sections 3.10 and 3.11, respectively.

7.2.5.5 Channel Integrity

Except as noted below, vendor certification was required that the RPS components would perform in accordance with the requirements listed on the purchase specifications as well as in the intended applications. (4.5)

A. Trip logic test switch - The trip logic test switch is not a trip channel component; rather, it is an element in the individual RPS trip logic strings.

B. Reactor protection system reset switch - The RPS reset switch is not a trip channel component; rather, its auxiliary relays are elements in the individual RPS trip logic strings.

C. Reactor protection systems outputs to other systems - Selection of output signals from the RPS to other systems has been done in such a manner to ensure that the integrity of the protection system channels remains intact and unchanged.

This design requirement is not applicable to the reactor protection system M-G sets and power distribution.

7.2.5.6 Channel Independence

The four subchannels of each protective function are electrically isolated and physically separated. Cables for the RPS outside of the enclosures in the control room are run in enclosed, rigid metallic conduits throughout the plant which are not used for other cables. The cables from duplicate sensors on a common process tap are run in separate conduits. Cables for sensors of different variables in the same RPS trip logic may run in the same conduit. The RPS cables have channel separation requirements which are maintained by the conduit system.

Low-level signal cables are routed separately from all power cables with a minimum separation of 3 feet wherever practical. Where the low-level signal cable runs at right angles to a power cable, a separation distance of less than 3 feet may be used, based upon the probable noise pickup relative to the allowable signal-to-noise ratio.

Except as otherwise noted in the following discussions, the RPS trip, reset, and bypass channels are physically separated and electrically isolated to meet the design requirements of IEEE 279-1968, Channel Independence (4.6):

A. Manual scram pushbuttons - The manual scram pushbutton is not a channel component; nevertheless, the channels are separated in that the contacts from one switch are wired into the A3 trip logic channel and the contacts of the second switch are wired into the B3 trip logic channel.

B. Trip logic test switch - While the test switch is not a trip channel component, it is imperative that its use in the RPS trip logic maintain the existing channel independent of the automatic protective trip channels. The application of four test switches, one per trip logic, ensures that this design requirement is satisfied.

C. Neutron monitoring system trip bypass - The neutron monitoring bypass channels comply with this design requirement. The bypass channel output to the individual APRM or IRM trip channel is obtained from an isolated relay contact. This contact output is physically separated and electrically connected with the other bypass channels in order to provide for one and only one bypass within one RPS trip system at any given time; however, this designed connection does not invalidate the isolated contact from each relay to the neutron monitoring system trip channel.

D. Scram discharge volume high water level trip bypass - The bypass circuitry complies with this design requirement. For operator convenience, a single switch has been selected for the bypass function. Factors considered in this selection were the number of bypass operations required in any given operating period and the expected duration of each bypass. Since the bypass switch is used only to permit manual reset of the RPS and to permit the operator to drain the discharge volume following reactor scram, the switch is used infrequently and for short time periods. These considerations suggest that a single switch is a better choice than multiple switches when viewed from a human factors perspective.

   Care has been taken to assure that sufficient physical separation and electrical isolation exists to assure that the bypass channels are satisfactorily independent. Moreover, the conditions for bypass have been made quite stringent in order to preclude spurious operation.

E. Reactor protection systems outputs to other systems - Use of isolated relay contacts from the RPS relays assures that the RPS trip channels are maintained independent of one another. The design has considered the effect of the output devices representing a potential point of common failure for all trip channels, and steps have been incorporated into the system to prevent this situation.

This design requirement is not applicable for the following equipment:

A. Reactor protection system M-G sets and power distribution; and

B. The combined RPS trip logic, actuators, and trip actuator logic.

7.2.5.7 Control and Protection System Interaction

The reactor protection system, which initiates scrams, does not share components or subsystems with other control systems. (4.7)

This separation is described below:

A. RPS power is obtained from two independent M-G sets, and only during shutdown of one M-G set or during testing of an EPA is alternate power manually switched into the RPS;

B. Trip channel signals to the RPS are obtained from isolated contacts on process sensors or relays associated with nuclear instrumentation;

C. In most instances, separate isolated contacts on these process sensors or relays used with the RPS are used to illuminate control room indicators and annunciators, or are used for digital inputs to the process computer system; and

D. Isolated contacts from the reactor low water level process sensor are used with the primary containment isolation system.

Trip channels providing inputs to the RPS are not used for automatic control of process systems; thus, the operations of protection and process control systems are separated. Sensors, trip channels, and trip logics of the RPS are not used directly for automatic control of process systems. Therefore, failure in the controls and instrumentation of process systems cannot induce failure of any portion of the protection system.

Reactor protection system inputs to annunciators, recorders, and the computer are arranged so that no malfunction of the annunciating, recording, or computing equipment can functionally disable the system. Signals directly from the RPS sensors are not used as inputs to annunciating or data logging equipment.

7.2.5.8 Derivation of System Inputs

Where practicable, sensor inputs are measures of the desired variable with the following exceptions: (4.8)

A. Loss of condenser vacuum, turbine stop valve partially closed, load reject, MSIV closure and turbine control valve partially closed: For these scram inputs, the desired input variable is "loss of heat sink." Since this variable cannot be measured directly, the inputs to these channels are

considered to be an indication that loss of heat sink has occurred or is imminent.

B. SDV level: The desired input is "loss of free volume." Since the total volume of the SDV is fixed, the measure of the water level in the SDV is considered to be an appropriate input.

7.2.5.9 Capability for Sensor Checks

The capability for sensor checks is provided in the design of the systems using substitute inputs where practical and cross-checking between channels where necessary. A further discussion of testing and surveillance is in Section 7.2.4. The following text discusses the applicability of the RPS functions to IEEE 279-1968, Capability of Sensor Checks. (4.9)

A. Neutron monitoring system scram trip - During reactor operation in the RUN mode, the IRM detectors are stored below the reactor core in a low flux region. Movement of the detectors into the core permits the operator to observe the instrument response from the different IRM channels and will confirm that the instrumentation is operable.

In the power range of operation, the individual LPRM detectors respond to local neutron flux and provide the operator with an indication that these instrument channels are responding properly. The six APRM channels may also be observed to respond to changes in the gross power level of the reactor to confirm their operation.

Each APRM instrument channel may also be calibrated with a simulated signal introduced into the amplifier input, and each IRM instrument channel may be calibrated by introducing an external signal source into the amplifier input.

Each OPRM module maybe calibrated with simulated signals introduced into the module input utilizing the OPRM Maintenance Terminal.

During these tests, proper instrument response may be confirmed by observation of instrument lights in the control room and trip annunciators.

B. Reactor vessel high pressure scram trip - One sensor may be valved out-of-service at a time to perform a periodic test of the trip channel. During this test, operation of the sensor, its contacts, and the balance of the RPS trip channel may be confirmed.

C. Reactor vessel low water level scram trip - Due to the one-out-of-two-twice configuration of the RPS trip logic for this protective function, one level sensor at a time may be removed from service to perform the periodic test on any trip channel.

D. Turbine stop valve closure scram -

For any single stop valve closure test, two of the trip channels will be placed in a tripped condition, but none of the trip logics will be tripped and no RPS annunciation or computer trip channel logging will be evident. This arrangement permits single valve testing without corresponding tripping of the RPS, and the observation that no RPS trips result is a valid and necessary test result.

At reduced power levels, two valves may be tested in sequence to produce RPS trips, annunciation of the trips, and computer printout of the trip channel identification. These observations are another important test result that confirms proper RPS operation.

In sequence, each combination of single valve closures and dual valve closures is performed to confirm proper operation of all trip channels.

E. Turbine control valve fast closure scram trip - During any control valve fast closure test, one RPS trip channel will be tripped and will produce both control room annunciation and computer record of the trip channel identification.

F. Main steam line isolation valve closure scram trip - For any single valve closure test, two of the trip channels will be placed in a tripped condition, but none of the trip logics will be tripped and no RPS annunciation or computer trip channel record will be evident. This arrangement permits single valve testing without a corresponding trip of the RPS. The observation that no RPS trip results is a valid and necessary test result.

At reduced power levels, two valves may be tested in sequence to produce RPS trips, annunciation of the trips, and computer printout of the trip channel identification. These observations are another important test result that confirms proper RPS operation.

In sequence, each combination of single valve closures in each of two main steam lines is performed to confirm proper operation of all eight trip channels.

These test results confirm that the valve limit switches operate as the valves are manually closed.

G. Scram discharge volume high water level scram trip - During reactor operation, the discharge volume differential-pressure type level sensors may be tested by using the instrument shut-off and test valves in proper sequence in conjunction with quantities of demineralized water.

H. Primary containment high-pressure scram trip - During reactor operation one pressure switch may be valved out-of-service at a time to perform periodic testing.

I. Deleted.

J. Reactor mode switch - Operation of the mode switch may be verified by the operator during plant operation by performing certain sensor tests to confirm proper RPS operation. Movement of the mode switch from one position to another is not required for these tests since the connection of appropriate sensors to the RPS logic, as well as disconnection of inappropriate sensors, may be confirmed from the sensor tests.

K. Turbine stop valve closure and turbine control valve fast closure trip bypass - Testing of individual pressure switches is permitted during plant operation by valving out-of-service one pressure switch at a time. A variable pressure source may then be introduced to the switch to confirm the setpoint value and switch operation.

L. Reactor protection systems outputs to other systems - Output signals from the RPS are not derived at the process sensor interface due to a lack of adequate isolation at this point. Rather, the outputs are obtained from the trip channel relays and trip actuator relays which do provide adequate isolation of the signal source.

M. Exceptions - This design requirement is not applicable to the following equipment:

1. Manual scram pushbuttons;

2. Trip logic test switch;

3. Reactor protection system reset switch;

4. Reactor protection system M-G sets and power distribution; and

5. Reactor protection system trip logic, actuators, and trip actuator logic.

7.2.5.10 Capability for Test and Calibration

Provisions are made for timely verification that each active or passive component in the RPS is capable of performing its intended function as an individual component

and/or in conjunction with other components. (4.10) In fulfillment of this general objective, tests are provided to verify that the following specific conditions exist:

A. Each instrument channel functions independent of all others;

B. Sensing devices will respond to process variables and provide channel trips at correct values;

C. Paralleled circuit elements can independently perform their intended function;

D. Series circuit elements are free from shorts that can nullify their function;

E. Redundant instrument or logic channels are free from interconnecting shorts that could violate independence in the event of a single malfunction;

F. No element of the system is omitted from the test if it can in any way impair operability of the system. If the test is done in parts, then the parts are overlapped to a sufficient degree to assure operability of the entire system; and

G. Each monitoring alarm or indication function is operable.

H. Neutron monitoring system trip bypass - At any time, the operator may confirm proper operation of the neutron monitoring system bypass channels by placing the bypass switch for any given trip system into specific positions and introducing trip conditions into the bypassed neutron monitoring system trip channel. A sequential combination of these operations will provide for complete verification of the neutron monitoring system bypass channels.

I. Scram discharge volume high water level trip bypass - During plant operation in the STARTUP/HOT STANDBY and RUN modes, imposition of this bypass function is inhibited by the reactor mode switch. Under these circumstances, operation of the bypass switch should not produce a bypass condition for any single trip channel. This fact can be determined from the control room annunciator, a visual inspection of the bypass relays, and the process computer printout of any discharge volume high water level trip channel placed in a tripped condition prior to the bypass switch test.

J. Main steam line isolation valve closure trip bypass - Testing of the bypass circuit is possible in the SHUTDOWN, REFUEL, or STARTUP/HOT STANDBY positions of the mode switch. Confirmation that the bypass is not in effect in the RUN mode may be made at operating conditions.

A further discussion of testing and surveillance is provided in Section 7.2.4.

7.2.5.11 Channel Bypass or Removal from Operation

A combination of administrative controls and physical interlocks prevent bypassing or removal of more than one channel at a time. The remaining channels are still capable of performing protective action when required. The requirements of IEEE 279-1968, Channel Bypass or Removal from Operation (4.11), are not applicable for the following functions and equipment:

A. Reactor protection system reset switch;

B. Reactor protection system M-G sets and power distribution;

C. Reactor protection system trip logic, actuators, and trip actuator logic; and

D. Reactor protection systems outputs to other systems.

7.2.5.12 Operating Bypasses

Operating bypasses, where applicable, are designed to the same requirements as the trip portion of the protective system. A list and further discussion of operating bypasses is provided in Section 7.2.2.4. A number of scram bypasses are provided to account for the varying protection requirements depending on reactor conditions and to allow for instrument maintenance during reactor operations. Some bypasses are automatic, others are manual.

Where automatic bypasses are employed, the bypass is automatically removed when the conditions for bypass no longer exist. Other operating bypasses are manually installed and are under the administrative control of the control room operator. These controls meet the intent of requirements of IEEE 279-1968, Operating Bypasses (4.12), for the following functions:

A. Neutron monitoring system scrams;

B. Turbine stop valve closure scram;

C. Turbine control valve fast closure scram (EHC low-pressure);

D. Deleted

E. Main steam line isolation valve closure scram;

F. Condenser low vacuum scram;

G. Scram discharge volume high water level scram;

The requirements of IEEE 279-1968, Operating Bypasses (4.12), are not applicable to the following functions and equipment.

A. Reactor vessel high-pressure scram trip;

B. Reactor vessel low water level scram trip;

C. Primary containment high-pressure scram trip;

D. Deleted.

E. Manual scram pushbuttons;

F. Trip logic test switch;

G. Reactor protection system reset switch;

H. Reactor protection system M-G sets and power distribution;

I. The combined RPS trip logic, actuators, and trip actuator logic; and

J. Reactor protection systems outputs to other systems.

7.2.5.13 Indication of Bypasses

Annunciation exists in the control room when a channel is bypassed. If the ability to trip some part of the system has been bypassed, this fact is continuously indicated in the control room. The requirements of IEEE 279-1968, Indication of Bypass (4.13), are met for the following RPS trip function's bypasses:

A. Neutron monitoring system IRM, OPRM and APRM scram;

B. Turbine stop valve closure and control valve fast closure (EHC low-pressure);

C. Main steam line isolation valve closure and condenser low vacuum scram;

D. Scram discharge volume high water level scram (if tripped); and

7.2.5.14 Access to Means for Bypassing

All manual bypass switches and the reactor mode switch are in the control room, under the direct control of the control room operator. (4.14) Manual bypasses are controlled by mechanical, electrical, or administrative controls to maintain trip function operability through other channels when one channel is bypassed. Trip functions which use inputs from fluid sensors may also have individual sensors valved out-of-service and returned to service under the administrative control of the operator. Trip functions which use limit switch or position switch inputs cannot be manually bypassed. The neutron monitoring system allows a single bypass in each

trip system which still yields at least two remaining active monitors in each trip system.

7.2.5.15 Multiple Trip Settings

Multiple setpoints are used where it is necessary to provide more restrictive reactor protection limits due to the mode of operation or operating conditions. (4.15) Multiple trip settings are utilized for the following trip channels:

A. Neutron monitoring - Setpoints are administratively controlled by reactor mode switch position (see Section 7.2.2);

B. IRM protection range - Setpoints are tracked by the operator's selection of the IRM range switch position.

7.2.5.16 Completion of Protective Action Once It Is Initiated

The IEEE 279-1968 requirement for Completion of Protective Action Once It Is Initiated (4.16) is addressed by the RPS in the following ways.

For the reactor protection system trip logic, actuators, and trip actuator logic, the interface of the RPS trip logic and the trip actuators assures that this design requirement is accomplished. The trip actuator is normally energized and is sealed in by one of the power contacts to the trip logic string. Once the trip logic string has been open-circuited as a result of a process sensor trip channel becoming tripped, the scram contactor seal-in contact opens. At this point in time, the completion of protection action is directed regardless of the state of the initiating process sensor trip channel.

The reactor protection system reset switch (when enabled) bypasses the seal-in contact to permit the RPS to be reset to its normally energized state when all process sensor trip channels are within their normal (untripped) range of operation. In the event of concurrent trips of both trip systems A and B, manual reset is automatically inhibited for a minimum time delay of 10 seconds. The time delay prevents reset prior to the insertion of all control rods.

7.2.5.17 Manual Actuation

Manual scram may be initiated through the operation of either the manual scram pushbuttons (one per trip channel), or placing the mode switch in the shutdown position. (4.17) A failure within the automatic scram initiation channels will not prevent the operation of the manual scram function.

7.2.5.18 Access to Setpoint Adjustments, Calibration, and Test Points

Administrative controls exist for the access to setpoint, calibration, and test points. (4.18) To gain access to the calibration and trip setting controls located outside the control room, a cover plate, access plug, or sealing device must be removed by operating or maintenance personnel before any adjustment in trip settings can be effected. Operating personnel are responsible for granting properly qualified plant personnel access to the setting controls for testing or calibration adjustments.

7.2.5.19 Identification of Protective Actions

The reactor protection system trip logic, actuators, and trip actuator logic use four control room annunciators to identify the tripped portions of the RPS in addition to the previously described trip channel annunciators (4.19):

A. A1 or A2 automatic trip logics tripped;

B. A3 manual trip logic tripped;

C. B1 or B2 automatic trip logics tripped; and

D. B3 manual trip logic tripped.

These annunciators are connected through independent auxiliary contacts of the scram contactors to the process computer to provide a typed record of the relay operations.

7.2.5.20 Information Readout

Sufficient information is provided to the operator concerning system status. Indication or annunciation is available for all parameters used by the RPS. (4.20)

Each of the eight scram groups (A1 through A4 and B1 through B4) is provided with a normally energized indicator light at the RPS cabinets and another on the main control panel. The scram group indicators extinguish when an actuator logic opens.

Whenever an RPS sensor trips, it lights a white annunciator window for that variable on the reactor control panel in the control room. The first trip system to trip also lights a red window to indicate which trip system tripped first.

An RPS trip channel trip also sounds a horn, which can be silenced by the operator. The annunciator window lights remain illuminated until manually reset, which is not possible until the condition causing the trip has been cleared. The red window is reset by a separate reset pushbutton. The individual sensors that tripped in a group of sensors monitoring the same variable may be identified by the position of the RPS relays (tripped or untripped). The location of the alarm windows on the annunciator provides the operator with the means to quickly identify the cause of RPS trips and to evaluate the threat to the fuel or nuclear system process barrier.

To provide the operator with the ability to analyze an abnormal transient during which events occur too rapidly for direct operator comprehension, RPS trips are monitored by the process computer system and recorded in historical archives that may be retrieved later for review. These archives are described in detail in the process computer documentation.

7.2.5.21 System Repair

The design of the following components, functions, and systems complies with the IEEE 279-1968, System Repair, design requirement. (4.21)

A. Reactor mode switch;

B. Trip logic test switch;

C. Reactor protection system reset switch;

D. Reactor protection system M-G sets and power distribution;

E. Reactor protection system trip logic, actuators, and trip actuator logic;

F. Neutron monitoring system trip bypass;

G. Scram discharge volume high water level trip bypass; and

H. Main steam line isolation valve closure trip bypass.

Conformance of other RPS functions to IEEE 279-1968, System Repair (4.21), requirements are as follows:

A. Neutron monitoring system scram trip - Replacement of IRM and LPRM detectors must be accomplished during plant shutdown. Repair of the remaining portions of the neutron monitoring system may be accomplished during plant operation by appropriate bypassing of the defective trip channel output. The design of the system facilitates rapid diagnosis and repair.

B. Reactor vessel high pressure scram trip – The one-to-one relationship between the pressure sensor and a trip channel output relay permits the plant personnel to identify any component failure during operation of the plant. Provisions have been made to facilitate repair of the channel components during plant operation.

C. Reactor vessel low water level scram trip - The one-to-one relationship between a level sensor and a trip channel output relay permits the plant personnel to identify any component failure during operation of the plant. Provisions have been made to facilitate repair of the channel components during plant operation.

D. Turbine stop valve closure scram trip - Due to the inherent simplicity of the valve limit switch for the process sensor and the relationship of one limit switch contact with one trip channel output relay, the design of the system facilitates maintenance of this protective function.

During power operation, it may be necessary to reduce power in order to close more than one turbine stop valve in order to accomplish a specific RPS test. The sequence of tests should permit the operator to determine a defective limit switch contact or trip channel output relay.

E. Turbine control valve fast closure scram trip - Periodic tests of portions of this protective function during plant operation will likely require a temporary reduction in plant output and may be accomplished with the provisions for testing of the turbine equipment.

F. Main steam line isolation valve closure scram trip - Due to the inherent simplicity of the valve limit switch for the process sensor and the relationship of one limit switch contact with one trip channel output relay, the design of the system facilitates maintenance of this protective function.

During power operation, it may be necessary to reduce power in order to close valves in more than one main steam line. With this arrangement, a sequence of valve tests will permit the operator to determine fully a defective component or isolate the difficulty to one of two limit switches in a given main steam line.

G. Scram discharge volume high water level scram trip - Because the water level measurement and its one-to-one relationship between a given level sensor and its associated trip channel output relay are inherently simple, the design facilitates maintenance of this protective function.

H. Primary containment high-pressure scram trip - Due to the one-to-one relationship of pressure switch and trip channel output relay, this design requirement is satisfied by this protective function.

I. Deleted.

J. Manual scram pushbuttons - Due to the simplicity of the manual scram function, the design complies with this requirement.

K. Reactor protection systems outputs to other systems - The design of these networks facilitates repair of the RPS by providing timely information readout and identification of failures for the operating personnel.

The system is designed in such a manner that it can be easily repaired.

7.2.6 References

1. APED-5179, I.M. Jacobs, "Reactor Protection System, A Reliability Analysis," June 1966.

2. NEDO-10139, Compliance of Protection Systems to Industry Criteria, General Electric BWR Nuclear Steam Supply System, June 1970.

Table 7.2-1

TYPICAL PROTECTION SYSTEMS ANALYTICAL LIMITS

Signal	Scram Analytical Limit(2)
Reactor High Pressure	1060 psig
Reactor Low Level	0" RWL (inside the shroud)(1)
Reactor Neutron Flux Oscillation (OPRM)	See Table 7.6-1
Reactor High Neutron Flux	
APRM – Fixed	125% RTP
- Setdown	20% RTP
IRM - Setdown	125/125 divisions of full scale
Primary Containment High Pressure	2.0 psig
Condenser Low Vacuum	20 in.Hg vacuum
Scram Discharge Volume High Level	Unit 2: ≤ 40.4 gallons Unit 3: ≤ 41 gallons
Turbine-Generator Load Rejection	460 psig oil pressure at the control valve
Main Steam Line Isolation Valve Closure	10% closure
Turbine Stop Valve Closure	10% closure

Notes:

1. 0" RWL = 503 inches above vessel zero (inside the core shroud) or 143 inches above the top of active fuel. The top of active fuel is defined as 360 inches above vessel zero.

2. Data on Allowable Values can be obtained from Technical Specifications .

7.3 ENGINEERED SAFETY FEATURE SYSTEMS INSTRUMENTATION AND CONTROL

The engineered safety features (ESF) systems are provided to mitigate the consequences of postulated accidents and transients. The ESF systems described in this section are not used during normal plant operations. These systems must, however, be operable as defined in the Technical Specifications. Refer to Section 6.0 for a complete listing of ESF systems.

The ESF systems addressed in this section are as follows:

A. Emergency core cooling systems (ECCS):

1. Core spray system,
2. Low pressure coolant injection (LPCI) system,
3. High pressure coolant injection (HPCI) system, and
4. Automatic depressurization system (ADS).

B. Containment isolation systems:

1. Primary containment isolation system (PCIS), and
2. Secondary containment isolation.

C. Isolation condenser.

7.3.1 Emergency Core Cooling Systems Instrumentation and Control

This section describes the instrumentation and controls used to automatically and manually operate the ECCS. Refer to Section 6.3 for ECCS design basis and description.

Analytical Limits are those values assumed in calculation and evaluations, which show that plant operation is safe during postulated transients and accidents. These values are found in calculations of record and design/license basis evaluations.

Allowable Values are selected to be conservative to the Analytical Limits due to the effects on the instrumentation from the accident or transient conditions, which are not present during instrument calibration. Allowable Values are specified in the Technical Specifications and apply to the applicable instrument function.

Protective and regulating function trip setpoints are specified in setpoint calculations. The setpoint and their associated tolerances are selected to ensure that with a high degree of probability the setpoint does not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the setpoint, but within the Allowable Value is acceptable. An instrument CHANNEL is inoperable when its actual trip setpoint is not within its Allowable Value.

Some Technical Specifications delineate Allowable Values associated with Reactor Water Level. These Allowable Values are referenced to Instrument Zero. Instrument Zero is 503 inches above Vessel Zero, or 143 inches above Top of Active Fuel (TAF). Top of Active Fuel (TAF) is 360 inches above Vessel Zero.

7.3.1.1 Core Spray System Instrumentation and Control

Two independent core spray loops are designed to pump water, under accident conditions, from the pressure suppression chamber pool directly to the reactor core.

The control system is arranged to provide redundancy for the two independent and separately isolated control and power circuits for operation of either of the two independent core spray subsystems (refer to Figure 7.3-1).

The core spray subsystems are automatically actuated by signals from the following sensors:

A. Four independent high drywell pressure switches;

B. Four independent low-low reactor water level transmitters and trip units; and

C. Two independent low reactor pressure switches.

The core spray initiation signal requires one of the following logic combinations:

A. High drywell pressure (one-out-of-two-twice);

B. Low-low reactor water level (one-out-of-two-twice) coincident with low reactor pressure (one-out-of-two); or

C. Low-low reactor level (one-out-of-two-twice) sustained for 8.5 minutes (one-out-of-one). This signal is generated by the ADS system logic.

The core spray initiation signal starts the core spray pumps, opens the suction valves (if closed) and closes the test bypass valves (if open). The operator can, in the event of a system line break, override the automatic opening of the suction valves and close them.

Opening of the admission valves is accomplished only after the reactor pressure decays to approximately the design discharge pressure of the pump. The reactor low pressure is detected by two pressure switches connected in a one-out-of-two logic array. The permissive signal which opens the core spray admission (discharge) valves requires this low reactor pressure signal and voltage at the applicable 4160-V ESF bus in addition to the core spray initiation signal.

With normal auxiliary ac power available, the actions described above occur automatically and without delay. A diesel generator start signal is generated by either a low-low reactor water level signal or high drywell pressure signal (both one-out-of-two-twice logic). If normal power is not available, the pumps are started sequentially as described in Sections 6.3 and 8.3.

While the pump is running but prior to the admission valve opening, flow is through minimum flow valves which automatically close when flow to the reactor vessel is established. The minimum flow valves are interlocked with the pump breakers such that stopping the core spray pump or placing the pump control switch in the PULL-TO-LOCK position allows the minimum flow valve to be positioned in either the open or closed position using its control switch. The minimum flow valves are provided with logic which allows the operator to close the valves from the control room even with a core spray initiation signal present. This logic allows the minimum flow valves to be closed to perform their closed loop isolation function as required by General Design Criteria (GDC) 57.[1]

7.3.1.1.1 Conformance to IEEE 279-1968

The following subsections present a point-by-point comparison of the core spray system with the requirements of proposed IEEE 279-1968 which has been summarized from GE Topical Report, NEDO-10139.[2] For more detailed information, refer to the topical report.

7.3.1.1.1.1 General Functional Requirement

The general functional requirements of IEEE 279-1968, Paragraph 4.1, and the provision of the core spray system to fulfill these requirements are summarized below:

A. Auto-initiation of appropriate action - Appropriate action for the core spray control system is defined as the activation of equipment for introducing low-pressure water through the core spray sparger when reactor water level drops below a predetermined point or the drywell pressure increases above a predetermined value, and the vessel pressure is below a predetermined value which is lower than the pump shutoff head. Equipment activation occurs automatically.

B. Precision - The sensory equipment positively initiates action before process variables exceed precisely established limits. In the case of vessel level sensors, high drywell ambient temperature can introduce errors that would lower the trip point for starting of the core spray pumps. Errors that result from drywell temperatures which are less than the temperature associated with a high drywell pressure trip are not large enough to be objectionable from a safety point of view. This discussion also applies to the LPCI system.

C. Reliability - The reliability of the control system is compatible with the controlled equipment so that the overall system reliability is not limited by the controls.

D. Action over the full range of environmental conditions - Refer to Section 3.11 for information on the current environmental qualification program. Specific environmental requirements evaluated for IEEE 279-1968 compliance include power supply voltage and frequency, temperature, humidity, pressure, vibration, malfunctions, accidents, fires, explosions, missiles, lightning, floods, earthquakes, high winds and tornados, system response time and accuracies, and abnormal ranges of sensed variables. This discussion also applies to the LPCI system.

The core spray system, as designed, complies with all points of Paragraph 4.1 of IEEE 279-1968, except for explosion, which is not defined in the design bases.

7.3.1.1.1.2 Single-Failure Criterion

The core spray system, which is comprised of two independent sets of controls for the two physically separate pumping systems, meets all credible aspects of the single-failure criterion (IEEE 279-1968, Paragraph 4.2).

7.3.1.1.1.3 Quality of Components

Components used in the core spray control system have been carefully selected on the basis of suitability for their specific application. All of the sensors and logic

relays are of the same types used in the reactor protection system (RPS) described in Section 7.2. Ratings have been selected with sufficient conservatism to insure against significant deterioration during anticipated duty over the lifetime of the plant (IEEE 279-1968, Paragraph 4.3).

7.3.1.1.1.4 Equipment Qualification

No components of the core spray or LPCI control system are required to operate in the drywell environment except for a portion of the reference legs for the vessel level transmitter. Dresden emergency operating procedures provide guidance and limitations on the level instruments during elevated drywell temperature. All sensory equipment is located in the reactor building outside the drywell and is capable of accurate operation even with wider swings in ambient temperature than those which result from normal or abnormal conditions (loss of ventilation and loss-of-coolant accident [LOCA]). The reactor vessel level sensors also provide input to the ATWS and are environmentally qualified.

All components used in the core spray control system have demonstrated reliable operation in similar nuclear power plant protection systems or industrial applications (IEEE 279-1968, Paragraph 4.4).

7.3.1.1.1.5 Channel Integrity

The core spray control system is designed to tolerate the spectrum of failures listed under general requirements (Section 7.3.1.1.1.1) and the single-failure criterion (Section 7.3.1.1.1.2); therefore, it satisfies the channel integrity objectives (IEEE 279-1968, Paragraph 4.5). Each of the two core spray loop sensors are backed up by sensors from the other loop so that neither system loses its integrity due to a failure or failures in its sensory equipment.

The core spray system control backup has been achieved without compromising the integrity of the channel being backed up. Analysis shows that complete destruction of a wireway (conduit) carrying wires between the two relay cabinets cannot prevent operation of both core spray loops. During a design basis accident, the control system environment does not differ significantly from normal.

7.3.1.1.1.6 Channel Independence

Channel independence of the sensors for each variable is provided by electrical isolation and mechanical separation (IEEE 279-1968, Paragraph 4.6). The A and C transmitters for the reactor vessel level are located on separate local instrument racks (identified as Division I equipment), and the B and D transmitters for reactor vessel level are located on separate local instrument racks (identified as Division II equipment) widely separated from the A and C local instrument racks. The A and C sensors have a common process tap which is widely separated from the corresponding tap for sensors B and D. Disabling of one or both sensors

at one location does not disable the control for either of the two core spray loops or two separate divisions of LPCI.

Relay cabinets for core spray system A are in a separate physical division from those for core spray system B. Likewise, relay cabinets for LPCI Division I are in a separate physical division from those for LPCI Division II. Each division is complete in itself, having its own station battery control, power distribution buses, and motor control centers. The divisional split is carried all the way from the process taps to the final control element. The split includes both control and motive power supplies.

7.3.1.1.1.7 Control and Protection Interaction

The core spray and LPCI systems are strictly on/off systems, and no signal whose failure could cause a need for core spray or LPCI can also prevent them from starting (IEEE 279-1968, Paragraph 4.7). Annunciator circuits using contacts of sensor relays and logic relays cannot impair the operability of system control due to the electrical separation between controls of the two core spray loops or the two LPCI divisions.

7.3.1.1.1.8 Derivation of System Inputs

The inputs which start the core spray and LPCI systems are direct measures of the variables that indicate the need for low pressure core cooling; reactor vessel low water, high drywell pressure, and reactor low pressure (IEEE 279-1968, Paragraph 4.8). Reactor vessel level is sensed by vessel water level transmitters. Drywell high pressure is sensed by nonindicating pressure switches on four separate sensing lines connected to two separate penetrations. Each sensing line has its own root valve, and each pressure switch has its own instrument valve. Two reactor vessel pressure switches for the low-pressure injection valve opening permissive are on two separate instrument lines going through the drywell at two different locations (the A line in one location and the B line in a separate location). The reactor vessel pressure switches operate relays whose contacts are connected in A and B logic for the core spray and LPCI valve opening permissives.

7.3.1.1.1.9 Capability for Sensor Checks

All sensors are pressure-sensing-type sensors and are installed with calibration taps and instrument valves to permit testing during normal plant operation or during shutdown (IEEE 279-1968, Paragraph 4.9). This discussion also applies to the LPCI system.

7.3.1.1.1.10 Capability for Test and Calibration

The core spray and LPCI control systems are capable of being completely tested during normal plant operation to verify that each element of the system, active or

passive, is capable of performing its intended function (IEEE 279-1968, Paragraph 4.10).

7.3.1.1.1.11 Channel Bypass or Removal from Operation

Calibration of any sensor introduces a single instrument channel trip. This trip does not cause a protective function without coincident operation of a second channel. Removal of an instrument channel from service during calibration is brief and in compliance with a special provision of IEEE 279-1968, Paragraph 4.11, for one-out-of-two-twice systems. This discussion also applies to the LPCI system.

7.3.1.1.1.12 Operating Bypasses

Manual Bypass

Access to switchgear, motor control centers and instrument valves is controlled as discussed in Section 7.3.1.1.1.14. Access to other means of bypassing are in the main control room and therefore under the direct supervision of the control room operator (IEEE279-1968, Paragraph 4.12). For example, the core spray (CS) pumps can be prevented from automatically starting upon a CS initiation signal if both of the main control board CS pump control switches are placed in the "Pull to Lock" position.

Automatic Bypasses

None.

7.3.1.1.1.13 Indication of Bypasses

There are no automatic bypasses of any part of the core spray or LPCI control systems, but manual bypassing of high drywell pressure inputs is permitted in order to purge the drywell as required. This bypass is annunciated (IEEE 279-1968, Paragraph 4.13). Deliberate opening of a valve motor breaker gives indication in the control room because both valve position lights would be deenergized.

7.3.1.1.1.14 Access to Means for Bypassing

Access to switchgear, motor control centers, and instrument valves is procedurally controlled. This discussion also applies to the LPCI system.

7.3.1.1.1.15 Multiple Trip Settings

Paragraph 4.15 of IEEE 279-1968, which deals with multiple trip settings, is not applicable because all setpoints are unique.

7.3.1.1.1.16 Completion of Protection Action Once Initiated

The final control elements for the core spray system are essentially bistable; that is, pump breakers stay closed without control power, and motor-operated valves stay open once they have reached their open position, even though the motor starter drops out when the valve open limit switch is reached. In the event of an interruption in ac power, the control system will reset itself and recycle on

restoration of power. Thus, protective action once initiated must go to completion or continue until terminated by deliberate operator action (IEEE 279-1968, Paragraph 4.16). This discussion also applies to the LPCI system.

7.3.1.1.1.17 Manual Actuation

Each piece of core spray actuation equipment (pump, valve, breaker, or starter) is capable of individual manual initiation, electrically from the control panel in the main control room and locally, if desired, by use of physical mechanisms (IEEE 279-1968, Paragraph 4.17). The valves have handwheels for manual operation, and the switchgear is capable of having the closing springs charged manually and the breaker closed by mechanical linkages on the switchgear.

In no event can failure of an automatic control circuit for one core spray loop disable the manual electrical control circuit for the other core spray loop. Single electrical failures cannot disable manual electric control of the core spray function.

7.3.1.1.1.18 Access to Setpoint Adjustments

Setpoint adjustments for the core spray and LPCI system reactor level signals are located on the slave trip units in the ATWS cabinets. A card file locking bar prevents unauthorized access to the setpoint adjustments. Test points are incorporated into the control relay cabinets which are located in limited access areas. The range of the drywell and reactor vessel pressure switches is not adjustable. The reactor vessel level transmitters have zero and span adjustments that are external to the transmitters but require removal of the nameplate. Because of these restrictions, compliance with the access requirements of IEEE 279-1968, Paragraph 4.18, is considered complete.

7.3.1.1.1.19 Identification of Protective Actions

Protective actions (Here interpreted to mean an action initiated by the protection system when a limit is exceeded) are directly indicated and identified by action of the sensor relay, which has an identification tag. Any one of the sensor relays actuates an annunciator, so no single-channel trip (relay pickup) can go unnoticed. This verification of relay actuation fulfills the requirements of IEEE 270-1968, Paragraph 4.19. This discussion also applies to the LPCI system.

7.3.1.1.1.20 Information Readout

The core spray and LPCI control systems are designed to provide the operator with accurate and timely information pertinent to its status. It does not introduce signals into other systems that could cause anomalous indications confusing to the

operator. There are many elements, both active and passive, of this energize-to-operate system which are not continuously monitored for operability. Two examples are: 1) circuits which are normally open and are not monitored for continuity on a continuous basis, and 2) pressure and level sensors, which although continuously active, are not continuously exercised and verified as operable. Verifying the operability of these components is accomplished by periodic testing and by proper selection of test periods to be compatible with the historically established reliability of the components tested. Sufficient information is provided on a continuous basis so that the operator can have a high degree of confidence that the core spray function is available and operating properly (IEEE 279-1968, paragraph 4.20).

7.3.1.1.1.21 System Repair

The core spray and LPCI control systems are designed to avoid a need for repair rather than to accommodate quick replacement of components. Thus, reliability is built-in rather than approached by rapid return-to-service maintenance (IEEE 279-1968, Paragraph 4.21). All devices in the system are designed for a 40-year lifetime under the imposed duty cycles. Since this duty cycle is composed mainly of periodic testing rather than operation, lifetime is more a matter of shelf life than active life. However, all components are selected for continuous duty plus thousands of cycles of operation, far beyond the usage anticipated in actual service. The pump breakers are an exception because they do not support the same large number of operating cycles. Nevertheless, even these breakers should not require contact replacement within 40 years, assuming periodic pump starts every 3 months.

7.3.1.1.2 Failure Mode and Effects Summary

No single component, cable, wireway, or cabinet failure can disable the core spray function. Therefore, the core spray system is considered to have fully met the single-failure criterion of IEEE 279-1968.

7.3.1.2 Low Pressure Coolant Injection Instrumentation and Control

7.3.1.2.1 Low Pressure Coolant Injection Initiation and Interlocks

The low pressure coolant injection system can be operated in two modes: LPCI injection and containment cooling. The LPCI mode instrumentation and controls are described in this section while the remainder of the LPCI mode is described in Section 6.3. Containment cooling is addressed in Section 6.2.2, and its logic is described in Section 7.4.

In general, LPCI operation involves restoring and maintaining sufficient reactor vessel water level for adequate core cooling after a LOCA. The LPCI logic system operates in conjunction with HPCI, ADS, and core spray logic.

The LPCI system is automatically actuated by the same signals and trip logic as described for the core spray system. These signals are generated by the following sensors:

A. Four independent high drywell pressure switches;

B. Four independent low-low reactor water level transmitters and trip units; and

C. Two independent low reactor pressure switches.

The LPCI initiation signal requires one of the following logic conditions:

A. High drywell pressure (one-out-of-two-twice).

B. Low-low reactor level (one-out-of-two-twice) coincident with low reactor pressure (one-out-of-two); or

C. Low-low reactor level actuation (one-out-of-two-twice) sustained for a time not to exceed the Technical Specification of ≤ 580 seconds (one-out-of-one). This signal is generated by the ADS system logic.

Figures 7.3-2A and 7.3-2B are functional control diagrams that show various interlocks in the LPCI subsystem.

Upon receipt of an initiation signal with normal ac power available, the following actions occur:

A. Diesel generators start;

B. Permissives become available to activate pumps and valves;

C. All four LPCI pumps start and run on minimum flow until loop selection is made;

D. Pump suction valves open (if closed), valves interlock in the open position;

E. Containment cooling service water pumps stop (if running) and containment cooling heat exchanger service water outlet valves close; and

F. Necessary valves close or open (as needed) to establish the full LPCI flow. (Injection valves do not open until reactor low pressure interlock has cleared.)

The operator can, in the event of a system line break, override the automatic opening of the suction valves and close them.

If normal ac power is not available, pumps are started sequentially once the diesel generators accelerate to operating speed. See Sections 6.3 and 8.3 for additional information.

The injection valves are opened on a preset reactor low-pressure signal. The valve operation is similar to that of the valving on the core spray system. Once the injection valves open, the operator can bypass the 5-minute timer interlock logic to re-close the valves to control LPCI injection (see Figure 7.3-3). This will allow the control of reactor water level for those transients and accidents that do not require core re-flooding.

Each LPCI loop has a minimum flow valve that opens (if closed) on pump start but prior to injection valve opening and automatically closes when sufficient cooling flow is established. The valve control is based on flow through its associated loop. The LPCI minimum flow valves are interlocked with the LPCI pump breakers. By stopping or placing the LPCI pump control switch for a given loop in the PULL-TO-LOCK position, the associated minimum flow valve may be positioned in either the open or closed position by operation of its control switch even with an accident signal present. If the LPCI pump starts, the minimum flow valve will operate properly to provide a minimum flow path as required. Logic is provided which allows the LPCI pump minimum flow valves to be maintained closed from the control room to perform their closed loop isolation function as required by General Design Criteria (GDC) 57.[1] Figure 7.3-4 is a functional control diagram for the minimum flow valve.

Interlocks are provided to prevent the diversion of LPCI injection flow, if any initiating signal is present, to ensure the flooding of the core (see Section 7.4).

For the injection 1501-22A or 150-22B, the operator can override automatic logic to re-close the valve or maintain the valve close to control LPCI injection (see Figure 7.3-2A). This will allow the control of reactor water level for those transients and accidents that do not require core re-flooding.

7.3.1.2.2 Loop Selection Logic

The loop selection logic ensures that LPCI injection flow is directed to an unbroken recirculation pump loop. The operation of the logic depends on the number of operating recirculation pumps and the break location. The basic loop selection logic sequence initiated by either high drywell pressure or low-low water level is as follows (see Figure 7.3-5):

A. If either or both recirculation pump is not running, the pumping mode selector section of the logic trips both recirculation pumps and waits for reactor pressure to decrease to a meaningful differential pressure measurement (Analytical Limit: 900 to 800 psig).

B. A time delay imposes a wait for momentum effects to establish the maximum differential pressure for loop selection (Allowable Value: 2.12 seconds).

C. Four differential pressure detectors compare the pressure between riser pipes in loop A and the corresponding riser pipes in loop B. The loop selection instrumentation is shown in Figures 7.3-6 (Unit 2) and 7.3-7 (Unit 3).

D. If the loop A pressure is greater than the loop B pressure, the logic selects loop A for injection.

E. If the loop A pressure is not greater than the loop B pressure (recirculation loop A is broken or neither recirculation loop is broken), a timer runs out causing loop B to be selected for injection (Allowable Value: 0.53 seconds).

F. The logic seals in the loop selection and sends a close signal to the recirculation pump discharge valve and its suction valve for the selected loop and to the LPCI injection valve for the other loop.

G. Upon receipt of the preset reactor low-pressure signal, previously described, the selected injection valve opens. Also, as previously described, once the injection valves open, the operator can bypass the 5-minute timer interlock logic to re-close the valves to control LPCI injection (see Figure 7.3-3).

Also, as previously described, for the injection valve 1501-22A or 1501-22B, the operator can override the automatic logic to re-close or maintain the valve close to control LPCI injection (see Figure 7.3-2A).

The pumping mode selector logic uses dP instruments which measure recirculation pump ΔP to determine the number of recirculation pumps running. The taps for these instruments are as close to the pump suction and discharge as practical. The trip setting is approximately +2 psid. The trip point should be repeatable within 0.2 psid. Only positive ΔP measurement is necessary.

If both recirculation pumps are running, the ΔP across both pumps will indicate greater than 2 psid. With both pumps running, the pumps will amplify the break detection ΔP (provide the greatest break detection sensitivity); therefore, the "two pump" side of the logic is used to allow measurement of the break detection ΔP with the recirculation pumps running.

If the ΔP across either or both pumps is less than 2 psid, the timer runs out causing the network to proceed on the "one pump" side of the network (Allowable Value: 0.53 seconds).

Seal-ins on the "one pump" or "two pump" sides are required to ensure that the pump coastdown or resumption of ac power does not result in changes in the network arrangement later.

If only one recirculation pump is operating, the recirculation pump trip provided by the pumping mode selector is required to allow detection of small breaks. Circuitry on the "one pump" side of the network provides a trip signal to both recirculation pumps unless both pumps are running.

A reactor vessel pressure permissive will delay the loop selection logic initiation until reactor pressure has dropped to between the Analytical Limits of 800 and 900 psig to allow for coast down of any recirculation pump which has just been tripped. This setpoint optimizes sensitivity while ensuring that injection is not delayed unnecessarily. The trip point is adjustable over a range of reactor pressure from 500 to 1000 psig. This trip point should be repeatable within 10 psig.

After satisfying the pressure permissive or verifying that both pumps are running (indicated by ΔP greater than 2 psi), the network must wait before loop selection (Allowable Value: 2.12 seconds). [HISTORICAL: The timer is adjustable from a 0- to 10-second delay.]

The delay in the break detection circuit is provided to allow time for momentum effects to establish the maximum pressure differential for break detection. Since the flow decay time constant of the fluid in one recirculation loop excluding ASD is about 1-second, an approximately 2-second delay will assure that the momentum effects have established the maximum pressure differential for loop selection.

If loop A pressure is greater than that of loop B, then loop B is broken and injection will occur in loop A. If the loop A pressure is not greater than that of loop B, the timer will run out causing loop B to be selected (Allowable Value: 0.53 seconds). Seal-ins are required so that pump coastdown, reductions in vessel pressure, or other effects will not cause

a change in the decision later. (This could occur if the ΔP decays to within the instrument error band.)

The ΔP is measured from each of four recirculation loop riser pipes to the corresponding riser pipe on the other recirculation loop. The taps are located as close to the reactor vessel as possible. This arrangement provides a one-out-of-two-twice capability. The instrument lines are separated and protected, as much as possible, so that damage to one instrument line does not result in damage to another line. The instrument lines are as short as possible to avoid instrument delays due to the sensor piping.

For any break location in the recirculation lines, maximum recirculation flowrate provides the maximum sensitivity for break detection using the dP instruments. Therefore, small breaks in conjunction with low recirculation flowrates are the most difficult to detect. However, the size of the smallest break which must be detected increases (required sensitivity decreases) with decreasing power and recirculation flow. It has been determined that the decrease in required leak detection sensitivity more than compensates for the actual loss of sensitivity resulting from the corresponding recirculation flow reduction.

Therefore, the dP instrumentation in the LPCI break detection system is effective over the complete range of recirculation flowrates as required for LPCI injection.

The dP instruments are positive-scale-type instruments with at least one trip unit adjustable over the full range of the instrument. The instrument range is approximately +10 psi. The trip point setting is about 0.75 psi and should be repeatable within 0.1 psi. Any positive ΔP (pressure of A greater than pressure of B) would result in the selection of loop A.

If the ΔP is negative (pressure of A not greater than pressure of B), loop B would be used. The response time for full scale movement does not exceed 0.2 seconds. The instruments are not adversely affected by overpressure of either side up to the design pressure of the instrument casing. The command to inject in a given loop results in closing the recirculation pump discharge valve on that loop and opening the LPCI injection valve to that loop. Here it is assumed that the pumps are already started by high drywell pressure or low reactor water level.

7.3.1.2.3 Conformance to IEEE 279-1968

The following subsections present a point-by-point comparison of the LPCI system with the requirements of proposed IEEE 279-1968 which has been summarized from GE Topical Report, NEDO-10139.[2] For more detailed information, refer to the topical report.

The low pressure core cooling system consists of three subsystems: core spray system loop A, core spray system loop B, and the LPCI system. Therefore, it is clear that the LPCI system by itself is not required to meet all the requirements of IEEE 279-1968 since it is backed up by the two core spray loops. The following comparison is provided only to show the adequacy of the LPCI system design.

7.3.1.2.3.1 General Functional Requirement

The general functional requirement of IEEE 279-1968, Paragraph 4.1, and the provisions of the LPCI system to fulfill the requirements are summarized below:

A. Auto-initiation of appropriate action - Appropriate action for the LPCI control system is defined as the activation of equipment for introducing low-pressure water into the reactor via the recirculation line when reactor vessel level drops below a predetermined point or the drywell pressure increases above a predetermined value, and reactor vessel pressure is below the pump shutoff head. Equipment activation occurs automatically.

B. Precision - The precision requirement for the core spray system is discussed in Section 7.3.1.1.1.1; this discussion applies equally to the LPCI and core spray systems. Sensors which initiate the core spray system are the same sensors as used to initiate the LPCI system.

C. Reliability - The reliability of the control system is commensurate with the controlled equipment so that the overall system reliability is not limited by the controls.

D. Action over the full range of environmental conditions - Refer to Section 3.11 for information on the current environmental qualification program. See Section 7.3.1.1.1.1 for the specific environmental requirements evaluated for IEEE 279-1968 compliance.

7.3.1.2.3.2 Single-Failure Criterion

The LPCI system is comprised of two loops with separate suction and discharge piping. One LPCI loop contains the LPCI A and B pumps discharging to the reactor recirculation A-train inlet header, and the other loop contains the LPCI C and D pumps discharging to the reactor recirculation B-train inlet header. The two LPCI loops are normally cross-tied. Redundancy in equipment and control logic is provided so that it is unlikely that the LPCI system could be rendered inoperative (IEEE 279-1968, Paragraph 4.2).

Two control logic circuits are provided. Control logic A is provided to initiate loop A pumps and valves and logic B is provided to initiate loop B equipment. The LPCI initiation logic is separate from the LPCI loop selection logic for controlling the injection valves.

Tolerance to single failures or events is provided in the control logic initiation circuitry so that failures will be limited to the possible disabling of the initiation of only one loop (two of four pumps available).

The LPCI system is designed to detect the location of a recirculation line break and to select the unbroken loop for injection. The sensing circuit for break detection and valve selection is arranged so that failure of a single device or circuit to function on demand will not prevent selection of the correct loop for injection. Tolerance to the following single failures or events has been incorporated into the loop selection control system design:

A. Single open circuit,

B. Single relay failure to pickup,

C. Single relay failure to dropout,

D. Single instrument failure, and

E. Single control power failure.

Reliability of the control system is compatible with and more reliable than the controlled equipment (injection valve). Single failures which could cause improper loop selection (i.e., selected short circuits which pickup specific relays) will not disable the core spray function. Therefore, failure of the loop selection scheme to fully comply with the single-failure criterion of IEEE 279-1968, Paragraph 4.2, does not constitute a violation of IEEE 279-1968 insofar as the low-pressure cooling function is concerned.

7.3.1.2.3.3 Quality of Components

The discussion of component capability for the core spray system (Section 7.3.1.1.1.3) also applies generally to the LPCI system.

7.3.1.2.3.4 Equipment Qualification

The discussion of equipment qualification for the core spray system (Section 7.3.1.1.1.4) also applies to the LPCI system.

7.3.1.2.3.5 Channel Integrity

The LPCI system initiation channels (low water level or high drywell pressure) are designed to meet the single-failure criterion (as discussed in Section 7.3.1.2.3.2). Therefore, they satisfy the channel integrity objective of IEEE 279-1968, Paragraph 4.5.

The LPCI logic backup has been achieved without compromising the integrity of the channel being backed up. Analysis shows that a complete destruction of a wireway (conduit) carrying wires between the two relay panels can do no more than introduce a ground on one side of the dc control bus; it will not prevent operation of either logic circuit.

The instrumentation provided for the loop selection logic does not initiate a protective action; therefore IEEE 279-1968 Paragraph 4.5 does not strictly apply to this instrumentation. However, as previously described, redundancy in instrumentation and control logic circuits has been provided so that it is extremely unlikely that a failure within this functional logic will prevent proper LPCI operation.

7.3.1.2.3.6 Channel Independence

The discussion of channel independence of the core spray system (Section 7.3.1.1.1.6) also applies to the LPCI system. By definition (IEEE 279-1968, Paragraph 2.2), a channel loses its identity where single action signals are combined. Therefore, since instrument channels are combined into a pair of single logic channel trip systems, IEEE 279-1968, Paragraph 4.6 does not strictly apply for the loop selection logic.

7.3.1.2.3.7 Control and Protection Interaction

The discussion of control protection and interaction for the core spray system (Section 7.3.1.1.1.7) also applies to the LPCI system.

7.3.1.2.3.8 Derivation of System Inputs

The discussion of derivation of system inputs for the core spray system (Section 7.3.1.1.1.8) also applies to the LPCI system. The inputs provided to determine which loop should be used for LPCI injection are direct measures of the variables required to make this decision (IEEE 279-1968, Paragraph 4.8).

7.3.1.2.3.9 Capability for Sensor Checks

The discussion of sensor checks for the core spray system (Section 7.3.1.1.1.9) also applies to the LPCI system.

7.3.1.2.3.10 Capability for Test and Calibration

The discussion of test and calibration capability for the core spray system (Section 7.3.1.1.1.10) also applies to the LPCI system. The only portion of the LPCI logic which cannot be tested with the reactor at full power is the recirculation pump trip portion of the loop selection logic (IEEE 279-1968, Paragraph 4.10).

7.3.1.2.3.11 Channel Bypass or Removal from Operation

The discussion of channel bypass for the core spray system (Section 7.3.1.1.1.11) also applies to the LPCI system.

7.3.1.2.3.12 Operating Bypasses

Manual Bypass

Access to switchgear, motor control centers and instrument valves is controlled as discussed in Section 7.3.1.2.3.14. Access to other means of bypassing are in the main control room and therefore under the direct supervision of the control room operator (IEEE 279-1968, Paragraph 4.12). For example, the four LPCI pumps can be prevented from automatically starting upon a LPCI initiation signal if all four main control board LPCI pump control switches are placed in the "Pull to Lock" position.

Automatic Bypasses

None

7.3.1.2.3.13 Indication of Bypasses

The discussion of indication of bypasses for the core spray system (Section 7.3.1.1.1.13) also applies to the LPCI system.

7.3.1.2.3.14 Access to Means for Bypassing

Access to switchgear, motor control centers, and instrument valves is controlled as discussed in Section 7.3.1.1.1.14. Access to other means of bypassing (i.e., closure of pump suction valves by means of a control switch) are located in the main control room and, therefore, under the administrative control of the operator (IEEE 279-1968, Paragraph 4.14).

7.3.1.2.3.15 Multiple Trip Settings

IEEE 279-1968, Paragraph 4.15, which deals with multiple trip settings, is not applicable because all setpoints are unique.

7.3.1.2.3.16 Completion of Protection Action Once Initiated

The discussion of completion of protective action for the core spray system (Section 7.3.1.1.1.16) also applies to the LPCI system.

7.3.1.2.3.17 Manual Actuation

Each piece of LPCI actuation equipment required to operate (pumps and valves) is capable of manual initiation electrically from the control panel in the main control room (IEEE 279-1968, Paragraph 4.17).

7.3.1.2.3.18 Access to Setpoint Adjustments

The discussion of setpoint adjustments for the core spray system (Section 7.3.1.1.1.18) also applies to the LPCI system.

7.3.1.2.3.19 Identification of Protective Actions

The discussion of identification of protective actions for the core spray (Section 7.3.1.1.1.19) also applies to the LPCI system.

7.3.1.2.3.20 Information Readout

Sufficient information is provided on a continuous basis so that the operator can have a high degree of confidence that the LPCI function is available and/or operating properly (IEEE 279-1968, paragraph 4.20).

7.3.1.2.3.21 System Repair

The discussion of system repair for the core spray system (Section 7.3.1.1.1.21) also applies to the LPCI system.

7.3.1.2.4 Failure Mode and Effects Summary

Since the LPCI system is by itself a single system and, as such, vulnerable to single failures in common components, a detailed failure mode and effects analysis is not presented here. No single component, cable, wireway, or cabinet failure can disable the LPCI injection function of the system except the injection valves and specific portions of the loop selection circuitry. Those single failures that could possibly disable the LPCI system will not directly affect the core spray system. The low-pressure core cooling system is designed such that for any single failure the availability of two core spray loops or one core spray loop and two LPCI pumps will be maintained.

7.3.1.3 High Pressure Coolant Injection System Instrumentation and Control

7.3.1.3.1 Initiation and Interlocks

The HPCI subsystem is designed to pump water into the reactor under LOCA conditions which do not result in rapid depressurization of the pressure vessel. The loss of coolant might be due to a loss of reactor feedwater or to a small line break which does not cause immediate depressurization of the reactor vessel.

Automatic initiation of the HPCI system occurs on low-low reactor water level or high drywell pressure. Low-low reactor water level and high drywell pressure are detected by four independent level transmitters and pressure switches connected in one-out-of-two-twice logic arrays. When the initiation signal is received, the HPCI turbine and its required auxiliary equipment starts automatically and the required valves reposition automatically. The HPCI injection valve opens after the HPCI pump discharge pressure reaches a preset value to prevent steam flashing and water hammer. A HPCI system initiation pushbutton is provided in the control room for rapid single action manual system initiation. Figures 7.3-8A, 7.3-8B and 7.3-8C are functional control diagrams of the HPCI system.

A minimum flow bypass valve which is provided for pump protection is automatically opened on low pump flow and closed on high flow whenever the steam supply valve to the turbine is open. Placing the minimum flow valve control switch in the PULL-TO-LOCK position closes the minimum flow valve under any

system condition. The position of the minimum flow valve PULL-TO-LOCK switch is administratively controlled by station procedures.

In the event of low water level in the condensate storage tank or high water level in the suppression pool, whichever comes first, the pump suction valves from the suppression chamber open and the suction valves from the condensate storage tank close. The valves are interlocked to prevent opening the valves from the condensate storage tank whenever both valves from the suppression chamber are fully open.

Automatic isolation of the HPCI system is discussed in Section 7.3.2.

HPCI turbine stop valve closure will occur upon receipt of any of the following signals:

A. Turbine overspeed trip - A spring-loaded mechanical-type plunger, located in a housing threaded to the high pressure end of the turbine shaft. In the event the turbine overspeeds, the overspeed trip operates to actuate the emergency tripping mechanism closing the stop valve to shut off steam flow to the turbine. The plunger's center of gravity is off the axis of rotation in a direction which results in centrifugal forces tending to unseat the plunger. A retaining spring is factory-adjusted to hold the plunger on its seat up to the desired tripping speed when the centrifugal force will overcome the spring force and unseat the plunger. This occurs in a small fraction of a revolution. The plunger strikes the emergency trip mechanism actuating trigger thereby tripping the turbine. The device automatically resets when shaft speed has reduced approximately 20% from the trip setpoint.

B. Low pump suction pressure - A single pressure switch is used to detect excessive vacuum conditions at the pump suction, i.e., provide pump protection in the event of lost suction. (This trip is bypassed during automatic initiation of HPCI.)

C. High turbine exhaust pressure - Two pressure switches, connected in one-out-of-two logic, protect the turbine casing from overpressure without relying on the pressure relief system logic. This trip is initiated at a pressure of 100 psig (assuming flashing steam flow through the turbine with a locked rotor, it would be possible to obtain this high pressure condition).

D. Reactor vessel high water level - Two level sensors, connected in series logic, shutdown the HPCI subsystem when water inventory is normal.

There are no provisions for overriding any signals which shut down the HPCI subsystem. For those signals which have seal-in logic, the operator may reset the logic at any time after the signal clears. If the shutdown signal is no longer present, the HPCI subsystem is capable of auto-restart upon receipt of an initiation signal.

Numerous combinations of instrumentation logic have been used for the automatic signals and the turbine trip signals for the HPCI system. The justification for the differences in logic used follows:

A. The design is such that no single failure will result in a breach of the primary containment pressure integrity.

B. Where there is a high probability of spurious signals (e.g., for the steam leak detection system), the full complement of instrumentation has been selected and connected in one-out-of-two-twice logic.

C. Where trip signals are employed for equipment protection, single or double instrumentation has been used for simplicity and economics. In these instances, there is a low probability that the instrument failure would prevent system operation.

D. Finally, it must be noted that the single-failure criterion has not been used as a design basis for the HPCI system. The ADS is its backup.

7.3.1.3.2 HPCI Turbine Control Logic

The HPCI turbine control logic consists of three major components for speed control:

A. Speed governor - A mechanical flyball device which positions the valve portion of a primary pilot valve and bushing assembly. The speed governor serves a twofold function: speed setting in response to the other components of the turbine control logic and speed limiting by providing physical stops on the allowable movement of the primary pilot valve bushing. The speed governor is capable of limiting turbine speed to 4000 rpm.

B. Motor speed changer (MSC) - A remote manual speed control device covering a speed range from 0 to 4000 rpm. The MSC is automatically returned to its low speed stop (LSS) whenever the turbine stop valve is tripped. The function of the MSC is twofold: to prevent opening the turbine control valves until the stop valve is fully open and to provide for controlled startup of the turbine.

C. Motor gear unit (MGU) - An automatic speed control device covering a speed range from 2000 to 4000 rpm, the required range for HPCI system operation. The MGU is automatically positioned by the output signal from the flow controller. This control logic is essentially identical to that used for control of turbine-driven feed pump systems.

When the HPCI turbine is in the standby condition, the MGU is above the MSC speed, preferably at its high-speed stop (4000 rpm), receiving a maximum demand signal from the flow controller since flow is zero. The MSC is at its low-speed stop (0 rpm) since the stop valve is closed. The turbine control valves are closed since the MSC is at its low-speed stop. The turbine stop valve is closed, with no hydraulic pressure.

When an initiation signal is received, the following actions occur:

A. The auxiliary oil pump is automatically started, and the stop valve reset solenoid is automatically energized.

B. Hydraulic oil pressure develops, opening the turbine stop valve with closed control valves. The MSC is at the (LSS).

C. Once the stop valve is fully open, the MSC automatically runs to the high speed stop at high speed.

D. The turbine control valves open at their maximum rate (MGU at its high-speed stop), accelerating the turbine.

E. The turbine speed is initially limited to slightly higher than 4000 rpm by the turbine speed governor. The MSC controls the rate of turbine acceleration.

F. Once pump discharge flow reaches its preset value, the output from the flow controller diminishes, and the MGU is ultimately reset below the limiting value of the speed governor, thereby controlling turbine speed. The pump discharge flow controller continues to adjust the MGU, changing the turbine speed setpoint as required to maintain the preset flow requirement over the range of HPCI operation (i.e., 4000 rpm down to approximately 2000 rpm). HPCI flowrate is dependent on steam flow available from the reactor.

Under normal operation, the turbine control valves are operated by the MGU to automatically maintain an injection flowrate determined by a flow indicating controller (FIC). The signal generated by the FIC is compared to the actual HPCI flow as determined by a flow transmitter. The resulting signal is applied to the signal converter which drives the MGU to properly position the turbine control valve through a series of mechanical and hydraulic linkages. A position signal corresponding to the MGU speed setting is also applied to the signal converter to stabilize its output. The MGU is also operable from a control room manual RAISE-LOWER control switch. In addition, a local handwheel provides manual speed control in the event of control circuit failure or burned-out MGU motor.

The MGU can be operated automatically or manually. Each mode has its own power source.

The HPCI MGU electrical controls transfer the dc power from the manual mode (control switch) to the automatic flow control mode (HPCI pump flow control signal converter) without electrically connecting the two sources. This prevents any ground in the automatic controls from being connected to the ungrounded battery systems.

The turbine speed is controlled by the lowest setting of the preceding components:

A. Limited to 4000 rpm by the speed governor (with MSC at the high speed stop).

B. Automatically controlled between 2000 and 4000 rpm by the MGU.

C. Manually controlled between 0 and 4000 rpm by the MSC. It should be noted that below 2000 rpm, turbine speed is maintained by control valve position only, i.e., there is no speed setting feedback from the speed governor due to the sizing of the primary pilot valve and the inertia of the flyball system.

7.3.1.3.3 Conformance with IEEE 279-1968

The following subsections present a point-by-point comparison of the HPCI system with the requirements of IEEE 279-1968 which has been summarized from GE Topical Report NEDO-10139.[2] The automatic depressurization system is provided to reduce reactor pressure in case the HPCI system is not sufficient to maintain the reactor water level, thereby allowing use of low pressure systems (CS, LPCI). Therefore, it is clear that the HPCI system is not required to meet all the requirements of IEEE 279-1968 since it is backed up by the independent ADS. The following comparison is provided only to show the adequacy of HPCI system design. For more detailed information, refer to the topical report.

7.3.1.3.3.1 General Functional Requirements

The general functional requirements of IEEE 279-1968, Paragraph 4.1, and the provisions of the HPCI system to fulfill the requirements are summarized below:

A. Auto-Initiation of Appropriate Action - Appropriate action for the HPCI control system is defined as the activation of equipment for introducing high-pressure water into the reactor via the feedwater line when reactor vessel level drops below a predetermined point or the drywell pressure increases above a predetermined value. Equipment actuation occurs automatically.

B. Precision - The process sensor equipment will initiate action before process variables exceed precisely established limits. In the case of vessel level sensors, the HPCI system water level initiation point is near the mid-range of the level thereby making the instrument trip point relatively independent of vessel pressure or drywell ambient temperature. Dresden operating procedures provide guidance and limitations on the level instrumentation during elevated drywell temperature conditions.

C. Reliability - The reliability of the control system is compatible with the controlled equipment so that the overall system reliability is not limited by the controls.

D. Action over the full range of environmental conditions - Refer to Section 3.11 for information on the current environmental qualification program. See Section 7.3.1.1.1.1 for the specific environmental requirements evaluated for IEEE 279-1968 compliance.

7.3.1.3.3.2 Single-Failure Criterion

The HPCI system, by itself, is not required to meet the single-failure criterion (IEEE 279-1968, Paragraph 4.2). The control logic circuits for the HPCI system initiation and control are housed in several relay cabinets and the power supply for most HPCI equipment is from a single dc power source. However, the relay cabinet and normal power source for ADS are independent of the HPCI system.

The HPCI initiation sensors and wiring up to the HPCI relay logic cabinet do, however, meet the single-failure criterion. Physical separation of instrument lines is provided so that no single instrument rack destruction or single instrument line (pipe) failure can prevent HPCI initiation. Wiring separation between divisions also provides tolerance to single wireway destruction (including shorts, opens, and grounds) in the accident detection portion of the control logic. This single-failure criterion is not applied to logic relay cabinet or to other equipment required to function for HPCI operation.

7.3.1.3.3.3 Quality of Components

The discussion of equipment qualification for the core spray system (Section 7.3.1.1.1.3) also applies generally to the HPCI system.

7.3.1.3.3.4 Equipment Qualification

No components of the HPCI control system are required to operate in the drywell environment except for a portion of the reference legs for the vessel level transmitters. Errors introduced under steam leak (high drywell temperature and reactor depressurization) for HPCI initiation are evaluated in Dresden level instrument setpoint error analysis calculations. The HPCI steam line isolation valve located inside the drywell is a normally open valve and is therefore not required to operate except for primary containment isolation (Group IV).

Other process sensor equipment for HPCI initiation is located in the reactor building and is capable of accurate operation in ambient temperature conditions that result from abnormal conditions (loss of ventilation and LOCA), IEEE 279-1968, Paragraph 4.4.

7.3.1.3.3.5 Channel Integrity

The HPCI system instrument initiation channels meet the single-failure criterion (as discussed in Section 7.3.1.3.3.2). Therefore, they satisfy the channel integrity objective of IEEE 279-1968, Paragraph 4.5.

By definition (IEEE 279-1968, Paragraph 2.2) a channel loses its identity where single action signals are combined. Therefore, since instrument channels are combined into a single trip system, IEEE 279-1968, Paragraph 4.5 does not strictly apply for the HPCI control system.

7.3.1.3.3.6 Channel Independence

Channel independence for initiation sensors monitoring each variable is provided by electrical and mechanical separation (IEEE 279-1968, Paragraph 4.6). The A and C transmitters for the reactor vessel level are located on separate local instrument racks (identified as Division I equipment), and the B and D transmitters for reactor vessel level are located on separate local instrument racks (identified as Division II equipment) widely separated from the A and C local instrument racks The A and C sensors have a common pair of process taps which are widely separated from the corresponding taps for sensors B and D. Disabling of one or both sensors in one location does not disable the control for HPCI initiation.

7.3.1.3.3.7 Control and Protection Interaction

The discussion of control protection and interaction for the core spray system (Section 7.3.1.1.1.7) also applies to the HPCI system.

7.3.1.3.3.8 Derivation of System Inputs

The inputs that start the HPCI system are direct measures of the variables that indicate need for high pressure core cooling, such as reactor vessel low water level or high drywell pressure (IEEE 279-1968, Paragraph 4.8).

7.3.1.3.3.9 Capability for Sensor Checks

The discussion of sensor checks for the core spray system (Section 7.3.1.1.1.9) also applies to the HPCI system.

7.3.1.3.3.10 Capability for Test and Calibration

The discussion of test and calibration capability for the core spray system (Section 7.3.1.1.1.10) also applies to the HPCI system.

7.3.1.3.3.11 Channel Bypass or Removal from Operation

Calibration of any sensor introduces a single instrument channel trip. This trip does not cause a protective function without the coincident trip of a second channel. There are no instrument channel bypasses as such in the HPCI system. Removal

of a sensor from operation during calibration does not prevent the redundant instrument channel from functioning if accident conditions occur. The time required for removal of an instrument channel from service during calibration is brief (IEEE 279-1968, Paragraph 4.11).

7.3.1.3.3.12 Operating Bypasses

Manual Bypasses

The HPCI system can be manually bypassed by switching the flow controller from AUTO to MANUAL operation in the main control room or adjusting AUTO operation. The controller is in the main control room and therefore under the direct supervision of the control room operator (IEEE 279-1968, Paragraph 4.12).

Automatic Bypasses

The following is a list of automatic bypasses which can render the HPCI system inoperative (IEEE 279-1968, Paragraph 4.12):

A. HPCI steam line isolation signal.

B. The following signals cause a HPCI turbine trip irrespective of an initiation:

   1. HPCI turbine exhaust pressure high,

   2. Reactor vessel water level high,

   3. HPCI turbine overspeed, or

C. HPCI pump suction pressure low when no initiation signal is present.

7.3.1.3.3.13 Indication of Bypasses

Indication of bypasses provided is as previously discussed in Section 7.3.1.3.3.12 above.

7.3.1.3.3.14 Access to Means for Bypassing

Access to switchgear, motor control centers, and instrument valves is procedurally controlled. Access to other means of bypass are located in the main control room and are, therefore, under administrative control (IEEE 279-1968, Paragraph 4.14).

7.3.1.3.3.15 Multiple Trip Settings

IEEE 279-1968, Paragraph 4.15, which deals with multiple trip settings, is not applicable because all setpoints are unique.

7.3.1.3.3.16 Completion of Protective Action Once Initiated

The final control elements for the HPCI system are essentially bistable; that is, a motor-operated valve stays open or closed once it has reached the desired position, even though its starter drops out when the limit switch is reached. In the case of pump starts, the auto-initiation signal will open the turbine steam supply and pump suction/discharge motor operated valves which are sealed in by their individual open/closed circuits.

Thus a protective action once initiated (e.g., flow established) must go to completion or continue until terminated by deliberate operator action or until it is automatically stopped on high vessel water level or system malfunction trip signals (IEEE 279-1968, Paragraph 4.16).

7.3.1.3.3.17 Manual Actuation

Each piece of HPCI actuation equipment required to operate (pump or valve) is capable of manual initiation electrically from the control panel in the main control room (IEEE 279-1968, Paragraph 4.17). Failure of logic circuitry to initiate the HPCI system will not affect the manual control of equipment.

However, failures of active components or control circuit failures which produce a turbine trip may disable the manual actuation of the HPCI system. Failures of this type are continuously monitored by alarms and as such cannot realistically be expected to occur when HPCI operation is required.

7.3.1.3.3.18 Access to Setpoint Adjustments

The discussion of setpoint adjustments for the core spray system (Section 7.3.1.1.1.18) also applies to the HPCI system.

The only adjustable setpoints provided in the HPCI system are those provided on the flow controller on the main control room panel. Adjustable setpoints are administratively controlled (IEEE 279-1968, Paragraph 4.18).

7.3.1.3.3.19 Identification of Protective Actions

Protective actions (here interpreted to mean pickup of a single sensor relay) are directly indicated and identified by action of the sensor relay which has an identification tag and a clear glass window front which permits convenient visible verification of the relay position. A sensor trip also actuates an annunciator so no single channel trip (relay pickup) can go unnoticed. This combination of

annunciation and visible relay actuation is considered to fulfill the requirements of IEEE 279-1968, Paragraph 4.19.

7.3.1.3.3.20 Information Readout

The HPCI control system is designed to provide the operator with accurate and timely information pertinent to its status. It does not introduce signals into other systems that could cause anomalous indications confusing to the operator. There are many elements of this energize-to-operate system, both active and passive, which are not continuously monitored for operability. Two examples are: 1) relay circuits which are normally open and are not monitored for continuity on a continuous basis, and 2) pressure and level sensors, which although continuously active are not continuously exercised and verified operable. Verifying the operability of these components is accomplished by periodic testing and by proper selection of test periods to be compatible with the historically established reliability of the components tested. Complete and timely indications are made available. Sufficient information is provided on a continuous basis so that the operator can have a high degree of confidence that the HPCI function is available and/or operating properly (IEEE 279-1968, Paragraph 4.20).

7.3.1.3.3.21 System Repair

The discussion of system repair for the core spray system (Section 7.3.1.1.1.21) applies equally to the HPCI system.

In addition to the recognition of failed components during test, components which fail so as to produce a trip condition are continuously monitored by alarm (IEEE 279-1968, Paragraph 4.21.

7.3.1.3.4 Failure Mode and Effects Summary

Since the HPCI system is by itself a single system, and as it is recognized that there are single failures that could disable the system, a detailed failure mode and effects analysis is not warranted.

No single failure in the initiation instrumentation can prevent HPCI operation if required. Again, those single failures that could possibly disable the HPCI system will in no way affect the ADS system and vice versa.

The only instrumentation and equipment common to the ADS and HPCI systems are the reactor vessel water level transmitters. Separate trip units on the shared transmitters are used for the two systems. Both physical and electrical separation are maintained so that no single failure of the level-sensing equipment or wiring (shorts or opens) can disable either HPCI or ADS.

Therefore, it is concluded that no single failure can disable both the HPCI and the ADS systems.

7.3.1.4 Automatic Depressurization System Instrumentation and Control

The automatic depressurization system is designed to depressurize the reactor to permit either the LPCI or core spray systems to cool the reactor core during a small break LOCA. As such it provides a backup for the HPCI system. Reactor vessel depressurization is accomplished by blowdown through the relief valves to vent steam to the suppression pool.

The ADS is initiated by instrumentation which monitors reactor vessel level and drywell pressure. Automatic actuation requires coincident indication of reactor water low-low level and drywell high pressure which is maintained for a period of 2 minutes. Each of these circuits is connected in a one-out-of-two-logic arrangement to provide redundancy. In addition, the design prevents blowdown until the discharge pressure of at least one LPCI pump or one core spray pump exceeds 100 psig. This design provides direct assurance that the low-pressure ECCS pumps are operating prior to automatic depressurization.

Four instrument channels monitor each initiating parameter. Two of the four channels monitoring each parameter are assigned to one-out-of-two logic divisions. The arrangement of these signals within each logic division is two-out-of-two (high pressure and low-low level) in coincidence with two-out-of-two (high pressure and low-low level). The trip in one of these coincidence signals is interlocked with and permits the starting of a timer which delays actuation of the relief valves to permit operator intervention and to allow the HPCI to restore reactor water inventory. The operator can reset the timer before it times out. The timer action completes the initiation circuitry. The time delay setting was chosen to be long enough so that HPCI has time to start yet not so long that core spray and LPCI are unable to adequately cool the fuel if HPCI fails to start. Each trip logic division actuates all five ADS valves, i.e., the four electromatic relief valves and the Target Rock safety relief valve. Figures 7.3-9 and 7.3-10 are functional control diagrams of the system.

An additional automatic actuation mode has been provided in the circuitry in response to NUREG-0737, Item II.K.3.18. This logic scheme is provided to assure automatic blowdown activation when necessary to mitigate events which do not pressurize the drywell, such as an isolation transient, steam line break outside the drywell, or stuck open relief valve with subsequent failure of HPCI and the isolation condenser. This ADS actuation sequence is initiated by low-low reactor water level alone, which starts timer with an Allowable Value of ≤ 580 seconds. If reactor level is not recovered within this time and indication is present of sufficient discharge pressure (100 psig) in LPCI or core spray, ADS will initiate without further operator action, unless manually inhibited. The LPCI and core spray pumps normally start upon indication of high drywell pressure or upon indication of reactor low-low level with a low reactor pressure permissive. However, the low reactor pressure permissive is bypassed once the actuation low-level timer times out, permitting the pumps to start and depressurization to occur. Once the low-low reactor water level signal starts the actuation timer, only restoration of water level above the low-low setpoint will reset the actuation timer (i.e., reset of the initiation timer does not affect the actuation timer).

An ADS inhibit switch is provided to prevent actuation on low-low reactor water level during an anticipated transient without scram (ATWS) event. The ADS inhibit switch does not affect the high-pressure relief function of the relief valves. Also, automatic ADS actuation can be prevented by depressing and holding the 2-

minute timer reset pushbutton. The use of the inhibit switch is alarmed in the control room.

Each train of blowdown logic is powered from a single bus associated with that train. Each valve is powered by a pair of circuits provided with power from separate dc buses. Train B has an alternate power source available which is automatically switched over upon loss of the primary power source.

The 2-minute time delay relays, used for ADS initiation, conform to 10 CFR 50, Appendix B; IEEE 323-1974; and IEEE 344-1975. The relays are mounted on panels 902(3)-32, which are located in the auxiliary electrical equipment rooms.

7.3.1.4.1 Conformance with IEEE 279-1968

The following subsections present a point-by-point comparison of the ADS with the design requirements of IEEE 279-1968 which has been summarized from GE Topical Report, NEDO-10139.[2] For more detailed information, refer to the topical report.

7.3.1.4.1.1 General Functional Requirement

The general functional requirement of IEEE 279-1968, Paragraph 4.1, and the provisions of the ADS to fulfill the requirements are summarized below:

A. Auto-initiation of appropriate action - Appropriate action is defined as initiating the opening of a specified number of valves when loss of primary coolant is detected by reactor vessel low level, persists for approximately 2 minutes, and is confirmed by high drywell pressure, provided that low pressure standby core cooling equipment is available and operating, or when reactor vessel low level is sensed for 8.5 minutes continuously. The ADS design accomplishes the appropriate action automatically.

B. Precision - The accuracy requirements for initiating ADS (like those for the core spray system) are not such that precision of measurement is required. Precision provided by these instruments is adequate to give positive automatic depressurization initiation before the vessel water level can drop below a tolerable point. The ADS control design achieves the degree of precision necessary to insure appropriate initiation of the protective function when needed and precludes inadvertent initiation under extremes of environment related errors in instrumentation.

C. Reliability - The reliability of the ADS control system is an estimated order of magnitude higher than the reliability of the actuated equipment (valves).

D. Action over the full range of environmental conditions - The corresponding discussion for the core spray system (Section 7.3.1.1.1.1)

applies to the ADS in all respects except fire and missiles. A single cabinet houses the redundant relays that energize all the auto-depressurization valves in unison. However, the circuits to the ADS valves emerge from this cabinet in independent metal conduits and are carried through separate penetrations into the drywell. Separate metal conduits are carried from the penetrations to the individual valves distributed among the four main steam lines.

Since wiring for the relief valve solenoids must survive the LOCA environment for an appreciable time (at least several minutes to perhaps an hour), cable has been selected which can easily tolerate this environment.

A destructive fire enveloping the control cabinet could disable all valve control circuits. Such a fire from electrical sources is not considered credible due to the low current available in the circuits involved and the fire-resistant nature of the devices and wiring within the cabinet. Thus, external, non-electrical fires are considered the only possible fire damage source.

Separate routing of the ADS conduits within the drywell reduces to a very low probability the possibility of missile damage to more than one ADS conduit or damage to the pilot solenoid assembly of ADS valves. The HPCI system will provide backup for the ADS under all conditions unless the HPCI line is the source of the missile or jet, in which case damage to a single ADS valve or conduit is considered credible.

If a valve were rendered inoperable by a jet of water and/or steam associated with a pipe break (Section 3.6), the redundancy of the ADS provides adequate protection for all possible break situations. Protection exists even for breaks in the feedwater line used for HPCI injection (which is the worst case, since the HPCI function could then be impaired or lost). The situation leaves all but one relief valve and all low-pressure ECCS operable. The ECCS design is such that after any single failure as identified in the LOCA analysis (Section 6.3), the remaining ECCS will provide adequate core cooling for all postulated LOCA over the entire pressure range of the event. The scenario with a break in the feedwater line used for HPCI injection and the single failure of an ADS valve leaves the LPCI pumps, two core spray loops, and four ADS valves operable. This scenario has been evaluated to be bounded by the LOCA scenarios described in section 6.3.

Furthermore, it is clear that the situation described above would require an extremely unlikely combination of circumstances.

Therefore, the ADS fulfills the minimum requirement of IEEE 279-1968, Paragraph 4.1, without benefit of backup from HPCI.

7.3.1.4.1.2 Single-Failure Criterion

The single-failure criterion of IEEE 279-1968, Paragraph 4.2, is not directly applicable to ADS because HPCI and ADS are diverse functional backups to each

other insofar as depressurization is concerned. However, ADS has been designed to accommodate all of the single failures listed under the core spray systems, except single wireway destruction, as described in Section 7.3.1.4.1.6, or a single control cabinet section destruction.

It is not considered credible that any single event occurring within the automatic depressurization cabinet could disable more than one valve.

Inadvertent operation of the ADS cannot result from failure or malfunction of any single component, including single shorts or single opens. Only one valve can be opened by any single short.

7.3.1.4.1.3 Quality of Components

The discussion of component quality for the core spray system (Section 7.3.1.1.1.3) also applies to ADS.

7.3.1.4.1.4 Equipment Qualification

The discussion of equipment qualification for the core spray (Section 7.3.1.1.1.4) also applies to ADS insofar as the level sensors are concerned.

7.3.1.4.1.5 Channel Integrity

The discussion of channel integrity for the core spray system (Section 7.3.1.1.1.5) also applies to ADS.

7.3.1.4.1.6 Channel Independence

Channel independence for sensors exposed to each variable is provided by electrical and mechanical separation (IEEE 279-1968, paragraph 4.6). The A and C transmitters for the reactor vessel level are located on separate local instrument racks (identified as Division I equipment), and the B and D transmitters for reactor vessel level are located on separate local instrument racks (identified as Division II equipment) widely separated from the A and C local instrument racks. The A and C sensors have a common pair of process taps which are widely separated from the corresponding taps for sensors B and D. Disabling of one or both sensors in one location would not disable the control for both of the ADS control channels.

Two level and two pressure sensors in one division are mechanically and electrically independent from those in the second division to initiate automatic depressurization. Therefore, these sensors are redundant to each other. The logic for each trip channel is four-out-of-four. So, the overall ADS trip logic becomes one of two, four-out-of-four logics. In addition to the sensors that initiate automatic depressurization, there are ADS permissive sensors associated with the discharge pressure of the low-pressure ECCS pumps. An interlock is provided in each trip system in order to assure that low-pressure core coolant is available before ADS

actually permits depressurization of the reactor vessel. This interlock tends to degrade the reliability of ADS, but it is arranged so that this degradation is reduced to a practical minimum. Two pressure switches, one per trip channel, (12 total) on the discharge of each core spray and each LPCI pump are connected through relays in redundant groups so that each ADS trip system is blocked from actuating unless at least one low-pressure pump shows verified discharge pressure. These pressure switch relay circuits are monitored continuously during normal plant operation so that if any pressure switch circuit gives a false signal of the presence of pressure in the low-pressure system, an annunciator will immediately alert the operator.

7.3.1.4.1.7 Control and Protection Interaction

The automatic depressurization system is strictly an on/off system. No signal can fail in such a manner that it requires ADS system actuation but simultaneously prevents the system from starting (IEEE 279-1968, Paragraph 4.7).

7.3.1.4.1.8 Derivation of System Inputs

Inputs which start automatic depressurization system are direct measures of the variables that indicate the need for and acceptable conditions for rapid depressurization of the reactor vessel (e.g., reactor vessel low water level sensed for 8.5 minutes continuously, or reactor vessel low water level verified by high drywell pressure and at least one low pressure core cooling system developing adequate discharge pressure) (IEEE 279-1968, Paragraph 4.8).

7.3.1.4.1.9 Capability for Sensor Checks

All sensors are pressure-sensing-type sensors and are installed with calibration taps and instrument valves which allow for the application of test pressure for calibration and/or functional tests during normal plant operation or during shutdown (IEEE 279-1968, paragraph 4.9).

7.3.1.4.1.10 Capability for Test and Calibration

The automatic depressurization system is not tested in its entirety during actual plant operation, but provisions are incorporated so that operability of all elements of the system can be verified at periodic intervals (IEEE 279-1968, paragraph 4.10).

7.3.1.4.1.11 Channel Bypass or Removal from Operation

Calibration of any sensor introduces a single instrument channel trip. This trip does not cause a protective action without the coincident trip of three other channels. Removal of an instrument channel from service during calibration is

brief and does not significantly increase the probability of system failure. There are no channel bypasses as such in ADS. Removal of a sensor from operation during calibration does not prevent the redundant trip circuit from functioning if accident conditions occur because they will be sensed by the redundant sensors (IEEE 279-1968, paragraph 4.11). The manual reset button can interrupt the automatic depressurization for a limited time. However, releasing the reset button will allow automatic timing and action to resume. The ADS inhibit switch will prevent blowdown if placed in the INHIBIT position. This switch is keylocked and administratively controlled.

7.3.1.4.1.12 Operating Bypasses

The discussion of operating bypasses for the core spray system (Section 7.3.1.1.1.12) also generally applies to the ADS. Disabling two selected sensors would also disable the auto-depressurization action. Disabling of the sensors would result from selective closing of one or more sensor instrument valves for each of the two sets of four sensors. This mechanism of disabling the system is not considered to be an operating bypass, so no exception to IEEE 279-1968, Paragraph 4.12, is taken.

7.3.1.4.1.13 Indication of Bypasses

The ADS inhibit switch, as well as the manual opening of the control power breakers, can disable the automatic depressurization function. Placing the ADS inhibit switch in the INHIBIT position or losing control power, is annunciated. Disabling the sensors by deliberately closing instrument valves is not indicated (IEEE 279-1968, Paragraph 4.13).

7.3.1.4.1.14 Access to Means for Bypassing

Instrument valves are maintained in their normal operating positions and cannot be operated without permission of responsible authorized personnel. Reset buttons are on the control panel in the main control room. Control power breakers are in dc distribution cabinets which are located in limited access areas. (IEEE 279-1968, Paragraph 4.14).

7.3.1.4.1.15 Multiple Trip Settings

IEEE 279-1968, Paragraph 4.15, which deals with multiple trip settings, is not applicable because all trip points are unique.

7.3.1.4.1.16 Completion of Protection Action Once Initiated

Each of the two trip systems for the automatic depressurization control seals-in electrically and remains energized until manually reset by the reset pushbutton (IEEE 279-1968, Paragraph 4.16).

7.3.1.4.1.17 Manual Actuation

Each valve has its individual manual control switch which can operate the valve even when the automatic control relays cannot operate for any reason, including loss of control power fuses. Each valve has its own fused solenoid power circuit which is coordinated with the breaker and provides power for ADS control. Manual control is therefore independent of automatic control (IEEE 279-1968, Paragraph 4.17). (Refer to Section 5.2.2 for a description of relief valve reopening restrictions.)

7.3.1.4.1.18 Access to Setpoint Adjustments

The discussion of setpoint adjustments for the core spray system (Section 7.3.1.1.1.18) also applied to ADS.

7.3.1.4.1.19 Identification of Protective Actions

The discussion of identification of protective actions for the core spray system (Section 7.3.1.1.1.19) also applies to ADS.

7.3.1.4.1.20 Information Readout

The following indication pertinent to ADS status is provided to the operator.

A. Annunciators,

B. Valve position lights for each valve, and

C. Reactor vessel level indication.

The change of state of any active component from its normal condition is called to the operator's attention; therefore, the indication is considered to be complete and timely (IEEE 279-1968, Paragraph 4.20).

7.3.1.4.1.21 System Repair

As with the core spray system, the ADS is designed to avoid the need for repair rather than to accommodate quick replacement of components. Thus, reliability is

built-in rather than approached by accelerated maintenance. All devices in the system are designed for a 40-year lifetime under the imposed duty cycles. Since this duty cycle is composed completely of testing at infrequent intervals, the durability of active components other than sensors is more a matter of shelf life than active life. However, all components are selected for continuous duty plus thousands of cycles of operation (far beyond anticipated usage in actual service). Recognition and location of a failed component is accomplished during periodic testing (IEEE 279-1968, Paragraph 4.21).

7.3.2 Primary Containment Isolation System

7.3.2.1 Design Basis

The primary containment isolation system (PCIS) provides automatic isolation of appropriate pipelines which penetrate the primary containment whenever certain monitored variables exceed their preselected operational limits. To achieve this objective, PCIS was designed using the following criteria:

A. Prevent the release of radioactive materials in excess of the limits in 10 CFR 100 as a result of the design basis accidents;

B. Function safely following any single component malfunction; and

C. Function independently of other plant controls and instrumentation.

7.3.2.2 Isolation Logic Description

The PCIS logic is arranged as a dual logic channel system, similar to the reactor protection system logic (Section 7.2). Sensor relays in the PCIS receive their power either from one of the reactor protection system channel buses or from the essential service ac bus. The sensor relays are normally energized, as in the reactor protection system. Deenergization of the sensor relays causes operation of contacts in trip channel logic circuits. Trip channel logic circuit relays cause a single logic channel trip. In most cases both logic channels must trip to initiate isolation.

Isolation valves use various methods of operation: ac motor, dc motor, solenoid, or pilot solenoid and instrument air pressure. For those valves closed by ac or dc motor operation, deenergizing the trip channel isolation logic relays closes contacts in the valve motor control circuitry. Solenoid-operated valves normally have their solenoids energized when open; isolation logic relays open contacts in the solenoid power supply. Air-operated isolation valves are actuated through solenoid-controlled pilot air valves.

Primary containment isolation functions are initiated by groups, according to the trip channel logic associated with each group. Additionally, manual switches on the control room panel are available to back up all trip signals. In addition to providing isolation, the system initiates other actions designed to limit radioactive release. Analytical Limits are listed in Table 7.3-1. Figure 7.3-11 identifies the

actuated valves and the initiating signals. Table 6.2-9 provides information on the valves actuated by the system.

There are five groups of isolation valves, as follows:

A. Group 1 - this group includes isolation valves for the following:

1. Main steam lines,

2. Main steam line drain,

3. Isolation condenser steam line vent, and

4. Recirculation sample line.

Two solenoid-operated pilot valves are used to control the air supply for each main steam line isolation valve (see Section 6.2.4 for a description of the MSIVs). One solenoid is powered by ac, the other by dc. The arrangement is such that both must be deenergized to actuate valve closure. Two of the trip channels controlling the isolation logic relays are powered from a reactor protection system channel bus; the other two trip channels receive power from the essential service ac bus. Each sensor relay circuit receives power from the same source as the trip channel in which it actuates contacts. Upon loss of all ac, the circuits receiving power from the essential bus will continue to receive ac power through the dc/ac inverter. Since trip channels powered from the essential service ac bus do not lose power, a loss of all ac will neither cause nor prevent main steam line isolation.

B. Group 2 - this group includes the isolation valves for the following (refer to Table 6.2-9 for specific valve information):

1. Drywell equipment and floor drain sump isolation,

2. Reactor head cooling isolation,

3. Drywell vent isolation,

4. Drywell vent relief isolation (2-inch bypass),

5. Drywell purge isolation,

6. Drywell and torus nitrogen makeup isolation,

7. Drywell and torus inert isolation,

8. Torus purge isolation,

9. Drywell and torus vent from reactor building isolation,

10. Drywell vent to standby gas treatment isolation,

11. Torus vent isolation,

12. Torus vent relief isolation (2-inch bypass),

13. Drywell air sampling isolation,

14. Torus air sampling isolation,

15. Torus-to-condenser drain isolation,

16. Drywell sample (ILRT) isolation, and

17. Traversing incore probe (TIP) isolation valves. (Group 2 isolation initiates TIP withdrawal; the isolation valves close when TIP withdrawal is past the limit switch. See Section 7.6 for a description.)

A Group 2 isolation signal also initiates secondary containment isolation. The secondary containment system is described in Section 6.2.3.

The Group 2 inboard and outboard isolation valves are maintained in their normal positions while their respective solenoids are energized. These solenoids are energized by a series/parallel combination of four trip relays: 595-104B in series with 595-104D in Division I and 595-104A in series with 595-104C in Division II. The divisional series combinations are in parallel.

Each trip relay is energized by a series combination of contacts. If at least one trip relay opens in each division, the inboard and outboard isolation valve solenoids deenergize, closing the valves and causing a Group 2 isolation.

C. Group 3 - a reactor low water level signal initiates reactor water cleanup system isolation, and shutdown cooling system isolation.

D. Group 4 - included in this group are the valves for HPCI steam line isolation, and HPCI torus suction.

There are two valves in the steam line for isolation service: one inside primary containment and the other outside. The outside valve is a dc-powered, motor-operated valve taking power from the station batteries. The inside valve is an ac-motor-operated valve that is powered from the standby ac systems. The power and control wiring to the two valves are physically separated and run by separate routes to the control cubicles. At least one valve will close when system isolation is required.

A time delay has been added to the steam line high flow isolation to prevent spurious steam line isolation.

E. Group 5 - Isolation valves associated with the isolation condenser are closed upon indication of either high isolation condenser steam or condensate flow.

The isolation functions and trip settings used for the electrical control of isolation valves are described in the following paragraphs.

7.3.2.2.1 Low Reactor Vessel Water Level

The low reactor level instrumentation is set to trip at greater than the analytical limit of 0 inches on the level instrument. After allowing for the full power pressure drop across the steam dryer, the low-level trip is greater than 494 inches above vessel zero or 136 inches above the top of active fuel (inside shroud). This trip initiates closure of Group 2 and 3 primary containment isolation valves. For an analytical limit of 0 inches on the instrument scale and a 60-second valve closure time, the valves will be closed before perforation of the cladding occurs even for the maximum break: the setting is therefore adequate.

The low-low reactor level instrumentation is analytically assumed to trip before reactor water level reaches-59 inches on the instrument scale. This trip initiates closure of Group 1 primary containment isolation valves. This trip setting level was chosen to be high enough to prevent spurious operation but low enough to initiate ECCS operation and primary system isolation so that no melting of the fuel cladding will occur, post-accident cooling can be accomplished and the guidelines of 10 CFR 100 will not be exceeded. For the complete circumferential break of a 28-inch recirculation line and with the trip setting given above, ECCS initiation and primary isolation are initiated in time to meet the above criteria. The instrumentation also covers the full spectrum of breaks and meets the above criteria.

7.3.2.2.2 Main Steam Line High Radiation

Deleted.

7.3.2.2.3 Main Steam Line Space High Temperature

Temperature monitoring instrumentation is provided in the main steam line tunnel to detect leaks in this area. Trips are provided by this instrumentation which cause closure of Group 1 isolation valves. The allowable value of less than or equal to 200°F is low enough to detect leaks of the order of less than one percent of rated steam flow; thus, this trip is capable of covering the entire spectrum of breaks. For large breaks, it is a backup to high steam flow instrumentation discussed below. For small breaks with the resultant small release of radioactivity, it provides isolation before the guidelines of 10 CFR 100 are exceeded.

7.3.2.2.4 Main Steam Line High Flow

Venturis are provided in the main steam lines as a means of measuring steam flow and also limiting the loss of mass inventory from the vessel during a steam line break accident. In addition to monitoring steam flow, instrumentation is provided which causes a trip of Group 1 isolation valves. The primary function of the instrumentation is to detect a break in the main steam line outside the drywell; thus only Group 1 valves are closed. For the worst case accident, main steam line break outside the drywell, the high steam line flow trip, in conjunction with the flow limiters and main steam line valve closure, would limit the mass inventory loss such that the fuel meets the criteria of 10 CFR 50.46, and release of radioactivity to the environs is well below 10 CFR 100 guidelines.

7.3.2.2.5 Low Steam Line Pressure

Pressure instrumentation trips when main steam line pressure drops belowa pre-set value. A trip of this instrumentation results in closure of Group 1 isolation valves. In the REFUEL, SHUTDOWN, and STARTUP/HOT STANDBY modes, this trip function is bypassed. This function provides protection against a pressure regulator malfunction which would cause the control and/or bypass valves to go full open. With the trip set at greater than or equal to the pre-set value, inventory loss is limited so that fuel meets the criteria of 10 CFR 50.46; thus, there are no fission products available for release other than those in the reactor water.

7.3.2.2.6 Primary Containment (Drywell) High Pressure

The high drywell pressure instrumentation is a backup to the water level instrumentation, and, in addition to initiating ECCS, it causes isolation of Group 2 isolation valves. For the breaks discussed above, this instrumentation will initiate ECCS operation about the same time as the low-low water level instrumentation. Thus the results given above are applicable here. Also, Group 2 isolation valves include the drywell vent, purge and sump isolation valves. High drywell pressure activates only these valves because high drywell pressure could occur as the result of nonsafety-related causes such as not purging the drywell air during startup.

Total system isolation is not desirable for these conditions, and only the Group 2 valves are required to close. The low-low water level instrumentation initiates protection for the full spectrum of LOCAs and causes a trip of Group 1 primary system isolation valves.

7.3.2.2.7 Primary Containment (Drywell) High Radiation

The primary containment (drywell) high radiation signal initiates a Group 2 isolation signal in the event that high drywell radiation is experienced. The intention of the isolation is to minimize releases to the public. This signal provides a backup within the existing Group 2 isolation function. The backup function would only be necessary in the unlikely event that high radiation were present in the drywell without low reactor water level or high drywell pressure.

7.3.2.2.8 High Pressure Coolant Injection Turbine Area High Temperature

The HPCI high temperature instrumentation is provided to detect a break of the HPCI turbine steam line in the HPCI compartment. Tripping of this instrumentation results in actuation of HPCI isolation valves, i.e., Group 4 valves. All sensors are required to be operable to meet the single-failure criterion for design flow and valve closure times are such that core uncovery is prevented and fission product release is within limits.

7.3.2.2.9 High Pressure Coolant Injection High Steam Line Flow

The HPCI high flow instrumentation is provided to detect a break in the HPCI turbine steam line. Tripping of this instrumentation results in actuation of HPCI isolation valves, i.e., Group 4 valves. All sensors are required to be operable to meet the single-failure criterion for design flow and valve closure times are such that core uncovery is prevented and fission product release is within limits.

7.3.2.2.10 High Pressure Coolant Injection Low Steam Line Pressure

The low-pressure signal provides automatic isolation of the turbine loop prior to stalling the turbine on low available energy. With the low-pressure condition present, the isolation signal will block the auto-initiation logic of the HPCI. If, however, reactor pressure should rise above the pressure switch setpoint, the isolation signal will auto-reset, and the HPCI will be capable of auto-restart upon receipt of an initiation signal.

7.3.2.2.11 Isolation Condenser High Flow

Two sensors on the isolation condenser supply and return lines are provided to detect the failure of isolation condenser lines and actuate isolation action. All

sensors and instrumentation are required to be operable. The allowable values as defined in the technical specifications and valve closure time prevent uncovering the core or exceeding site limits. The Unit 3 high-flow isolation logic has a time delay of 2 ± 0.5 seconds to eliminate spurious isolation. The sensors will actuate due to high flow in either direction.

7.3.2.3 Primary Containment Isolation System Instrumentation

The sensors for the PCIS are described in the following paragraphs.

A. Reactor water level pressure sensors are identical to those utilized in the reactor protection system and are described in Section 7.2.

B. Deleted.

C. Steam line tunnel temperatures are sensed by 16 temperature switches. Four switches are used in each instrumentation trip channel. High temperature is indicative of a steam line break.

D. High main steam line flow is sensed by 16 indicating differential pressure switches operating from flow restrictor devices. Each main steam line has one flow restrictor: four separate differential pressure switches operate across each flow restrictor, providing an input from each flow restrictor into each logic trip channel. A trip is actuated by a high differential pressure, indicating high flow.

E. Main steam line low pressure is sensed by four bourdon-tube-operated pressure switches, sensing pressure directly downstream of the main steam equalizing header. Each pressure switch provides an input to one instrumentation trip channel. These switches are mounted on shock absorbing isolators to prevent spurious actuation of the switches.

   A bypass is provided for the main steam line low pressure trip. The bypass is effective when the mode switch is in any position other than RUN.

F. High drywell pressure is sensed by four diaphragm-operated pressure switches. Each switch provides an input to one instrumentation subchannel.

G. High drywell radiation is detected by two radiation monitors in the drywell. This isolation has a two-out-of-two-once logic.

H. There are two HPCI differential-pressure-type flow switches, both connected in one-out-of-two logic, across a single set of sensing lines across the steam line elbow within the primary containment vessel (drywell). The flow sensors are electrically connected to the isolation system such that a trip in either one or both sensors will initiate isolation. A failure of one sensor in the nontrip mode will neither initiate isolation nor prevent the other sensor from initiating isolation on

high flow. Therefore, failure of any single component will not result in violation of primary containment isolation criteria. The isolation signal is sealed-in upon receipt, and in addition to closing the HPCI steam isolation valves, the signal blocks the auto-initiation of the HPCI subsystem.

The differential pressure (ΔP) across the elbow taps at reactor vessel rated flow of 145,000 lb/hr of steam at 1135 psia and 102,500 lb/hr of steam at 165 psia is below the isolation trip setting.

The HPCI steam line isolates by high-flow indicative of an HPCI steam line break. The high steam flow trip setting is selected high enough to avoid spurious isolation yet low enough to provide timely detection of an HPCI steam line break. The isolation allowable value is 3 times maximum rated flow or 435,000 lb/hr of steam at the reactor vessel maximum operating pressure of 1135 psia, corresponding to a break size of approximately 0.05 square feet. The switches trip for flow in either direction, which protects against breaks on either side of the transducers. The HPCI high steam flow isolation incorporates a time delay setting (analytical limits: 3 seconds to 9 seconds) which prevents inadvertent isolation on high steam flow after the subsystem automatically initiates.

Analysis shows that only 3000 gal/min of saturated water is required to produce the isolation trip differential pressure. The sensor is designed to produce a signal indicative of steam flow. As such, it does not give a reliable indication of moisture carryover. However, should a water slug occur and pass down the HPCI steam line at a velocity near that of rated steam flow, an isolation signal would definitely be generated.

I. Four sets of temperature switches are used to detect high temperature in the vicinity of the HPCI turbine. Each set consists of four temperature switches connected in one-out-of-two-twice logic. The analytical limit for the switches is 200°F. The one-out-of-two-twice logic was selected to avoid spurious trips since the area temperature closely approaches the setpoint (within 50°F). This high temperature is indicative of steam leakage including that from the turbine shaft seals. This isolation signal is also sealed-in upon receipt, and blocks the auto-initiation logic of the HPCI subsystem.

J. Four pressure switches which are used to initiate low steam line pressure isolation are connected in a one-out-of-two-twice logic. The pressure switches initiate the trip before the reactor pressure decreases to the allowable value of 100 psig. The low-pressure signal provides automatic isolation of the turbine loop prior to stalling the turbine on low available energy. With the steam supply open to the turbine in the stalled condition, the reserve coolant in the gland seal condenser would ultimately rise in temperature, resulting in possible external steam leakage from the shaft seals. This isolation signal is not sealed-in. With the low-pressure condition present, the isolation signal will block the automatic initiation logic of the HPCI subsystem. If reactor pressure should rise above the pressure switch setpoint, the isolation signal will auto-reset, and the HPCI subsystem will auto-restart upon receipt of an initiation signal.

K. The isolation condenser system has two flow measuring points: one in the steam line and the other in the condensate return line. Two differential pressure switches are used at each point; any one of the four switches can cause isolation.

7.3.2.4 Design Evaluation

The discussion regarding reactor protection system reliability (Section 7.2) applies with equal validity to those portions of the primary containment isolation system using an identical, dual logic channel arrangement.

Double isolation valves are provided on lines penetrating the primary containment and open to the free space of the containment. Closure of one of the valves in each line would be sufficient to maintain the integrity of the pressure suppression system. Automatic initiation is required to minimize the potential leakage paths from the containment in the event of a LOCA.

Those large pipes comprising a portion of the reactor coolant system, whose failure could result in uncovering the reactor core, are supplied with automatic isolation valves (except those lines needed for ECCS operation or containment cooling). The closure times specified herein are adequate to prevent loss of more coolant from the circumferential rupture of any of these lines outside the containment than from a steam line rupture. Therefore, this isolation valve closure time is sufficient to prevent uncovering the core.

The logic for Groups 1, 2, and 5 primary containment isolation valves has been modified to prevent the valves from automatically opening when the isolation signal is reset. The margin of safety increases since it now requires an operator to individually open the valves.

Chapter 15 evaluates the response of the primary containment system subsequent to design basis accidents. In none of the cases analyzed do radioactive releases in excess of the limitations of 10 CFR 100 occur.

Manual initiation is available for all primary containment isolation functions.

Primary containment isolation control has its sensory functions separated in a manner similar to the reactor protection system (except for the main steam flow switches explained below) and its logic relays are included in the four protection system panels. Auxiliary relays are located in two separate cabinets: one for inboard and one for outboard valves. Cables to the redundant motor operated valves (ac inboard and dc outboard) are in separate trays or conduits as are cables to air-operated valves inside and outside the drywell (e.g., main steam isolation valves). Separation of wiring to redundant fail-closed valves outside the drywell (solenoid-piloted, air-operated valves on drywell ventilation systems) is not required because safe failures will result from any circuit damage considered credible.

Each main steam line has flow switches which operate from a single pair of sensing lines from each of the steam flow elements. Thus, a single sensing line failure can cause failure of four switches on a line. Such a failure is readily detectable by indication through the steam flow indication instruments. In addition, a measure of backup is provided by the temperature sensors in the pipe tunnel and flow

switches on the other three lines. Electrical circuit separation is maintained from the flow switches to the protection panels.

The arrangement of the high-flow isolation logic for the HPCI and isolation condenser systems is such that any one signal can cause isolation of the system. Any single component failure will not prevent isolation.

The HPCI isolation control function includes the sensors, trip channels, switches, and remotely activated valve closing mechanisms associated with the valves in the HPCI steam line, which when closed, effect isolation of the primary containment or reactor vessel, or both.

A failure of the low-pressure (reference) flow sensing line will appear as high flow to both sensors and initiate isolation. A failure of the high-pressure flow sensing line will drive both flow sensors downscale appearing as instrument failure (below zero reading on one or both sensors) and initiate isolation. Both flow sensors will read zero in event of failure of both flow sensing lines and neither will initiate isolation, however backup is provided by the pressure sensors described in the next paragraph.

The differential pressure (ΔP) across the elbow taps at reactor vessel rated flow of 145,000 lb/hr of steam at 1135 psia, and at reactor vessel rated flow of 102,500 lb/hr of steam at 165 psia, is below the isolation trip setting.

The isolation allowable value is 3 times the rated flow, or 435,000 lb/hr of steam at 1135 psia. Analysis shows that only 3000 gal/min of saturated water would be required to produce the isolation trip differential pressure. The sensor is designed to produce a signal indicative of steam flow. As such, it does not give a reliable indication of moisture carryover. However, should a water slug occur and pass down the HPCI steam line at a velocity near that of rated steam flow, an isolation signal would definitely be generated.

There are four static pressure sensors piped to the same sensing lines as the flow sensors and connected in a one-out-of-two-twice logic that will initiate isolation in event of simultaneous failure of both sensing lines or upon low steam line static pressure. It is clear that no mode of failure of pressure or flow sensing devices will prevent isolation; although, inadvertent isolation will be initiated for some modes of failure.

The HPCI steam line isolation valves are also closed by high space temperature in the HPCI equipment compartment. Sixteen temperature switches are used for this function. The sixteen sensors are grouped, four to a group, and each group is connected in a one out of two twice logic to provide the isolation trip. The trip setting is 200°F to automatically close the valves. This setting is well above the expected ambient condition but low enough to detect steam line leakage. Failure of any one sensor or group of sensors does not prevent isolation by the other sensors.

The HPCI turbine stop valve that closes off the steam line for system control purposes is not safety-related but does offer a secondary means of isolating the steam lines. The turbine stop valve closes as follows:

A. Reactor high water level trips the HPCI turbine stop valve upon an increase in normal operating level (Analytical Limit: 51" RWL).

This point is about 14 inches below the HPCI steam center-line outlet from the reactor. The stop valve is designed to close within 5 seconds following trip signal. The turbine control valves also close as a result of stop valve closure so that a double valve closure of the line is effective under trip conditions.

B. Pressure switches in the turbine exhaust line trip the stop valve upon high exhaust line pressure. In the event of two-phase mixture carryover with enough moisture to cause failure of the turbine thrust bearing, the turbine exhaust pressure would increase and initiate closure of the turbine stop valve to isolate the turbine.

7.3.2.5 Surveillance and Testing

Since electrical components used in the primary containment isolation system are normally energized, most failures result in the deenergization of the component involved. Such failures initiate an alarm and/or a trip of one of the two channels. Surveillance is attained by this self-annunciation upon failure. Any failures which are not self-annunciating will be identified by a testing schedule; the schedule assures that such failures are found and corrected on a routine basis. Valves within the system may be tested periodically to verify operational capability.

7.3.2.6 Conformance to IEEE 279-1968

The following subsections present a point-by-point comparison of the containment isolation control system with the requirements of IEEE 279-1968 which has been summarized from GE Topical Report, NEDO-10139.[2] For more detailed information, refer to the topical report.

7.3.2.6.1 General Functional Requirements

A. Auto-Initiation of Appropriate Action - The control system action from sensor to final control signal to the valve actuator is capable of initiating appropriate action within a time commensurate with the need for valve closure. Total time assumed in the analysis, from the point where a process out-of-limits condition is sensed to the energizing or deenergizing of appropriate valve actuators, is less than the analytical limit of 500 milliseconds. The closure time of valves ranges upward from a minimum allowable of 3 seconds for the main steam isolation valves, depending upon the urgency for isolation considering possible release of radioactivity. Thus, it can be seen that the control initiation time is at least an order of magnitude lower than the minimum required valve closure time.

B. Precision - Accuracies of each of the sensing elements are sufficient to accomplish the isolation initiation within required limits without interfering with normal plant operation.

C. Reliability - The reliability of the PCIS is compatible with and higher by at least an order of magnitude than the reliability of the actuated equipment (valves).

D. Action over the full range of environmental conditions - The corresponding discussion for core spray system (Section 7.3.1.1.1.1) applies here to all isolation control equipment, except the manual control switches for the HPCI isolation valves. Since both of the control switches for the redundant valves are in the same control panel in the main control room, it is conceivable that destruction of this cabinet by fire or missile could affect the control of both valves in these two lines in such a way as to prevent the valves from closing. However, it is highly unlikely that such an event could occur coincident with an independent event requiring system isolation such as a steam line break. Refer to Sections 9.5.1 and 3.5 (IEEE 279-1968, Paragraph 4.1).

7.3.2.6.2 Single-Failure Criterion

The design of the PCIS fully complies with the single-failure criterion of IEEE 279-1968, Paragraph 4.2.

7.3.2.6.3 Quality of Components and Modules

The discussion of component capability for the core spray system (Section 7.3.1.1.1.3) also applies to the PCIS. However, most of the isolation control is deenergized to trip (instead of energized to trip). Thus, failures that may occur in coil circuits, connections, or contacts are more likely to be noticed (IEEE 279-1968, Paragraph 4.3).

7.3.2.6.4 Equipment Qualifications

The discussion of equipment qualification for the core spray system (Section 7.3.1.1.1.4) also applies to PCIS.

7.3.2.6.5 Channel Integrity

The discussion of channel integrity for the core spray system (Section 7.3.1.1.1.5) also applies to PCIS. However, the fail-safe design of the isolation control and the operation of a grounded ac system improve fail-safe operation (IEEE 279-1968, Paragraph 4.5).

7.3.2.6.6 Channel Independence

Channel independence for sensors exposed to each process variable is provided by electrical and mechanical separation (IEEE 279-1968, Paragraph 4.6). Physical separation is maintained between redundant elements of the redundant control systems where it adds to reliability of operation. The manual control switches for the HPCI isolation valves are an exception to this objective, but they are sufficiently separated to give a high degree of reliability and to meet a literal interpretation of Paragraph 4.6 of IEEE 279-1968.

7.3.2.6.7 Control and Protection Interaction

The isolation control system is a strictly on/off system, and no signal whose failure could cause a need for isolation can also prevent it (IEEE 279-1968, Paragraph 4.7).

7.3.2.6.8 Derivation of System Inputs

The inputs which initiate isolation valve closure are direct measures of variables that indicate a need for isolation (such as reactor vessel low level, drywell high pressure, and pipe break detection) (IEEE 279-1968, Paragraph 4.8). Pipe break detection utilizes methods of recognition of the presence of a material that has escaped from the pipe rather than detecting actual physical changes in the pipe itself.

7.3.2.6.9 Capability for Sensor Checks

The reactor vessel instruments including level, pressure, radiation, and flow, can be checked one at a time by application of simulated signals (IEEE 279-1968, Paragraph 4.9). Temperature sensors along the main steam lines are testable only during shutdown, but they are sufficient in number so that testing between refueling outages is not necessary to achieve the reliability level required. Temperature sensors can be checked periodically by removing them and applying heat to the sensitive zone, or by oven calibration, which requires removing the sensors from the circuit and replacing them with calibrated units.

7.3.2.6.10 Capability for Test and Calibration

All active components of PCIS, with the exception of the main steam line high temperature sensors can be tested and calibrated during plant operation (IEEE 279-1968, Paragraph 4.10).

7.3.2.6.11 Channel Bypass or Removal from Operation

Calibration of any sensor introduces a single instrument channel trip. This trip does not cause a protective function without the coincident trip of at least one other instrument channel, except for the HPCI system where leak detection flow sensors have a one-out-of-two logic (IEEE 279-1968, Paragraph 4.11).

7.3.2.6.12 Operating Bypasses

The only bypass in PCIS is the main steam line low-pressure bypass which is imposed by the mode switch when the switch is not in the run mode. The mode switch cannot be left in other than RUN with neutron flux measuring power above 15% of rated power without imposing a scram. Therefore the bypass is considered to be removed in accordance with the intent of IEEE 279-1968, Paragraph 4.12; although manual action removes the bypass, rather than an automatic one. In the case of the motor-operated valves, automatic or manual closure can be prevented by shutting off electric power.

7.3.2.6.13 Indication of Bypasses

The bypass of the main steam line low-pressure isolation signal is not indicated directly in the control room except by the position of the mode switch. This switch is under strict operator control. Its specific bypass functions are a matter of operator training. Therefore, no bypass indication is required when the mode switch is not in RUN. Since the bypass is not removed by any automatic action, it is positively in effect any time the mode switch is in position to impose it (IEEE 279-1968, Paragraph 4.13).

7.3.2.6.14 Access to Means for Bypassing

The mode switch is the only bypass switch affecting PCIS, and it is centrally located on the main control console (IEEE 279-1968, Paragraph 4.14).

7.3.2.6.15 Multiple Trip Settings

IEEE 279-1968, Paragraph 4.15, which deals with multiple trip settings, is not applicable because all setpoints are unique.

7.3.2.6.16 Completion of Protection Action Once Initiated

All isolation decisions are sealed-in downstream of the decision-making logic, so valves go to the closed position, which ends protective action (IEEE 279-1968,

Paragraph 4.16). Manual reset action is provided by a three-position reset switch so that inboard valves can be reset independent of outboard valves.

The HPCI isolation valve reset is separated from the reset for the rest of the isolation valves.

7.3.2.6.17 Manual Actuation

All isolation valves are capable of manual actuation independent of active components of the automatic actuation circuitry, with the exception of the motor starters for the motor-operated valves (IEEE 279-1968, Paragraph 4.17).

7.3.2.6.18 Access to Setpoint Adjustments

The discussion of access to setpoint adjustments for core spray system (Section 7.3.1.1.1.18) is also applicable to PCIS.

7.3.2.6.19 Identification of Protective Actions

The statements regarding identification of protective actions for core spray system (Section 7.3.1.1.1.19) are applicable to PCIS.

7.3.2.6.20 Information Readout

The following information is presented to the operator:

A. Annunciation of each process variable which has reached a trip point;

B. Computer readout of trips from main steam line tunnel temperature or main steam line excess flow;

C. Control power failure annunciation on each channel;

D. Annunciation of steam leaks in each of the systems monitored, such as, main steam, reactor water cleanup, and HPCI; and

E. Open and closed position lights for each isolation valve.

This information is considered to fulfill the requirements for information readout (IEEE 279-1968, Paragraph 4.20).

7.3.2.6.21 System Repair

Those components which are expected to have a moderate need for replacement (including the temperature amplifier units and thermocouples in the ventilation ducts) are designed for convenient removal. The amplifier units employ a circuit card or replaceable module construction and the thermocouples or resistance temperature detectors are replaceable units with disconnectable heads. Pressure sensors, vessel level sensors, etc., can be replaced in a reasonable length of time, but are considered to be permanently installed. They have nonwelded connections at the instrument which allow replacement.

7.3.3 Secondary Containment Isolation System

The secondary containment isolation system is described in Section 6.2.3.

7.3.4 Isolation Condenser Instrumentation and Control

The isolation condenser provides reactor core cooling in the event that the reactor becomes isolated from the main condenser by closure of the main steam isolation valves. The isolation condenser is described in Section 5.4.6. The PCIS description relating to the isolation condenser is in Section 7.3.2.

The isolation condenser is automatically placed in service on a sustained high reactor pressure signal as defined in the Technical Specifications in a one-out-of-two-twice logic. This initiation signal will close the vent line valves and open the outboard condensate return valve, completing the flow path through the isolation condenser. The maximum time delay allowable value for reactor pressure to be above the actuation setpoint is $\leq$ 15 seconds for initiation of the isolation condenser function.

The isolation condenser steam supply lines have a vent line which returns steam and noncondensibles to the "A" main steam line. The two valves in the vent line automatically close on one of the following signals:

A. Isolation condenser initiation (one-out-of-two logic);

B. Isolation condenser line break (PCIS signal) (one-out-of-two logic); and

C. Main steam line isolation signal (one-out-of-two twice logic).

The isolation condenser return valve control switch has PULL-TO-LOCK, CLOSE, AUTO, and OPEN positions, with spring return to AUTO from the CLOSE position to avoid the inadvertent override of an initiation signal. The AUTO and OPEN positions are maintained contact. The PULL-TO-LOCK position overrides the automatic signals to reopen and permits valve isolation with deliberate operator action.

7.3.5 References

1. 10 CFR 50 Appendix A, General Design Criteria (GDC) 57, Closed System Isolation Valves.

2. General Electric Topical Report, NEDO-10139, Compliance of Protection Systems to Industry Criteria: General Electric BWR Nuclear Steam Supply System, June 1970.

Table 7.3-1

GROUP ISOLATION SIGNALS AND SETPOINTS

Valve Isolation Group	Isolation Signal	Analytical Limit
Group 1	Reactor low-low water level	-59 in.
	Main steam line high flow	125% of rated flow (Unit 2) 140% of rated flow (Unit 3)
	Main steam line tunnel high temperature	200°F
	Main steam line low pressure	785 psig
Group 2	Reactor low water level	0 in.
	High drywell pressure	2 psig
	High drywell radiation level	100 R/hr
Group 3	Reactor low water level	0 in.
Group 4	HPCI steam line high flow	≤ 300% rated steamflow
	HPCI vicinity high temperature	200°F
	Low reactor pressure	100 psig
Group 5	High flow isolation condenser steam supply	≤ 300% rated steamflow ≤32 in.H_2O differential (Unit 2) ≤14.8 in.H_2O differential (Unit 3)
	High flow isolation condenser condensate return	

7.4 SAFE SHUTDOWN

The following section describes the instrumentation and control system aspects of the containment cooling mode of the low pressure coolant injection (LPCI) system. This section also provides a description of shutdown outside the control room.

7.4.1 Containment Cooling

The containment cooling function is provided by the low pressure coolant injection system after the core is flooded. Suppression pool water can be recirculated through the heat exchangers for cooling. The cooled water can also be used to spray the drywell and/or torus. For a complete description of the design basis, system functions and components, refer to Section 6.2.

The containment cooling mode of LPCI is initiated manually from the control room by alignment of the proper combination of valves, pumps, and heat exchangers. No automatic start function is provided.

A LPCI initiation signal actuates interlocks which close valves to prevent flow to the suppression pool and containment sprays, thus directing all LPCI flow to the core. With a LPCI initiation signal present, the containment spray normal manual keylock switch must be placed in the MANUAL position to permit alignment of flow for suppression pool cooling or for containment sprays. Placing this switch in MANUAL also permits opening the outboard injection valve in the loop not selected by the LPCI loop selection logic. This provides capability for suppression pool cooling through one loop while injecting through the other.

A LPCI initiation signal also trips any running containment cooling service water (CCSW) pumps and prevents starting CCSW pumps unless the containment cooling service pumps permissive keylock switch is placed in the MANUAL OVERRIDE position.

Two level transmitters are used to monitor water level inside the core shroud. If the water level drops below ⅔ core height, interlocks close valves in the flow paths for suppression pool cooling and containment sprays. The ⅔ core height permissive keylock switch in conjunction with the containment spray permissive keylock switch allows these valves to be opened, if necessary, when placed in the MANUAL OVERRIDE position. The ⅔ core height interlock uses a one-out-of-one logic.

To initiate or maintain drywell and/or torus spray, drywell pressure must be above the low limit setpoint. This parameter is measured by two pressure switches per division arranged in one-out-of-two-twice logic. This condition does not have a bypass switch.

Once containment cooling has been placed in operation, if any of the preceding requirements do not continue to be either met or bypassed, the associated valves will close to allow full LPCI injection flow.

7.4.2 Shutdown Outside the Control Room

Because fire protection is afforded in the control room and smoke protection masks are available, there is a very low probability that control room habitability would be lost.

The plant design facilitates bringing the reactor to the hot shutdown condition. The operator scrams the reactor, closes the main steam isolation valves (MSIVs) and inhibits the automatic depressurization system (ADS). To initiate cooldown of the reactor, the water return valve from the isolation condenser is opened, placing the isolation condenser in operation. The operator then leaves the control room. Since the MSIVs are closed, makeup requirements are minimal and can be met by the control rod drive (CRD) system.

After leaving the control room, various steps are taken by procedure (Dresden Safe Shutdown Procedures) to insure that a fire will not cause the spurious actuation of equipment. The reactor water level can be monitored at two different instrument racks located in the reactor building. Reactor vessel pressure is also displayed on these instrument racks. The operation of the isolation condenser system and the isolation condenser makeup system can be controlled from the reactor building. Further detail on makeup to the isolation condenser is provided in Section 5.4.6.

The above actions place the reactor in a safe, cooldown mode with essentially no coolant inventory loss, yet makeup capability remains available via the feedwater system, either automatically or manually and the control rod drive pumps. The feedwater pumps and control rod drive pumps can be shut off manually to prevent overfilling the reactor vessel.

Operation of the isolation condenser would be continued until the reactor temperature decreases to about 350°F. At this time, the shutdown cooling system can be initiated to continue the cooldown. The initiation of the shutdown cooling system can be accomplished at remote stations. The closed cooling water system would have been in operation prior to evacuation of the control room. Cooldown with the shutdown cooling system could be continued indefinitely.

Required communications can be made from each location outside the control room where shutdown activities are performed or monitored using local communications equipment.

Various systems such as the diesel generators, diesel generator cooling water system, reactor building closed cooling water system, and the service water system are available to provide necessary support functions for the alternate shutdown system. Local control and monitoring capability for these support systems is also provided.

During the entire shutdown process, no reliance is placed on regaining entry to the control room. Instrumentation is provided which enables the operator to observe the reactor vessel level and pressure while the cooldown is made. Thus, a safe shutdown of the reactor can be made to a cold shutdown condition without access to the main control room.

For a more detailed discussion of safe shutdown and 10 CFR 50 Appendix R requirements, see Section 9.5.1 and the Fire Protection Report.

7.5 DISPLAY INSTRUMENTATION

The following section describes display instrumentation required by the operator for operation and safe shutdown of the unit, under normal and post-accident conditions. Included is a discussion of instruments classified as post-accident monitors, a description of the process computer, a description of the safety parameter display system, and a summary of the detailed control room design review.

7.5.1 Post-Accident Monitors

Certain instruments have been designated as post-accident monitors, and as such have been determined to comply with Regulatory Guide 1.97.[1] These instruments are identified in the Master Equipment List (MEL).

7.5.1.1 Description

Post-accident monitoring instruments are assigned to meet one of three design categories described in detail in regulatory position 1.4 of Regulatory Guide 1.97. Category 1 requirements are the most stringent, with requirements very similar to requirements for safety-related instruments. Category 2 requirements are not quite as stringent, but many of the same standards are recommended. Category 3 instruments are commercial grade.

In accordance with R.G. 1.97, process variables used in post-accident monitoring are grouped into 5 types: A, B, C, D, and E. The following definitions are from the regulatory guide and explain the basis for a given variable being listed in a given category.

Type A variables are those variables to be monitored that provide the primary information needed to permit the control room operating personnel to take the specified manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident events. Primary information is information that is essential for the direct accomplishment of the specified safety functions; it does not include those variables that are associated with contingency actions that may also be identified in written procedures. A variable included as Type A does not preclude it from being included as Type B, C, D or E, or vice versa.

Type B variables are those variables that provide information to indicate whether plant safety functions are being accomplished. Plant safety functions are reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity (including radioactive effluent control). Variables are listed (in Regulatory Guide 1.97) with designated ranges and category for design and qualification requirements. Key variables are indicated by design and qualification as Category 1.

Type C variables are those variables that provide information to indicate the potential for breaching or the actual breach of the barriers to fission product

releases. The barriers are fuel cladding, primary coolant pressure boundary, and containment.

Type D variables are those variables that provide information to indicate the operation of individual safety systems and other systems important to safety. These variables are to help the operator make appropriate decisions in using the individual systems important to safety in mitigating the consequences of an accident.

Type E variables are those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and in continually assessing such releases.

Type A, B, and C variables relate to the determination of the safety condition of the plant and provide the operator with the information to perform tasks needed to mitigate accidents. The following parameters have been identified as Type A variables per R.G. 1.97:[1]

A. Coolant level in the reactor;

B. Reactor pressure;

C. Drywell pressure;

D. Suppression chamber pressure;

E. Suppression pool water level; and

F. Suppression pool water temperature.

The instruments monitored by these variables meet the intent of Category 1 requirements per R.G. 1.97,[1] or deviations from these requirements have been justified.

The Master Equipment List identifies the instrument numbers and the variable types associated with these parameters.

The seismic qualification criteria for these instruments are described in Section 3.10.

7.5.1.2 Analysis

A review of the post-accident monitoring instruments indicated that Dresden Station is in compliance with the intent of R.G. 1.97. Control room instrumentation provides sufficient information for operators to identify, mitigate, and monitor all design basis accidents.

The following sections provide details of Dresden acceptability with respect to seismic, power, environmental, and separation requirements.

7.5.1.2.1 Seismic Qualification

Safety-related instruments installed prior to R.G. 1.97 that either fulfilled the requirements of R.G. 1.97, Revision 2, Category 1, or were previously designated as seismic by the 1980 FSAR Safety-Related and ASME Classification Valve, Equipment, and Instrument List, the Master Equipment List, or the instrument data sheets did not undergo further seismic qualification. Replacement instruments, or new instruments installed to meet R.G. 1.97, meet the seismic requirements of IEEE 344-1975 and station requirements. Safety-related instrument racks have been seismically upgraded by adding bracing as required (refer to Section 3.10).

7.5.1.2.2 Environmental Qualification

In order to show that electrical equipment important to safety is capable of functioning in a harsh environment, CECo provided a response to IEB 79-01B for Dresden Station Units 2 and 3. Environmental zone maps were established which identified the temperature, pressure, humidity, and radiation values in various locations of the station (refer to Section 3.11). Equipment which performed a safety-related or R.G. 1.97 Category 1 or Category 2 function and was required to function or not to fail in a fashion as to impair the ability of other equipment to perform their safety-related function while exposed to the harsh environment following the associated design basis event was included in the program to be environmentally qualified. Equipment located in a mild environment, regardless of its function, was not required to be environmentally qualified.

The analysis applied the 10 CFR 50.49.k rule allowing the use of instrumentation qualified under the IEB 79-01B program. Instruments not covered under the IEB 79-01B program, but required to fulfill Category 1 or Category 2 requirements of R.G. 1.97, are qualified under the station environmental qualification (EQ) program (refer to Section 3.11).

Required instrument cables are included in the environmental qualification program. Under this program, the cable tabulations were checked to catalogue instrument cables by manufacturer and cable type. The purchase specifications for these cable types were then checked to identify the approved vendors. The EQ program included original station design instrumentation cable.

7.5.1.2.3 Redundancy of Power

Power sources for instrumentation have been verified for their ability to provide power under post-accident conditions. Each instrument bus has a main source and at least one backup or reserve source of power. See Section 8.3 for power supply information.

Each Category 1 variable is redundant to ensure that at least one channel is available to provide the necessary information to the operator. In strumentation for every Category 1 variable, with the exception of valve position indication, has a redundant loop that receives power from an alternate bus.

Neither Category 2 nor Category 3 instrumentation requires redundant monitoring channels. Therefore, only one power source for these categories of monitoring instrumentation is required. Even though this station received its construction permit prior to the categorization of power sources as Class 1E or non-1E, the power sources and the reserve sources provide the required reliability to meet the intent of R.G. 1.97.

This station was licensed before R.G. 1.75 established the requirements for physical independence of electrical systems. Existing instrumentation used for post-accident monitoring does not follow these separation requirements. To fulfill a Category 1 requirement, new instrument loops added after August 1, 1985, will comply with the requirements of R.G. 1.75 whenever possible.

7.5.2 Process Computer

This section contains information on the process computer programs, the function of the process computer, the operation of its major components, and the different kinds of programs comprising the computer software. Section 8.3.1.4.4 describes the computer UPS in more detail. Section 7.5.2.2 describes in more detail the computer equipment (excluding rod worth minimizer hardware) with which the plant operator is primarily concerned and provides functional and operating descriptions for the Nuclear Steam Supply System (NSSS), Balance of Plant (BOP), and Scan, Log and Alarm (SLA) programs. Section 7.5.3 provides details of the SPDS program.

7.5.2.1 System Description

The Dresden Process Computers are a distributed process computer system that provides on-line monitoring of over 1500 input points (digital, pulse, and analog) representing significant plant process variables. The system scans digital and analog inputs at specified intervals and issues appropriate alarm indications and messages if monitored analog values exceed predefined limits or if digital trip signals occur. It performs calculations with selected input data to provide the operator with essential core performance information through a variety of logs, trends, displays, and summaries. Computer outputs include various front panel displays (digital lights, trend recorders and color graphic displays). By making a wide range of plant performance data immediately available, in a summary format, the computer greatly increases the speed with which operating personnel can respond to changing plant conditions. It thereby contributes significantly to the maintenance of optimum core power distribution, economical utilization of nuclear fuel, and overall plant operating efficiency.

In general, the process computer system drives all peripherals that display or log real-time data, while a separate computer drives all devices which run the nuclear program for core calculation. Typical peripherals include: operator workstations, printers and color graphic displays.

7.5.2.2 Equipment Operation

Analog voltage and current inputs representing reactor flux levels, flows, pressures, temperatures, and power levels are applied directly to the I/O cabinets. Digital inputs for both units, which include various trips and alarms, traversing incore probe (TIP) system signals, control rod positions, rod worth minimizer (RWM) inputs and pulse inputs for TIP positions are applied directly to the I/O cabinets. The process computer performs calculations required for the programs being run, assigns priorities to the various programs and computer functions, and provides for data storage.

An alarm horn is included in the nuclear station operator (NSO) console to provide audible alarm indications. The alarm horn is sounded under program control as a result of various alarm or abnormal conditions.

Included with the process computer system are two trend recorders, located in panel 902-5(903-5). Each is a two-pen strip chart recorder. Each of the four pens on the two recorders can be individually selected from the NSO request CRT for trending of selected analog values.

The Station Process Computers are located in the Station's Main Computer Room which is located in the Unit 1 Turbine Building ground floor.

7.5.2.3 Operational Functions

This subsection contains program descriptions for the NSSS periodic and on-demand programs. These programs calculate and edit the periodic, daily, and monthly core performance logs and provide a variety of operator-demandable data arrays related to nuclear boiler performance.

The NSSS periodic and on-demand programs operate within the constraints of the static and dynamic priority structures, as do certain associated interface and control programs.

The current NSSS programs perform the calculations required to provide reactor core performance information. The core monitoring software system is run on a separate computer. The core monitoring software is the heart of the NSSS programs. It runs periodically at specified intervals and is triggered based on specified plant conditions, calculating fuel assembly power, flows, void distributions, peak heat fluxes, critical power ratios, and reactor operating thermal limits. This information is output on a periodic basis supplying operating personnel with the current status of significant nuclear system parameters. This information is stored to provide a historical record of these important nuclear parameters. Another useful feature of the core monitoring software is the predictive mode which can assist the nuclear engineer in deciding operating strategy by predicting future core conditions based on present or past power and exposure distributions.

The computer is interfaced with the process computer which supplies the core monitoring software with the appropriate plant operating data. The process computer also provides various demandable programs used by operating personnel to display information (pressures, flows, temperatures, etc.). These programs are used in conjunction with the TIP system for performing whole core or individual LPRM calibrations. This integrated system provides operating personnel with a reliable method of monitoring core and plant performance information.

7.5.2.3.3 Scan, Log, and Alarm Programs/ Steam Electric Evaluation and Recording Programs

Scan, log, and alarm programs perform continuous monitoring of process input points, test scanned analog values against prescribed process and sensor limits, and issue appropriate alarm messages and indications if these limits are exceeded or if digital trip signals occur.

7.5.2.3.4 Balance of Plant Program

The balance of plant program runs automatically at regular intervals and performs calculation of plant performance data not directly related to the nuclear system.

7.5.3 Safety Parameter Display System

Supplement 1 of NUREG-0737 required all operating plants to provide a Safety Parameter Display System (SPDS) in the control room. The purpose of SPDS is to provide a concise display of critical plant variables to aid in rapidly and reliably determining the safety status of the plant. NUREG-0737 required that SPDS provide, as a minimum, information concerning:

A. Reactivity control;

B. Reactor core cooling and heat removal from the primary system;

C. Reactor coolant system integrity;

D. Radioactivity control; and

E. Containment conditions.

These functions have been designated as critical safety functions. The parameters required for these functions include:

A. Reactivity control

1. Average power range monitor
2. Source range monitor

B. Core cooling

1. Reactor water level
2. Core spray system status

C. Reactor coolant system integrity

1. Reactor vessel pressure
2. Drywell pressure
3. Containment activity
4. Safety relief valve (SRV) position
5. Isolation valve status

D. Radioactivity control

1. Main stack monitor
2. Off-gas pretreatment monitor
3. Standby gas treatment monitor
4. Liquid discharge monitors

E. Containment conditions

1. Drywell pressure
2. Drywell temperature
3. Suppression pool level
4. Suppression pool temperature
5. Containment isolation valve status

7.5.3.1 Description

The SPDS is displayed on color graphics displays in the control room and technical support center for key plant parameters. The system takes its input from several sources for each parameter and determines which sensors are valid. It then calculates the best value from available sensors.

Displayed colors have the following significance:

A. Red - indicates an alarm condition with a parameter being in an abnormal state,

B. Yellow - indicates an alert (pre-alarm) condition,

C. Cyan (light blue) - means input is invalid or inoperable, and

D. Green - indicates a normal condition of a parameter.

The SPDS at Dresden is a software package incorporated into the process computer, a nonsafety-related system utilizing computer inputs for data. The computer has been suitably isolated from safety-related process inputs.

Safety Parameter Display System Displayed Variables

Reactor vessel water level is displayed by a bar chart. The chart indicates the present level. The color of the chart reflects the condition of water level. In addition, a digital reading of current level and rate of change of level is displayed above the chart and an arrow indicating trend is displayed. (This is also applicable to the following parameters).

Reactor vessel pressure is displayed by a bar chart. The chart indicates the present reactor pressure. The color of the chart reflects the condition of reactor pressure.

Drywell pressure is displayed by a bar chart. The chart indicates the present drywell pressure. The color of the chart reflects the condition of drywell pressure.

Drywell temperature is displayed by a bar chart. The chart indicates the present drywell temperature. The color of the chart reflects the condition of drywell temperature.

Torus water level is displayed by a bar chart. The scale reflects the reading of the narrow and wide range torus level instrumentation. The color of the bar reflects the condition of the torus level.

Torus water temperature is displayed by a bar chart. The chart indicates the present temperature. The color of the bar reflects the condition of torus temperature.

Reactor power is displayed by a bar chart. The chart indicates the present reactor power. The color of the bar reflects the condition of reactor power. The background will turn red for an unverified scram.

A safety relief valve status box monitors the status of all relief valves and safety valves based on a signal from the acoustic monitors. The box displays the word OPEN if any valve is open and CLSD if all valves are closed. In addition, the color of the box shows the status of the relief valves. If a relief valve should be open (based on plant parameters) and a valve indicates open, the box will be green. If no valve is open when a valve is required to be open, then the box will be red. When plant conditions do not require a relief valve to be open, and all valves indicate CLSD, the box will be green. If plant conditions require all valves closed, and a valve indicates open, the box will be red.

The core spray box indicates the status of the core spray system. The words ON and OFF are used to indicate the status. If a core spray pump is running with adequate flow, the box indicates ON. If both pumps are off, or inadequate flow is indicated, the box will display OFF. In addition, the color of the box gives the status of core spray. If a core spray initiation signal is present and core spray is off, the box will be red. The box will be green when there is no core spray initiation signal and core spray is off, or when there is an initiation signal and core spray is on.

The PCIS box indicates the status of the Group 1 and 2 isolations. The box is green when no isolation signals are present, or when at least one valve in each process line is closed for the lines in the isolation groups which have an isolation signal. The box is red when an isolation signal is present and a line in that isolation group does not have at least one valve closed.

The RAD RELEASE box displays the status of the release paths for radioactive release. The systems monitored are the main chimney, the reactor building stack, the off-gas system, the service water system, and the liquid radwaste effluent monitor. If a monitor in any of these paths indicates a release alarm above a predetermined setpoint, the box turns red. When no release from any path is indicated, the box turns green. If monitoring is lost to any release path, the box turns cyan, indicating invalid data. Any sensor indicating release above its setpoint will drive the color red regardless of the status of the other release paths.

The CONTAIN RAD box will be red and read HIGH if any of the process computer inputs for the drywell and torus monitors are in high alarm or if any one input is offscale high, otherwise it will be green and read NORM. The CONTAIN RAD box will be cyan if all the inputs are offscale and none are upscale and the wording will be NORM/HIGH.

Invalid data to SPDS is indicated by the color cyan. With the exception of radioactive release, all parameters are monitored by multiple sensors. When all sensors for a parameter are lost, the bar chart or box for that parameter turns cyan. The bar charts will indicate full scale. This does not mean that the parameter is reading full scale, but only that the computer input for that parameter is not valid.

7.5.3.2 Analysis

A human factors review of SPDS was conducted as part of the detailed control room design review (DCRDR). SPDS was evaluated to ensure that the design of the installed SPDS complied with sound human factors engineering principles and to verify the parameter selection by referring to the task analysis data collected during the DCRDR and the criteria established in NUREG-0737, Supplement 1.

The human factors evaluation assessed the appropriateness and completeness of the information available through the SPDS, the effectiveness of the display format and coding techniques, the location and positioning of the CRTs in the control room, the readability of the display given hardware and environment factors, and the adequacy of procedures and documentation for interpreting the display.

To assure that the parameters displayed on SPDS adequately monitor plant safety status during emergency conditions (which is accomplished by monitoring the critical safety functions), a comparison was made between the DCRDR task analysis and the SPDS display parameters.

The findings of the DCRDR evaluation confirmed that the parameters displayed on SPDS indicate the accomplishment or maintenance of plant safety functions. Discrepancies identified during the data collection phase represented minor modifications to SPDS. The verification and validation of SPDS confirmed that the final product met the criteria of NUREG-0737, Supplement 1.

7.5.4 Detailed Control Room Design Review

Commonwealth Edison committed to performing a detailed control room design review (DCRDR) in accordance with NUREG-0737, Supplement 1. NUREG-0700 was used as a guide for developing the Human Factors Engineering Design Criteria and Standards Manual. Items which did not conform to the requirements of the Human Factors Engineering Design Criteria and Standards Manual were documented as human engineering discrepancies (HEDs). The significance of each HED was addressed by the human engineering discrepancy assessment team (HEDAT), which was composed of station, corporate, and consultant representatives. The HEDAT either justified each of the HEDs as acceptable or proposed a resolution of individual HEDs to the NRC. A schedule for resolution was also determined by the HEDAT.

The purpose of the DCRDR was to assess and evaluate the control room work space, instrumentation, controls, and other equipment from a human engineering perspective. The process took into account both system demands and operating capacities and then identified essential and select control room improvements which would correct inadequate or unacceptable items. The ultimate goal was to ensure that proper human engineering principles and practices were incorporated into the design of the control room to help ensure the ability of control room operators to prevent accidents or cope with accidents if they occur.

The investigative process included the following elements:

A. A control room survey which compared control room design features with CECo Human Factors Guidelines;

B. A verification of instrumentation and control availability and the verification that operator task performance is not affected by the operator/control board interface; and

C. A validation of the control room functions to ensure the functions allocated to the control room operating crew can be accomplished within the structure of the defined emergency operating procedures and the design of the control room as it exists.

7.5.5 References

1. "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," NRC Regulatory Guide 1.97, Revision 2, December 1980.

2. "Supplement 1 to NUREG-0737-Requirements for Emergency Response Capability," Generic Letter 82-33.

7.6 CORE AND VESSEL INSTRUMENTATION

This section describes core and vessel instrumentation systems. Included are nuclear instrumentation systems and vessel instrumentation.

7.6.1 Nuclear Instrumentation

7.6.1.1 Design Basis

The nuclear instrumentation is designed to:

A. Provide the operator with the information required for optimum, safe operation of the reactor core.

B. Provide inputs to the reactor protection system (RPS) and the rod block circuitry to assure that the local power density, power oscillations, and bulk power level do not exceed preset limits.

In order to meet the design requirements, the nuclear instrumentation must:

A. Detect, measure, and indicate neutron flux from the source range level through the power range level;

B. Annunciate an alarm on component failures; and

C. When reactor power is in the power range;

1. Indicate local neutron flux;

2. Compute and indicate average reactor power; and

3. Detect and suppress core power oscillations.

Specific design requirements are listed in this section for each nuclear instrumentation subsystem.

7.6.1.2 General Description

The nuclear instrumentation uses three types of neutron monitors.[1] The neutron flux level for operation in the region of subcritical to an intermediate flux level at which the reactor is critical is monitored by the source range monitor (SRM). The intermediate range monitor (IRM) is used for a neutron flux level of just above criticality to approximately 10% of full power (refer to Figure 7.6-1). From about 3% power to full power operation, the local power range monitor (LPRM) is used. The detectors for the SRM and IRM subsystems are withdrawn from the core during power range operation. The detectors for the power range are fixed in place.

During operation in the power range, the LPRM signals are used in four separate subsystems:

A. LPRM flux level is indicated, and a high flux alarm is annunciated if the level reaches a preselected point.

B. The average power range monitors (APRMs) average the outputs of selected LPRMs to provide indication of average reactor power. The APRM generates scram signals on high-high APRM flux level.

C. During control rod motion, the average of a set of LPRMs adjacent to the selected control rod is used by the rod block monitor (RBM) to limit increases in local power.

D. The OPRM utilizes the LPRM signals to detect and suppress core instabilities that are known to take place in certain portions of the core power to flow operating domain.

Figure 7.6-2 presents a block diagram of the various nuclear instruments. Figure 7.6-1 shows the instrumentation ranges as they relate to neutron flux and percent power.

A traversing incore probe (TIP) may be inserted in the core to obtain an axial neutron flux distribution at each LPRM detector location. The information obtained from the TIP is used to calibrate the LPRM subsystem and to provide a relative core flux distribution to the process computer.

7.6.1.3 Source Range Monitoring Subsystem

7.6.1.3.1 Design Bases

To meet the general design requirement to provide the nuclear information needed for knowledgeable and efficient reactor startup and low flux level operation, the SRM subsystem must:

A. Provide a minimum signal-to-noise ratio of 3:1 and a minimum count rate of 3 cps with all control rods inserted prior to initial power operation (for the original core, this included the contribution of neutron-emitting sources - see Section 7.6.1.3.2).

B. Show a measurable increase in output signal from at least one detector before the neutron flux multiplication exceeds a factor of 2000 during the most limiting startup control rod withdrawal condition.

C. Provide a signal overlap of approximately one decade to the IRM signal with the SRM detectors in the fully-inserted position.

7.6.1.3.2 System Description

The SRM subsystem is used to provide the necessary information for reactor startup from subcritical to an intermediate flux level and for refueling operations. The subsystem consists of four miniature fission chambers which are operated in the pulse-counting mode. These detectors have a nominal sensitivity of 2×10^{-3}

cps/nv (nv is neutrons per square centimeter per second) and are located radially in the core as shown in Figure 7.6-3. The detectors are attached to drive mechanisms, which can position the chambers from the fully-inserted location (approximately 1.5 ft above core center), to a position approximately 2.5 feet below the reactor core.

The detector drive system consists of a detector drive, a flexible drive shaft, a motor module, and a drive tube for each detector. The drive is mounted through an adapter to the instrumentation nozzle, well below the vessel, in a location that does not interfere with control rod operation and maintenance. The drive tube is a long hollow tube which acts as a guide. A long, slender shuttle tube is mounted on the upper end of the drive tube. This combination tube, housing the fission chamber detector assembly, is driven up and down inside the dry tube.

A flexible drive shaft transmits power to the gearbox of the detector drive assembly from the motor module located approximately 20 feet away. Four limit switches provide detector position information and also interlock the motor power circuits to establish insert and retract limits.

Seven neutron-emitting antimony-beryllium sources were located radially within the reactor core as indicated in Figure 7.6-3. These sources were designed to provide at least 3 cps in each SRM channel with the reactor in the cold, xenon-free, fully shutdown condition. This requirement continued to be met during routine reactor operation by reactivation of the radioactive source (Sb-124) through capture of reactor neutrons by Sb-123. These sources have been removed, since photoneutron production is high enough to provide the required neutron flux without these sources.

The SRM detector assembly consists of a fission chamber attached to a low-loss quartz fiber-insulated transmission cable terminated with a connector. The detector cable is connected below the reactor vessel to a triple-shielded cable which carries the detector electrical output to the monitor circuitry. The output from each of the four SRM detectors is amplified and the signal is conditioned. The resulting signal, proportional to the logarithm of the counts per second occurring in the detector, is continuously displayed on log count rate meters. The time derivative of this signal is formed and displayed on four reactor period meters which indicate reactor period in seconds. A two-pen strip chart recorder is available to the operator to allow recording of two of the four log count rate signals by switch selection. Annunciators are activated by various conditions including short reactor period and high count rate.

Performance of Shutdown Margin Demonstrations (multiple control rods withdrawn) with the vessel head removed or de-tensioned required additional restrictions in order to provide additional protection against a reactivity excursion above what the IRMs alone provide. It is necessary to provide non-coincidence scram protection to meet these additional restrictions. Non-coincidence reactor scram is achieved by removal of the shorting links normally installed in the reactor protection system manual scram logic (see section 7.2).

Each of the four SRM channels initiates a rod block (see Section 7.7) with the mode switch in STARTUP/HOT STANDBY, or REFUEL under the following conditions:

A. SRM count level high (greater than 10^5 cps);

B. SRM channel inoperative; or

C. SRM detectors not fully inserted into the reactor core with the SRM count level below 100 cps.

The SRM detector position rod block is actuated by a position indicator on the retract mechanism. The SRM channel inoperative rod block is effective whenever the high voltage supply drops below a preset level, one of the channel modules is

not plugged in, or the channel is not in its OPERATE mode. A rod block signal from any one of the four channels prevents rod withdrawal.

Any one of the four SRM channels may be bypassed by operation of a bypass switch on the control panel. An automatic bypass of the SRM channel detector position rod block occurs when the count rate is greater than 100 cps.

Reactor startup is begun with the unbypassed SRM chambers fully inserted. At least two of the SRM chambers are required for startup. (One of the four may be bypassed and another downscale, for example.) Withdrawal of control rods increases the reactivity of the reactor core and hence, the multiplication of source neutrons. Although the withdrawal of an individual control rod may not show as a measurable increase on all chambers, the approach to criticality through distributed control rod withdrawal will be indicated by an appreciable increase in the count rate. Both the log count rate meters and the period meters provide a predictable indication as the reactor approaches criticality, becomes critical, and, with further withdrawal of control rods, becomes supercritical. After sufficient rod withdrawal to obtain a useful reactor period (on the order of 60 to 300 seconds), the reactor power is allowed to increase exponentially.

The SRM chambers may be withdrawn from the fully inserted position when the count rate is greater than 100 cps on the chamber to be withdrawn. To continue the reactor startup, withdrawal of the SRM detectors must be gradual, maintaining the SRM count rates between the low level (100 cps) and high level (10^5 cps) rod block set points. Each SRM chamber can be withdrawn individually and may be stopped at any intermediate point in its travel.

The useful range of the SRM channels is from 10^{-1} cps to 10^6 cps, which corresponds to a flux range of 10^4 nv to 5 x 10^8 nv.

7.6.1.3.3 Design Evaluation

The number and location of the SRM detectors and neutron-emitting sources have been analytically and experimentally determined to be sufficient to result in a count rate of 3 cps with all rods inserted in the cold, xenon-free condition prior to initial power operation. Verification of conformance to the minimum count rate was made at the time of fuel loading. The sources are not necessary following extended power operation. The detector sensitivity and monitor electronic characteristics have been chosen to guarantee a minimum signal to noise ratio of 3:1.

The primary safety function of the SRM subsystem is to verify that an adequate neutron flux background exists during an approach to criticality. The number of SRM channels and sources was selected to permit positive detection of an approach to criticality performed by withdrawing control rods in the region most remote from the chambers. In this worst case, the nearest unbypassed SRM channel would show a factor of 1.1 signal increase at the time criticality is achieved.

Since the SRM detectors can be retracted as reactor startup is continued, a large overlap of indication is possible during transition from the SRM to the IRM. Figure 7.6-1 depicts the possible overlap between the two monitoring subsystems. Even with the SRM detectors fully inserted, an overlap of approximately one

decade is provided. The SRM/IRM detector range overlap reduces the uncertainty in the neutron level indication during the transition from the SRM to the IRM.

The detector is designed to function in the environment in which it is located. An SRM component or power supply failure is annunciated. Failure of any SRM channel during low-flux operations with the mode switch in REFUEL or STARTUP/HOT STANDBY will initiate a rod block, thus preventing control rod withdrawal. The bypass switch arrangement permits only one SRM channel to be bypassed, guaranteeing the required detection capability during source range reactor operation.

The SRM detector position rod block assures that reactivity insertion will not be made under very low-flux level conditions unless the SRM detectors are inserted to the optimum position for flux detection. Administrative controls exist to ensure that at least two SRMs are fully inserted and operable prior to control rod withdrawal for startup.

7.6.1.3.4 Surveillance and Testing

Source range monitor failures are annunciated. All components in the SRM circuitry can be calibrated using built-in calibration equipment.

7.6.1.4 Intermediate Range Monitoring Subsystem

7.6.1.4.1 Design Basis

The intermediate range monitoring (IRM) subsystem is designed to:

A. Detect and indicate neutron flux level in a range between the SRM detection capability and the power range instrumentation capability (approximately 10^8 to 10^{12} nv), and

B. Generate trip signals to prevent fuel damage from a single operator error or a single equipment malfunction.

7.6.1.4.2 System Description

The IRM subsystem is composed of eight miniature fission chambers located radially in the core as shown in Figure 7.6-4. The figure also shows the assignment of IRM detectors to each RPS logic channel. The assignment is made to provide coverage of each quadrant of the reactor core with one detector in each channel bypassed. The detectors are attached to drive mechanisms which can position the chamber from the fully-inserted location (approximately 1.5 ft above core center), to a position approximately 2.5 feet below the reactor core. The detectors and the drive systems are similar to those used in the SRM subsystem except for the range of measurement. The detectors are not withdrawn from their fully inserted position until the mode switch has been turned to the RUN position.

The output of each fission chamber is processed through a wide-band amplifier to a voltage variance circuit (Campbelling or root mean square technique)[2] and a signal conditioner to produce an output which is linearly proportional to the reaction rate in the chamber. This output is provided to a trip unit and is used to drive one pen in one of four two-pen strip chart recorders.

The IRM subsystem can detect flux levels from the upper end of the SRM range to approximately 34% of full power.

A neutron flux of 5×10^7 nv (upper source range) provides a signal of approximately 0.1 full scale on the lowest IRM range.

In order to handle the wide range of IRM detection, the IRM equipment is provided with a remote range switch which selects various ranges of attenuation of the detector signal. As the neutron flux level changes during reactor startup, the operator manually up-ranges the IRM.

The IRM subsystem provides trip signals for both the RPS and the rod block circuitry; all the trips but one, as described in the following, are in effect with the mode selector switch in the REFUEL or STARTUP/HOT STANDBY positions.

Each IRM detector provides a trip signal to the RPS scram logic circuitry under the following conditions:

A. IRM high-high flux level,

B. IRM channel inoperative, or

C. IRM high-high and companion APRM downscale in the "RUN" mode.

In order for a scram to occur, a scram trip signal must be received in both RPS logic channels. The scram-initiating high-high-level trips provide automatic shutdown capability for operation from just critical to the lower portion of the power range.

Although the IRM instrumentation is calibrated to read core average power, because of the difference of location, the inner set of chambers during a startup will read higher than those located in the periphery. This results in the inner IRM's reaching scram level before the outer IRMs reach the same level and the APRM reading has exceeded the downscale trip. To provide a better indication of core average power and therefore a better scram setting, a fixed power scram is utilized on the APRM system when the mode switch is in the STARTUP/HOT STANDBY position (Analytical Limit: 20% RTP). This scram provides a better means of achieving a power scram in the low power region. The IRM scram provides backup protection to the APRM in addition to providing protection against single control rod withdrawal errors (Analytical Limit: 125/125 divisions of full scale). By not having the restriction of a fixed power scram on the IRM, all ranges of the IRM are available for indication and adequate overlap between the IRM and APRM exists.

When the reactor mode switch is in REFUEL or STARTUP/HOT STANDBY, the IRM subsystem provides a rod block signal to the rod block circuitry under the following conditions:

A. IRM high-flux level,

B. IRM inoperative,

C. IRM downscale on any range but the lowest, or

D. IRM detectors not fully inserted into the core.

Any one of the eight IRM channels can initiate a rod block.

Any one IRM detector channel in each RPS logic channel may be manually bypassed, making ineffective the scram and rod block trips associated with that individual IRM channel.

7.6.1.4.3 Design Evaluation

The number and location of the IRM detectors have been analytically and experimentally determined to provide sufficient intermediate range flux level information under the worst permitted bypass and chamber failure conditions. Figure 7.6-1 shows the range capability of the IRM channels. The ability of the monitor output to provide an accurate measurement of the detector reaction rate over the flux range of interest has been verified by experimentation with the root mean square technique.[2] IRM channel redundancy provides a margin for component failure and allows continued reactor operation with one IRM bypassed in each RPS logic channel. The scaling arrangement in the IRM subsystem assures that for all unbypassed IRM channels, the scram and rod block trips are no more than a factor of 10 above the IRM level at the time. This assures that, should scram or rod block action be needed due to rapid or unintentional neutron flux increases, the trip signal will be generated before the flux increases by a factor greater than ten, thus providing a conservative margin to fuel damage.

A range of rod withdrawal accidents has been analyzed. The most severe case involves an initial condition in which the reactor is just subcritical and the IRM subsystem is not yet on-scale. This condition exists at the three-quarter rod density illustrated in Figure 7.6-5 (rod density is the total notches inserted in the core divided by the number of notches which would be inserted when all rods are fully inserted). Full withdrawal of the worst-case control rod will result in the power distribution indicated in Figure 7.6-6; it should be noted that this is an out-of-sequence rod which would normally be blocked by the rod worth minimizer (see Section 7.7). Figure 7.6-5 indicates the location of the withdrawn rod and the distance to the IRM chambers in the two RPS logic channels which will initiate a scram if the IRM channels nearest to the withdrawn rod are bypassed.

The power distribution shown in Figure 7.6-6 indicates that the ratio of the resultant neutron flux at the farthest detector to the neutron flux peak is 2.2×10^{-4}. As the trip of the IRM channel associated with this detector is set to operate at a flux of less than 6×10^{8} nv (rod is blocked if not set on the proper range), the flux in the power peak is less than 2.7×10^{12} nv. At this flux level, the power at the peak is limited to 7.7% of rated average power; hence, it will be within thermal limits, even if the recirculation pumps are shut down.

The overlap between the IRM and the power range monitoring subsystem is sufficient to guarantee a safe transition between the instrumentation ranges (Figure 7.6-1). Overlap between the SRM and IRM ranges is discussed in Section 7.6.1.3.3.

During periods of reactor operation when the IRM is required for flux level indication the IRM detector position rod block prevents rod withdrawal unless the detectors are fully inserted.

The IRM detectors are chosen with characteristics which permit reliable performance in the reactor environment.

IRM failures are annunciated and, during low-flux level reactor operation, result in a RPS single logic channel trip and rod block. Thus, further rod withdrawal is prevented, and a reactor scram would be initiated by any condition resulting in a trip of the other RPS logic channel.

7.6.1.4.4 Surveillance and Testing

IRM component or power supply failures are annunciated in the control room. Built-in calibration equipment is provided to periodically check and reset the IRM equipment.

7.6.1.5 Power Range Monitoring Subsystem

Power range instruments include LPRMs, APRMs, OPRMs, RBM, and TIP (see Figure 7.6-1 and 7.6-2).

7.6.1.5.1 Local Power Range Monitoring Subsystem

7.6.1.5.1.1 Design Basis

In order for the power range instrumentation to meet the general design requirements for power range flux monitoring and prevention of excessive local and bulk power densities, the LPRM subsystem must:

A. Continuously monitor, over its design range, local neutron flux and alarm on excessive conditions;

B. Permit evaluation of the critical core parameters (fuel thermal limits) to an accuracy consistent with core design and established limits; and

C. Permit demonstration of compliance with the critical core parameters (fuel thermal limits) with a speed and ease consistent with efficient operation of the plant.

7.6.1.5.1.2 System Description

The LPRM subsystem output signals are used to demonstrate that the core is operating within the established limits for minimum critical power ratio (MCPR), maximum average planar linear heat generation rate (MAPLHGR), and maximum fraction limiting power density (MFLPD). This subsystem provides the information needed for evaluating the detailed characteristics of the power distribution and for other technical evaluations. The LPRM subsystem provides input to the average power range monitoring subsystem, the oscillating power range monitor, and rod block monitor subsystem, which are described below.

The LPRM subsystem, which uses dc measurement techniques, consists of miniature fission chambers located within the reactor core, electronic signal conditioning equipment located in the control room, and a TIP calibration system.

Each LPRM has a high neutron flux level alarm and a common annunciator located on the control board.

Figures 7.6-7 and 7.6-8 indicate the core location of the LPRM strings. Each LPRM string consists of four miniature fission chambers which are spaced vertically at 3-foot intervals.

The top and bottom chambers are located 1.5 feet from the core boundaries, thereby providing uniform core coverage in the axial direction. Also included in each detector string is a calibration tube which accepts the TIP used to measure the axial flux distribution and calibrate the LPRM subsystem (see Figure 7.6-8).

Figure 7.6-9 illustrates that, due to the equivalence of locations resulting from symmetry, the LPRM subsystem monitors all unique locations within the central region of the core when the core is operated with quadrant symmetric control rod patterns.

The LPRM flux amplifiers are calibrated using data from the TIP calibration system, heat balance data, and some analytical data. The basic process involves:

A. Running the TIP system and accumulating axial profile data,

B. Normalizing the axial profile data,

C. Determining for each detector elevation the average nodal heat flux in four adjacent fuel nodes at that elevation, and

D. Adjusting flux amplifiers until meter readings are proportional to heat flux.

These calculations are performed using the process computer (see Section 7.5). When these adjustments have been made, the LPRM signals are proportional to the average nodal heat flux in the four adjacent fuel nodes at the detector elevation. The 16 LPRM amplifier signals adjacent to a control rod selected (four detectors in each of four adjacent strings) are displayed on 16 centrally located meters. This display directs the attention of the operator to the local power level prior to and during rod motion. These 16 signals are also used by the RBM. When

rods near the edge of the core are selected, two or three detector strings may be used. When rods on the core periphery are selected, the RBM is bypassed. In both previous cases, the readings are zeroed on the corresponding unused meters. The operator may view any desired region of the core by selecting the control rod in the area of interest. A selected set of LPRM signals is used as an input to each of the six APRM channels.

7.6.1.5.1.3 Design Evaluation

The number and location of LPRM detectors provides the capability to determine local heat flux in all unique locations in the central region of the core. Although each unique location in each core quadrant is not specifically monitored, the quadrant symmetry, illustrated in Figure 7.6-9, effectively provides knowledge of the flux level throughout the core.

The previously described method of calibration using the TIP provides a method of correlating LPRM measurements with local thermal conditions; thus, the LPRM measurements are a valid representation of local thermal conditions.

Each individual LPRM channel annunciates an alarm upon detection of a flux level exceeding a preset limit. Thus the operator receives warning of local high or low flux conditions or LPRM component failure.

The LPRM detectors are selected with characteristics which guarantee reliable operation in the reactor environment; reactor temperature, pressure, neutron and gamma flux, and detector electrical requirements are considered in detector selection.

The use of the LPRM signals in the rod block monitor provides a positive assurance that local thermal peaks which would cause fuel damage will be prevented.

7.6.1.5.2 Average Power Range Monitoring Subsystem

7.6.1.5.2.1 Design Basis

The APRM subsystem must continuously indicate core average flux level and initiate trips to prevent excessive average power density. In order to fulfill its design requirement, the APRM subsystem must:

A. Initiate trip signals which scram the reactor automatically before the neutron flux level exceeds specified values;

B. Initiate a rod block trip signal, thereby preventing core average power increases to excessive levels with reduced recirculation flow (the rod block trip setpoint is lower than the scram setpoint);

C. Provide a continuous indication and record of the bulk thermal power of the reactor in the power range;

D. During the worst permitted bypass and chamber failure conditions, generate a scram signal during neutron flux level transients before fuel damage has occurred.

E. Continue to perform its function following any single component failure within the subsystem. In order for the APRM to satisfy this requirement, there must be two operable APRMs in each RPS logic channel. In a practical sense, this requirement results in three APRM channels for each bus to permit bypassing for calibration and maintenance during operation.

7.6.1.5.2.2 System Description

The APRM subsystem consists of electronic equipment which averages the output signals from selected groups of LPRM flux amplifiers. As shown on Figures 7.6-10 and 7.6-11, the system consists of six channels. Each of these channels averages the output signals of 20 or 21 LPRM flux amplifiers.

Three of the APRM channels provide trip inputs to one RPS logic channel, and the other three APRM channels feed the other logic channel.

Each APRM channel provides a rod block trip under the following conditions:

A. High-neutron flux (flow referenced and fixed level);

B. APRM channel inoperative:

1. Module unplugged,

2. Less than 50% of assigned LPRMs operative, or

3. Function switch not in OPERATE position.

C. APRM downscale with the mode switch in RUN, or

D. Flow converter inoperative.

Each APRM channel provides a scram trip signal under the following conditions:

A. High-high neutron flux (flow referenced and fixed level), or

B. APRM channel inoperative:

1. Module unplugged,

2. Less than 50% of assigned LPRMs operative, or

3. Function switch not in OPERATE position.

In order for a scram to occur, a scram trip signal must be received by both RPS logic channels. Any one of the six APRM channels can initiate a rod block. Switches located on the reactor console allow the operator to bypass the trips from

one of the APRM channels in each of the RPS logic channels; the bypass is effective for both the scram and rod block trip signals.

Figure 7.6-2 depicts half of the neutron monitoring system. A recirculation (driving) loop flow signal is supplied to the APRMs and the RBM assigned to RPS trip system A and an identical signal is supplied to the APRMs and the RBM associated with RPS trip system B. Note that the RBMs are assigned to an RPS trip system only for convenience. The sensor and signal conditioner arrangement furnishing this signal is shown in Figure 7.6-12. There are two recirculation (driving) flow loops, each loop containing one flow sensor. The differential pressure reading obtained from the flow sensor is supplied to parallel dP transmitters. The resultant current signals are further conditioned and fed to summers so that there are two signal outputs, each equal to the total driving loop flow. These two signals are fed to the flow converters which further condition the flow signals for use by the APRMs and the RBMs as a reference signal for the rod block alarms and the APRM scram. Since both flow converter outputs should be proportional to the sum of the two driving loop flows, a comparison is made of the two flow converter outputs; and a rod block is actuated if the difference between these two signals exceeds approximately 10%. The purpose of this comparison alarm is to allow for identification of a failed flow signal converter which would cause an erroneous reference signal to be supplied to one set of APRMs or one RBM.

Because each driving loop signal furnished to each flow converter is proportional to the sum of the two driving loop flows (total flow), single-loop operation results in the two signals indicating that fraction of total flow supplied by the loop in operation.

With single-loop operation and with the equalizer valves closed as required by the Unit 2 license (Unit 3 equalizer valves have been removed), there is a slight difference (approximately 1%) between the measured flow and the actual core flow. This difference is not considered significant. Since the loop flow indication is always greater than the actual core flow, the setpoints of the APRM scram and rod block are reduced (see the plant Technical Specifications and Technical Requirements Manual for operating limits).

The rod block setpoint is automatically varied with recirculation flow (with mode switch in RUN) as shown in Figure 7.6-13. The slope of the trip vs. flow relationship is determined by the characteristic bulk power vs. flow relationship of the reactor which was determined experimentally. The absolute magnitude of the trip setpoint was established to prevent operation significantly above the flow control characteristic that includes the 100% flow and 100% power point.

The flow dependent bias which determines the trip level is subject to both positive and negative errors originating, in the flow monitoring equipment. However, the equipment limits the trip bias so that the trip level can never exceed the intended level for 100% flow, regardless of the magnitude of positive errors in flow signal. Negative errors are in the conservative direction.

The readout equipment for the APRM system is located in the control room. The APRM channel output signals are continuously displayed on recorders shared with the IRM channels and located on the control board. The output signals are adjusted so that the meter deflections indicate percent of rated bulk thermal power. Bulk thermal power is determined using heat balance techniques. Adjustment of the APRM channel readings is not possible from the control board and does not

affect the output signals of the LPRM amplifiers which are averaged in the APRM channel.

If an LPRM used to provide input to an APRM channel fails, the operator can manually bypass this invalid input. The APRM channel then properly averages the inputs from the remaining LPRM channels. If the number of bypassed LPRMs used as inputs to an APRM channel exceeds a preset number, the APRM instrument inoperative alarm is actuated. This feature assures that the APRM system will adequately perform its safety function of terminating average neutron flux level transients through scram initiation. In addition to the automatic input monitoring, administrative controls require at least 50% of all LPRMs and at least 2 LPRMs per level for an APRM to be operable. The "too few input trip" feature also automatically provides a high degree of assurance that the APRM system will be capable of preventing fuel damage due to rod withdrawal errors.

7.6.1.5.2.3 Design Evaluation

As shown in Figures 7.6-10 and 7.6-11, the LPRM inputs to the APRM channels provide a wide sampling of local flux levels on which to base an average power level measurement. The fact that three APRM channels are provided for each RPS logic channel assures that at least two independent average power measurements will be available under the worst permitted bypass or failure conditions. The six APRM channels provide continuous indications of core average power level based on different samplings of local flux levels. Figures 7.6-14 and 7.6-15, which are the results of analysis, show that the APRM provides valid average power measurements during typical rod- or flow-induced power level maneuvering.

Using a plant heat balance technique, the APRM measurements are calculated such that the meter indications are within ±2% of the rated bulk thermal power when the power level is ≥25% of rated; this calibration is maintained by procedure.

The effectiveness of the APRM high-flux scram signals in preventing fuel damage following single component failures or single operational errors is shown in each section of this report where system failures are analyzed; in all such failures, no fuel damage occurs. Since only two APRM channels in each RPS logic channel are required for effective detection of bulk power level transients, the same effectiveness is attained even under the worst permitted bypass conditions.

The APRM rod block setpoint is set lower than the scram setpoint; thus, reactivity insertions due to rod withdrawal errors are terminated well before fuel damage limits are approached.

To account for the decreasing margin to fuel damage at a given power level with reduced recirculation flow, the APRM rod block setpoint is varied with flow.

Average power range monitor component failures which result in upscale, downscale, or instrument inoperative conditions are annunciated, and the reduction of LPRM inputs for any APRM channel below a preset number gives an alarm, rod block, and a logic channel trip. These features warn of loss of APRM capability.

7.6.1.5.3 Rod Block Monitor

7.6.1.5.3.1 Design Basis

The RBM system is designed to prevent local fuel damage as a result of a single rod withdrawal error under the worst permitted RBM bypass conditions and to provide a signal to permit operator evaluation of the change in the local relative power level in the vicinity of a rod that is being withdrawn.

7.6.1.5.3.2 System Description

The RBM system uses signals from the four LPRM strings adjacent to the selected control rod (Figure 7.6-16) and the recirculation flow sensors. The eight signals from the A and C levels are averaged in one channel and the eight signals from the B and D levels are used in the second channel. The RBM output is automatically adjusted upon rod selection so that its output is equal to (or in some circumstances greater than) the reading of a preselected APRM channel. This gain setting is held until a new control rod is selected. An in-depth description of the RBM system is given in Topical Report APED 5706, "In-Core Neutron Monitoring System for General Electric Boiling Water Reactors," Revision 1, April 1969.

Both RBMs are located in a single bay and each derives its input signals from a LPRM input assignment matrix within that RBM.

No indexing mechanism is provided in the RBM for selection of LPRM strings. Selection of a rod automatically energizes a "hard wired" circuit, closing relays connected to the LPRMs associated with the rod selected, and providing their input to the RBM. Thus improper LPRM selection cannot occur, although it is possible that previously selected LPRMs will not be deselected. Failure to deselect requires either a failure in the rod pushbutton selection matrix or a short in the circuits to the RBM. The first failure would be indicated to the operator as two rods selected by multiple lights on the pushbutton selection board and would also cause a rod withdrawal prohibit due to a multiple rod selection signal. The second failure, a short, would result in two sets of LPRM inputs to the RBM. In this event the RBM would select the higher value or the combined values and thus read a more conservative power condition.

The RBM alarm signals are routed to the reactor manual control system to provide a rod block if a predetermined level is exceeded. The rod block portion of the reactor manual control system associated with the RBM is arranged in a two-channel configuration to provide some redundancy. Other signals associated with the RBM (e.g., the nonannunciated rod block signal obtained when the RBMs are adjusting their gains to obtain the same reading as the reference APRMs) are fed to a single point in the reactor manual control system.

Either channel independently prevents rod withdrawal under the following conditions:

A. High neutron flux (flow referenced),

B. RBM channel inoperative, or

C. Channel reading below RBM downscale trip setpoint.

The RBM system is equipped with an automatic bypass feature so that both RBMs are bypassed in the event that the power level is below a level where local damage is possible (30% power; this signal is derived from the reference APRMs) or if a peripheral rod is selected; i.e., a rod in the outer region of the core, which cannot be instrumental in causing local fuel damage. A manual bypass switch allows the operator to manually bypass either RBM for maintenance or calibration.

Since all APRMs are measuring the core average flux with the same precision, any APRM may be selected for use as the primary reference APRM. The channels which were selected are APRM channel 3 for RBM channel 7, and APRM channel 4 for RBM channel 8. The alternate reference APRMs are channels 2 and 5 for RBMs 7 and 8, respectively. These reference signals are routed to the RBMs via contacts associated with the APRM bypass switches, arranged so that if the primary reference APRM is bypassed, the alternate reference APRM signal is automatically routed to the RBM. Note that the primary reference APRM and the alternate reference APRM cannot be bypassed at the same time because they are both assigned to the same RPS trip system.

An inoperative APRM will cause a rod block; therefore, no rod can be withdrawn until either the inoperative condition is corrected or the inoperative APRM is bypassed (in which case the alternate APRM reference is used). In any event, the RBM will be operable when it is needed.

RBM gain adjustment can be expressed as follows:

If $P_L \geq P_A$, then gain = 1.0

If $P_L < P_A$, then gain = P_A/P_L

where:

P_L = average power in vicinity of rod selected for withdrawal. (This is the power seen by the RBM.)

P_A = core average (bulk) power

Upon selection of a rod, signals directed to the LPRM Input/Rod Selected Matrix which routes the appropriate LPRM signals to the RBM inputs. An operational amplifier in each of the RBMs averages these LPRM signals and the result is compared with the reference APRM signal as the amplifier gain factor is adjusted upward in small steps from a value of 1.0. The comparator terminates the gain adjustment sequence when the average is equal to or slightly greater than the reference signal value. If the gain cannot be properly adjusted, a "failure to null" inoperative trip will be generated.

The RBM high trip varies linearly with recirculation flow along power-flow lines, the appropriate trip setpoint (HIGH, INTERMEDIATE, or LOW) is automatically selected by the RBM when a new rod is selected. The setting for the intermediate and low lines are set below the high line and are set to their lowest value as they are not used in the cycle specific core analysis. For increases in power, the operator can transfer to the next higher block by pushing a set-up button.

7.6.1.5.3.3 Design Evaluation

Since the RBM uses LPRM, signals, it can identify the approach of local thermal flux conditions which could result in local fuel damage. The fact that either RBM channel can independently initiate a rod block provides assurance that a rod withdrawal error will be terminated even with one RBM channel bypassed.

The effectiveness of the RBM to prevent local fuel damage as a result of a single rod withdrawal error has been analytically determined. The initial condition is conservatively defined such that the reactor is operating at maximum permitted power with fuel thermal margins (MCPR, TLHGR and SLHGR or MLHGR) at steady-state and transient limits in a region adjacent to a fully inserted control rod; no credit is taken for the action of the rod worth minimizer. The response of the least responsive RBM channel is calculated as a function of rod withdrawal distance. The thermal margins are also calculated as a function of rod position. The analysis indicates that the rod block level is reached well before MCPR reaches 1.0 and before the linear heat generation rate reaches the damage level.

7.6.1.5.3.3.1 Analysis of Rod Block Monitor Design Requirements

A detailed analysis was made of the functional requirements of the RBM. The analysis revealed that the rod block monitor system performs no primary reactor protection function, and the system, as designed with redundancy of channels and equipment for testing and maintenance, will reliably and accurately serve its intended functions, i.e., to avoid local fuel damage as a result of extreme abnormal transients. It was thus concluded that designing the RBM to the requirements of IEEE 279 would provide no substantial addition to the protection of the public health and safety.

7.6.1.5.3.3.1.1 Comparison to IEEE 279

The RBM system contains some redundancy in that two independent RBM channels are provided. Each of these channels independently blocks rod withdrawal, receives inputs from different LPRMs and has its own power supply.

A comparison has been made of the RBM conformance to IEEE 279. The following list represents various aspects wherein the rod block monitor system does not comply with RPS grade separation, redundancy, and isolation.

A. Two redundant RBM channels are provided; however, these channels are located in the same cabinets and thus are not separated or isolated;

B. The rod selection information, including the rod selection pushbutton, is not redundant;

C. A single set of taps are provided on the flow measurement venturi in each recirculation loop;

D. The flow sensing lines used for each RBM are not separated or isolated;

E. The flow signal transducers for the two RBMs are not separated or isolated;

F. The LPRM amplifier signal inputs and outputs are neither separated nor isolated from each other;

G. The APRM reference signals which are input to each RBM channel through the LPRM select matrix are independent, but are located in the same cabinets and thus not separated;

H. The independent RBM level readouts and status displays are neither separated nor isolated However, signals to the Neutron Monitoring Process Recorders are isolated; and

I. The independent rod block signals to the reactor manual control system circuitry are neither separated nor isolated.

7.6.1.5.4 Traversing Incore Probe

The TIP system includes five TIP machines, each of which has the following components:

A. One traversing incore probe,

B. One cable drive mechanism,

C. One indexing mechanism, and

D. Ten guide tubes of which one is to a common core location.

The TIP system's primary purpose is to provide a means to measure axial core flux profile through the radially located guide tubes. The system also allows calibration of LPRM signals by correlating TIP signals to LPRM signals. The guide tubes inside the reactor are divided into groups. Each group has its own associated TIP machine.

A TIP machine uses a fission chamber attached to a flexible drive cable, which is driven from its lead shielded storage chamber located outside the primary containment by a pinion gear box assembly. The flexible cable is contained by guide tubes that continue into the reactor core. The guide tubes are specially prepared to provide a durable, low-friction surface and are a part of the LPRM detector assembly. The indexing mechanism allows the use of a single detector in any one of 10 different tube paths. The control system provides both manual and semiautomatic operation. The TIP signal is amplified and displayed on a meter and input to the process computer. Core position versus neutron flux is recorded on an x-y plotter.

The cable drive mechanism contains the drive motor, the cable takeup reel, an analog probe position indicator, which drives a recorder, and a counter to provide digital pulses to the control unit for positioning the TIP at specific locations along the guide tube.

The cable drive mechanism inserts and withdraws the TIP and its cable from the reactor and provides detector position indication signals. The drive mechanism consists of a motor and drive gear box which drives the cable in the manner of a rack and pinion. A two-speed motor provides a high speed for insertion and withdrawal and a low speed for scanning the reactor core.

The analog position indicator and the counter (digital) are also driven directly from the output shaft of the cable drive motor. The analog position signal is generated from a potentiometer and a flux amplifier output are used to plot neutron flux versus incore position of the TIP. The digital counter is used to position the TIP in the guide tube through the control logic with a linear position accuracy of plus-or-minus 1 inch. The digital counter can control TIP positions at the top of the core, for initiation of scan, and at the bottom of the core, for changing to fast withdrawal speed.

A position limit switch provides an electrical interlock release when the probe is withdrawn clear of the indexing mechanism to allow the TIP to be indexed to the next guide tube location. The limit switch is actuated when the end of the TIP passes a switch in the guide tube in use. The cable drive motor includes an ac voltage-operated brake to prevent coasting of the TIP after a desired incore position is reached.

Each indexing mechanism functions as a circular transfer machine with 10 selectable indexing points. Nine of these locations are for the guide tubes uniquely associated with that particular TIP machine. The final location is for the guide tube common to all the TIP machines. Indexing to a particular tube location is accomplished manually at the control panel by means of a position selector switch which energizes the electrically-actuated rotating mechanism. The tube transfer mechanism is part of the indexing mechanism and consists of a fixed circular plate containing 10 holes on the reactor side of the primary containment which mates to a rotating single-hole plate. The rotating plate aligns and mechanically locks with each fixed hole position in succession. The indexing mechanism is actuated by a motor-operated rotating drive. Electrical interlocks prevent the indexing mechanism from changing positions until the probe cable has been completely retracted beyond the transfer point. Additional electrical interlocks prevent the cable drive motor from moving the cable until the transfer mechanism has indexed to the preselected guide tube location.

A valve system is provided with a valve on each guide tube entering the primary containment. These valves are closed except when the TIP system is in operation. A ball valve and a cable-shearing valve are mounted in the guide tubing just outside of the primary containment. A valve is also provided for gas purge line to the indexing mechanisms. A guide tube ball valve opens only when the TIP is being inserted. The shear valve is used only if a containment isolation occurs when the TIP is beyond the ball valve and cannot be withdrawn. The shear valve, which is controlled by a manually-operated keylock switch, can cut the cable and close off the guide tube. The shear valves are actuated by detonation squibs. The continuity of the squib circuit is monitored by indicator lights in the control room.

An additional manual ball valve is installed between the automatic ball valve and the drywell penetration.

A guide tube ball valve is normally de-energized and in the closed position. When the TIP starts forward the valve is energized and opens. As it opens it actuates a set of contacts which gives a signal light indication at the TIP control panel and bypasses an inhibit limit which automatically stops TIP motion if the ball valve does not open on command. A Group 2 containment isolation signal initiates TIP drive withdrawal and closes the ball valve when the TIP is retracted.

7.6.1.5.5 Surveillance and Testing

Power range nuclear instrumentation failures are annunciated. Monitor circuitry is arranged to facilitate testing with simulated signals. The TIP system provides information used to periodically calibrate the system.

7.6.1.6 Oscillation Power Range Monitoring Subsystem

The Oscillation Power Range Monitor (OPRM) subsystem is a microprocessor-based monitoring and protection system, which will:

- detect a thermal-hydraulic instability,
- provide an alarm on detection of an oscillation (based on period-based algorithm only), and
- when armed, initiate an Automatic Suppression System (ASF) trip to suppress an oscillation prior to exceeding fuel safety limits.

The subsystem design, technical details, equipment qualifications, and validation are discussed in Reference 3. The NRC has accepted the above reference, and had issued a safety evaluation report (Reference 4).

7.6.1.6.1 Design Basis

7.6.1.6.1.1 Safety Design Bases

Boiling water reactor cores may exhibit thermal-hydraulic reactor instabilities in certain portions of the core power and flow operating domain. General Design Criterion 10 (GDC 10) requires that the reactor core be designed with appropriate margin to assure that acceptable fuel design limits will not be exceeded during any condition of normal operation including the effects of anticipated operational occurrences. GDC 12 requires assurance that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are either not possible or can be reliably and readily detected and suppressed. The OPRM is provided to meet the requirements of these GDCs by adding a detect and suppress feature to the Reactor Protection System.

7.6.1.6.1.2 Power Generation Design Bases

The power generation design basis of OPRM consists of assuring that spurious scrams do not occur. This objective is accomplished in part by establishing an exclusion region, as discussed below in Section 7.6.1.6.2, where the thermal-hydraulic oscillations are not postulated to occur.

7.6.1.6.2 System Description

Detailed description of OPRM subsystem design and physical arrangements are provided in the Generic Topical Report (Reference 3). Basic and station specific information is summarized here.

The OPRM subsystem consists of 4 OPRM trip channels, each channel consisting of two OPRM modules. Each OPRM module receives input from a group of LPRMs combined into localized monitoring cells. It also receives input from the Average Power Range Monitor (APRM) power and Reactor Recirculation flow signals to automatically enable the trip function of the OPRM module, when it is armed. A block diagram showing the relationship of OPRM with other nuclear instrumentation is shown in Figure 7.6-2. Reactor coolant flow instrumentation feed to the OPRM is shown in Figure 7.6-12.

The OPRMs are capable of detecting thermal-hydraulic instabilities within the reactor core. The OPRMs are designed to provide an alarm and initiate an automatic suppression function (ASF) trip, when they are fully armed, to suppress oscillations prior to exceeding the MCPR safety limits. The OPRMs are auto enabled at the specified reactor recirculation flow and reactor power setpoints. The ASF outputs initiate an ASF trip through the RPS based on the existing plant trip logic and configuration. The OPRM System provides annunciator windows, SER messages and indicating lights for pre-trip conditions and other alarm functions such as Trip, Alarm, Trouble, Inip Bypass and Trip Enabled to be displayed in the Main Control Room (MCR).

Each OPRM includes a signal processing module, Automatic Suppression Function (ASF) Trip Relay Assembly , OPRM Annunciator Relay Assembly, two Digital Isolation Blocks (DIBs) and Enable and Bypass Selector Switches.

The OPRM trip circuits may be bypassed by a selector switch. The bypass is accomplished through hardwired bypass of ASF trip relay contact by a selector switch-actuated auxiliary relay contact and through actuation of OPRM logic circuits and software. The bypass condition of the OPRM module is indicated by the sequence of events monitor and by indicating lights. The OPRMs may be manually enabled by the selector switch for any recirculation flow and reactor power levels.

a) Modes of Operation

The OPRM has two modes of operation, operate and test. In the operate mode, it performs all of its normal trip and alarm functions as well as broadcasting status information to fiber optic output ports. The test mode is utilized for test, calibration, setpoint adjustment and downloading of the event buffer. In the test mode, the OPRM's trip output is bypassed and the channel is considered inoperable. Entry into the test mode is controlled by a key switch and is annunciated in the control room.

With the OPRM in its operate mode and the maintenance terminal connected, the maintenance terminal may only be used to collect data which is broadcast by the OPRM at fixed intervals. Communications in this mode are one way, namely OPRM to maintenance terminal. The OPRM will not respond to commands from the maintenance terminal when in the operate mode. Thus, the maintenance terminal cannot affect OPRM operation.

In the OPRM test mode and the maintenance terminal connected, bi-directional, fiber optic communications are established between the OPRM and its maintenance terminal. In this mode, commands may be sent from the maintenance terminal to the OPRM to perform such actions as altering the OPRM configurations and setpoints, downloading event buffers and error logs and testing various OPRM functions. Additional, conventional test cables may be connected between the maintenance terminal and a test port on the OPRm for use in calibration and testing. To access this test port, a shorting plug must be removed from the OPRM. Removal of the shorting plug causes the OPRm to become inoperable and is annunciated in the control room.

b) Event Buffer

When a trip occurs, data immediately prior to and following the trip is captured in an event buffer. This buffer may be downloaded to aid in the analysis of the trip. The event buffer can also be captured and downloaded at any time for non-trip analysis by placing the OPRM in the test mode.

c) Maintenance Terminal

A portable maintenance terminal is utilized for system testing, calibration and data collection. It is connected to the OPRM via fiber optic cables. This maintains isolation between the safety related OPRM and the non-safety related maintenance terminal.

d) Power Supply

Power supplies for the OPRMs are the same as those for the APRM and LPRM Group channels. These power supplies provide the required voltage sources for OPRM signal processing modules, DIBs, ASF Trip Relay Assemblies, OPRM Annunciator Relay Assemblies, the new flow units, analog isolators and the existing APRM, RBM and LPRM channels.

e) Physical Arrangement

The OPRM signal processing modules are installed in APRM and LPRM Pages of the Power Range Neutron Monitoring System (PRNMS) Panel (see Figure 7.6-13). Selector switches required for the manual enable functions and the bypass selector switches are installed in the 902-5 panel. Indicating lights for the enable and bypass functions will be installed in the 902-5 panel. Automatic Suppression Function (ASF) Trip Relay Assembles, OPRM Annunciator Relay Assemblies, Analog Isolators and Digital Isolation Blocks are installed in the PRNMS Panel.

f) Exclusion Region

The OPRM is required to be operable in order to detect and suppress neutron flux oscillations in the event of thermal-hydraulic instability. As described in Reference 3, the region of anticipated oscillation is defined by reactor thermal power (RTP) $\geq$30% and core flow <60% or rated core flow. However, to protect against anticipated transients, the OPRM is set to be operable with reactor thermal power $\geq$30%. This provides sufficient margin to account for potential instabilities as a result of a loss of feedwater heater transient. It is not necessary for the OPRM to be operable with reactor thermal power <30% and core flow >60%, which is defined as the exclusion region.

g) Algorithm

Reference 3 describes three separate algorithms for detecting stability related oscillations: the period based detection algorithm, the amplitude based algorithm, and the growth rate algorithm. The OPRM System hardware implements these algorithms in microprocessor based modules. These modules execute the algorithms based on LPRM inputs and generate alarms and trips based on these calculations. These trips result in tripping the Reactor Protection System (RPS) when the appropriate RPS trip logic is satisfied. Only the period based detection algorithm is used in the safety analysis. The remaining algorithms provide defense in depth and additional protection against unanticipated oscillations.

h) Trip Function

The OPRMs are designed to provide an alarm (based on period-based algorithm only) and initiate, when armed, an automatic suppression function (ASF) trip to suppress oscillations prior to exceeding the MCPR safety limits. The OPRMs are auto enabled at the specified reactor recirculation flow and reactor power setpoints. The OPRM initiates an ASF trip through the RPS based on the existing plant trip logic and configuration. The OPRMs provide alarm for pre-trip conditions and other functions such as Trouble, INOP, and Trip Enabled to be displayed in the Main Control Room (MCR). Table 7.6-1 lists the OPRM trip functions and setpoints.

i) Alternate Backup Method

At times when OPRM channels may be inoperable, and until they can be restored to operable status, an alternate method of detecting and suppressing thermal hydraulic instability oscillations can be used. This alternate method is described in Reference 7. It consists of increased operator awareness and monitoring for neutron flux oscillations when operating in the region where oscillations are possible. If indications of oscillation, as described in Reference 7, are observed by the operator, the operator will take the actions described by procedures, which include initiating a manual scram of the reactor.

j) Component Qualification Considerations

The OPRM devices are designed Class 1E, Seismic Category I and are qualified to the applicable portions of IEEE-381 and IEEE-344.

k) Single Failure Considerations

Since the OPRMs perform a protective function, they are required to withstand a single failure. To ensure acceptable defense against single random failures the combination or architecture, wiring practices and use of isolation devices is applied to provide required redundancy, isolation and physical independence.

There are two redundant OPRM channels in each RPS division. OPRMs in each RPS division are electrically isolated and physically separated from OPRMs in other RPS divisions. Within each OPRM channel there are two OPRM modules. The use of the two OPRM modules per channel provides redundancy against an OPRM hardware failure in the same channel. The redundant OPRM modules in the same RPS division share the same Class 1E power supplies as those used by the safety-related APRM modules in that RPS division. However, each OPRM module is electrically isolated from the companion module in the same channel.

Common software failures do not lend themselves well to single failure analyses. System reliability and safety requirements are examined in the description of the software design process and quality assurance considerations as discussed in Reference 3.

l) Redundancy, Diversity, and Separation

Since the OPRM's operation is based on interface with PRNMS and RPS, its redundancy, diversity and separation requirements are the same as the requirements for these systems. The LPRM analog signals, which are locally wired, are provided to OPRMs with the same redundancy and separation as provided to the APRM channels and LPRM groups. One exception is that the output to the RPS from shared APRM Channels 3 and 4 is fanned out by OPRM Channels 3, 4, 7 and 8. This eliminates the double up of Channels 3 and 4 in RPS divisions A2 and BI. Thus, two OPRM channels fall into each RPS division for the RPS trip circuits providing the required redundancy between RPS divisions and between the OPRM channels. The assignment of OPRM channels and existing APRM channels for each RPS division is as follows:

RPS Division	OPRM Channel	APRM Channel
A1	1,3	1,3
A2	2,7	2,3
B1	8,5	4,5
B2	4,6	4,6

7.6.1.6.3 Design Evaluation

7.6.1.6.3.1 Conformance to Functional Requirements

The OPRM subsystem is designed to alarm when a stability-related thermal-hydraulic oscillation is detected (based on period-based algorithm only), and to initiate, when armed, as ASF trip when oscillations are large enough to threaten fuel safety limits. The OPRM design assures high reliability as it is governed by Quality Assurance requirements, and applicable industry standards. The system performs self-health tests on a continuous basis.

Reference 5 describes the licensing basis and methodology that demonstrates the adequacy of the hardware and software to meet the functional requirements. The requirements of Reference 5 were later supplemented with the need to perform cycle-specific DIVOM calculations. For AREVA reload cores this is accomplished with the RAMONA5-FA methodology of Reference 8.

AREVA ATRIUM 10XM methods and fuel are only applicable to Unit 3.

7.6.1.6.3.2 Regulatory Guides

Conformance to Regulatory Guides is discussed in the FSAR, Section 1.8.

7.6.6.6.3.3 General Design Criteria

The GDCs applicable to OPRM are 10 and 12. The OPRM subsystem is designed to conform to the applicable requirements of these GDCs.

7.6.2 Reactor Vessel Instrumentation

The following section describes instrumentation associated with the reactor pressure vessel. This includes those instruments which measure vessel water level, reactor pressure, vessel metal temperature, and head flange leakage.

7.6.2.1 Design Bases and Design Features

A. Design Bases

The reactor vessel instrumentation is designed to fulfill a number of requirements pertaining to the vessel itself or the reactor core. The instrumentation must:

1. Provide the operator with sufficient information in the control room to protect the vessel from undue stresses;

2. Provide information which can be used to assure that the reactor core remains covered with water and that the separators are not flooded. (Inputs to ESF systems are discussed in Section 7.3.);

3. Provide redundant, reliable inputs to the reactor protection system to shut the reactor down when fuel damage limits are approached. (Also see Section 7.2.); and

4. Provide a method of detecting leakage from the reactor vessel head flange.

B. Design Features

1. Provide inputs to ECCS and ATWS to assure initiating and interlocking signals occur as required; and

2. Provide signals to operate the reactor relief valves.

7.6.2.2 Description

The reactor vessel instrumentation system provides sensing, indication and alarms of various reactor parameters to the operators and inputs these signals to various control and protective systems. For details of reactor vessel instrumentation refer to Drawings M-26, Sheet 1 and M-357, Sheet 1. The parameters monitored by this instrumentation system and addressed in this section are:

A. Reactor vessel temperature,

B. Reactor vessel pressure,

C. Reactor vessel level,

D. Reactor feedwater flow,

E. Reactor steam flow, and

F. Reactor vessel flange leak detection.

The instruments described in the section may have, depending on their functions, various classifications. The classification of all instruments are listed in the master equipment list (MEL). Those instruments designated as post-accident monitors are described in Section 7.5.

7.6.2.2.1 Reactor Vessel Temperature

Thermocouples are attached to the reactor vessel to measure the temperature at a number of points chosen to provide data representative of thick, thin, and transitional sections of the vessel. The data obtained from this instrumentation provides the basis for controlling the rate of heating or cooling the vessel so that the stress set up between sections of the reactor vessel is held within allowable limits. The stress is computed from the temperature difference between the various points. The temperatures of the various vessel locations are recorded on a multipoint recorder. The thermocouples are copper-constantan, insulated with braided glass, and clad with stainless steel. They are positioned under pads welded to the reactor vessel. The nine reactor vessel flange and shell thermocouples (TE-2-263-69A1, 69A2, 69A3, 69B1, 69B2, 69B3, 69C1, 69C2 and 69C3) were replaced as part of minor plant change P12-2-91-698. The replacements are Type "T", copper-constantan dual-element thermocouples with magnesium oxide ceramic insulation and enclosed in a 316 stainless steel sheath.

7.6.2.2.2 Reactor Vessel Pressure

Reactor vessel pressure is both indicated and recorded in the control room and is indicated on local pressure indicators. These sensors are not the same as the RPS

sensors. Additionally, reactor pressure is monitored to provide control signals for the RPS high pressure trip, the core spray and low pressure coolant injection (LPCI) low pressure emergency core cooling system (ECCS) injection permissive and LPCI loop select logic, automatic relief valve operation, and anticipated transient without scram (ATWS) system operation.

The reactor pressure inputs to the RPS are from local non-indicating type pressure sensors. The pressure is tapped off the vessel through two sensor lines on opposite sides of the reactor vessel. The sensor lines are extended outside the drywell to separate instrument racks. The RPS pressure senosors on the two independent sensing lines are grouped so that a single event cannot jeopardize the ability of the RPS to initiate a scram.

Core spray and LPCI reactor vessel low pressure ECCS injection permissive pressure switches, isolation condenser initiation pressure switches, and ATWS pressure transmitters are grouped into separate divisions and connected to the same two sensing lines used for the RPS pressure switches.

The logic and sequencing, bypasses and interlocks, actuated devices, and system design bases of the systems to which these instruments connect, are discussed in their respective UFSAR instrumentation and control or system functional description sections:

A. Emergency core cooling systems (HPCI, LPCI, ADS, and core spray)	7.3, 6.3
B. Reactor protection system	7.2, 4.6
C. Anticipated transient without scram	7.8
D. Safety relief valve	5.4
E. Isolation condenser	7.3, 5.4

7.6.2.2.3 Reactor Vessel Water Level

Two sets of sensing lines on opposite sides of the reactor vessel are extended outside the drywell to separate instrument racks. The switches and transmitters are grouped so that a single event cannot jeopardize the ability of the RPS to initiate a scram. Each set of sensing lines comprising one division provides level measurement to the FW control system, primary containment isolation system (PCIS), the ECCS, containment cooling 2/3 core height interlock, and the analog trip system (ATS).

Reactor vessel water level is indicated and recorded in the control room. Level is measured to provide ECCS initiation signals by non-indicating differential pressure transitters which also provide trip functions in the anticipated transient without scram (ATWS) system. The water level is also monitored by level transmitters coupled to the same sensing lines to provide (ATS) signals for the RPS and PCIS.

The reactor water level is controlled by the reactor feedwater control system which receives inputs from water level, steam flow, and feedwater flow instrumentation when operated in three-element control. (See Section 7.7).

"The Reactor Vessel Water Level Instrumentation System (RVWLIS) Backfill System (installed in response to NRC Bulletin 93-03) provides a continuous low flow backfill from the CRD drive header through a flow control station to the RVWLIS reference legs to prevent noncondensible gases from forming in the reference legs over time during normal operation. These gases, when exposed to a normal or rapid depressurization event, could exit solution causing a change to the reference leg head, impacting water level measurement. The backfill system reduces the possibility of these level discrepancies."

Level instruments provide inputs to other systems and are described in sections listed below:

A.	Reactor protection system	7.2
B.	Anticipated transient without scram	7.8
C.	Emergency core cooling system	7.3.1, 6.3
D.	Diesel start	8.3
E.	Primary containment isolation system	7.3.2
F.	Feed pump and turbine trip	7.7, 10.2, 10.4
G.	Containment cooling ⅔ core height	7.4

Complete testing of this level instrumentation is possible during any mode of reactor operation. If an accident were to occur during a test, the core water level could still be detected by the redundant differential pressure instrumentation.

7.6.2.2.3.1 Reactor Water Level Instrumentation Replacement

The original reactor level switches have been replaced in response to environmental qualification of electrical equipment program, I.E. Bulletin 79-01B.

The replacement system is an analog transmitter-trip unit system and is installed as a seismic category I divisionalized system. This includes conduit routing from the transmitter location to a new divisionalized cable tray system which runs from the reactor building to the mezzanine level of the Unit 2 turbine building where the trip unit cabinets are located. Pressure, flow, differential pressure and reactor water level switches have been replaced with an analog system which consists of transmitters and trip units.

The function of the present transmitter/trip unit remains unchanged. The interfaces required for installation are within their design capabilities. The present instruments operate throughout the design ranges of the existing switches. The present instruments are not prone to the same failure mechanisms of the original switches and have demonstrated greater reliability.

These instruments are qualified and maintained in accordance with the station environmental qualification program (see Section 3.11).

Functional Testing Requirements

The functional testing requirements are found in the Licensing Topical Report NEDO-21617-A (December, 1978), "Analog Transmitter/Trip Unit System for Engineered Safeguard Sensor Trip Units."

7.6.2.2.3.2 Reactor High Pressure Trip Instrumentation Replacement

The replacement system is an analog transmitter-trip unit system and is installed as a seismic category I divisionalized system. This includes conduit routing from the transmitter location to a new divisionalized cable tray system which runs from the reactor building to the mezzanine level of the Unit 2 turbine building where the trip unit cabinets are located. The high pressure trip switches have been replaced with an analog trip system which consists of transmitters and trip units.

The function of the present transmitter/trip unit remains unchanged. The interfaces required for installation are within their design capabilities. The present instruments operate throughout the design ranges of the existing switches. The present instruments are not prone to the same failure mechanisms of the original switches and have demonstrated greater reliability.

These instruments are qualified and maintained in accordance with the station environmental qualification program (see Section 3.11).

Functional Testing Requirements

The functional testing requirements are found in the Licensing Topical Report NEDO-21617-A (December, 1978), “Analog Transmitter/Trip Unit System for Engineered Safeguard Sensor Trip Units.”

7.6.2.2.4 Reactor Feedwater Flow

Reactor feedwater flow is monitored by flow transmitters coupled to flow nozzles in the feedwater lines. This signal is sent to the feedwater control system (refer to Section 7.7).

In addition to the flow nozzles, feedwater flow is also monitored by an ultrasonic measurement system. This system consists of an electronics cabinet and spool pieces installed in each of the three feedwater pump discharge lines. Each spool piece contains ultrasonic flow transducers, pressure tap for pressure transmitters, and a temperature detector that feed signals back to the electronics cabinet. This system is used for feedwater flow measurement and does not provide input into the feedwater level control system. The system does provide input into the Plant Process Computer for core thermal power calculation.

7.6.2.2.5 Reactor Steam Flow

Reactor steam flow is monitored by flow transmitters coupled to the flow restrictors in each main steam line. The total steam flow is obtained by summing the flow signal from each main steam line. This signal is sent to the feedwater level control system (refer to Section 7.7) and to the primary containment isolation system (see Section 7.3).

7.6.2.2.6 Reactor Vessel Flange Leak Detection

Integrity of the seal between the reactor vessel body and head is continuously monitored at the drain line connected to the flange face between the two large concentric O-rings. The drain line is normally closed. Leakage from the reactor vessel through the inner O-ring collects in a chamber that is piped to a pressure indicator and a pressure switch that annunciates an alarm. A solenoid-operated valve permits draining the leak system piping so that a measurement of the severity of this leak can be made as the piping and chamber pressurizes.

7.6.2.3 Design Evaluation

Reactor vessel temperature and pressure are sensed and indicated in the control room to provide the operator with the information required to prevent excessive vessel stresses. Both the vessel temperature sensors and pressure sensors are provided in quantities which allow a margin for sensor failures. Pressure sensors used for control room indication and recording have a history of reliable performance.

Thermocouples on the reactor vessel were particularly important during the first few cycles of heating and cooling of the reactor vessel. Once a good record was obtained and analyzed, the limiting rates of temperature change were related to the temperature observations from a relatively few thermocouples. Redundant thermocouples are installed to ensure that the operator always has adequate information to operate the reactor safely. The thermocouples meet the requirements of USAS-C96.1.

Reactor vessel water level is measured to provide information which can be used to assure that the core is covered and that the separators are not flooded. The use of the level signals in the RPS, ECCS, and the feedwater control system assures that

either the proper level is maintained, or that the reactor will be shut down automatically.

Tests have been conducted to determine the stability of the vessel level instrumentation in the presence of rapidly decaying pressures. These tests were conducted at 1500 psig on a standard temperature compensated head chamber. A series of test runs, starting at 1500 psig, verified that the level instrumentation assembly would withstand a depressurization rate of 200 psi/s for the first 3 seconds. At this point, the surface of the water started simmering. Thereafter, the rate was 100 psi/s. Thus, the pressure was dropped rapidly without interfering with the stability of the constant head chamber level and the accuracy of the connected level instrumentation.

Redundant level indicating switches and transmitters are provided, and there are a sufficient number of sensing lines so that plugging of a line will not cause a failure to scram. The arrangement provides assurance that vital protection functions will occur, if necessary, in spite of a failure in the system.

The feedwater control system level sensors are independent of the RPS level sensors with the exception of an isolated input to the feedwater control system from one medium range reactor water level instrument. A failure in the level control which causes the water level to exceed limits will in no way influence the level signals feeding the RPS. Feedwater control system failures are discussed in Sections 7.7, 15.1, and 15.6.

Reactor pressure is also sensed for core protection purposes. A damaging core power transient resulting from a reactor vessel pressure rise is prevented through the control actions initiated by the reactor pressure signal. The four pressure sensors used by the RPS are arranged so that a plugged line or any other single failure will not prevent a reactor scram initiated by high pressure.

The reactor vessel flange leak detection system gives immediate qualitative information about a leak by sensing a pressure buildup. The sensitivity of the reactor vessel flange leak detection system is such that degradation of the seal is noted long before excessive leakage occurs.

7.6.2.4 Surveillance and Testing

All reactor vessel instrumentation inputs to the RPS and ECCS are derived from pressure or differential pressure measurements. The sensing devices are piped so that they may be individually actuated with a known signal during shutdown to initiate a protection system single logic channel trip. The master trip units have indicators so that the readings can be compared to check for nonconformity.

During equilibrium conditions, either hot or cold, thermocouples monitor an approximately uniform temperature; this information is used to detect abnormalities.

The reactor feedwater system control scheme is a dynamic system and malfunctions become self-evident. The system can at all times be cross compared with the other level measurements.

7.6.3 References

1. See APED-5706, detailed report of in-core flux monitoring instrumentation, GE Topical Report, December 1968.

2. DuBridge, R.A., et al., "Reactor Control Systems Based on Counting and Campbelling Techniques, Full Range Instrumentation Development Program, Final Progress Report," AEC Research and Development Report, U.S. Atomic Energy Commission Contract AT (04-3)-189, Project Agreement 22, GEAP-4900 (July 1965).

3. Licensing Topical Report CEND-400-P, Rev. 01, "Generic Topical Report for the ABB Option III Oscillation Power Range Monitor (OPRM)", prepared for the BWR Owners Group by ABB Combustion Engineering, May 1995.

4. C. Thadani to L. A. England, "Acceptance for Referencing of Topical Reports NEDO-3 1960 and NEDO-3 1960, Supplement 1, "BWR Owners' Group Long-Term Stability Solutions Licensing Methodology," (TAC NO. M 75928) dated July 12, 1993 (SER attached)

5. NEDO-32465-A, "BWR Owners Group Reactor Stability Detect and Suppress Solution Licensing Basis Methodology and Reload Application," August 1996.

6. U.S. Nuclear Regulatory Commission Safety Evaluation Report, "Acceptance of Licensing Topical Report CEND-400-P", transmitted from B. A. Boger to R. A. Pinelli of GPU Nuclear, August 16, 1995.

7. BWROG Letter OG-0119-260, “Backup Stability Protection (BSP) for Inoperable Option III Solution,” July 17, 2002.

8. BAW-10255PA, Revision 2, “Cycle-Specific DIVOM Methodology Using the RAMONA5-FA Code,” AREVA NP, May 2008. (Unit 3 only).

Table 7.6-1

OPRM SYSTEM TRIPS

TRIP FUNCTION	TRIP SETPOINT	CONFIRMATION COUNT SETPOINT	ACTION
OPRM Alarm	N/A	8*	Annunciator
OPRM Trip	1.1**	10**	Annunciator, Automatic suppression function (ASF) trip signal to RPS
OPRM Bypass	Selector switch contact	N/A	Annunciator
OPRM Inoperative/Trouble	OPRM annunciator relays	N/A	Annunciator
System Enable	Setpoints are based on the analytical limits: 30% thermal power increasing, 60% core flow decreasing	N/A	Annunciator

*Initial value - can be varied to meet operating needs.
**Refer to cycle specific values in Core Operating Limits Report.

7.7 OTHER INSTRUMENTATION

This section discusses instrumentation and control systems whose functions are not essential for the safety of the plant. These systems include the following:

A. Reactor control rod control systems, including:

1. Control rod adjustment control,
2. Rod block interlocks,
3. Rod position indication system (RPIS), and
4. Control room indicators and alarms.

B. Rod worth minimizer (RWM);

C. Recirculation flow control;

D. Pressure regulator and turbine-generator controls;

E. Feedwater (reactor level) controls; and

F. Condenser, condensate, and condensate demineralizer controls.

7.7.1 Reactor Control Rod Control Systems

7.7.1.1 Design Bases

The reactor control rod control system, in conjunction with the recirculation flow control system discussed in Sections 7.7.3 and 5.4.1, is designed to:

A. Provide capability to control reactor power level;

B. Provide capability to balance the power distribution within the reactor core;

C. Prevent a single component malfunction or single operator error from causing damage to the reactor or reactor coolant system;

D. Prevent a malfunction from interfering with plant protective functions; and

E. Provide the reactivity control capability to prevent fuel damage by meeting the specific core characteristics, parameters, and limitations listed and described in Sections 4.2, 4.3, and 4.4.

7.7.1.2 Control Rod Adjustment Control (Reactor Manual Control System)

7.7.1.2.1 Control Rod Adjustment Control

Withdrawing a control rod inserts positive reactivity, causing reactor power to increase until the negative reactivity resulting from increased boiling, void formation, and fuel temperature balance the change in reactivity caused by the rod withdrawal. An increased voiding rate tends to raise reactor vessel pressure, causing the pressure regulator to open the turbine control valves to maintain a constant turbine inlet pressure. When a control rod is inserted, the converse effect takes place.

The hydraulic portion of the control rod drive system is described and evaluated in Section 4.6. Each control rod has its own drive, including separate control and scram devices. Each rod is electrically and hydraulically independent of the others, except that a common hydraulic pressure source is used for normal operation and a common discharge volume is used for scram operation. Each rod has an individual pressure source for scram operation. Rod position is mechanically controlled by the design of the rod index tube and collet assembly.

Scram operation of all rods is completely independent of the circuitry involved in rod positioning during normal operation. Scram operation is described in Section 7.2.

Electrical power for the reactor manual control system (RMCS) is received from an instrument bus and the essential service system (ESS) bus which is fed from the uninterruptible power supply (UPS). The control rod drive system is actuated for normal operation by energizing solenoid-operated valves which direct the drive water to insert or withdraw the rod.

Control rods are operated one at a time and are withdrawn in preplanned, symmetrical patterns. The allowable patterns have been chosen such that control rod worths will remain below the fuel damage limits and power distribution in the core will be properly balanced. The rod selected for withdrawal is electrically and mechanically controlled so that movement is not more than 6-inches (one notch) at a time. The one notch withdrawal restriction may be overridden by the operator simultaneously manipulating two switches.Multiple notch rod insertions can be accomplished by holding the rod movement control in the rod in position.

7.7.1.2.2 Rod Block Interlocks

To prevent inadvertent withdrawals in improper rod patterns, the movement of a control rod is prohibited (rod block) under certain conditions described below (see Figure 7.7-1). Some of these rod blocks are in effect only for specific positions of the mode selector switch. With the mode switch in SHUTDOWN, no control rod can be withdrawn. This enforces compliance with the intent of the shutdown mode.

A. The circuitry is arranged to initiate a rod block regardless of the mode selector switch position for any of the following conditions.

1. Average power range monitor (APRM) high-flux alarm - the purpose of this rod block function is to avoid conditions that would require reactor protection system action if allowed to proceed. The APRM upscale rod block alarm setting is selected to initiate a rod block before the APRM high neutron flux scram setting is reached. The APRM system is also recirculation flow referenced in the RUN mode to initiate trip signals to inhibit rod withdrawal to prevent operating the reactor at excessive power levels with reduced recirculation flow.

2. Any APRM inoperative alarm - this assures that no control rod is withdrawn unless the average power range neutron monitoring channels are either in service or properly bypassed.

3. Either rod block monitor (RBM) upscale (high-flux alarm) - this function is provided to stop the erroneous withdrawal of a control rod so that local fuel damage does not result. Although local fuel damage poses no significant threat in terms of radioactive material release from the nuclear system, the trip setting is selected so that no local fuel damage results from a single control rod withdrawal error during power range operation. The RBM system is also recirculation flow referenced and operates when power is above 30%.

4. Either RBM inoperative - this assures that no control rod is withdrawn unless the RBM channels are in service or properly bypassed.

5. APRM flow unit upscale or inoperative - this assures that no control rod is withdrawn unless the recirculation flow converters, which are necessary for the proper operation of the RBMs, and APRM system are operable.

6. Scram discharge volume high water level - this assures that no control rod is withdrawn unless enough capacity is available in the scram discharge volume to accommodate a scram. The setting is selected to initiate a rod block prior to the scram signal that is initiated on scram discharge volume high water level.

7. The rod worth minimizer (RWM) rod block - this occurs whenever the rod selection is incorrect or the rod being moved has traveled one notch further than the preplanned rod pattern allows. The operation of the RWM is described in Section 7.7.2.

8. Rod movement timer switch malfunction.

B. With the mode selector switch in RUN, either of the following conditions also initiate a rod block:

1. Any APRM downscale alarm - this assures that no control rod is withdrawn during power range operation unless the average power range neutron monitoring channels are operating properly or are correctly bypassed. All unbypassed APRMs must be on scale during reactor operation in the RUN mode, or

2. Either RBM downscale alarm - this assures that no control rod is withdrawn during power range operation unless the RBM channels are operating properly or are correctly bypassed. Unbypassed RBMs must be on scale during reactor operation in the RUN mode.

C. With the mode selector switch in STARTUP/HOT STANDBY or REFUEL any of the following conditions also initiate a rod block:

1. Any source range monitor (SRM) detector not fully inserted into core with the SRM count level low - this assures that no control rod is withdrawn unless all SRM detectors are properly inserted when they must be relied upon to provide the operator with neutron flux level information,

2. Any SRM upscale (high-flux alarm) - this assures that no control rod is withdrawn unless the SRM detectors are properly retracted during a reactor startup. The rod block setting is selected at the upper end of the range over which the SRM is designed to detect and measure neutron flux,

3. Any SRM inoperative - this assures that no control rod is withdrawn during low neutron flux level operations without having proper neutron monitoring capability available, in that all SRM channels are in service or properly bypassed,

4. Any intermediate range monitor (IRM) detector not fully inserted into core - this assures that no control rod is withdrawn during low neutron flux level operations unless proper neutron monitoring capability is available, in that all IRM detectors are properly located,

5. Any IRM upscale (high-flux alarm) - this assures that no control rod is withdrawn unless the intermediate range neutron monitoring equipment is properly upranged during a reactor startup. This rod block also provides a means to stop rod withdrawal in time to avoid conditions requiring RPS action (scram) in the event that a rod withdrawal error is made during low neutron flux level operations,

6. Any IRM downscale except when on the lowest range - this assures that no control rod is withdrawn during low neutron flux level operations unless the neutron flux is being properly monitored. This rod block prevents the continuation of a reactor startup if the operator upranges the IRM too far for the existing flux level; thus, the rod block ensures that the intermediate range monitor is onscale if control rods are to be withdrawn,

7. Any IRM inoperative - this assures that no control rod is withdrawn during low neutron flux level operations unless proper neutron monitoring capability is available in that all IRM channels are in service or properly bypassed, or

8. Service platform hoist loaded - this assures that no control rod is withdrawn when fuel is being loaded into the reactor.

D. With the mode switch in REFUEL, either of the following conditions also result in a rod block:

1. Refueling platform over the core with any of the three hoists (frame mounted hoist, trolley mounted hoist, or fuel grapple) loaded or the fuel grapple not in its fully raised position - this assures that no control rod is withdrawn when fuel is being loaded into the reactor, or

2. Selection of a second control rod movement when any other rod is not fully inserted - this assures that no more than one control rod is withdrawn during control rod and/or control rod drive maintenance.

The rod block logic circuitry is arranged as a two-channel system in which a trip of either channel results in a rod block.

In most cases, the relays associated with the rod block function deenergize to produce a rod block. Two SRM channels, four IRM channels, three APRM channels, and one RBM channel provide inputs into each rod block trip channel. The channel arrangements within the neutron monitoring system are described in Section 7.6. The APRM rod block setpoint is varied as a function of recirculation flow. The RBM setpoint is also biased by recirculation flow, but the 100% flow setpoint depends on the power-flow characteristic along which the reactor is operating. For increases in power, the RBM setpoint must be manually reset by the operator; for decreases in power, the setpoint is automatically reduced. Both the APRM- and RBM-biasing arrangements are described in Section 7.6.

A limited number of manual bypasses are permitted in the rod block circuitry: one bypass in the source range, intermediate range, and power range nuclear instrumentation is allowed in each rod block channel. One of the two rod block monitor inputs may be bypassed. An automatic bypass of the SRM detector position rod block is effected as the neutron flux increases beyond a preset level on the SRM instrumentation; the bypass allows the detectors to be withdrawn as a reactor startup is continued. See Section 7.6 for additional information regarding the nuclear instrumentation and RBM rod block bypasses.

7.7.1.2.3 Rod Position Indication System

Control rod position indication is provided by a bank of magnetically operated reed switches which open and close when a magnet attached to the rod drive piston passes during rod movement. Indication is provided for each 3 inches of travel and whenever the travel limits of the control rod drive are reached. Since a notch is 6 inches, indication is available for each half-notch of rod travel.

A visual, full core display of all rod positions is continuously available to the operator. In addition, when a control rod is selected for movement, the positions of the selected rod and the three adjacent rods are separately displayed, along with the readings from the 16 local power range monitor (LPRM) detectors in the vicinity. Thus, the operator is supplied with all the available information from the core volume adjacent to the selected rod.

7.7.1.2.4 Control Room Indicators and Alarms

Numerous alarms and indications are available to inform the operator of rod control system status. They include:

A. Rod position,

B. Rod drive flow control valve position,

C. Rod drive water pressure control valve position,

D. Rod drive cooling water control valve position,

E. Rod out permissive,

F. Rod moving out,

G. Rod moving in,

H. Refueling mode rod selection permissive,

I. Rod drift,

J. Rod selection,

K. Rod block,

L. Notch override,

M. Rod worth minimizer conditions (Section 7.7.2),

N. Nuclear instrumentation system trips (Section 7.6), and

O. Rod movement timer malfunction.

7.7.1.3 Design Evaluation

The controls and instrumentation associated with the control rod drive system provide a reliable means of controlling core reactivity. The collet finger arrangement mechanically limits rod travel during withdrawal. The rod velocity limiter, described in Section 4.6, limits the reactivity insertion rate should a rod become uncoupled from its drive. Only one rod may be selected at a time, thus limiting the magnitude of a reactivity insertion. The operator is provided with information regarding rod positions, average and local neutron flux levels, and indications from the rod drive hydraulic system. This information allows the operator to be fully cognizant of the status of the core and the control rod pattern.

Each rod is controlled as an individual unit. The failure of any individual control rod drive component does not affect other control rods, thereby providing assurance that single component failures will not inhibit reactivity control capability. Also, a single rod failure will not prevent achieving shutdown margin requirements.

Inadvertent reactivity additions are discussed in Sections 4.6.3.1 and 15.4.9.

A failure in the electrical supply to the rod drive solenoids in no way interferes with scram operation since the scram hydraulic and electrical systems act separately from the rod drive portion of the system.

Since control rods are individually positioned and since local and bulk power levels are indicated in the control room, the proper balancing of the power distribution is possible.

To prevent the operator from selecting an improper rod pattern, automatic rod blocks are provided. The full range of nuclear instrumentation is used to provide rod blocks depending on the core condition. Figures 7.6-12 and 7.6-17 show the rod block interlocks as a function of flow.

Although the reactor protection system provides timely protection against the onset and consequences of conditions that could otherwise lead to a gross failure of the fuel, the rod block interlocks act to increase the margin to gross fuel failure by terminating a rod withdrawal before scram settings are reached. The RBM rod block trip setting was selected to prevent local fuel damage for rod withdrawal errors initiated under the worst bypass condition and is thus adequate in providing a safety margin to gross fuel damage in excess of that afforded by the reactor protection system.

For low neutron flux level operations, the SRM and IRM upscale alarm rod blocks terminate a rod withdrawal if the neutron flux indication is on the verge of going off-scale at the upper end of any range. These upscale trips provide both additional margin to gross fuel damage from rod withdrawal errors and assurance that no control rod will be withdrawn unless the neutron monitoring equipment is selected to the proper range.

The rod blocks initiated by the RWM, scram discharge volume high water level scram bypass, flow converter trips, and neutron monitoring channel downscale and inoperative trips reinforce operating procedures. These rod block functions assure that equipment pertinent to the safe operation of the reactor is in service and properly operating before rod withdrawal is permitted. These rod blocks are provided as an operating convenience and are not directly related to fuel failure. The RWM also aids in preventing the design basis rod drop accident (RDA).

The reliability of the rod block interlock circuitry is consistent with its functions of providing additional safety margin to gross fuel damage and preventing unnecessary scrams. A single sensor could fail in such a way that a rod block would be initiated. The bypass provisions in the rod block circuitry allow such a failure to be bypassed without preventing other sensors of the same monitored variable from initiating a rod block, if required. A complete loss of power to the rod block circuitry would cause a rod block. It is possible, but unlikely, that a short circuit occurring in certain locations could degrade the interlocks. A failure of one RBM channel while the other is bypassed could result in the RBM channel not operating. In either of these cases, the result is no loss of excess safety margin to gross fuel failure. The safety margin provided by the reactor protection system is, by itself, adequate.

In considering the various failure modes of the rod block circuitry, it is important to note the standby nature of the interlocks. A rod block interlock failure, by itself, cannot result in any fuel damage. A failure of the rod block interlocks combined with a rod withdrawal error is required before even a chance of local fuel damage can occur. The design performance and safety margins provided by the reactor protection system are not affected by any rod block interlock failure. The details of this analysis are presented in Hatch Nuclear Plant, Docket 50-321, Amendment 6. Section 7.2 describes the scram setpoints.

7.7.1.4 Inspection and Testing

Plant Technical Specifications specify required rod block testing (a particular rod block must be periodically tested during any plant condition when it is required to be operable). This testing includes specified functional tests, instrument checks, and calibration.

7.7.2 Rod Worth Minimizer

7.7.2.1 Design Basis

The design basis of the RWM is to serve as a backup to procedural control during startup and low-power operation to limit control rod worth and the reactivity addition rate resulting from a control rod drop and thus assure that peak fuel enthalpy would be less than 280 cal/g. Operating procedures are the primary defense against high-worth control rod patterns. Preplanned, normal rod patterns result in low individual control rod worths. The RWM is not designed to replace a Qualified Nuclear Engineer's selection of control rod patterns but is intended to monitor and partially enforce approved control rod movements. The RWM will produce a rod block below the low power setpoint (LPSP). The RWM's function is performed with minimal interference with normal operation and is designed for continuous operation at all power levels.

7.7.2.2 Definitions

7.7.2.2.1 Operator Interface

The color graphics terminal is located within the 902(3)-5 panel in the control room. The computer-driven color-coded screen provides all the information necessary for the control room operator to monitor the system's response. Operator informational requests and implementation of special functions are performed by touching screen areas associated with specific actions.

The control rod positions are color coded as follows:

A. Red - Withdraw error,

B. Magenta - Insert error,

C. Cyan - Rod out of service,

D. Yellow - Substituted position,

E. Green - Rod is in latched step,

F. White - Rod is not in latched step.

7.7.2.2.2 Sequence Step

Steps are the sequential subdivisions of an operating sequence. Each step consists of an array of rods and a set of insert and withdraw limits that apply to each rod in the array. The steps are numbered in the order they are to be followed when going up in power. For example, Step 1 contains the array of rods which are to be moved first when going up in power. When all the rods within the specified array are at the withdraw limit for Step 1, then Step 2 specifies the next set of control rod moves. The withdraw limit of the array specified in a step is the same as the insert limit of that array in the nearest higher step in the sequence containing that array. Thus, after any completed step (Step i) in the sequence, assuming the sequence has been followed strictly, all rods in arrays specified in Step 1 through Step i should be at the withdraw limit of the last (previous) step containing those rods. No rod in an array in the next (following) step containing that array, ([Step i + 1] through the end of the sequence), should be withdrawn past the insert limit for that step.

7.7.2.2.3 Sequence Array

An array consists of a list of control rods. One or more arrays combine to form "group(s)." Any control rod is assigned to one and only one array. Rods can only be assigned to an array when a sequence is prepared. An array can be moved any number of times within a sequence and at any step. The sequence may optionally contain an array with rods which are to be termed "out of service." Rods within this out-of-service array should be fully inserted and are blocked from movement if selected. The total number of out-of-service rods should not exceed eight.

7.7.2.2.4 Cram Array

A cram array consists of a list of control rods selected by a Qualified Nuclear Engineer based on reactor conditions and control rod patterns. Cram arrays are used when the operator needs to reduce power quickly in an emergency situation (e.g., loss of feedwater heater[s]).

7.7.2.2.5 Operating Sequence

An operating sequence is a schedule to be followed by the plant operator when withdrawing or inserting control rods. The sequence can be printed out or viewed at the operator's RWM screen at any time. A sequence consists of an ordered list of sequence steps each containing a list of rods (array) and the position the rods should be moved to, from the current position, at that step. The sequence must have continuous limits. The withdraw limit of an array after a step must correspond exactly to the insert limit of that array in the nearest higher step containing that array. The sequence is enforced in reverse order when coming down in power. A new sequence can be loaded only when the computer is in a load sequence mode, as signified by the position of the mode switch on the 902(3)-5 panel, or when offline and in a test mode as initiated at the system console.

7.7.2.2.6 Latched Step

The latched step is the step within the operating sequence compatible at a given time with the existing distribution of control rod positions. The current control rod pattern is compared to the loaded sequence and the total number of errors calculated at each step. The latched step is the step with the least number of total errors. If this criteria yields more than one step, then the lowest step within this list is defined as the latched step. The RWM will latch at any other step containing zero errors if that step contains the selected rod.

7.7.2.2.7 Notch Position

A notch position of a control rod is defined as any even number 00 through 48. Physically these numbers correspond to notches located 6 inches apart on the control rod drive mechanism. A control rod in movement passes through the odd numbers but can only be mechanically latched at an even-numbered position. An odd position is not even transmitted electronically to the RWM. A control rod not latched at an even position, unless selected and driving, will be considered a drifting rod.

7.7.2.2.8 Selection Error

A selection error appears in white background on the full core display for the operator if a control rod outside of the latched step is selected. Since it is normal operating practice to select control rods not within the current step for testing purposes, a selection error is only considered as such if movement is intended. The RWM will attempt to relatch upon any new selection of a control rod. If unable to latch to a step containing the selected rod, the selection is in error. All rod movements of selection error rods are blocked if movement is attempted.

7.7.2.2.9 Insertion Error

An insertion error is defined as the insertion of a control rod inconsistent with the latched operation sequence. For example, if the operator is withdrawing control rods exactly according to procedures and has withdrawn several of the rods which are defined to be in Group 4, the insertion of any withdrawn rod of Group 4 at that time is not considered an insertion error even though it may be a deviation from planned procedures. However, if he were to insert a rod from another group which was withdrawn previously in the sequence, that action is inconsistent with the operating sequence and is an insertion error. This definition is independent of how far the rod is inserted.

An insertion error occurs when:

A. A control rod in the array of the currently latched step (Step i) is inserted past the insert limit at that step; or

B. A control rod is inserted past the withdraw limit of the closest lower step (Step i - 1 down to Step 1) containing that control rod.

7.7.2.2.10 Withdrawal Error

A withdrawal error is defined similarly to an insertion error. For example, if several rods in Group 4 are not withdrawn, the withdrawal of a rod from a different group which should be withdrawn later in the sequence is a withdrawal error regardless of how far the rod is moved.

A withdrawal error occurs when:

A. A control rod in the array of the currently latched step (Step i) is withdrawn past the withdraw limit at that step; or

B. A control rod is withdrawn past the withdraw limit of the closest lower step (Step i - 1 down to Step 1) containing that rod.

7.7.2.2.11 Low Power Setpoint

The low power setpoint (LPSP) is the core thermal power level below which alarms and rod movement blocks are enabled if generated due to sequence violations. Above the LPSP, sequence violations are alarmed but rod movement blocks may be disabled by the Nuclear Station Operator (NSO). Rod blocks are normally left in effect to enforce sequences to full power. Sequence violations with rod blocks in effect require movement of a mispositioned rod before constraints are removed from other rod movements. The LPSP is determined by steam flow and feed flow measurements and is output from the feedwater control system instrumentation to the RWM program as a digital signal (reset = below LPSP). The LPSP signal is set to a percentage of rated core thermal power listed in Technical Specifications and may be raised or lowered by adjustment of the field sensors.

7.7.2.2.12 Insert Block, Permissive

An insert block is interlocked with the reactor manual control system in such a manner as to permit or inhibit the insertion of the selected control rod. An insert block is imposed when a rod has moved so as to violate the sequence. The following conditions will cause rod movement insert blocks:

A. Selection and attempted movement of a rod not within the currently latched step;

B. Selection of a rod deemed to be an insert error (it may be possible to remove this insert block by declaring the rod inoperable and inserting it fully using the out-of-service function from the RWM screen);

C. Selection of an improper rod when attempting to recover from an insert error;

D. Selection of any rod other than a withdraw error rod when attempting to recover from a withdraw error;

E. Various other rod selections when implementing special modes such as rod test or out-of-service; or

F. System initialization, hardware errors, or diagnostic request.

7.7.2.2.13 Withdraw Block, Permissive

A withdraw block is interlocked with the reactor manual control system in such a manner as to permit or inhibit the withdrawal of the selected control rod. A withdraw block is imposed when a rod has moved so as to violate the sequence. The following conditions will cause rod movement withdraw blocks:

A. Selection of a rod not within the currently latched step;

B. Selection of any rod when attempting to recover from a withdraw error;

C. Selection of any rod other than an insert error rod when attempting to recover from an insert error;

D. Various other rod selections when implementing special modes such as rod test or out-of-service; or

E. System initialization, hardware errors, or diagnostic request.

7.7.2.2.14 Alternate Control Rod Limit

In addition to the insert and withdraw limits specified in the loaded sequence, an alternate control rod limit may be selected for any rod. The alternate control rod limit for a rod is defined as being one notch position less than the position limit for

that rod at that step. The only exception to this rule is that the alternate position to the limit of 00 is 02.

7.7.2.2.15 Out of Service Rod

An out of service (OOS) rod is a rod which is "pinned" at 00 with no movement or alternate limits allowed. A control rod which can not be fully inserted may be declared OOS although more restrictive rules apply to rods incapable of insertion. Placing a rod OOS effectively removes the rod from its associated array. The rod is ignored during the latch procedure and will not be considered as an insert or withdraw error during other rod movements. Rods may be taken OOS in one of two ways: inclusion in an OOS array defined by the sequence builder, or through use of the RWM screen function "Rod Out Of Service." A control rod which has been declared OOS is not allowed to be moved in any direction. The total number of OOS rods shall not exceed eight.

7.7.2.2.16 Substituted Rod Position

A substitute rod position can be entered through the RWM screen for rods whose positions are undefined. A substitute value can not be entered for any rod with a "good" position (00, 02, 04, 46, 48, etc.,). A rod with a position that cannot be determined may have a substitute value entered if all attempts by the RWM fail in locating its position. When a substitute rod's position becomes known, the substitute value is replaced automatically with the good value and the operator is notified. A maximum of 10 rods may have substitute values entered. If a substitute rod is selected and driven, the entered substitute value will be discarded and a new substitute value entered if the new position is bad.

7.7.2.2.17 System Mode

System mode is selected by a two position switch (NORMAL and BYPASS) in the control room. This switch is used by the operator to bypass the RWM system, if necessary, to remedy hardware problems.

7.7.2.2.18 Deleted

7.7.2.2.19 Operational State - Computer Ready

The computer ready operational state is applicable only when the selected system mode is normal. The RWM program will determine if it can latch and verify a sequence. If the RWM program is able to complete all of its diagnostics and has a valid sequence loaded, it indicates a ready state.

7.7.2.2.20 Rod Test Function

The rod test function is a special case of the normal mode and is selected through the operator interface. Rod test mode can only be entered if one or fewer control rods are not fully inserted. When in this mode, one rod may be fully withdrawn and reinserted only if all other rods are fully inserted. Movement of a control rod is blocked when selected if any other rod is not fully inserted. If placed in this mode with more than one rod withdrawn past the fully inserted position, withdrawn rods are highlighted on the full core display and all rod movements are blocked until the rod test mode is exited.

7.7.2.2.21 Control Rod Position

The control rod position is the axial position of a control rod in the core. Valid control rod positions have numbers 00 through 48, even numbers only. Number 00 is fully inserted and number 48 is fully withdrawn.

7.7.2.2.22 Control Rod Condition

The condition of a control rod describes the validity of the control rod position. A control rod may be one or more of the following:

A. Normal,

B. Bad,

C. Substituted,

D. Out of service,

E. Alternate enabled,

F. Selected,

G. Drifting,

H. Insert error, or

I. Withdraw error.

7.7.2.2.23 Rod Drift

A rod drift is indicated if a control rod moves from an even-notched position (unless, of course, that control rod is selected and driving). A rod drifting input signifies the presence of a rod not at an even position in the core. Scans are undertaken to find the drifting rod.

7.7.2.2.24 Control Rod Withdrawal Sequence Restrictions

In order to limit the amount of energy deposited in the fuel in the event of a control rod drop accident, sequencing restrictions are imposed. Two options exist to bound control rod sequencing. Either option will limit rod worth such that the peak fuel enthalpy remains $\leq$280 calories per gram.

The first option is a generic approach to limit rod worth by a sequencing technique called BPWS. The banked position withdrawal sequence (BPWS) are rules designed to minimize rod worth and reduce peak fuel enthalpy below limits in the event of a rod drop accident. These rules are to be followed to the LPSP defined in the Technical Specifications. Additional detail on the BPWS rules is included in "Banked Position Withdrawal Sequence," Licensing Topical Report General Electric Co., January 1977 (NEDO-21231).

The second option removes some of the generic conservatism by analyzing an acceptable rod withdrawal sequence on a cycle specific basis. This non-generic analysis provides sequencing restrictions to limit the rod worth and peak fuel enthalpy to $\leq$280 calories per gram.

A third sequencing option eliminates the possibility of a rod drop accident, and may be used for reactor shutdowns below the LPSP. The “Improved BPWS Control Rod Insertion Process” requires that all withdrawn control rods have been verified coupled prior to reducing power below the LPSP, and any control rods which have not been confirmed coupled must be fully inserted above the LPSP. This allows rod insertion straight to position 00, and removes unnecessary banking during a reactor shutdown. Additional detail on the Improved BPWS for shutdowns is included in “Improved BPWS Control Rod Insertion Process”, NEDO-33091-A Revision 2, July 2004.

7.7.2.2.25 Deleted

7.7.2.3 System Components

The RWM function is provided by a computer program running on the redundant Process Computer system as well as a dedicated redundant data acquisition system (DAS). The component interconnections are shown on the block diagram in Figure 7.7-2.

A. Redundant Digital Computers PPC-A and PPC-B

B. Redundant DAS components

C. Graphic Display and control panel switch, and

D. Relays interfacing with Reactor Manual Control System to provide rod blocks.

The block diagram illustrates the role of the digital computers in the RWM process. RWM software resides on both the PPC and the DAS components.

7.7.2.4 Arrangement

The RWM function consists of a computer program running on the redundant process computers as well as a computer program running on a redundant DAS system. The DAS and process computer communicate using a redundant Ethernet link dedicated to that application.

The color graphics monitor is located on the reactor controls section of the main control board 902(3)-5" in the control room. A touch screen system is used as the operator input device. Touching certain areas of the screen enables certain actions. The only other control located on the main control board is a bypass switch used to disable the rod block ability of the RWM.

The DAS obtains inputs from the Rod Position Information System (RPIS), Reactor Manual Control System (RMCS), and other plant instrumentation. Outputs from the DAS are used to drive relays that interface with RMCS to provide insert and withdraw rod blocks when required.

Control rod sequence transfers are allowed to the RWM under the direction of the nuclear engineering group.

7.7.2.5 Features

The operator is presented with a display on the graphics monitor to represent the following conditions:

A. Rod step number, position, limits

B. Insertion error rod identification

C. Withdraw error rod identification, and

D. Current position of all control rods.

A two-position selector switch with normal and bypass positions on the operator's panel determines the mode of operation. In the normal mode, the active PPC will perform the function of the RWM. In the bypass mode, the rod blocks will be bypassed by a relay contact. The RWM will receive a signal that it is in bypass mode. The RWM program will continue to display current rod positions and perform a subset of its normal functions, but will not provide rod blocks or alarms when errors are detected.

The withdraw/insert permissive is achieved by sets of output relays driven by digital outputs from the DAS. The output relays are arranged in a one-out-of-two-taken-twice logic to provide reliability and redundancy.

This page has been intentionally deleted.

7.7.2.6 Design Evaluation

During routine operation, the RWM selector switch is placed in the NORMAL position. In this mode, the RWM enforces the control rod sequence as loaded by the Qualified Nuclear Engineer. The RWM sequence consists of a preapproved list of steps that detail specific control rod movements. Each step specifies an array (an array is a list of control rod identifications) and movement limits for that step. When latching to the appropriate step in the sequence, the RWM scans the core and compares the current control rod positions to the positions specified in each step of the sequence. The step which results in the lowest number of total errors (withdraw or insert) is considered the currently latched step.

To perform the primary function of the RWM, enforcement of the preprogrammed sequence, insertion or withdrawal of control rods is permitted for rods selected in the latched step. If the RWM detects a control rod movement inconsistent with the loaded sequence, control rod blocks are initiated and the alarm is energized. The operator is required to correct the position error before any further movements are allowed. The secondary functions are available to overcome minor malfunctions in the RPIS and RMCS system. The secondary functions include:

A. Rod out-of-service - This function allows the operator to move a control rod to zero and remove it from service. In this mode, the control rod is displayed in cyan on the color graphics monitor and its movement is blocked until it is placed back in service. Placing a rod out-of-service effectively removes the control rod from its associated array. The out-of-service rod is ignored by the RWM latching procedure and consequently will not be considered an insert or withdraw error during other control rod movements. Analyzed sequences restrict the number and location of control rods that can be taken out-of-service.

B. Substitute control rod position - This function allows an operator to manually enter a position value for a control rod that does not have valid position indication from the RPIS system, provided the actual position of the control can be determined. There is a limit of 10 substitute positions; they will be displayed in yellow on the color graphics monitor.

C. Enable/disable a control rod alternate limit - An alternate limit is defined as one notch position in from the target rod position. Since missing positions frequently occur from the RPIS system, the alternate positions allow the operator to insert a control rod one notch from the target position and continue with control rod movements. There is a limit of two alternate limits corresponding to any of the defined banking limits (except for control rods at positions 00 and 48); they will be displayed in cyan on the color graphics monitor.

The RWM function is bypassed by a relay contact when the selector switch is placed to BYPASS.

During normal operation in any sequence, with the operator withdrawing and inserting control rods according to the predetermined procedures, the RWM will neither block nor noticeably delay rod movement. During such operation there will be no alarms except for equipment malfunctions, i.e., control rod drift of input/output errors.

If the core power level exceeds the low power setpoint, the RWM will not inhibit the selection, insertion, or withdrawal of any control rod, but will only annunciate errors unless blocks have been enabled to full power by the operator.

When the reactor is operating below the low power setpoint or with blocks enabled to full power by the operator, the RWM will block movement of a selected control rod in the latched step upon violation of either the insert or withdraw limit by one notch. The adherence to the loaded sequence, when in the normal mode, can only be suspended when the operator selects one of the special modes provided for testing conditions. Bypassing the RWM will also disable the rod block functions of the RWM.

The control room operator interactions with the RWM program are primarily through the touch screen. Any other PPC screen in the control room may also be used for this function, providing a means for the operator to control the RWM in the event of a failure of the provided touch screen. All information necessary for rod movement will be available on the screen. Different colors are used for quick recognition of an abnormal situation.

The primary screen will normally be displayed on the touch screen and will be the default screen displayed when that screen is started. Other screens may be displayed at the discretion of the operator.

7.7.2.7 Surveillance and Testing

Detailed on-demand system diagnostic routines are provided to test the computer and the control rod interlock networks.

Technical Specifications specify required RWM surveillance tests.

7.7.3 Load Control Design

Load control of a BWR power plant differs from a conventional fossil fuel power plant due primarily to the sensitivity of boiling to pressure variations. In a conventional plant, the turbine control valves are controlled by the speed/load governor responding directly to system frequency and load demand via the governor setpoint. The resulting pressure changes in the boiler cause a pressure regulator to adjust the firing rate of the boiler furnace to match the steaming rate with the turbine steam flow.

In a nuclear boiler, power (and hence steaming rate) is directly affected by the steam volume in the reactor core. In turn, the steam volume is sensitive to pressure variations. If a BWR turbine were controlled as in a conventional plant, opening the control valves would cause decreasing reactor pressure, which would cause the steam volume in the core to increase, which in turn would cause the neutron flux (fission power) to decrease; exactly the opposite of the effect desired. Conversely, closing the control valves would cause the reactor power to increase rather than decrease. The greater the rate of change of pressure, the greater the short-term change in neutron flux. However, the difference in the neutron flux between two steady-state pressure levels (e.g., 1000 and 1020 psia) is small, provided only the operating pressure is changed.

The heat addition rate of a BWR boiler can be changed much faster than that of a conventional boiler, but even so, it cannot be changed fast enough to cope with the effect of a rapid pressure change on reactor power. A control scheme was adopted which placed the turbine control valves under control of a high performance pressure regulator (refer to Section 7.7.4). To get the load response, the speed/load signal from the turbine governing system controls the reactor recirculation flow which directly and strongly affects the reactor power. Therefore, the steam generation rate in the reactor must first be changed before the pressure regulator will react to change the turbine steam flow.

This load control scheme is made up of two control systems, a turbine control system which is supplied with the turbine, and a recirculation flow control system which is supplied with the reactor. Figure 7.7-3 a diagram of the plant load control scheme, shows the basic features in the power operating mode. Reactor pressure and turbine-generator controls are addressed in Section 7.7.4. Additional turbine controls are addressed in Section 10.2.

7.7.3.1 Recirculation Flow Control System

7.7.3.1.1 System Description

Reactor power may be varied by varying recirculation flowrate.
At a steady state, there is constant steam (void) volume in the core. As recirculation flowrate is increased, steam voids are removed from the core faster, thus reducing the existing void accumulation. This reduction in the steam volume within the core volume increases the moderation of neutrons within the core thus inserting positive reactivity. The positive reactivity causes an increase in reactor power, consequently steam generation rate. When the negative reactivity associated with the increased steam generation (voids) and the increased fuel temperature (doppler) equals the original positive reactivity insertion, power stabilizes at an increased level corresponding to the increased recirculation flow.

Power-flow characteristics are shown in Figure 4.4-1. The flow control range is shown as 58 to 100% power along the 100% load line.

There are two possible modes of recirculation flow control:

A. Individual manual operation where each recirculation pump is controlled via its individual control station, and

B. Master manual operation where both pumps are manually controlled from one controller, the master controller;

For Unit 2 and Unit 3, the Adjustable Speed Drive (ASD) directly varies the frequency to the motor to give the desired pump speed. The speed (frequency) control is manual only for each pump, using increasing and decreasing pushbuttons, or with common master manual control pushbuttons. The recirculating pump motor adjusts its speed in accordance with the frequency of the set output voltage.

7.7.3.1.2 Design Evaluation

The recirculation flow control arrangement contributes to the stable response of the reactor. The stability of the unit is discussed in Section 4.3. Section 4.4 describes reactor margins under the flow control mode. Figure 7.6-13 depicts a typical reactor behavior line: with flow and power initially at any point on the curve, a flow change will cause the power to change along the path indicated by the curve. Malfunction of the flow controller can cause either a recirculation flow increase (insertion of positive reactivity) or a decrease (high power-to-flow ratio). Inadvertent recirculation flow increases from ASDs are milder than the transient caused by starting a recirculation pump in a cold loop, and inadvertent recirculation flow decreases are less severe than a trip of one or two recirculating pumps. These malfunctions are discussed in Sections 15.4 and 15.3, respectively.

The dP instrument trip points are selected such that the instruments null (essentially zero differential) when the reactor recirculation pumps are delivering rated flow. Zero differential pressure will optimize the setting of the instruments should there be even a slight difference in the loss coefficient of the jet pump assemblies.

The trip point is set at about 0.75 psi. The only requirement is that any positive ΔP would result in the selection of Loop A; any negative ΔP would result in the selection of Loop B.

7.7.3.2 Economic Generation Control System

7.7.3.2.1 Deleted.

7.7.3.2.2 Failure Mode and Effects Analyses

7.7.3.2.2.1 Reactor Recirculation Master Flow Controller Failures

This Page Intentionally Left Blank

Due to the input limits on the individual speed controllers, failure modes caused by malfunction in the master flow controller would not be as severe as similar failures of a single loop, variable speed, coupler scoop positioner.

7.7.3.2.2.2 Load Demand Error Signal Failures

The load demand error signal originates from the turbine control system and is the input signal to both the master flow controller and the pressure setpoint adjuster when the flow control system is in the automatic mode of operation. As indicated in the previous section, the signal is limited to about ±25% load demand error.

Failure of the setpoint adjuster in the direction to cause positive pressure changes would most likely cause reactor flux scram if the reactor were near the top end of the flow control range and the setpoint change were as large as a step demand increase of 40 psi. A 10-psi positive setpoint change from turbine-generator design conditions causes neutron flux to rise transiently to about a 110% value. Such a failure, if occurring when the reactor is near the low end of the flow control range, should not result in flux or pressure scram. No safety problems are encountered since the only consequence is the possibility of an unwanted scram.

Failure of the setpoint adjuster in the direction to cause negative pressure changes has the opposite effect. The negative step change in pressure setpoint would cause the opening of the control valves, and depending upon the initial power level, possibly the opening of the bypass valves. Total transient steam flow from the reactor vessel would be limited by the maximum combined flow limit. The steam flow is further reduced if turbine bypass valves are out of service. See the cycle specific reload documentation for the analysis assumptions on combined steam flow through turbine control valves and turbine bypass valves. Pressure would fall, causing a decrease in reactor power until as much as a 40-psi drop in pressure is experienced at the turbine end of the steam line.

7.7.3.2.2.3 Load Set Mechanism Failures

The load set mechanism is the device used to control plant loading manually by increase/decrease signals initiated by the reactor operator. The load set mechanism can control reactor power only when the master flow controller is in the automatic flow control mode of operation. The maximum rate at which the load reference can be changed is 0 to 100% in 43 seconds, from which maximum load demand rates of ± 2-% per second can be inferred.

Failure modes associated with the load set mechanisms are no more severe than the normal expected maneuvers originating from this device.

A failure calling for increased loading can cause a demand increase no greater than 2-% per second, and a failure calling for decreased loading can cause a demand decrease no greater than 2-% per second. The automatic flow control system is

capable of accepting demand rates in excess of these values with no safety consequences for the reactor.

7.7.3.3 Other Reactivity Control Systems

The standby liquid control system is described and evaluated in Section 9.3.

7.7.4 Pressure Regulator and Turbine-Generator Controls

7.7.4.1 Design Basis

The pressure regulator and turbine-generator controls are integrally connected to accomplish the functions of controlling reactor pressure and turbine speed. Specifically, reactor pressure must be prevented from increasing too high during load maneuvers, and turbine speed must be maintained below design limits. The system response must be stable for all anticipated maneuvering rates.

7.7.4.2 System Description

Control and supervisory equipment for the turbine generator are arranged for remote operation from the turbine-generator control panel board or console in the control room. In addition, turbine oil pressure is transmitted to an indicator on the panel board. Normally, the pressure regulator controls turbine control valve position to maintain constant reactor pressure. The ability of the plant to follow system load is accomplished by adjusting the reactor power level, either by regulating the reactor coolant recirculation system flow or by moving control rods.

However, the turbine speed control can override the pressure regulator, and the turbine control valves will close when an increase in system frequency or a loss of generator load causes the speed of the turbine to exceed the setpoint. In the event that the reactor is delivering more steam than the turbine control valves will pass, the excess steam will be bypassed directly to the main condenser automatically by pressure-controlled bypass valves.

The total capacity of the bypass valves is equal to 33.5% of the rated reactor flow. Load rejection in excess of the bypass valves' capacity, which occurs due to generator or tie-line breaker trips, will cause the reactor to scram.

The Pressure Regulator and Turbine-Generator Controls utilize a triple modular redundant (TMR) design with a separate Turbine Controller, Pressure Controller and Overspeed Protection Module. Each controller / module consists of three (3) separate processors, utilizing a software-implemented fault tolerance (SIFT) technology that allows the controller to remain on-line if one of the processors fail.

The TMR Turbine Controller is tasked with turbine control and protection, the TMR Pressure Controller performs the steam bypass and pressure control functions and the TMR Protection Module provides a second level of overspeed protection. The Turbine Controller and Pressure Controller communicate over hardwired analog inputs and outputs to coordinate turbine and pressure control requirements. The Protection Module functions independent from the Turbine and pressure Controllers with dedicated speed sensor inputs.

The separate TMR system for control of the turbine bypass valves and control of the turbine allows the two functions to maintain independence from a control hardware and software standpoint. For critical functions, the controllers utilize triple-redundant process sensors and will continue operation if one of the process sensors fail. The Pressure Controller is designed to continue operation even if two (2) of the three (3) sensors fail.

The pressure control system controls reactor pressure during plant startup, power generation and shutdown modes of operation. The Mark VI pressure controllers act to ensure that the desired pressure setpoint is achieved through the positioning of the turbine control valves and steam bypass valves in response to changes in the pressure setpoint error.

The reactor pressure control algorithm is designed to operate using three pressure transmitter inputs from one of two locations in the steam flow path. In effect, two pressure control strategies are offered, either of which is selectable by the operator. The control strategy offered by the three pressure transmitters tapped into reactor vessel dome structure is called reactor vessel (dome) pressure control. The second control strategy uses three pressure transmitters tapped into the main steam line just upstream of the main stop valves and is called turbine inlet main steam (throttle) pressure control.

A maximum combined flow limit is provided to limit the total steam flow through the turbine control valves and bypass valves. See the cycle specific reload documentation for the analysis assumptions on combined steam flow through turbine control valves and turbine bypass valves.

As seen in Figure 7.7-4a, the pressure regulator with the higher value controls through the low value gate because the other input to the gate, the speed/load signal, is normally set to be larger by about the equivalent of 10% steam flow (or 0.5% speed for 5% speed regulation). A bias signal of this amount is subtracted from the speed/load signal resulting in the load demand signal. The difference between this signal and the output signal from the high-pressure regulator (which represents the steam flow required to satisfy the pressure control requirement), is the load demand error signal. This load demand error signal is the control signal for the recirculation flow control system which adjusts the core recirculation flow until the load demand error signal is zero. This same signal is used to add the equivalent of a setpoint adjustment, at a controlled rate and magnitude, to the pressure regulator to cause the control valves to respond immediately. This effect is temporary since the load demand error signal returns to zero as the load demand is satisfied (see Section 7.7.3).

The speed/load signal will take over control of the turbine control valves should the speed increase over 0.5% (due to overspeed caused by load rejection or system frequency rise due to an upset) or should the load set signal be decreased greater than 10% and faster than the recirculation flow control system can change the reactor steaming rate. In such event of takeover, the steam flow required signal will exceed the control valve flow demand signal. When this difference exceeds a small bias signal (equivalent to about 1%), the bypass valves will open and control the pressure if the rejected load does not exceed the bypass capacity. If the bypass capacity is exceeded, the reactor will scram.

The reactor steaming rate can keep up with normal load maneuvering and, therefore, bypassing of steam is not normally required.

Typical pressure/steam flow relationships are shown in Figure 7.7-9. The pressure regulator setpoint is fixed and both turbine and reactor pressures vary with steam flow - the turbine due to the regulation of the pressure controller and the reactor due to this same regulation plus the variable steam line pressure drop. There appears to be no penalty to this mode of operation (which is recommended for a BWR plant).

The turbine stop valves are equipped with limit switches which open when the valve has moved from its fully opened position. These switches provide a scram signal to the reactor protection system, anticipating the resulting reactor high pressure condition. The turbine stop valve scram signal is discussed in Section 7.2.

To protect the turbine, closure of the four turbine stop valves is initiated for various abnormal conditions as listed in Section 10.2.

7.7.4.3 Design Evaluation

The pressure regulator and turbine-generator design is such that the system provides a stable response to normal maneuvering transients. Section 4.3 evaluates the stability of the overall boiling water reactor cycle, including the pressure and turbine control. Section 15.2.3 analyzes transients due to turbine trips.

The bypass valves are capable of responding to the maximum closure rate of the turbine control valves such that reactor steam flow is not significantly affected until the magnitude of the load rejection exceeds the capacity of the bypass valves. Load rejections in excess of bypass valve capacity may cause the reactor to scram due to high pressure, high neutron flux, or rapid electrical load reduction. When first stage turbine pressure is above that corresponding to 38.5% power, any condition causing the turbine stop valves to close will directly initiate a scram before reactor pressure or neutron flux have risen to the trip level.

The pressure regulator or controller can be assumed to fail by closing the turbine control valves or the bypass valves. These malfunctions are discussed in Chapter 15, fuel damage does not occur in either case. The triple modular redundant design reduces the probability that pressure regulator malfunction will cause operational problems.

7.7.5 Feedwater Control System

7.7.5.1 Design Basis

The feedwater control system (FCS) is designed to regulate the feedwater flow to the reactor vessel such that proper reactor vessel water level is maintained.

7.7.5.2 System Description

During steady-state operation, feedwater flow closely matches steam flow and the water level is maintained by the microprocessor-based, digital control system.

The level of the water in the reactor is controlled by the digital feedwater controller which receives inputs in one of two ways as selected by the operator: from reactor vessel water level, steam flow, and feedwater flow transmitters (three-element control) or from reactor vessel water level only (single-element control). In three-element control, signals from feedwater flow, steam flow, and reactor vessel level are used to provide a quick response to power changes by reacting to feedwater and steam flow changes before a level change could be detected by level instrumentation. In single-element control a change in water level is immediately sensed and the system adjusts the opening of the feedwater control valves to maintain level. The water level is monitored by level transmitters coupled to two separate sensing lines from the proper elevations on the vessel shell. Level sensors are described in Section 7.6.

Feedwater flow is monitored by flow transmitters coupled to flow nozzles in the feedwater lines. The total feedwater flow is the summation of the signals from the three feedwater lines.

Steam flow is monitored by four flow transmitters coupled to four flow restrictors in the steam lines. The total steam flow is the summation of the signals from the four steam lines.

The Feedwater System and Main Turbine High Water Level Trip Instrumentation is designed to detect a potential failure of the Feedwater Level Control System that causes excessive feedwater flow.

With excessive feedwater flow, the water level in the reactor vessel rises toward the high water level reference point, causing the trip of the three feedwater pumps and the main turbine.

Reactor Vessel Water Level-High signals are provided by level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level in the reactor vessel (variable leg). Four channels of Reactor Vessel Water Level-High instrumentation are provided as input to two trip systems. Each trip system is arranged with a two-out-of-two initiation logic that trips the three feedwater pumps and the main turbine. The channels include electronic equipment (e.g., trip units) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the channel output relay actuates, which then outputs a feedwater pump and main turbine trip signal to the trip logic.

A trip of the feedwater pumps limits further increase in reactor vessel water level by limiting further addition of feedwater to the reactor vessel. A trip of the main turbine and closure of the stop valves protects the turbine from damage due to water entering the turbine.

The Feedwater System and Main Turbine High Water Level Trip Instrumentation is assumed to be capable of providing a feedwater pump and main turbine trip in the design basis transient analysis for a feedwater controller failure, maximum demand event. The high level trip indirectly initiates a reactor scram from the main turbine trip (above approximately 45% RTP) and trips the feedwater pumps, thereby terminating the event. The reactor scram mitigates the reduction in MCPR.

Instrument zero = 503 inches above Vessel Zero or 143 inches above Top of Active Fuel (TAF).

TAF = 360 inches above Vessel Zero.

The LCO requires four channels of the Reactor Vessel Water Level-High instrumentation to be OPERABLE to ensure that no single instrument failure will prevent the feedwater pumps and main turbine trip on a valid high level signal. Two channels are needed to provide trip signals in order for the feedwater pump and main turbine trips to occur. Each channel must have its setpoint set within the specified Allowable Value. The Allowable Value is set to ensure that the thermal limits are not exceeded during the event. The actual setpoint is calibrated to be consistent with the applicable setpoint methodology assumptions. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure that the setpoints do not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., reactor vessel water level), and when the measured output value of the process parameter exceeds the setpoints, the associated device (e.g., trip unit) changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. The trip setpoints are determined from the analytic limits, corrected for defined process, calibration, and instrument errors. The Allowable Values are then determined, based on the trip setpoint values, by accounting for the calibration based errors. These calibration based errors are limited to reference accuracy, instrument drift, errors associated with measurement and test equipment, and calibration tolerance of loop components. The trip setpoints and Allowable Values determined in this manner provide adequate protection because instrument uncertainties, process effects, calibration tolerances, instrument drift, and severe environment errors (for channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for and appropriately applied for the instrumentation.

Reactor vessel water level, feedwater flow, and steam flow are recorded in the control room. High and low reactor vessel water levels are annunciated in the control room.

Each reactor feedwater pump has recirculation controls which pass feedwater back to the condenser when individual feed pump flow is below minimum flow required to cool the pumps. Each feed pump is shutdown automatically on low suction pressure (see Sections 10.4).

In the control room, a microprocessor-based digital control system is installed. The microprocessor-based system provides improved reliability of operation.

7.7.5.3 Design Evaluation

Key feedwater system parameters are recorded and, upon abnormal conditions, annunciated in the control room; the operator can monitor system operation continuously.

Feedwater level control signals are redundant, providing assurance that malfunctions will not result in operational difficulties.

Feedwater control system malfunctions could result in maximum or zero feedwater flow. These malfunctions are discussed in Sections 15.1.2, 15.2.7 and 15.8.3. In all cases, fuel damage does not occur. Section 15.1.2.2 also discusses the Reactor Vessel Water Level-High turbine /FW pump trip logic and the setpoint values.

7.7.6 Main Condenser, Condensate, and Condensate Demineralizer Systems' Control

7.7.6.1 Design Basis

The main condenser, condensate, and condensate demineralizer systems' control is designed to provide indications of system trouble. Main condenser sensors must provide inputs to the reactor protection system to anticipate loss of the main heat sink and to protect against condenser overpressure. The condensate system controls must ensure adequate cooling to the condensate pumps.

7.7.6.2 System Description

The condensate/condensate booster pumps discharge without throttling to the suction of the reactor feedwater pumps. See Section 10.4.7 for a description of the condensate system.

Discharge pressure of the condensate pumps is indicated. When a condensate/condensate booster pump is in standby, low pressure on the Reactor Feed Pump (RFP) suction header starts the additional pump. A modulating control valve, located downstream of the condensate booster pumps, recirculates condensate back to the main condenser on low loads. Recirculation maintains a minimum cooling flow through the condensate/condensate booster pumps, steam jet air ejector condensers, gland seal steam condenser, and off-gas condenser.

If a LOCA is detected, when all four pumping units are running, the D pumping unit will trip to limit the loading on the 4-kV busses. This trip can be reset to permit any three of the four pumping units to run during a LOCA.

The 100% condensate filter system (CFS) alarms on trouble indication.

Conductivity of condensate both upstream and downstream of the demineralizer is measured, recorded, and actuates an alarm on high conductivity.

Main condenser hotwell level is indicated in the control room and is automatically controlled by either making up or returning condensate from the condensate storage tank. Vacuum switches monitoring condenser vacuum provide scram signals to protect the reactor from loss of the main heat sink; protection for the condenser itself is assured by closure of the turbine stop and bypass valves as vacuum decreases below a preset low level.

7.7.6.3 Design Evaluation

Indication of key parameters from the main condenser, condensate system, and condensate demineralizer system are provided in the control room. The operator is kept fully cognizant of the conditions of the systems. Abnormal conditions are annunciated so that the operator may take appropriate action. The reactor is protected from loss of the main heat sink by main condenser low vacuum scram signals; the vacuum sensors meet the design requirements established for all reactor protection system functions (Section 7.2). To protect the condenser from overpressure, continued decrease of condenser vacuum below the scram setpoint will initiate closure of the turbine stop valves and bypass valves.

7.7.7 References

1. Licensing Topical Report NEDO-21231, "Banked Position Withdrawal Sequence", January 1977.

2. Licensing Topical Report NEDO-33091-A, Revision 2, "Improved BPWS Control Rod Insertion Process", July 2004.

3. General Electric GEK 111056 October 2004, "General Description of BWR Mark VI Controls".

7.8 ANTICIPATED TRANSIENT WITHOUT SCRAM MITIGATION SYSTEM

7.8.1 Introduction

This section describes the anticipated transient without scram (ATWS) mitigation system. Related topics and systems include the standby liquid control (SBLC) system, described in Section 9.3.5; the control rod drive (CRD) system, Section 4.6; the reactor recirculation system, Section 5.4.1; the reactor protection system (RPS), Section 7.2; the low pressure coolant injection (LPCI) system (suppression pool cooling mode), Section 6.2.2; and the ATWS accident analyses, Section 15.8.

An anticipated transient without scram is a postulated operational transient (such as loss of feedwater, loss of condenser vacuum, or loss of offsite power) accompanied by a failure of the reactor protection or control rod drive systems to shut down the reactor. Even though the reactor protection and control rod drive systems have been shown to be highly reliable, it is postulated that a common mode electrical or mechanical failure is possible.

If the control rods fail to insert following a transient which isolates the reactor from the normal cooling system, the resulting pressure rise could be large enough to threaten the integrity of the reactor coolant pressure boundary. Unless core power and system pressure are reduced to within the capacities of the standby cooling and makeup systems within a few minutes, the core can be uncovered and melting can occur, resulting in large releases of radioactive fission products.

Since a normal scram is assumed to be unavailable for reducing reactor power and since the transient event is one in which power reduction is necessary, another method of reducing the power is needed. Two automatic ATWS functions are provided: recirculation pump trip (RPT) and alternate rod insertion (ARI). Should both the RPS and ARI fail to insert the control rods, the SBLC would be manually initiated to control reactivity.

The trip of the reactor recirculation pumps causes a quick reduction in core flow which increases core void generation. These increased voids introduce negative reactivity thus decreasing the reactor power. The quick power reduction brings reactor pressure, neutron flux, and fuel surface heat flux down rapidly enough to limit the peak pressure, clad oxidation, and peak fuel enthalpy so that neither reactor coolant pressure boundary breach nor fuel failure occur.

Alternate rod insertion is a means of control rod insertion which is motivated mechanically by the normal hydraulic control units and control rod drives but which utilizes totally separate and diverse logic from RPS. Alternate rod insertion energizes valves which cause the scram valve pilot air header to bleed down. Although this type of alternate rod insertion does not eliminate the short-term consequences of the assumed failure of normal scram action, it does reduce the long-term consequences. The most significant long-term consequences involve containment limits, particularly suppression pool temperature.

7.8.2 Design Requirements

The ATWS rule (10 CFR 50.62) requires the following three elements to mitigate ATWS events:

A. Recirculation pump automatic trip equipment;

B. An alternate rod insertion system, diverse from RPS, with redundant scram air header exhaust valves; and

C. A standby liquid control system that meets minimum flow and concentration requirements.

The RPT portion of the ATWS mitigation system is designed to perform its function in a reliable manner and to conform to the NRC-approved Monticello tripping logic design.[1]

The overall requirements for the ARI portion of the ATWS mitigation system are as follows:

A. The system should be diverse from RPS;

B. The system shall be designed so that any component whose single failure can cause insertion of all control rods shall be highly reliable;

C. The system should be testable in service;

D. The system should be designed so that, as much as possible, no single component failure can prevent total mitigation action; and

E. All hardware should be of high quality and environmentally qualified.

For an ATWS (per 10 CFR 50.62), the standby liquid control system must be capable of injecting into the reactor pressure vessel a borated water solution equivalent in reactivity control to injecting 86 gal/min of 13 wt% sodium pentaborate at natural B-10 concentration into a 251-inch inside diameter reactor vessel for a given core design. The specific requirements of flowrate and concentration for Dresden Station are addressed in Section 9.3.5.

7.8.3 Mitigation System Description

All of the anticipated transients which require mitigation in the unlikely event of an ATWS quickly reach at least one of two conditions which are readily sensed and from which mitigating actions may be initiated. These conditions are high reactor vessel pressure and low-low reactor water level.

The ATWS mitigation system consists of reactor pressure and reactor water level sensors and trip units, logic, power supplies, and instrumentation to automatically initiate RPT and ARI. The reactor dome pressure automatic actuation was chosen to be slightly above relief valve actuation. (The value used in analysis was 1250 psig for Unit 2 (Reference 4) and 1200 psig for Unit 3, Reference 3). The low-low reactor water level automatic actuation analytical limit (-59 inches) is that level before which the recirculation

pumps trip (ATWS mitigation function) and low and high pressure coolant injection and core spray (ECCS mitigation function) are initiated. For each division, both mitigation functions are initiated by two independent level transmitters which feed reactor water level signals to a set of dedicated master and slave trip units.

Certain manual actions are required of the operator. Suppression pool cooling and standby liquid control must be initiated manually as required by the Emergency Operating Procedures (EOPs). The following subsections describe the capability and requirements for manual initiation of RPT and ARI. Alarms and indications are available to the operator to allow performance of manual actions within the time limits. In addition to the alarms and indications which are initiated by RPS scram logic, other annunciator windows actuate when the reactor water level or reactor pressure reach the ATWS setpoints. Therefore, during an ATWS event, the operator is alerted that an ATWS event has occurred and then has sufficient time to perform the required manual actions. Figure 7.8-1 shows the ATWS mitigation system block diagram.

7.8.3.1 Recirculation Pump Trip

The ATWS mitigation system automatically initiates a RPT for Unit 2, or for Unit 3 both adjustable speed drive (ASD) Controller and ASD feed breaker on a two-out-of-two trip logic in either of two channels upon either continuous low-low reactor water level for a period of time (Analytical Limit: 8.0 to 9.0 seconds) or high reactor pressure. The performance characteristics are as follows:

A.	Logic delay for trip (seconds) (Including dynamic response of the sensors, logic action of the breakers and for Unit 2 or Unit 3 either the ASD feed breaker tripped or ASD emergency stop.)	< 0.53
B.	Pump inertial constant (JN/ft, seconds)	< 3.0

Manual RPT is achieved by a manual trip of the recirculation pump drive motor breakers for Unit 2, or for Unit 3 the ASD feed breakers or ASD controller. Drive motor breaker control switches are located at panel 902-4 and at the switchgear breakers for Unit 2, and for Unit 3 at panel 903-4 for the ASD feed breakers and ASD emergency stop pushbuttons along with the ASD emergency stop pushbuttons on the ASD local control panel. Manual RPT should be performed following receipt of alarms indicating an ATWS has occurred if automatic RPT does not occur:

A. High torus water average temperature alarm
B. High reactor dome pressure alarm
C. Reactor low low water level alarm

7.8.3.2 Alternate Rod Insertion

The ATWS mitigation system logic automatically energizes the ARI valves when the ATWS reactor vessel high pressure trip setpoint is reached, the ATWS low-low reactor water level trip setpoint is reached, or the manual switches are actuated.

Two manual initiation pushbutton switches are provided in the control room at panel 902(3) for each division of ARI logic. Failure of automatic initiation cannot prevent manual initiation. In order to avoid an inadvertent manual initiation of ARI, the two initiation switches per division must first be armed by rotating a

collar integral to each pushbutton. Once armed and then depressed, the pair of switches associated with either division activate the ARI trip function.

Manual ARI should be initiated upon reaching any of the following alarm conditions:

A. High torus water average temperature alarm
B. High reactor dome pressure alarm
C. Reactor low low water level alarm
D. Control rod drive position indication not inserted after scram annunciation

7.8.3.3 Alternate Rod Insertion Valves

Upon ATWS initiation (automatic or manual), the ARI solenoid valves (see Section 4.6 and Drawings M-34 and M-365) are energized to block the instrument air supply to the scram air header and to depressurize the scram air header by venting air to atmosphere. Depressurization of the scram air header causes the scram valves to open resulting in the drives scramming. All ARI valves are normally deenergized. The ARI valving system operates as follows:

A. There are two divisions of valves installed on the scram air header. Each division has sufficient capacity to accomplish rod insertion. Each division of valves consists of the following valves:

    1. Two ARI valves which are normally closed but open when energized to depressurize the scram air header.

    2. One ARI valve three-way ARI valve which is installed in the scram air header supply line. This valve is normally positioned to allow air to be supplied to the scram air header. When energized, this valve repositions to close off the supply air and vent the scram air header to the atmosphere.

B. Once actuated, the ARI valves remain energized for a minimum of 44.2, but not to exceed 54.2 seconds to ensure the scram air header is adequately depressurized. After this delay, if the initiation signal has cleared, the ARI valves are deenergized. If the initiation signal is still present after the delay, the ARI valves remain energized until the initiation signal clears.

C. Time delay does not exceed 54.2 seconds to ensure that the maximum permissible rod insertion time is not exceeded. Without this limit the design objective stated in Ref. 1 paragraph 3.2.1, i.e. the full rod insertion occurs within approximately 60 seconds of ARI initiation time before the pressure suppression pool temperature reaches 110°F, would not be met. If initiation signal has cleared, operator can reset the time, allow SDV to drain/vent and attempt to insert rods that may not have been fully inserted. [2][1]

7.8.4 Design Evaluation

For all transients, the Recirculation Pump Trip (RPT) effectively mitigates the short term ATWS response. The Alternate Rod Injection (ARI) effectively reduces the long term consequences to nearly those of normal scram situations.

The sensors, trip units, and actuation relays (with the exception of the RPT reactor low-low water level trip time delay and the ARI reset circuitry) are common to both RPT and ARI. Thus, the automatic initiations occur concurrently (except for the RPT low-low water level time delay) at identical setpoints. Therefore, the following design analyses dealing with the inputs, the logic, and logic power supply apply equally to ARI and RPT. The RPT is modeled after the NRC-approved Monticello tripping logic design including two means of tripping each pump motor.

The ARI function requires start of control rod motion within 39.2 seconds and full insertion within 44.2 seconds of ARI actuation. Dresden specific analysis confirmed that these parameters are met. Section 7.8.3.3 describes the seal-in and reset time delay of the ARI valves. Based on the NRC-approved topical report,[1] ARI achieves the design objectives. The most limiting of these objectives (pressure suppression pool temperature) requires full rod insertion within approximately 60 seconds.

The ARI design is safety-related and segregated into two electrical divisions; namely, Division I and Division II, which are physically segregated. The RPS is a four-channel electrical arrangement (two trip systems with two subchannels each) and has individual channel separation. The RPS circuits are not routed with other divisionally segregated circuits of ARI.

The ARI system utilizes valves which are normally deenergized but which are energized to perform their safety function. The ARI valves are powered from dc sources. Conversely, the existing RPS employs ac-powered valves which are deengerized to initiate a scram.

The ARI system uses an analog transmitter/trip unit configuration. The transmitters are separate from sensors used for the RPS. In addition, the trip units utilized are separate from process instruments used for the RPS.

The analytical limit of the ARI trip for reactor pressure is 1250 psig for Unit 2 and 1200 psig for Unit 3 and for reactor vessel water level is -59 inches with respect to reactor level instrument zero (Reference 3). The RPS analytical limit for reactor pressure is 1060 psig and for vessel level is 8 inch with respect to reactor level instrument zero. Therefore, the automatic setpoints for ARI actuation have been selected such that they will not preempt the RPS scram function.

For each actuation parameter (low-low water level or high reactor pressure), the logic is arranged in a two-out-of-two configuration per division. This logic allows individual sensors, trip units, etc. to be tested or calibrated during plant operation without initiating the ARI system.

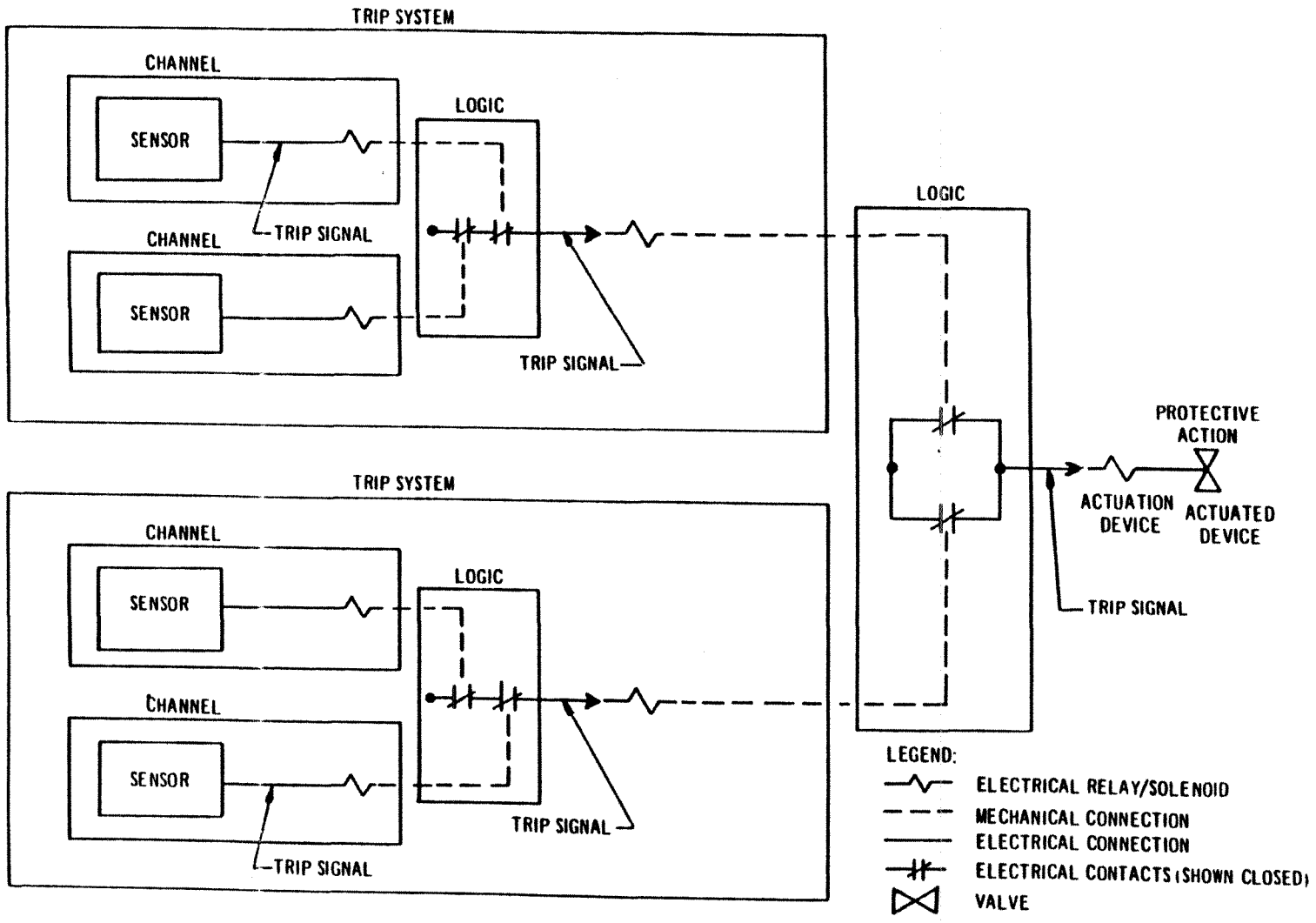
7.8.5 References

1. General Electric Licensing Topical Report, NEDE-31096-P-A, "Anticipated Transients Without Scram; Response to NRC ATWS Rule, 10 CFR 50.62," February 1987

2. General Electric Letter C1100261(65) dated 6/8/95 from Bertram W Joe to Paul Chennel.

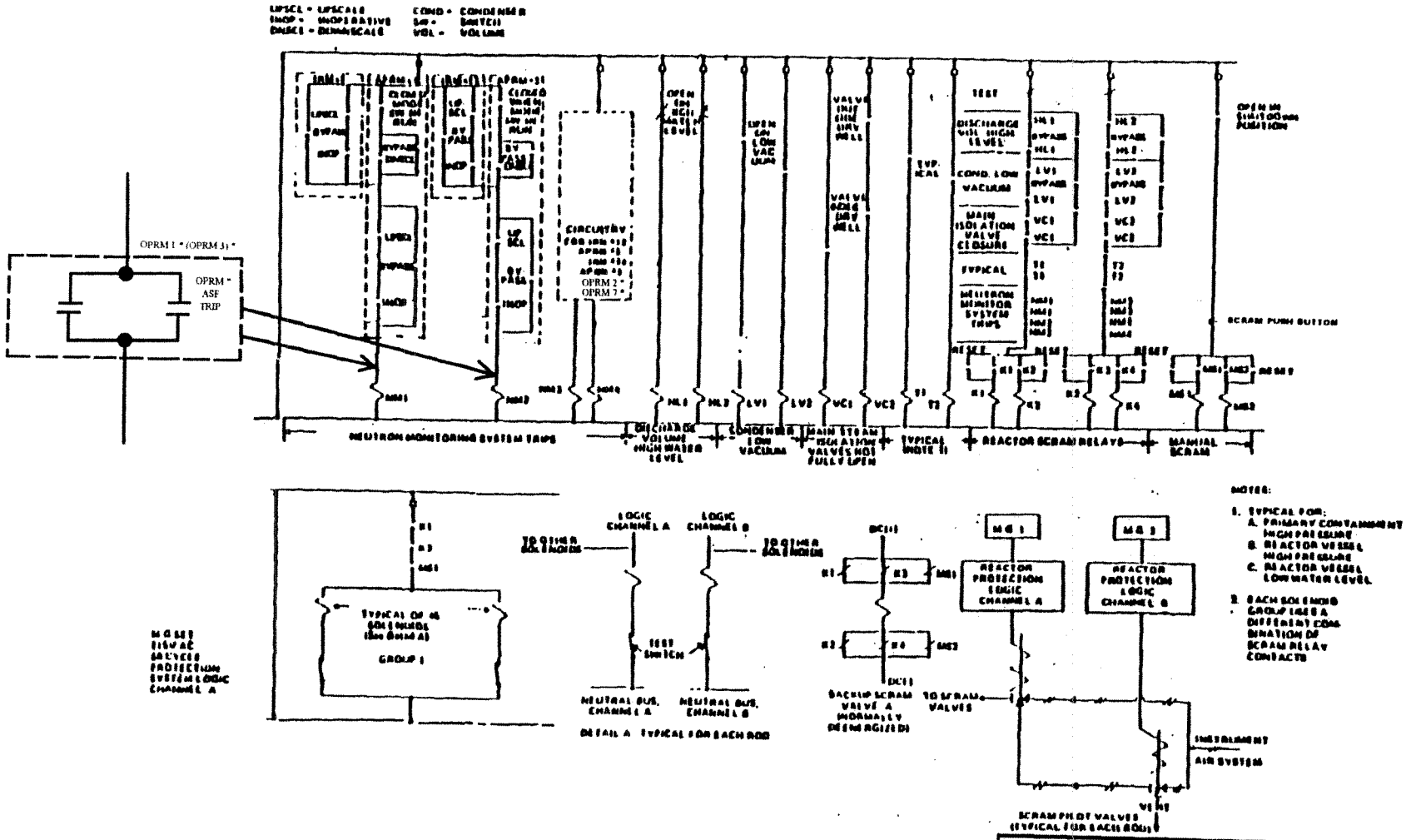
3. ANP-3516P, Revision 0, "Dresden Unit 3 Cycle 25 Reload Safety Analysis," AREVA, September 2016. (Unit 3 only).

4. Westinghouse Report OPTIMA2-TR051DR-ATWS, Revision 0, "ATWS Analysis for the Introduction of SVEA-96 Optima2 Fuel at Dresden Units 2&3," August 2006.



TYPICAL PROTECTION SYSTEM (CONTROL AND INSTRUMENTATION PORTIONS)

DRESDEN STATION UNITS 2 & 3
USE OF CONTROL AND INSTRUMENTATION DEFINITIONS
FIGURE 7.2-1



* UNIT 2 ONLY

UFSAR REVISION 4, JUNE 2001

DRESDEN STATION
UNITS 2 & 3

REACTOR PROTECTION SYSTEM -SINGLE LOGIC CHANNEL TRIPPING DIAGRAM

FIGURE 7.2-2

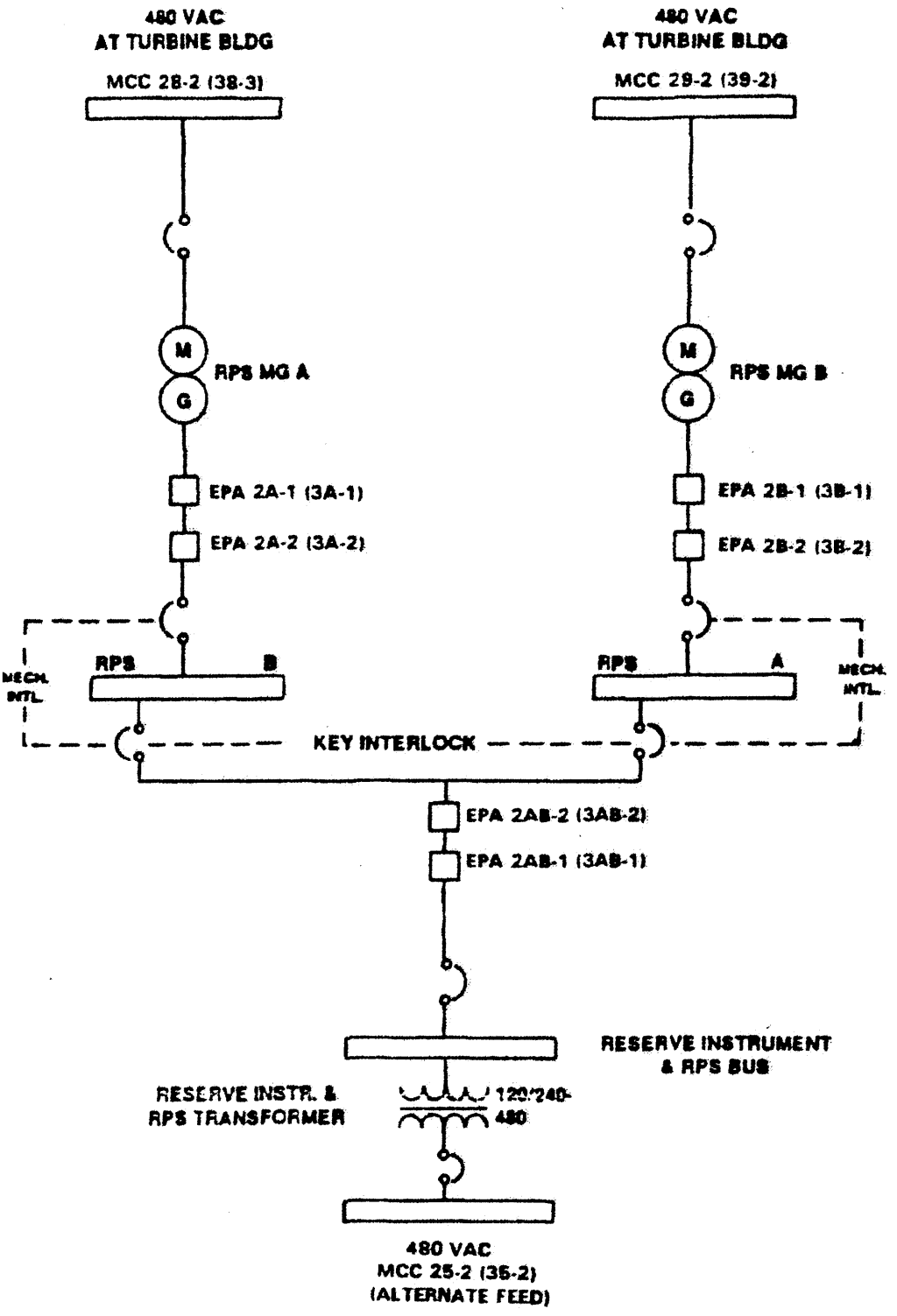
**Unit 2 only, when OPRM is armed.

UFSAR REVISION 6, JUNE 2005

DRESDEN STATION UNITS 2 & 3

REACTOR PROTECTION SYSTEM SCRAM FUNCTION

FIGURE 7.2-3



UFSAR Revision 8, June 2009
DRESDEN STATION UNITS 2 & 3
REACTOR PROTECTION SYSTEM POWER SUPPLY
FIGURE 7.2-4

REACTOR VESSEL LOW-LOW LEVEL — LT 263-23A — LOCAL
REACTOR VESSEL LOW-LOW LEVEL — LT 263-23B — LOCAL
REACTOR VESSEL LOW-LOW LEVEL — LT 263-23C — LOCAL
REACTOR VESSEL LOW-LOW LEVEL — LT 263-23D — LOCAL
REF. 3
SWITCH REQUIRES COINCIDENT TRIP UNITS 263-25A2 OR 263-25B2 AND 263-25C2 OR 263-25D2
START
SEE REF. DWG. 4,10B11 FOR ADDITIONAL FUNCTIONS PERFORMED BY THIS SET OF SWITCHES

HIGH DRYWELL PRESSURE — PS 1632A — LOCAL
HIGH DRYWELL PRESSURE — PS 1632B — LOCAL
HIGH DRYWELL PRESSURE — PS 1632C — LOCAL
HIGH DRYWELL PRESSURE — PS 1632D — LOCAL
REF. 3
SWITCH REQUIRES COINCIDENT TRIP OF SWITCH 1632A OR 1632B AND 1632C OR 1632D TO START SYSTEM
SEE REF. DWG. 4 & 10 FOR ADDITIONAL FUNCTIONS PERFORMED BY THIS SET OF SWITCHES

REACTOR PRESS PERMISSIVE WHEN LOW — PS 263-52A — LOCAL — REF. 3
REACTOR PRESS PERMISSIVE WHEN LOW — PS 263-52B — LOCAL — REF. 3
TIME DEVICE PERMISSIVE 8.5 MIN AFTER LOW-LOW REACTOR LEVEL — AUX DEVICE — CR

POWER AVAIL AT SYSTEM 1 PUMP MOTOR BUS — AUX DEVICE — CR
START — STAND BY DIESEL GEN
PERMISSIVE WHEN NORMAL AUX. POWER AVAIL. — AUX DEVICE — CR
TIME DEVICE PERMISSIVE 10 SEC. AFTER INITIATION — AUX DEVICE — CR

REACTOR PRESS. PERMISSIVE WHEN LOW — PS 263-52A — X
REACTOR PRESS. PERMISSIVE WHEN LOW — PS 263-52B — X

3 POSITION "CLOSE" "AUTO" "OPEN" SPRING RETURN TO "AUTO" FROM "CLOSE" "OPEN" TYPICAL 4 PLACES

CONTROL SW IN "CLOSE" POSITION — RMS — CR
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-4A
VALVE TORQUE SW PERMISSIVE WHILE CLOSING — TORQUE SW — BF VALVE 1402-4A
TRIP DRYWELL COOLING (DRIP (BY DIMERS) NOTE 9
NOT PERMISSIVE WITH AUTO CLOSE SIGNAL — AUX DEVICE — LOCAL
OPEN | CLOSE — REVERSING CONTACTOR (42) =

TEST BYPASS VALVE MO 1402-4A
(TYPICAL FOR VALVE 1402-4B)

CONTROL SW IN "OPEN" POSITION — RMS — CR
CONTROL SW IN "CLOSE" POSITION — RMS — X
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-3A
VALVE TORQUE SW PERMISSIVE WHILE CLOSING — TORQUE SW — BF VALVE 1402-3A
SEAL IN
NOT PERMISSIVE WITH AUTO OPEN SIGNAL — AUX DEVICE — LOCAL
NOTE 3 — OPEN | CLOSE — REVERSING CONTACTOR (42) =

SUCTION VALVE MO 1402-3A
(TYPICAL FOR VALVE 1402-3B)

PERMISSIVE WITH CONTROL SW. IN "AUTO" POSITION ONLY — RMS — X
4 POSITION SWITCH - "STOP" "AUTO" "START" "PULL TO LOCK" IN "STOP" POSITION, SPRING RETURN TO "AUTO" FROM "STOP" OR "START" POSITION ONLY
CONTROL SW IN "START" POSITION — RMS — CR
CONTROL SW IN "STOP" POSITION — RMS — CR
L (R) — CR (R) — CR (G) — L (G) — CR (A)
START | STOP | TRIP — AIR CIRCUIT BREAKER (52)=
NOTE 3

CORE SPRAY PUMP 1401-2A
(TYPICAL FOR PUMP 1401-2B)

CONTROL SW IN "OPEN" POSITION — RMS — CR
CONTROL SW IN "CLOSE" POSITION — RMS — X
VALVE LIMIT SW PERMISSIVE WHEN FULLY CLOSED — LIMIT SW — BF VALVE 1402-24A
VALVE TORQUE SW PERMISSIVE WHILE CLOSING — TORQUE SW — BF VALVE 1402-24A
SEAL IN
NOT PERMISSIVE AFTER INITIATED BY "CLOSE" SW PERMISSIVE WHEN RESET BY REMOVAL OF "AUTO" SIG — AUX DEVICE — CR
NOT PERMISSIVE WITH AUTO OPEN SIGNAL — AUX DEVICE — LOCAL
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-25A
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-24A
SEAL IN
NOTE 3 — OPEN | CLOSE — REVERSING CONTACTOR (42) =

CORE SPRAY INBOARD VALVE MO 1401-25A
(TYPICAL FOR VALVE 1401-25B)

CONTROL SW IN "OPEN" POSITION — RMS — CR
CONTROL SW IN "CLOSE" POSITION — RMS — X
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-24A
VALVE TORQUE SW PERMISSIVE WHILE CLOSING — TORQUE SW — BF VALVE 1402-24A
SEAL IN
NOT PERMISSIVE WITH AUTO OPEN SIGNAL — AUX DEVICE — LOCAL
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-24A
SEAL IN
NOTE 3 — OPEN | CLOSE — REVERSING CONTACTOR (42) =

CORE SPRAY OUTBOARD VALVE MO 1402-24A
(TYPICAL FOR VALVE 1402-24B)

CONTROL SW IN "OPEN" POSITION — RMS — CR
CONTROL SW IN "CLOSE" POSITION — RMS — X
VALVE LIMIT SW PERMISSIVE WHILE OPENING — LIMIT SW — BF VALVE 1402-38A
VALVE TORQUE SW PERMISSIVE WHILE CLOSING — TORQUE SW — BF VALVE 1402-38A
SEAL IN
SEAL IN
NOTE 3 — OPEN | CLOSE — REVERSING CONTACTOR (42) =

PUMP MAIN FLOW BYPASS LINE VALVE MO 1402-38A
(TYPICAL FOR VALVE 1402-38B)

CORE SPRAY SYSTEM "1" LOW FLOW — PS 1464A — LOCAL
CORE SPRAY SYS "1" FLOW GREATER THAN LOW FLOW TRIP SET — PS 1464A — LOCAL
CORE SPRAY PUMP "A" RUNNING — AUX DEVICE — LOCAL
CORE SPRAY PUMP "A" RUNNING — AUX DEVICE — LOCAL

VALVE LEAKAGE TEST ALARM HIGH PRESSURE — INST 1402-6A — LOCAL — A CR
PUMP SEAL LEAKAGE — PS 3402-49A — LOCAL — A CR
VALVE NOT FULLY OPEN LEAKAGE — LIMIT SW — FB VALVE — G CR
VALVE NOT FULLY CLOSED LEAKAGE — LIMIT SW — FB VALVE — R CR
SPRAY HEADER TO TOP OF CORE PLATE HIGH — INST 1439A — LOCAL — A CR
TYP. 1439B

TYPICAL ALL MOTOR OPERATED & MANUAL OPERATED VALVES 1402-6A & 6B

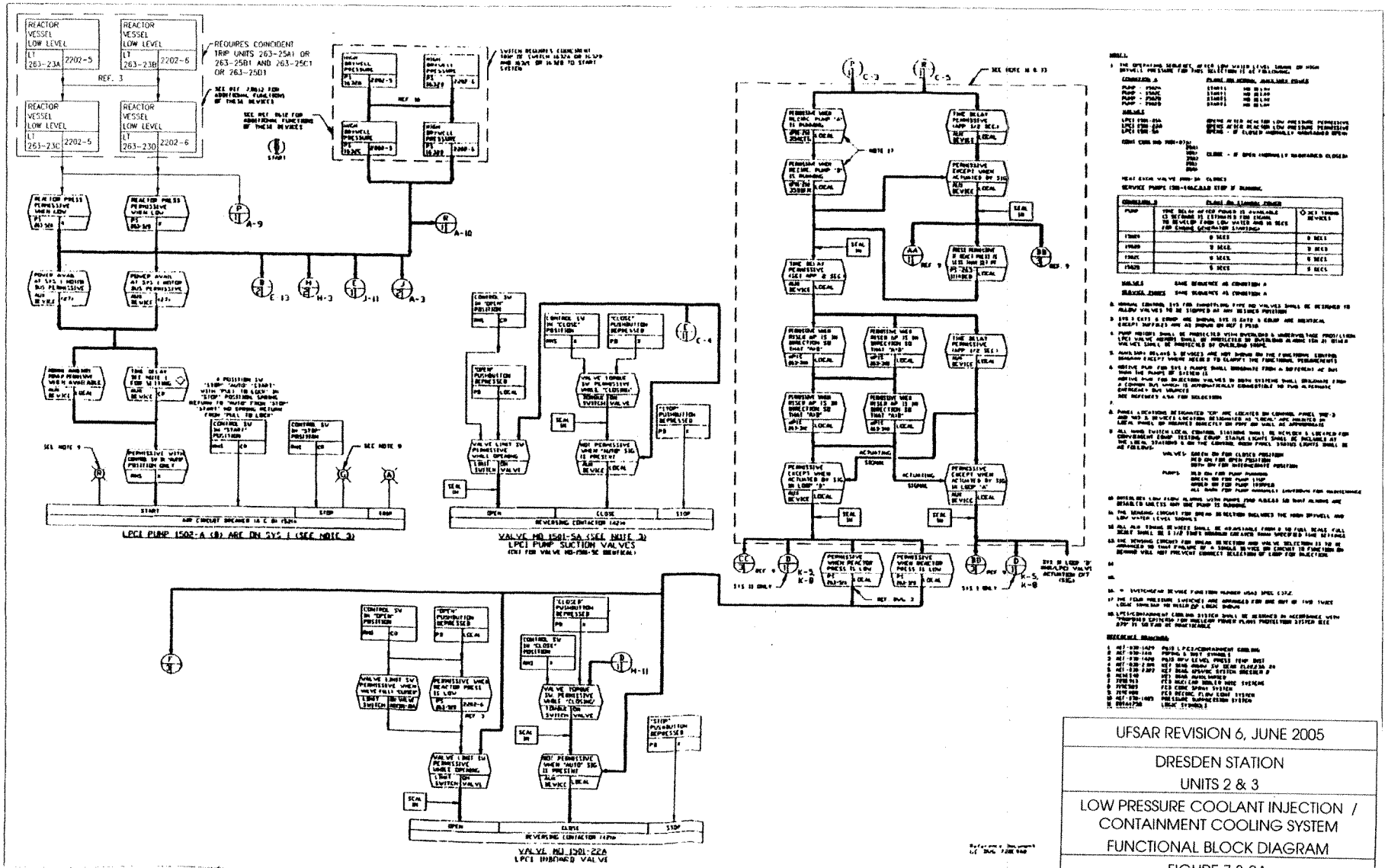
Reference Document
G.E. DWG 719E583

UFSAR REVISION 2, JUNE 1997

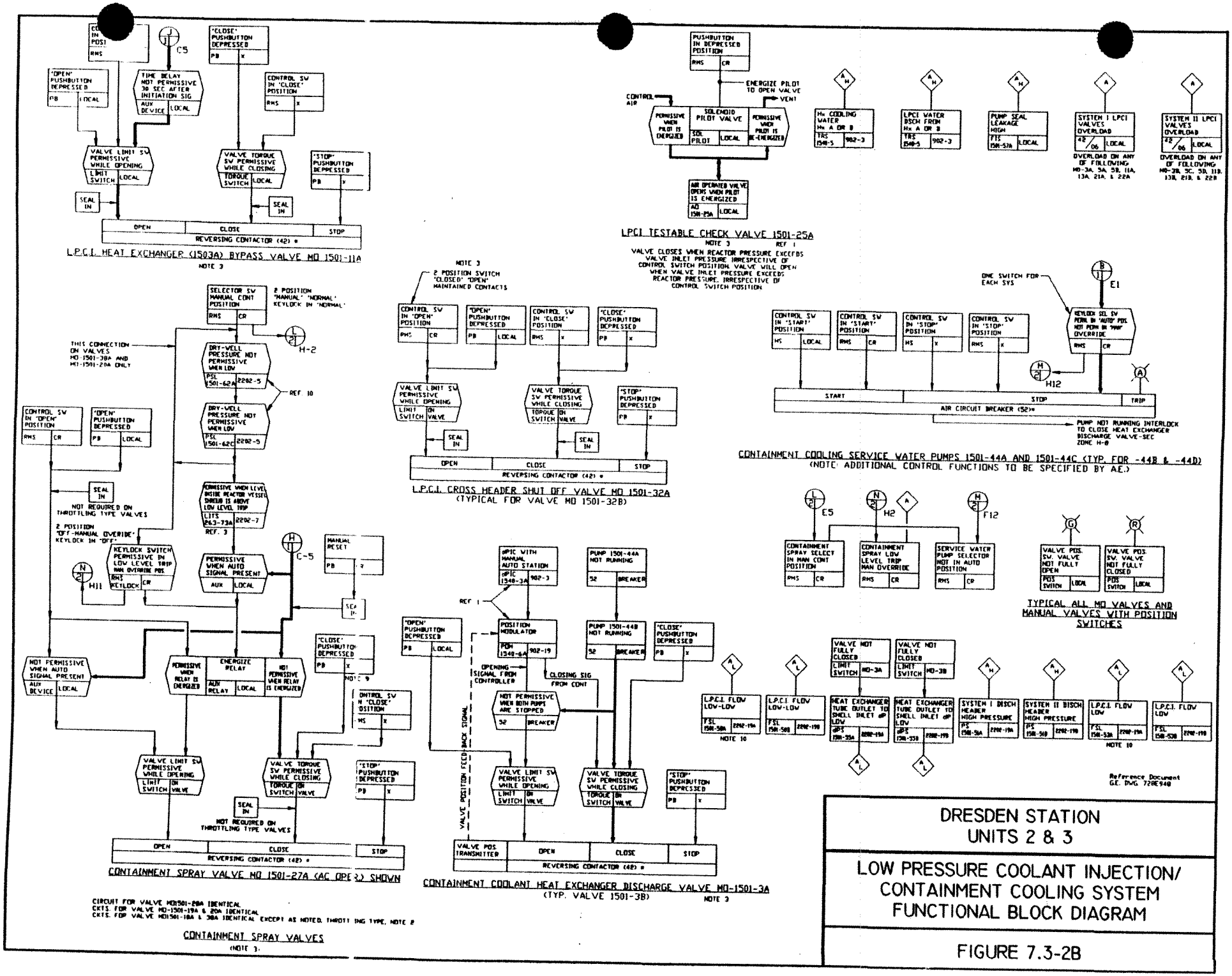
DRESDEN STATION
UNITS 2 & 3

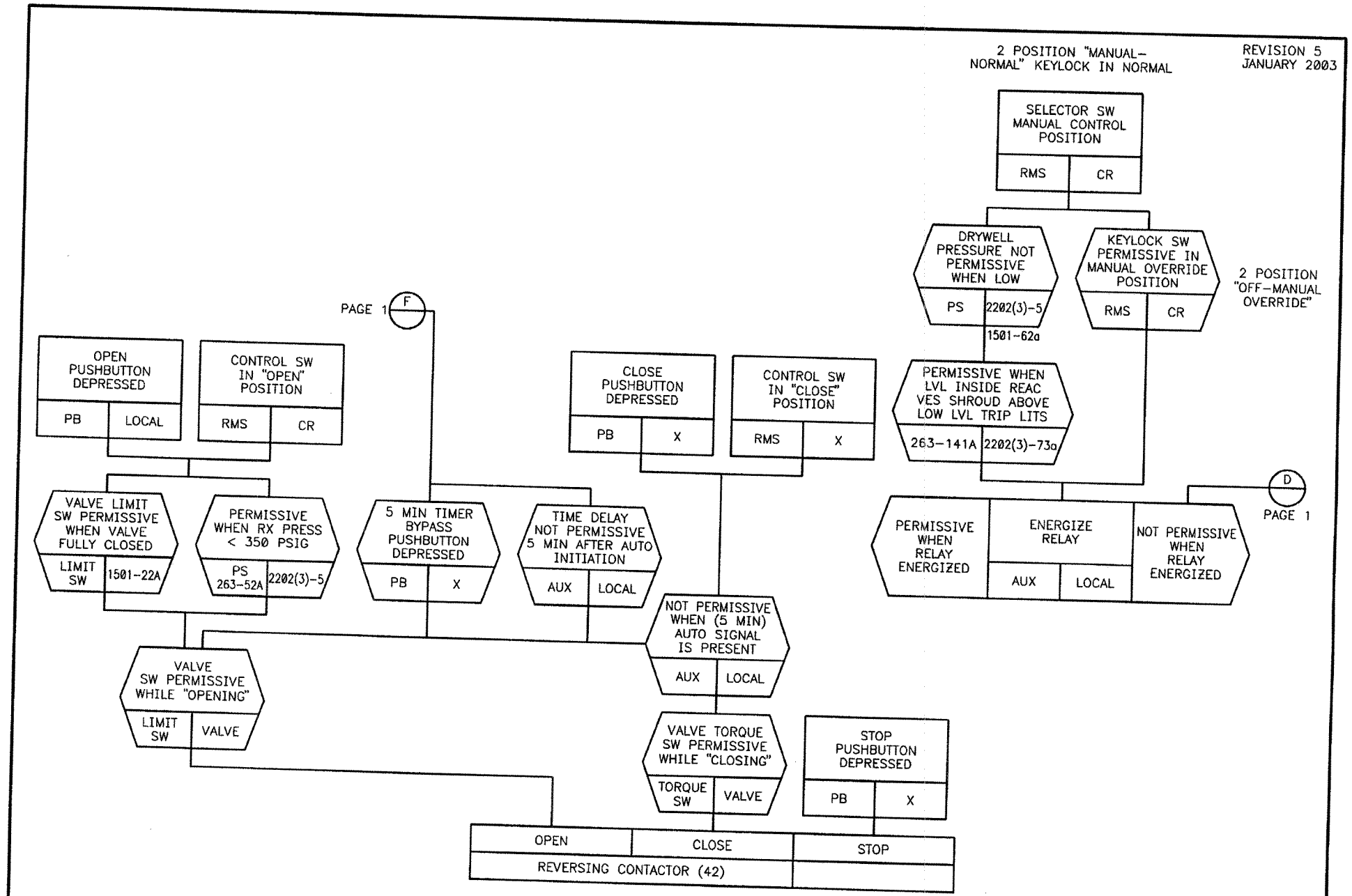
CORE SPRAY SYSTEM
FUNCTIONAL CONTROL DIAGAM

FIGURE 7.3-1



UFSAR REVISION 6, JUNE 2005
DRESDEN STATION UNITS 2 & 3
LOW PRESSURE COOLANT INJECTION / CONTAINMENT COOLING SYSTEM FUNCTIONAL BLOCK DIAGRAM
FIGURE 7.3-2A

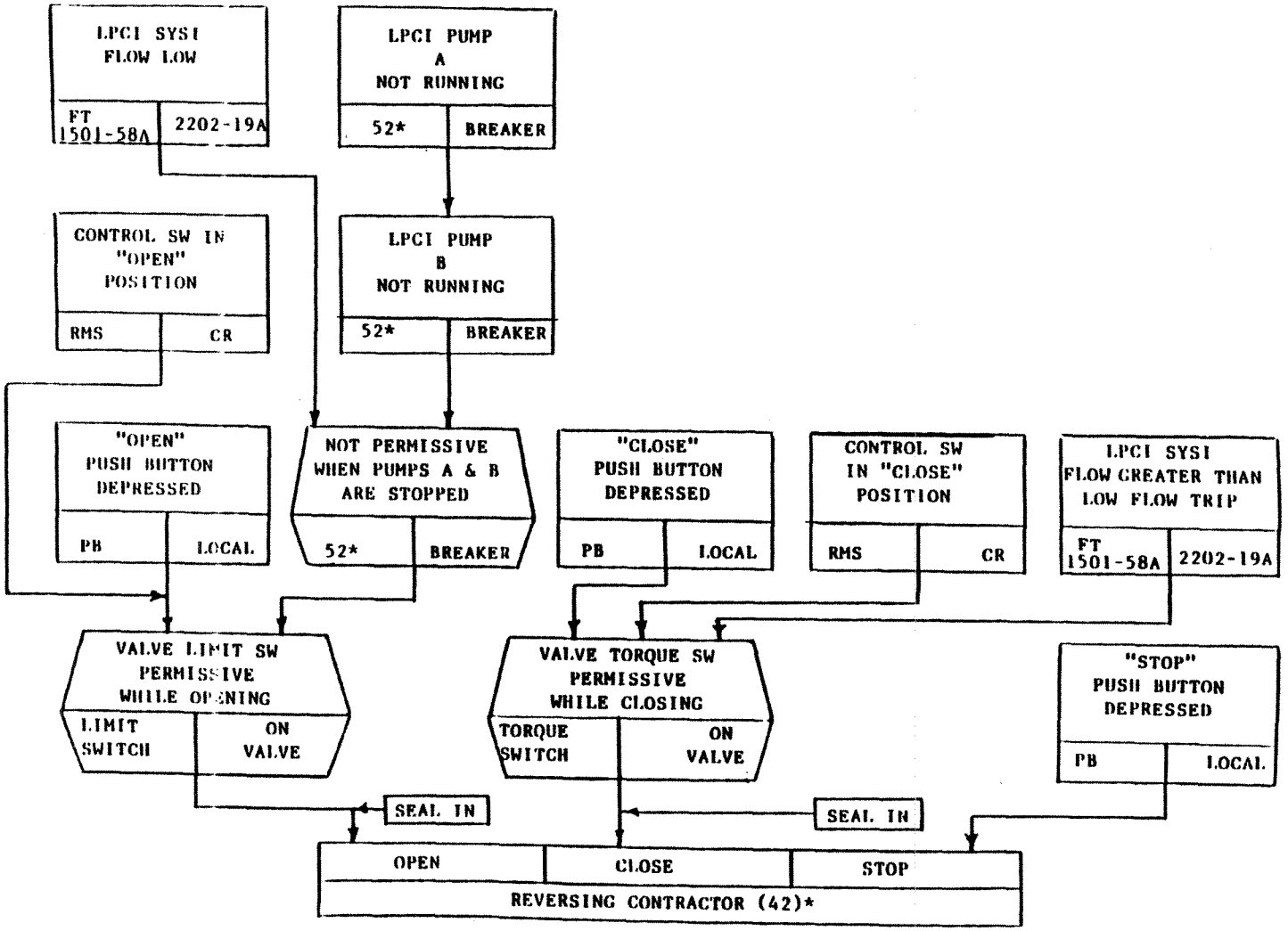

L.P.C.I. HEAT EXCHANGER (1503A) BYPASS VALVE MO 1501-11A
NOTE 3
LPCI TESTABLE CHECK VALVE 1501-25A
NOTE 3
REF 1
VALVE CLOSES WHEN REACTOR PRESSURE EXCEEDS VALVE INLET PRESSURE IRRESPECTIVE OF CONTROL SWITCH POSITION. VALVE WILL OPEN WHEN VALVE INLET PRESSURE EXCEEDS REACTOR PRESSURE, IRRESPECTIVE OF CONTROL SWITCH POSITION
L.P.C.I. CROSS HEADER SHUT OFF VALVE MO 1501-32A
(TYPICAL FOR VALVE MO 1501-32B)
CONTAINMENT COOLING SERVICE WATER PUMPS 1501-44A AND 1501-44C (TYP. FOR -44B & -44D)
(NOTE: ADDITIONAL CONTROL FUNCTIONS TO BE SPECIFIED BY A.E.)
TYPICAL ALL MO VALVES AND MANUAL VALVES WITH POSITION SWITCHES
CONTAINMENT SPRAY VALVES
(NOTE 3)
CONTAINMENT SPRAY VALVE MO 1501-27A (AC OPERATED) SHOWN
CONTAINMENT COOLANT HEAT EXCHANGER DISCHARGE VALVE MO-1501-3A
(TYP. VALVE 1501-3B)
NOTE 3
Reference Document G.E. DWG. 728E948
DRESDEN STATION
UNITS 2 & 3
LOW PRESSURE COOLANT INJECTION/
CONTAINMENT COOLING SYSTEM
FUNCTIONAL BLOCK DIAGRAM
FIGURE 7.3-2B



DRESDEN STATION UNITS 2 & 3

VALVE MO 1501–21A (THROTTLING)
LPCI OUTBOARD VALVE
FUNCTIONAL BLOCK DIAGRAM

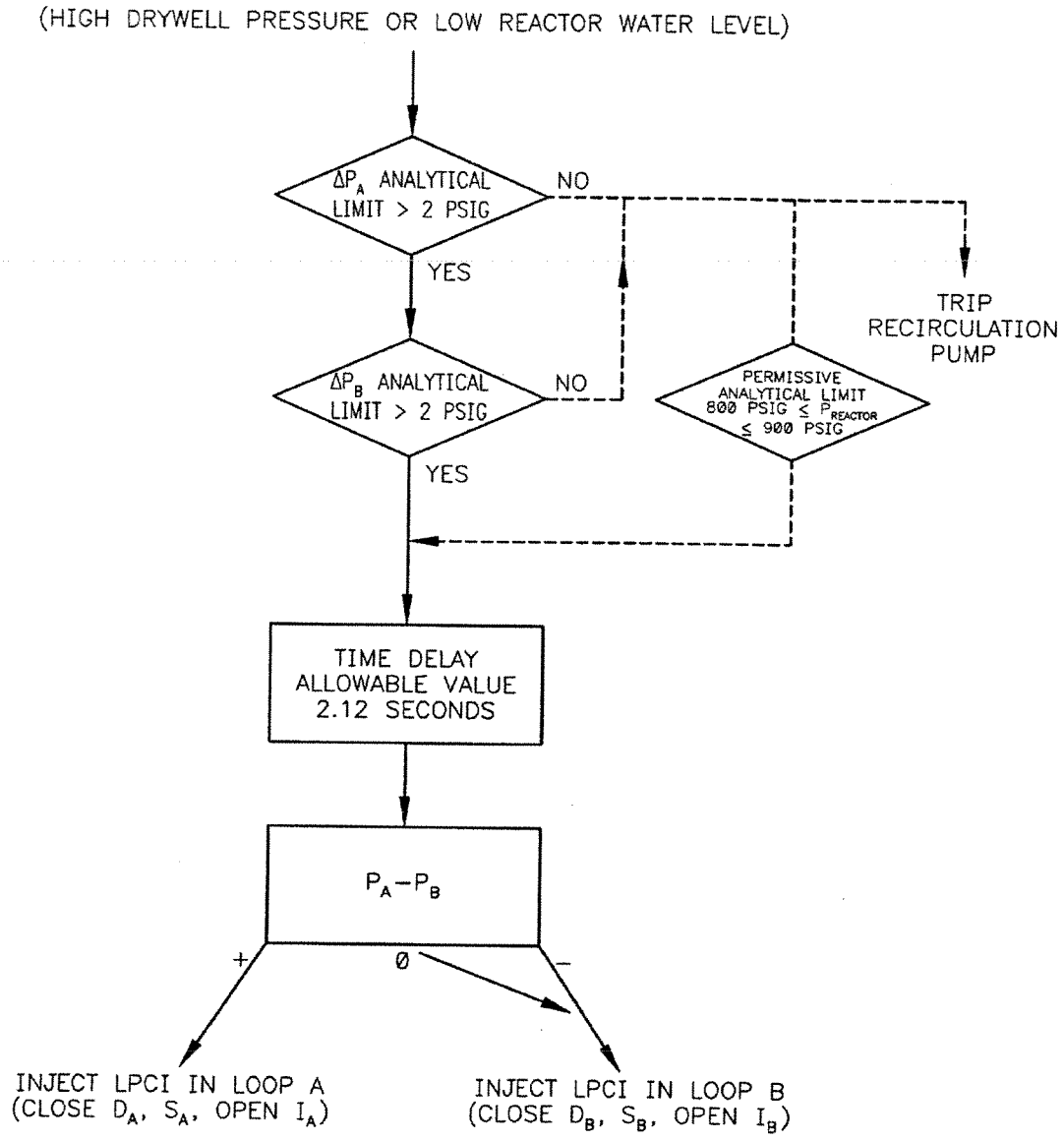
FIGURE 7.3–3



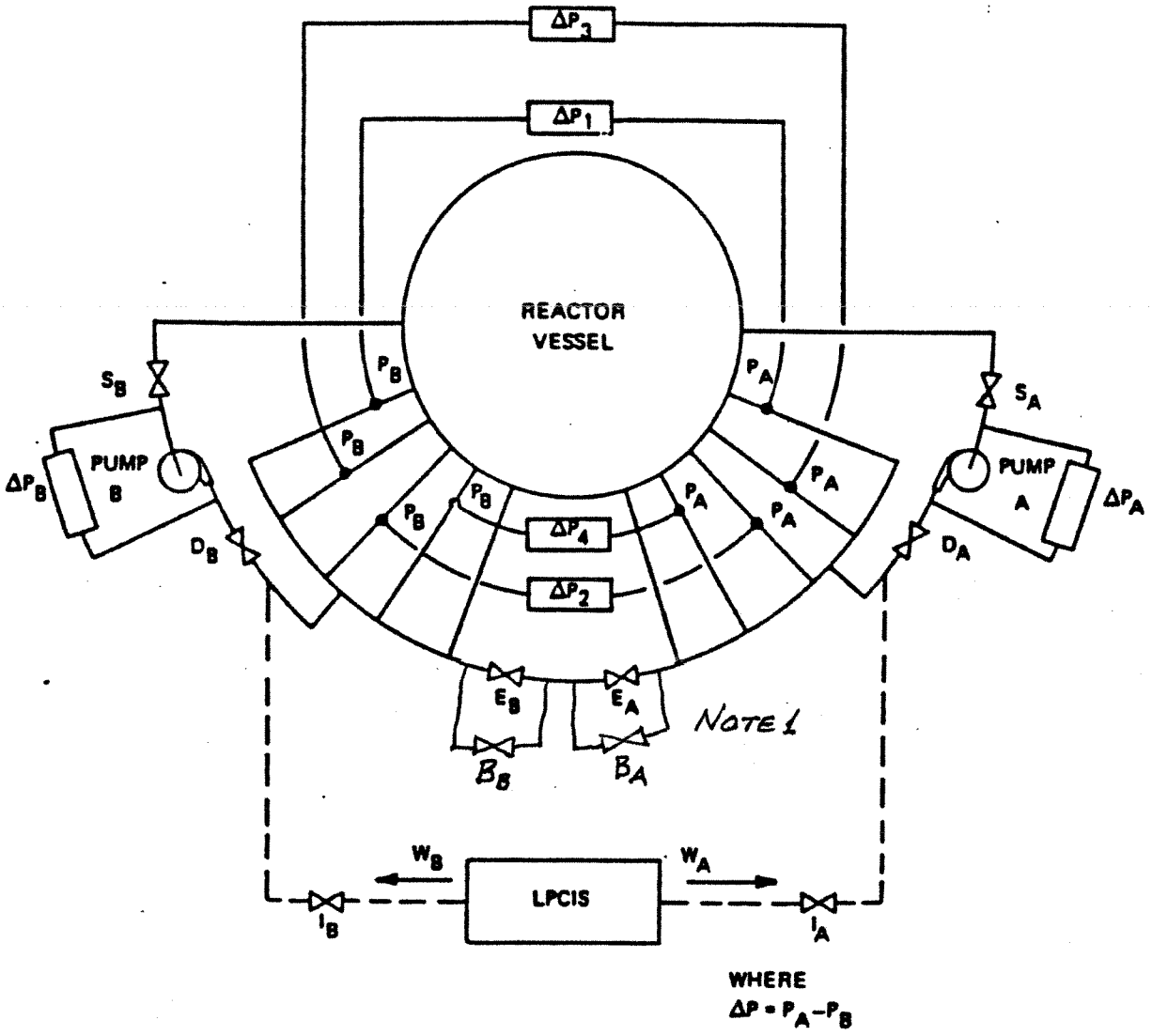
DRESDEN STATION
UNITS 2 & 3

LPCI PUMP MIN. FLOW VALVE MO-1501-13A
FUNCTIONAL BLOCK DIAGRAM

FIGURE 7.3-4

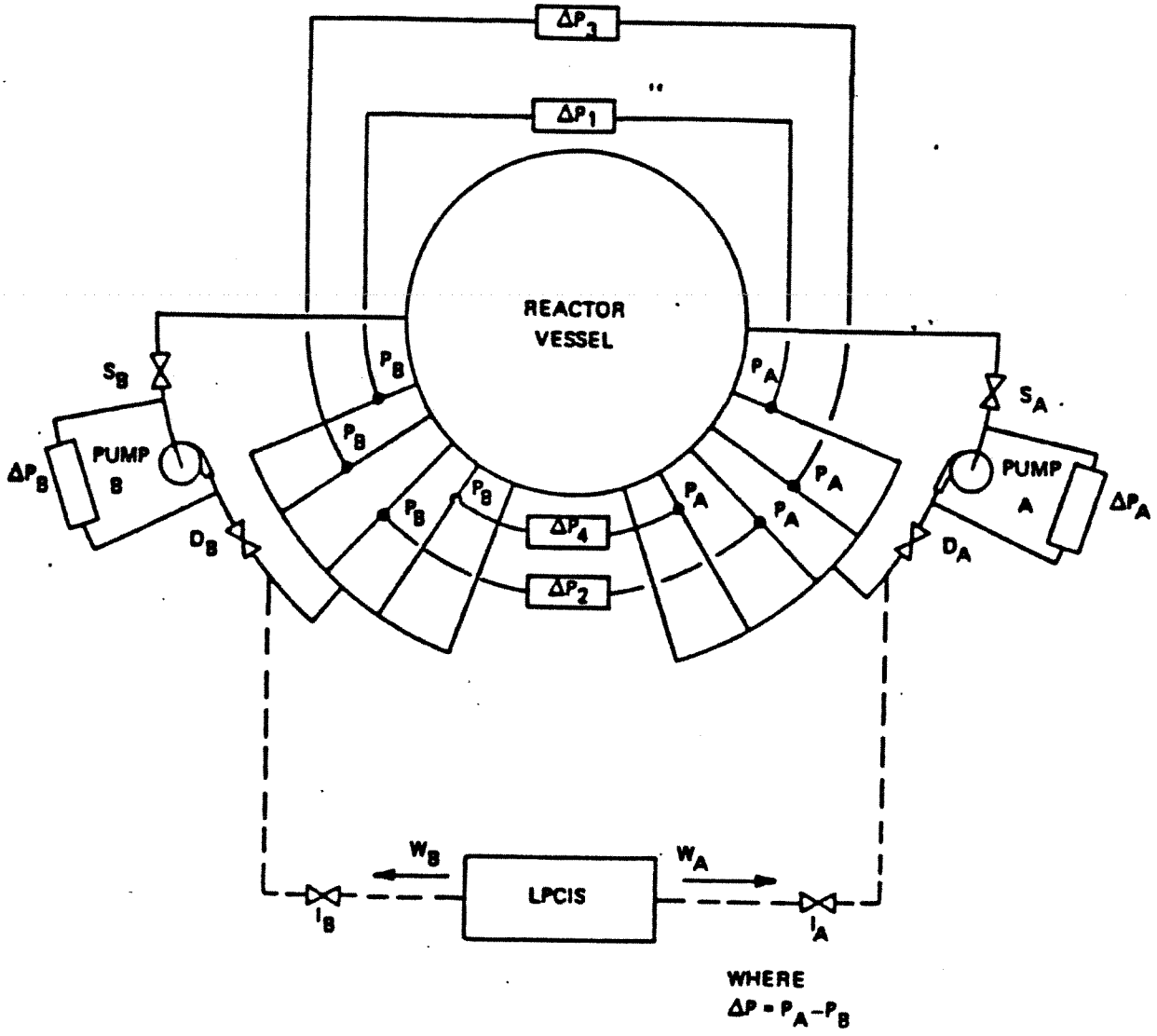


UFSAR REVISION 6, JUNE 2005
DRESDEN STATION UNITS 2 & 3
LPCI BREAK DETECTION SYSTEM LOGIC ARRANGEMENT
FIGURE 7.3-5



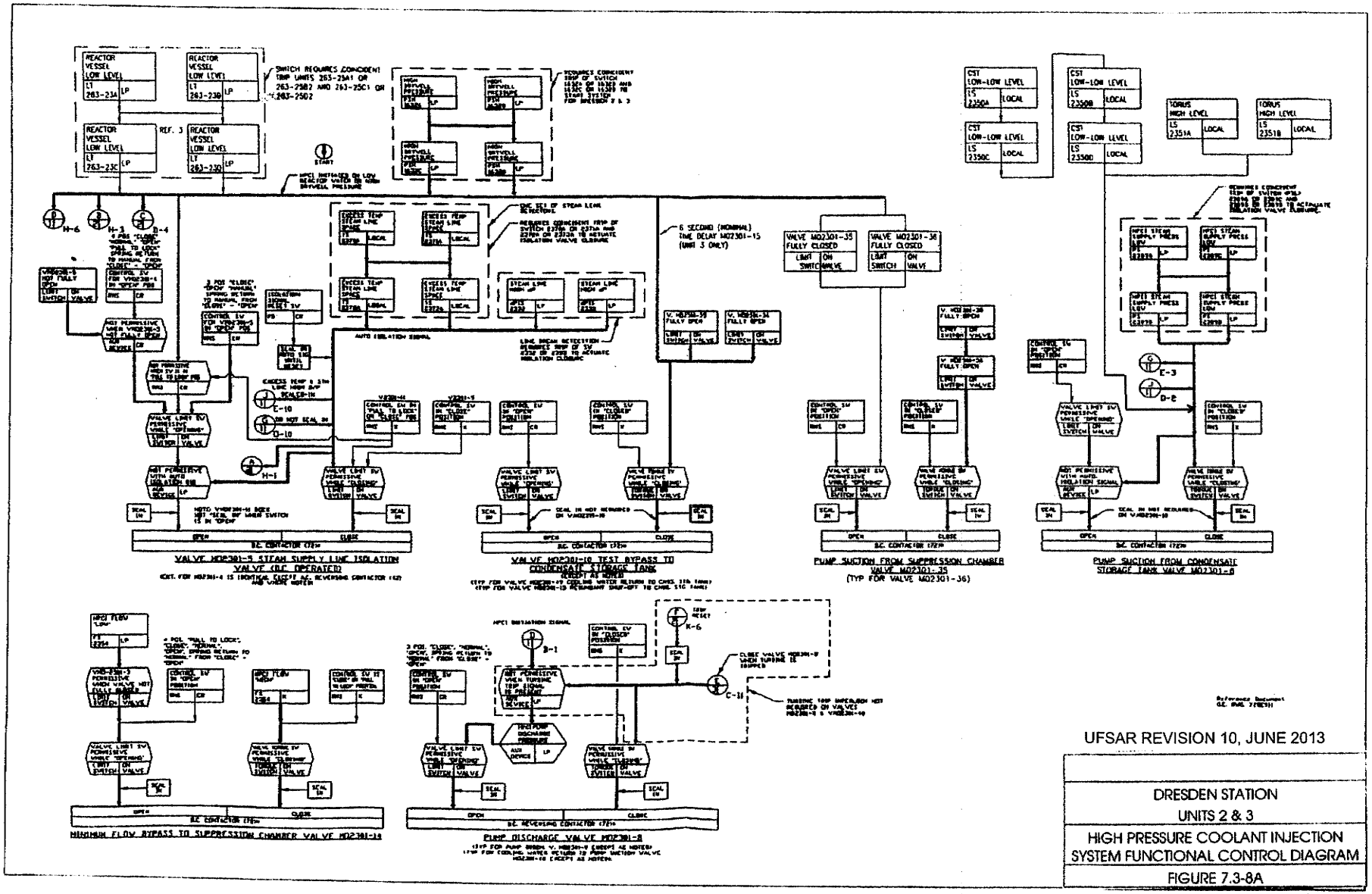
Note 1 Electrical connections to the equalizer valves (E_A, E_B) and equalizer bypass valves (B_A, B_B) for power, control, position indication, and LPCI interlocks are disconnected. Valves are manually positioned as shown. The B_A equalizer bypass valve is manually positioned open to prevent hydrostatic pressurization of the section of equalizer line between the isolation valves due to heatup (see Section 5.4.1.2.2 for additional information).

UFSAR REVISION 6, JUNE 2005
DRESDEN STATION UNITS 2 & 3
UNIT 2 LPCI LOGIC CONTROL SYSTEM ARRANGEMENT
FIGURE 7.3-6



NOTE: The equalizer line on Unit 3 was removed during the 1985-86 Recirculation Pipe Replacement Outage.

DRESDEN STATION UNITS 2 & 3
UNIT 3 LPCI LOGIC CONTROL SYTEM ARRANGEMENT
FIGURE 7.3-7

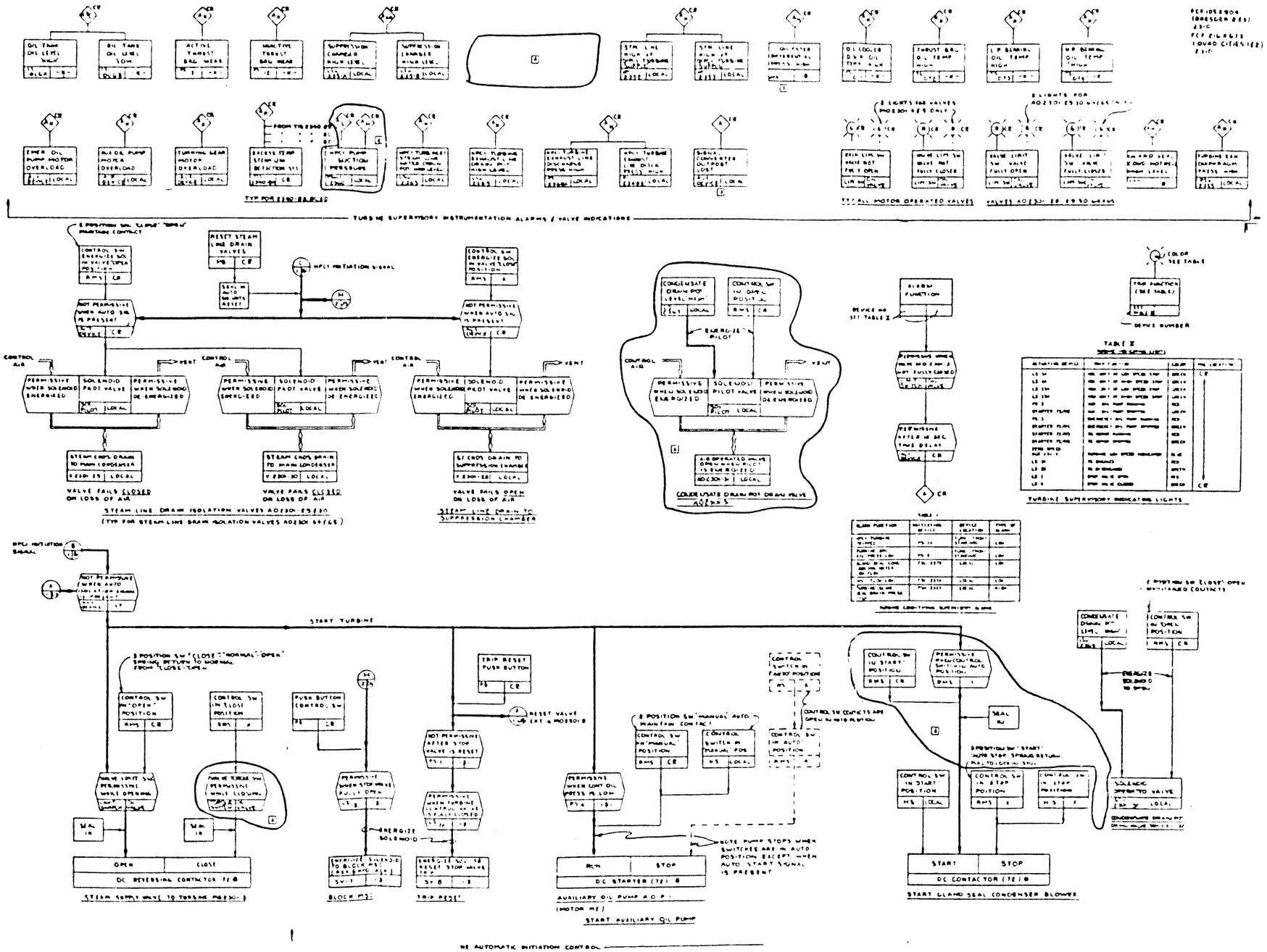


UFSAR REVISION 10, JUNE 2013

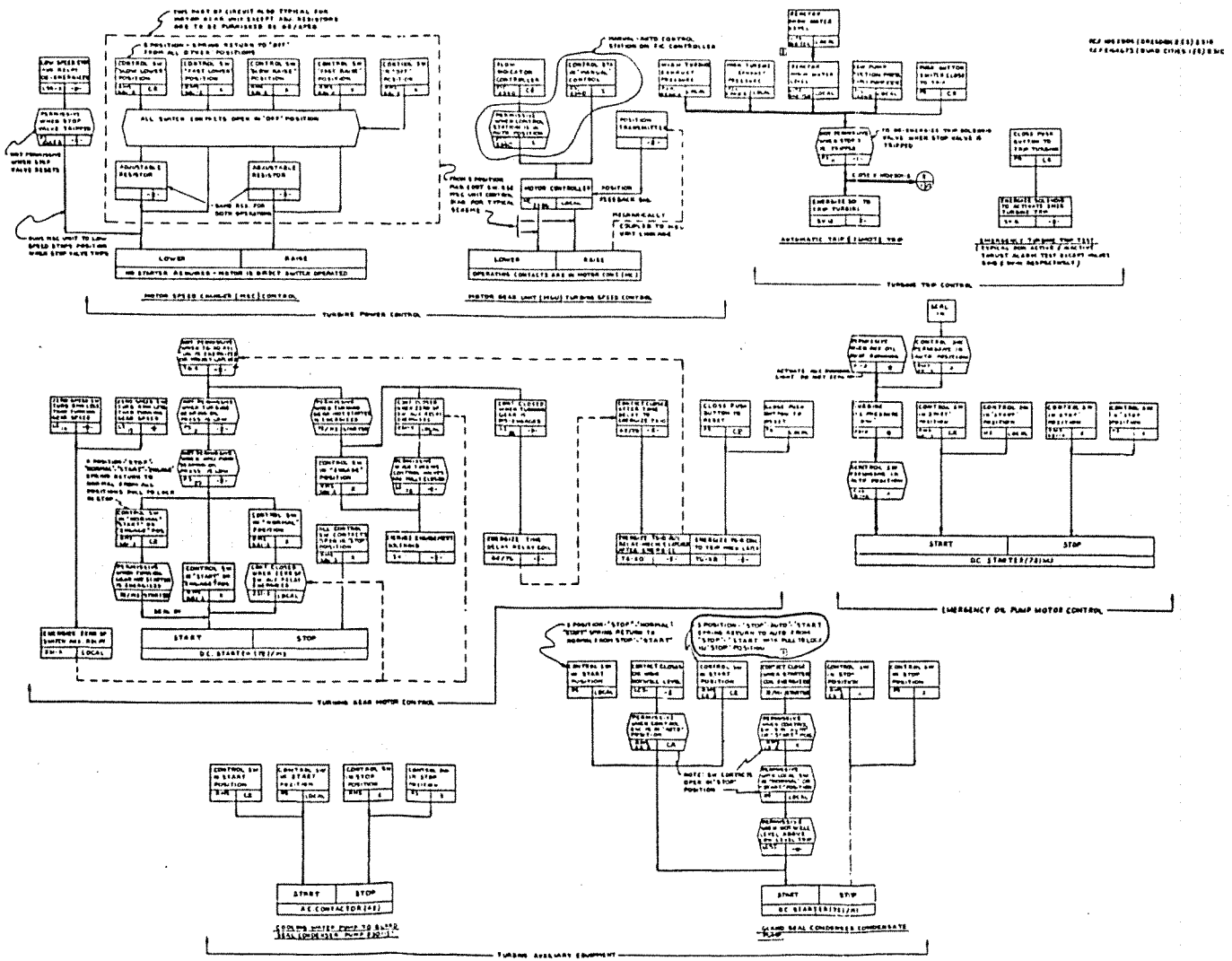
DRESDEN STATION
UNITS 2 & 3

HIGH PRESSURE COOLANT INJECTION SYSTEM FUNCTIONAL CONTROL DIAGRAM

FIGURE 7.3-8A



DRESDEN STATION UNITS 2 & 3
HIGH PRESSURE COOLANT INJECTION SYSTEM - FUNCTIONAL BLOCK DIAGRAM
FIGURE 7.3-8B



DRESDEN STATION UNITS 2 & 3
HIGH PRESSURE COOLANT INJECTION SYSTEM - FUNCTIONAL BLOCK DIAGRAM
FIGURE 7.3-8C

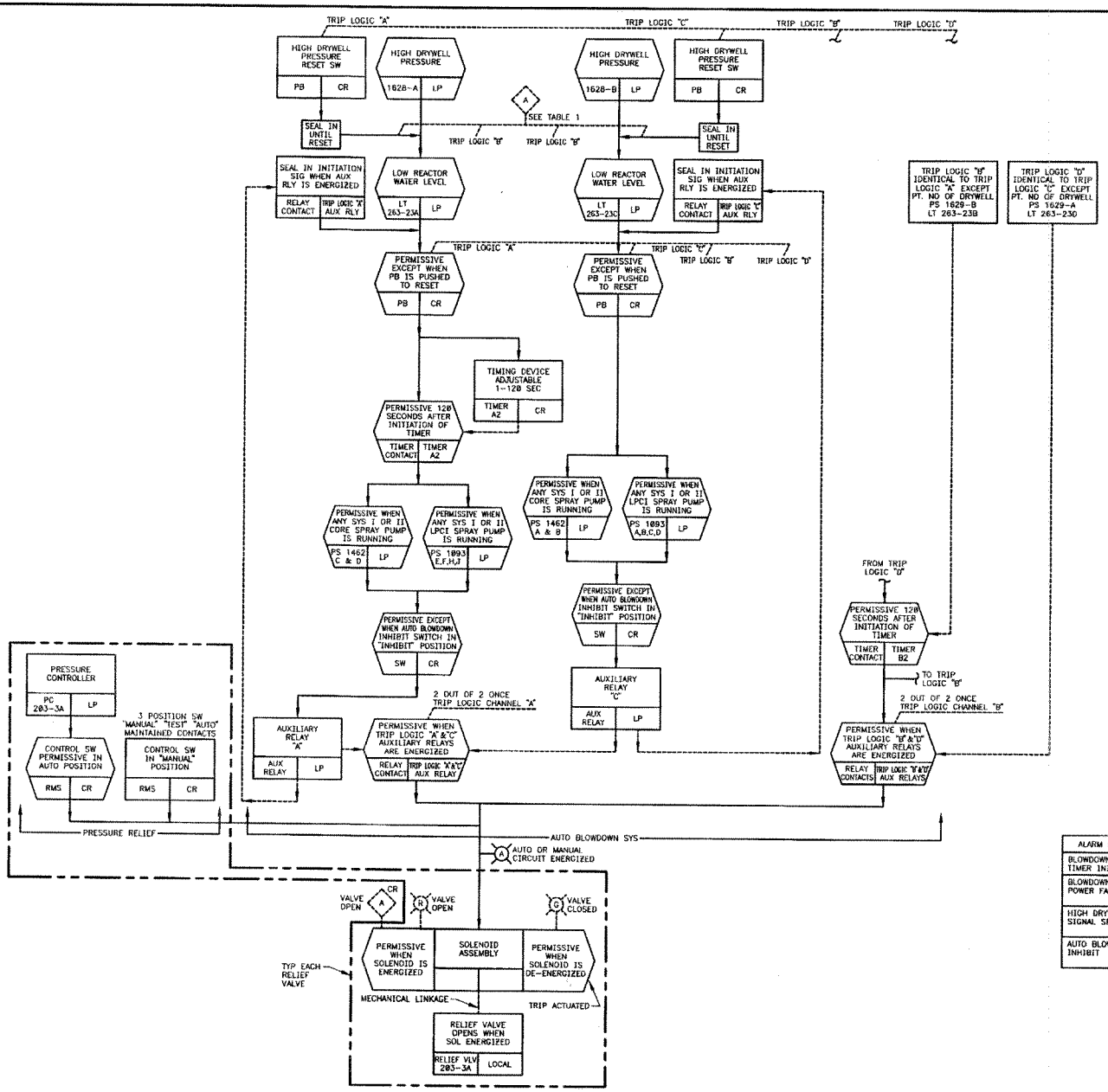


TABLE 1

ALARM FUNCTION	INITIATING DEVICE	DEVICE LOCATION
BLOWDOWN TIMER INITIATED	TIMING DEVICE (A2) OR (B2) TO ONE COMMON ANNUNCIATOR	CR
BLOWDOWN CIRCUIT POWER FAILURE	AUX POWER FAILURE RELAY FOR EACH LOGIC CHANNEL TO ONE COMMON ANNUNCIATOR	CR
HIGH DRYWELL PRESS SIGNAL SEALED-IN	EACH DRYWELL PRESSURE SWITCH AUX RELAY TO ONE COMMON ANNUNCIATOR	CR
AUTO BLOWDOWN INHIBIT	SWITCH CONTACT IN INHIBIT POSITION TO ONE ANNUNCIATOR	CR

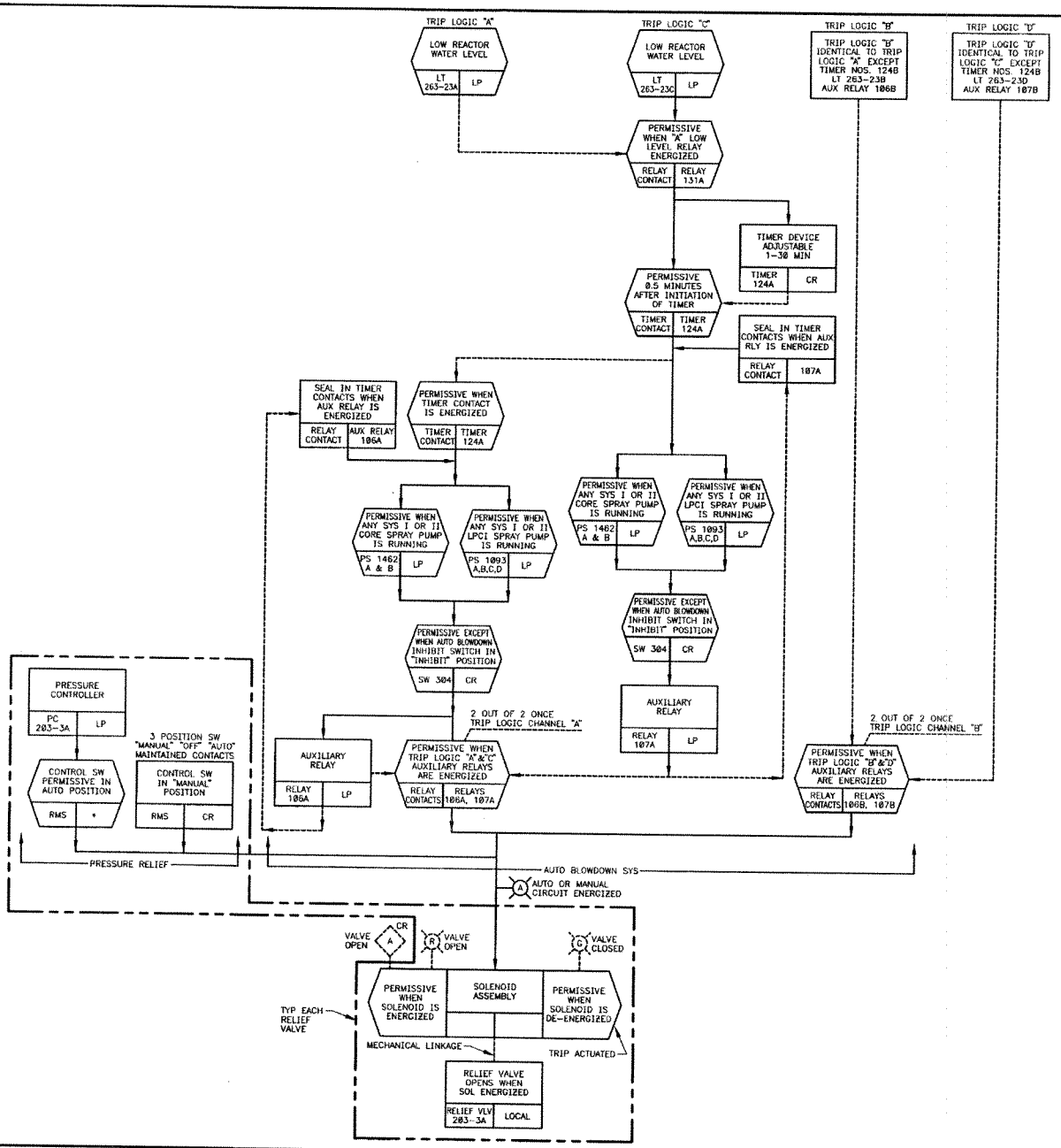
BLOWDOWN SYSTEM SPECIAL ALARMS

DRESDEN STATION UNITS 2 & 3

AUTOMATIC DEPRESSURIZATION SYSTEM FUNCTIONAL BLOCK DIAGRAM

FIGURE 7.3-9

REVISION 5, JANUARY 2003

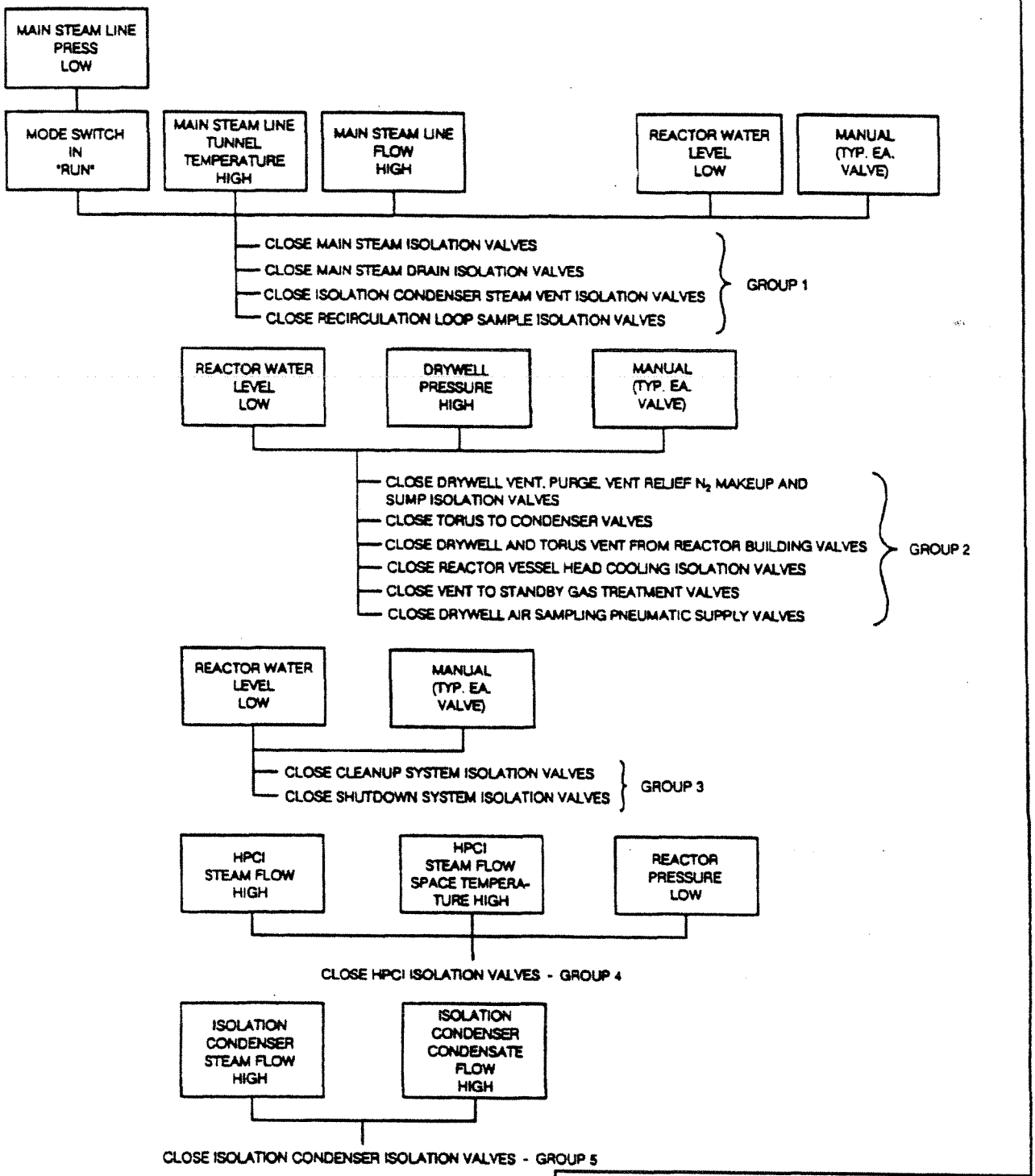


DRESDEN STATION UNITS 2 & 3

AUTOMATIC DEPRESSURIZATION SYSTEM
AUTO BLOWDOWN WITHOUT HIGH DRYWELL PRESSURE
FUNCTIONAL BLOCK DIAGRAM

FIGURE 7.3-10

REVISION 5, JANUARY 2003

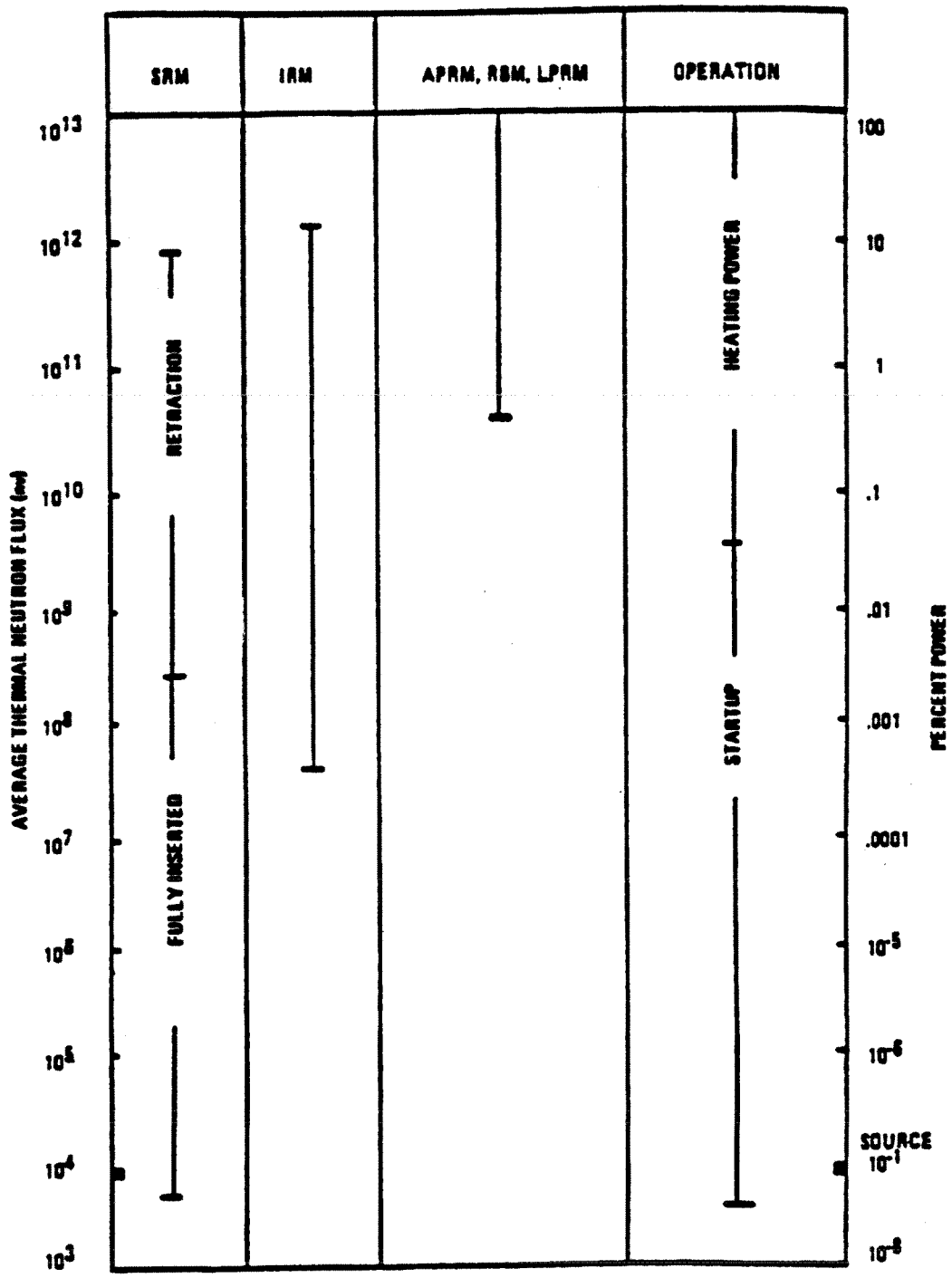


UFSAR REVISION 4, JUNE 2001

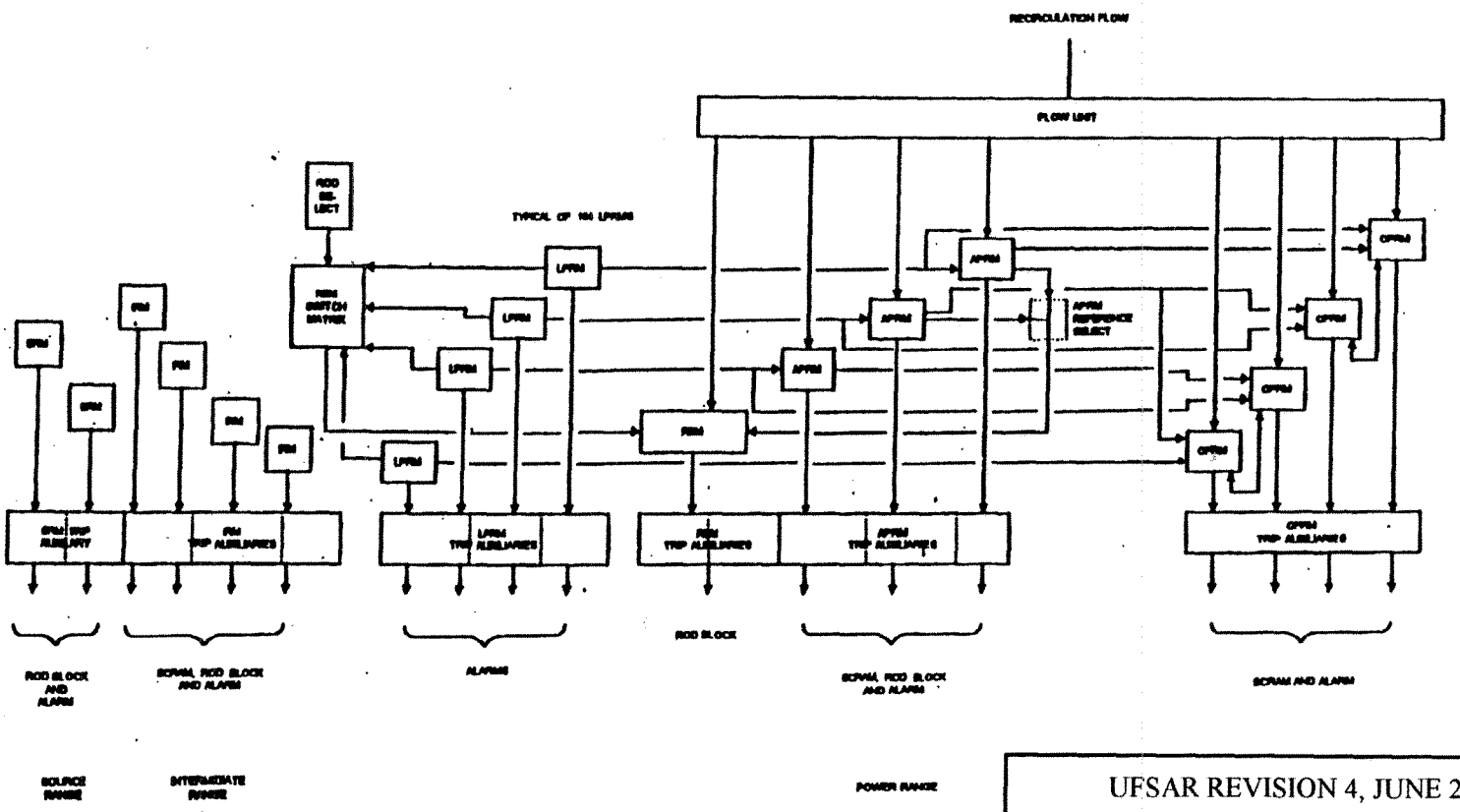
DRESDEN STATION
UNITS 2 & 3

BLOCK DIAGRAM - PRIMARY CONTAINMENT ISOLATION

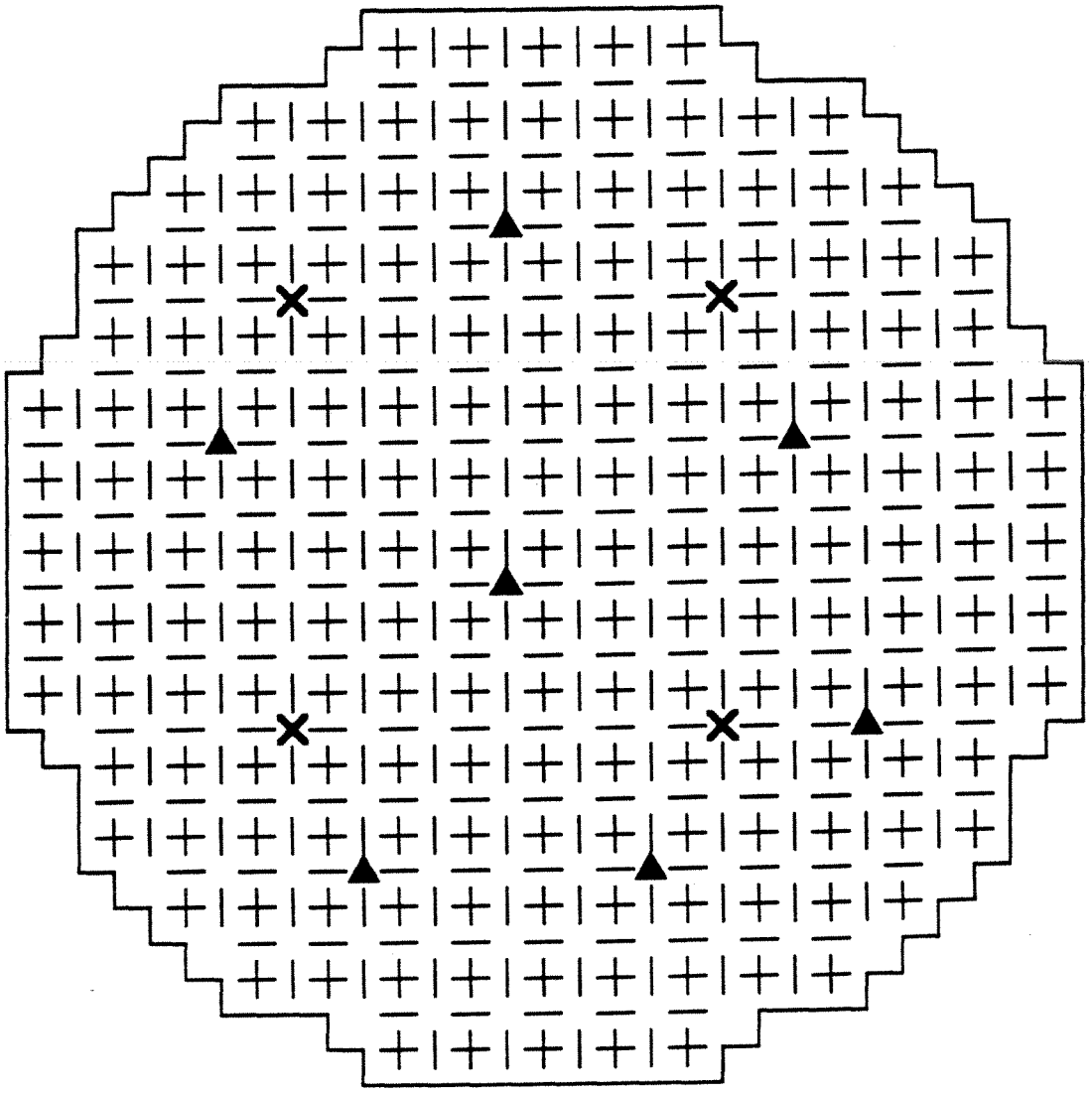
FIGURE 7.3-11



DRESDEN STATION UNITS 2 & 3
TYPICAL NUCLEAR INSTRUMENTATION SYSTEM RANGES AND OVERLAPS
FIGURE 7.6-1 REVISION 5, JANUARY 2003



UFSAR REVISION 4, JUNE 2001
DRESDEN STATION UNITS 2 & 3
NUCLEAR INSTRUMENTATION SYSTEM BLOCK DIAGRAM
FIGURE 7.6-2



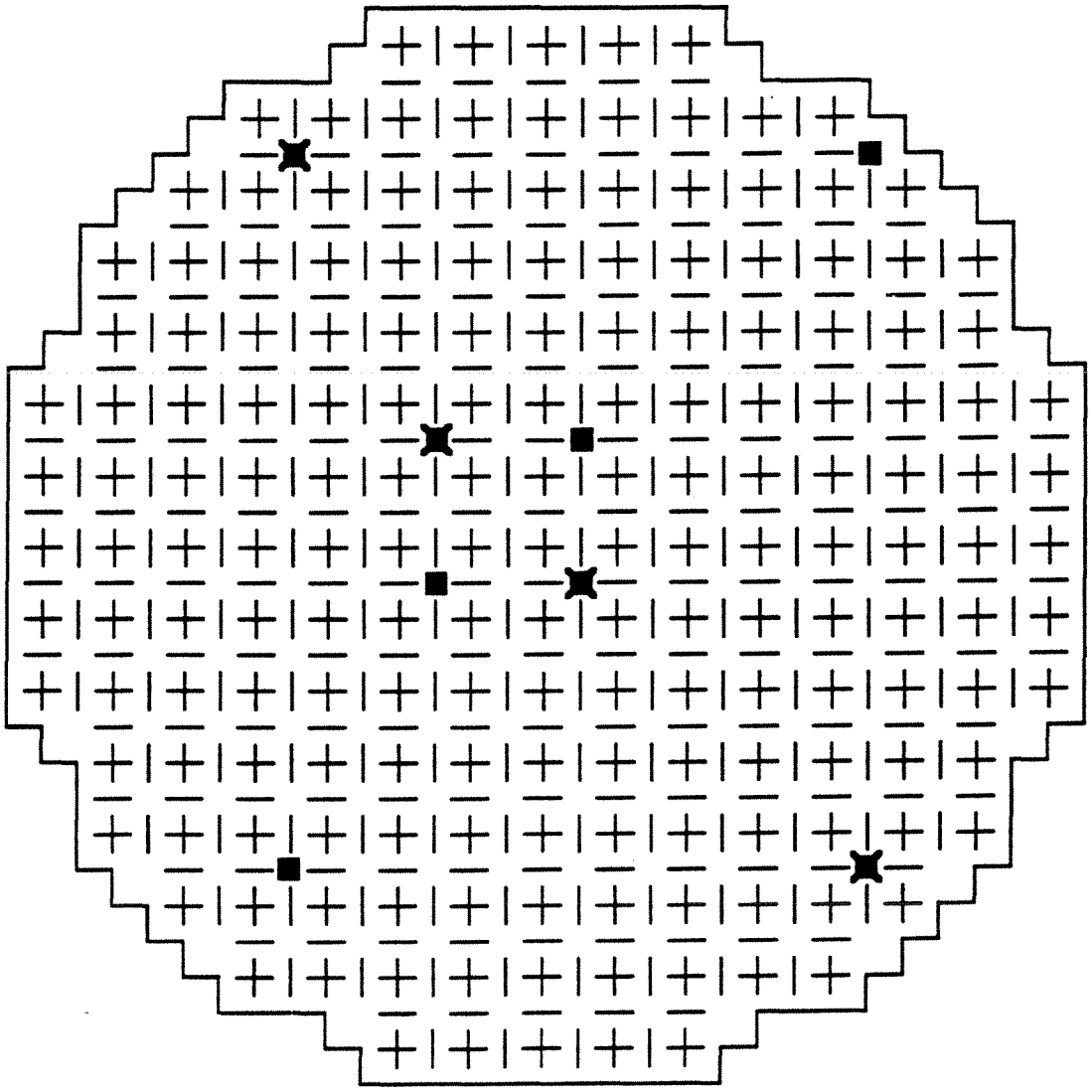
X – SOURCE RANGE MONITOR DETECTORS

▲ – NEUTRON -EMITTING SOURCES

DRESDEN STATION
UNITS 2 & 3

SRM DETECTOR AND SOURCE LOCATIONS

FIGURE 7.6-3



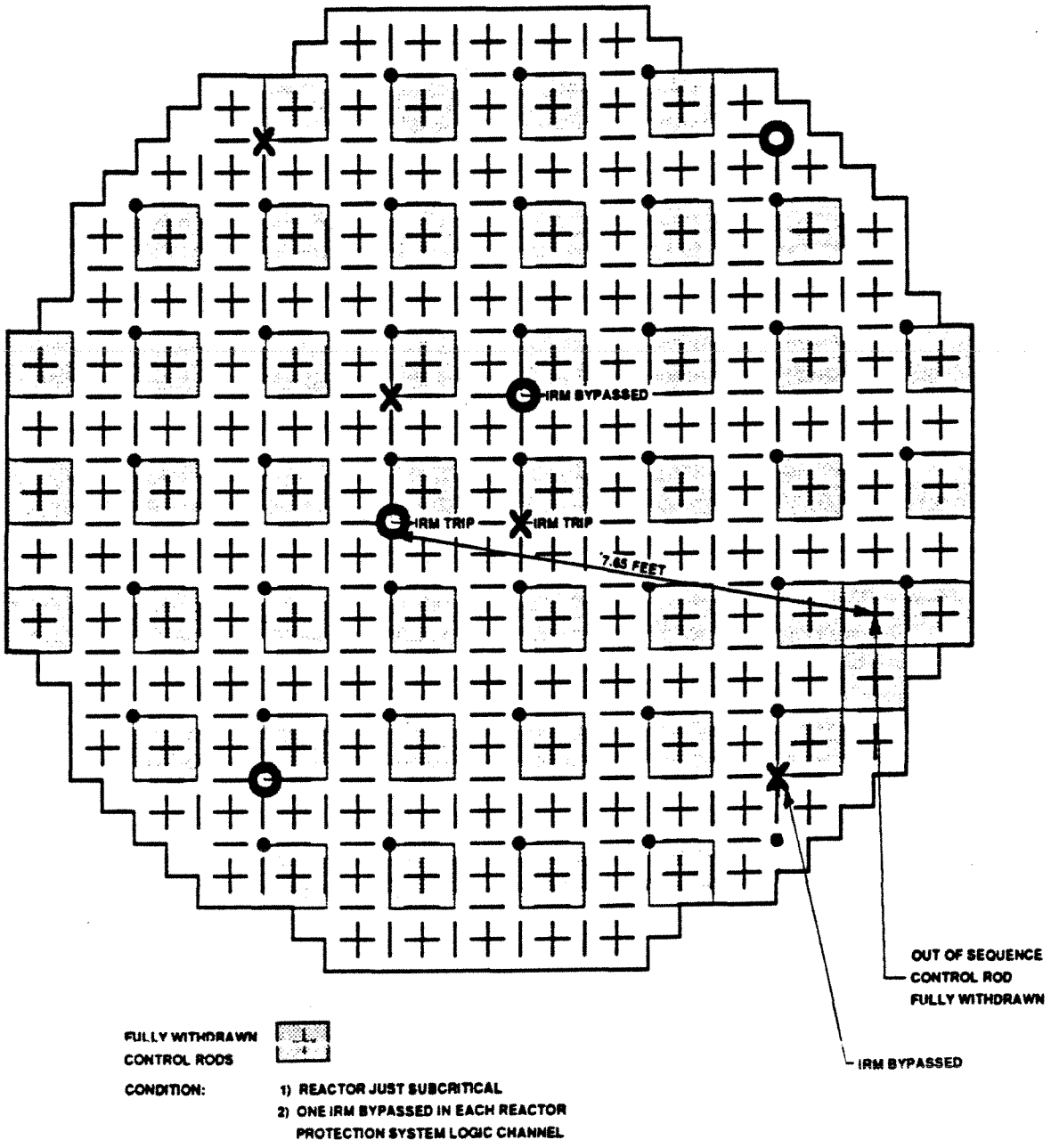
INTERMEDIATE RANGE MONITORING CHANNELS FOR REACTOR PROTECTION SYSTEM LOGIC CHANNEL A

INTERMEDIATE RANGE MONITORING CHANNELS FOR REACTOR PROTECTION SYSTEM LOGIC CHANNEL B

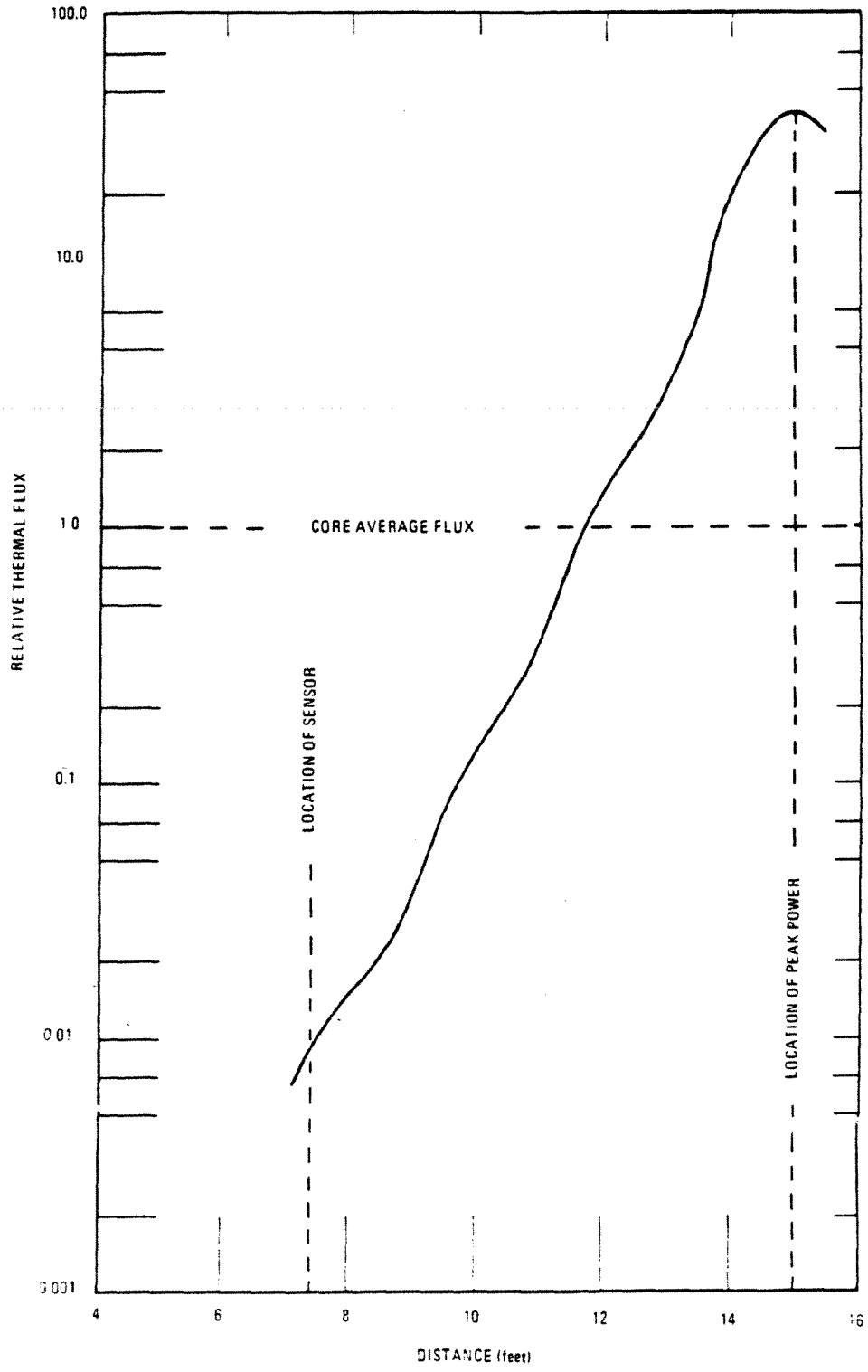
DRESDEN STATION
UNITS 2 & 3

IRM DETECTOR LOCATIONS

FIGURE 7.6-4



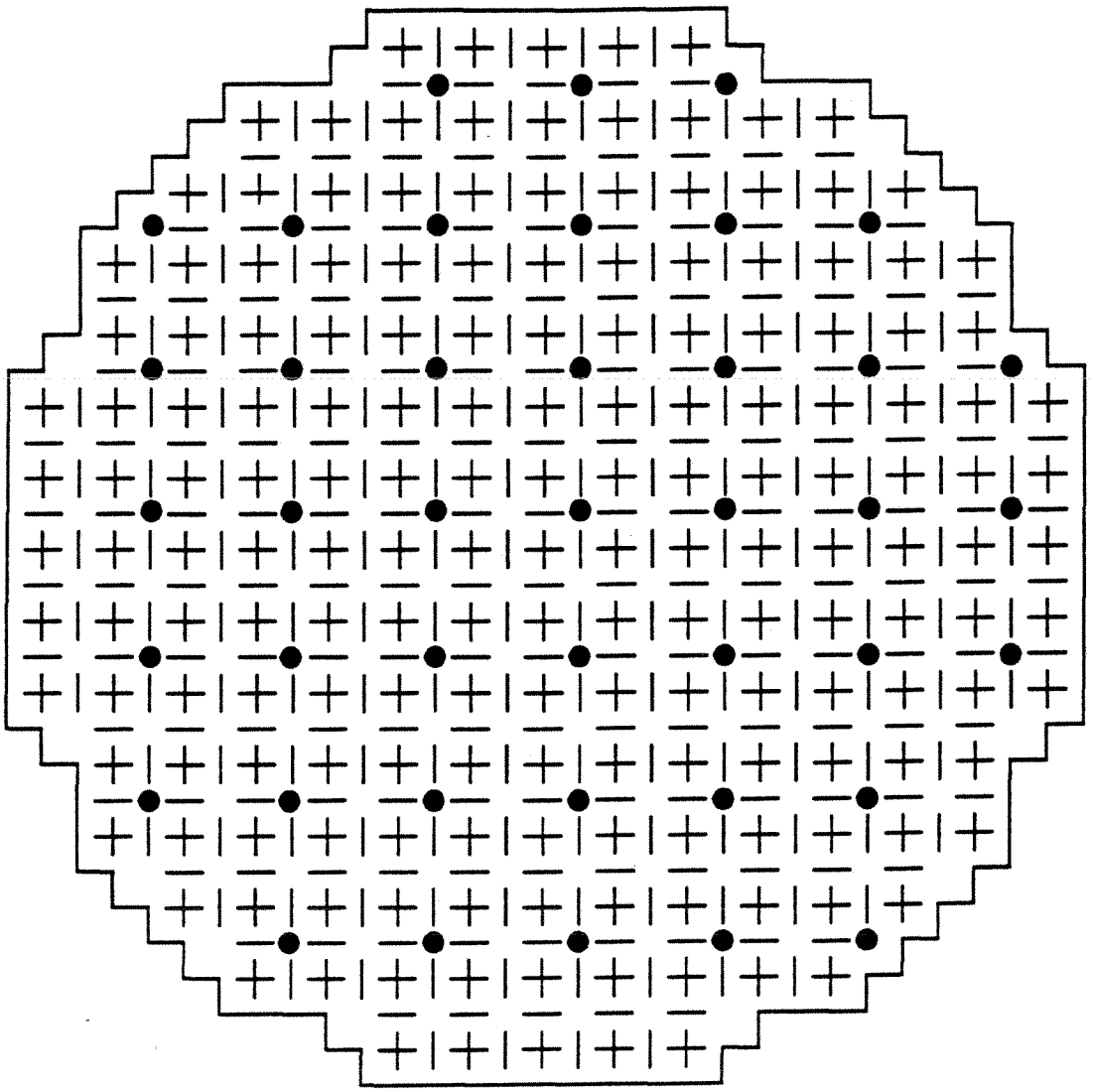
DRESDEN STATION UNITS 2 & 3
IRM RESPONSE TO ROD WITHDRAWAL ERROR
FIGURE 7.6-5



DRESDEN STATION
UNITS 2 & 3

IRM POWER DISTRIBUTION DURING
ROD WITHDRAWAL ERROR

FIGURE 7.6-6

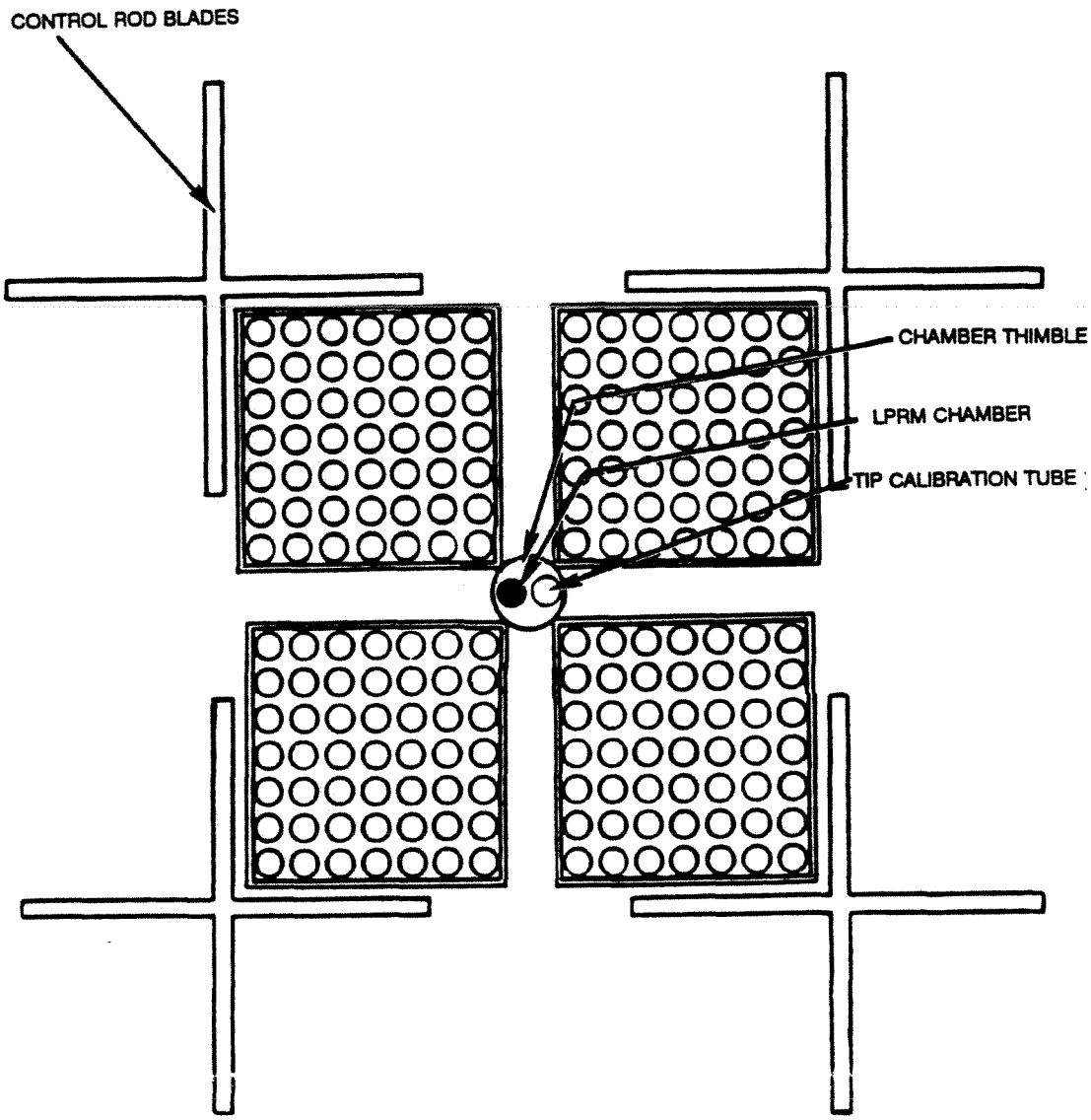


● INDICATES THE LOCATION OF A DETECTOR STRING. EACH STRING CONTAINS FOUR DETECTORS SPACED VERTICALLY THREE FEET APART.

DRESDEN STATION
UNITS 2 & 3

LPRM DETECTOR LOCATIONS

FIGURE 7.6-7



DRESDEN STATION
UNITS 2 & 3

LPRM DETECTOR LOCATIONS - DETAIL

FIGURE 7.6-8

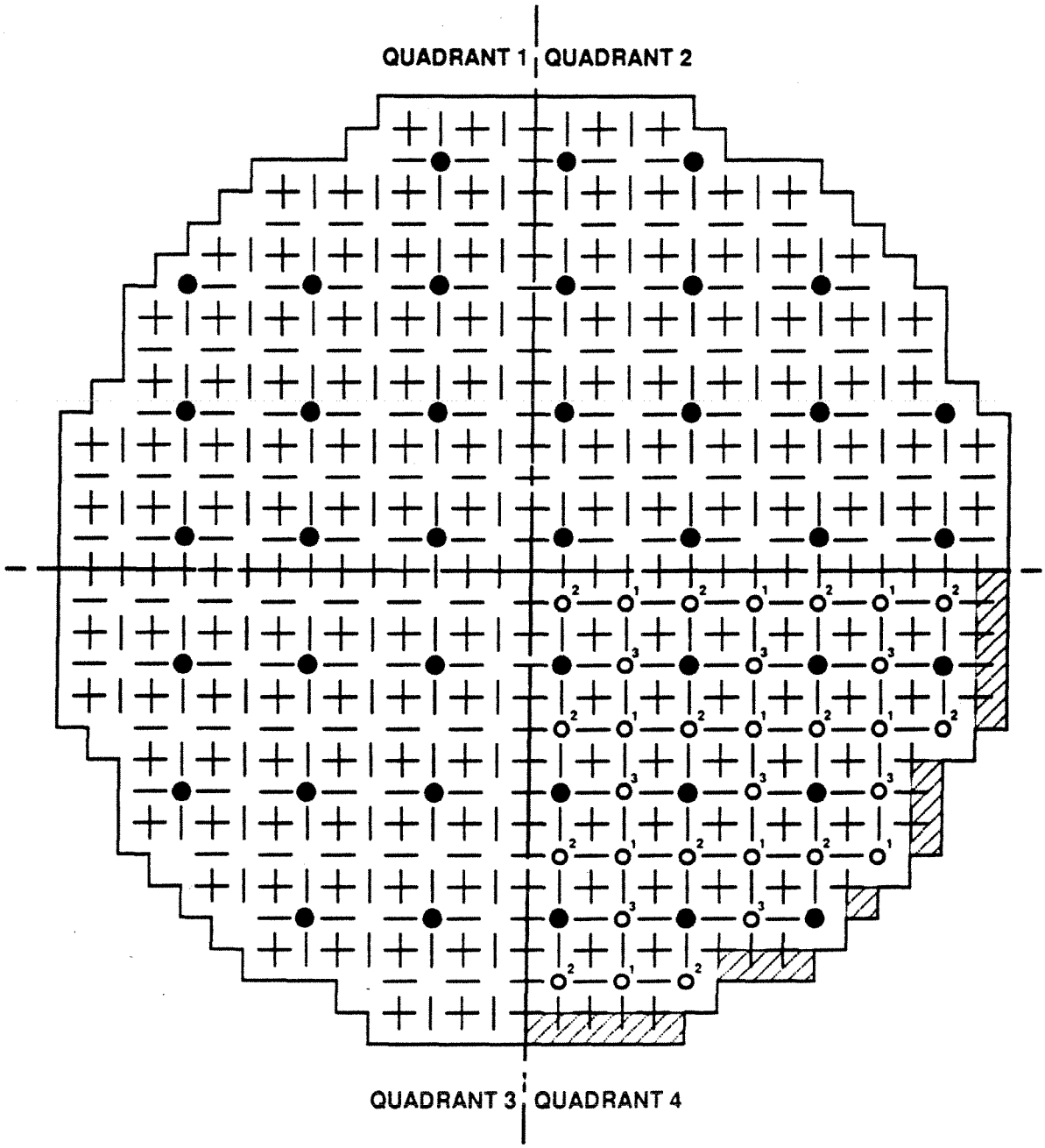
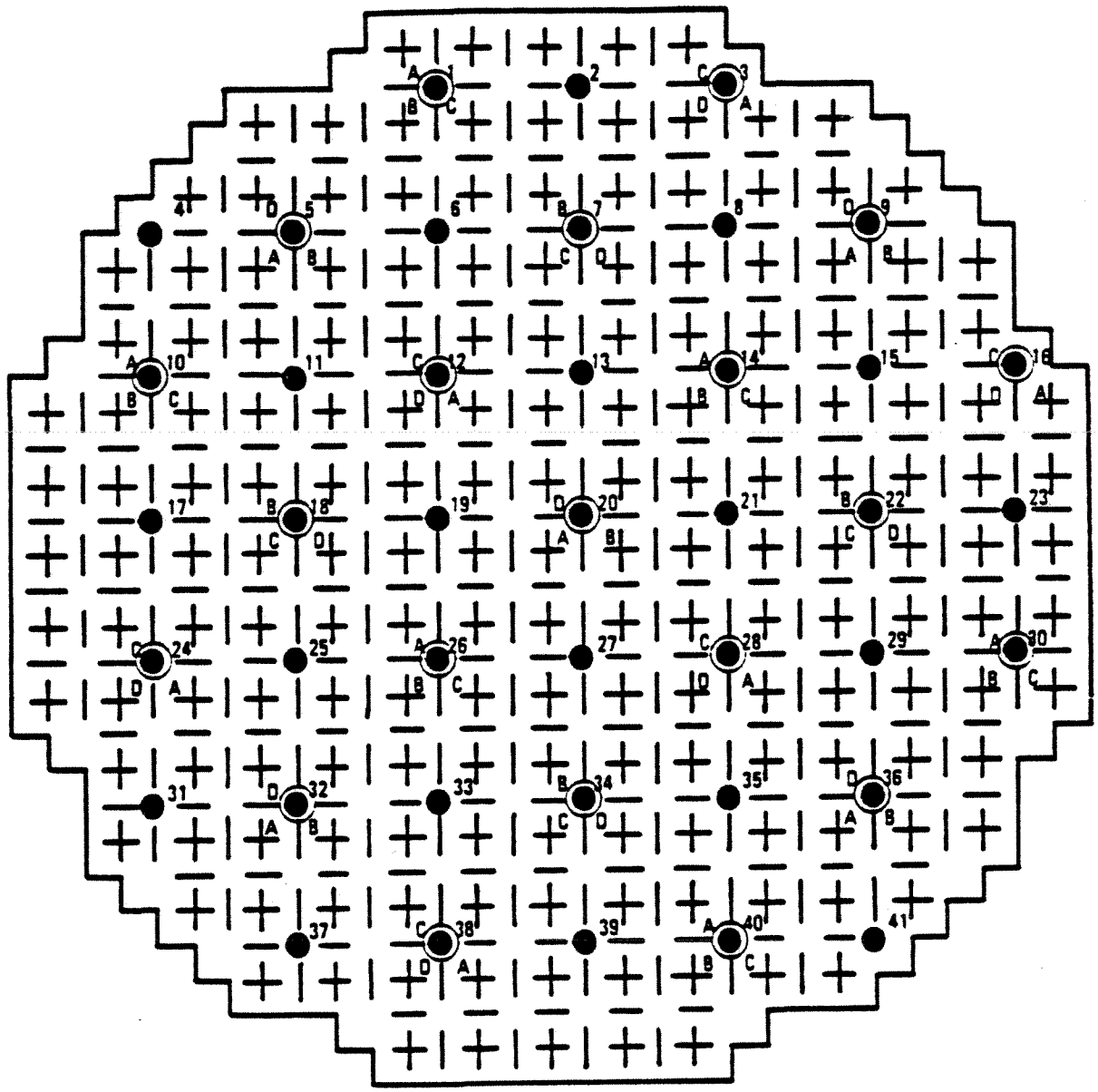


ILLUSTRATION OF MONITORING COVERAGE ASSUMING QUADRANT SYMMETRIC OPERATION

O_2^1 EQUIVALENT DATA ROTATED FROM QUADRANT 1
O_3^2 EQUIVALENT DATA ROTATED FROM QUADRANT 2
O^3 EQUIVALENT DATA ROTATED FROM QUADRANT 3
UNMONITORED PERIPHERAL ASSEMBLIES

DRESDEN STATION UNITS 2 & 3
LPRM QUADRANT SYMMETRY
FIGURE 7.6-9

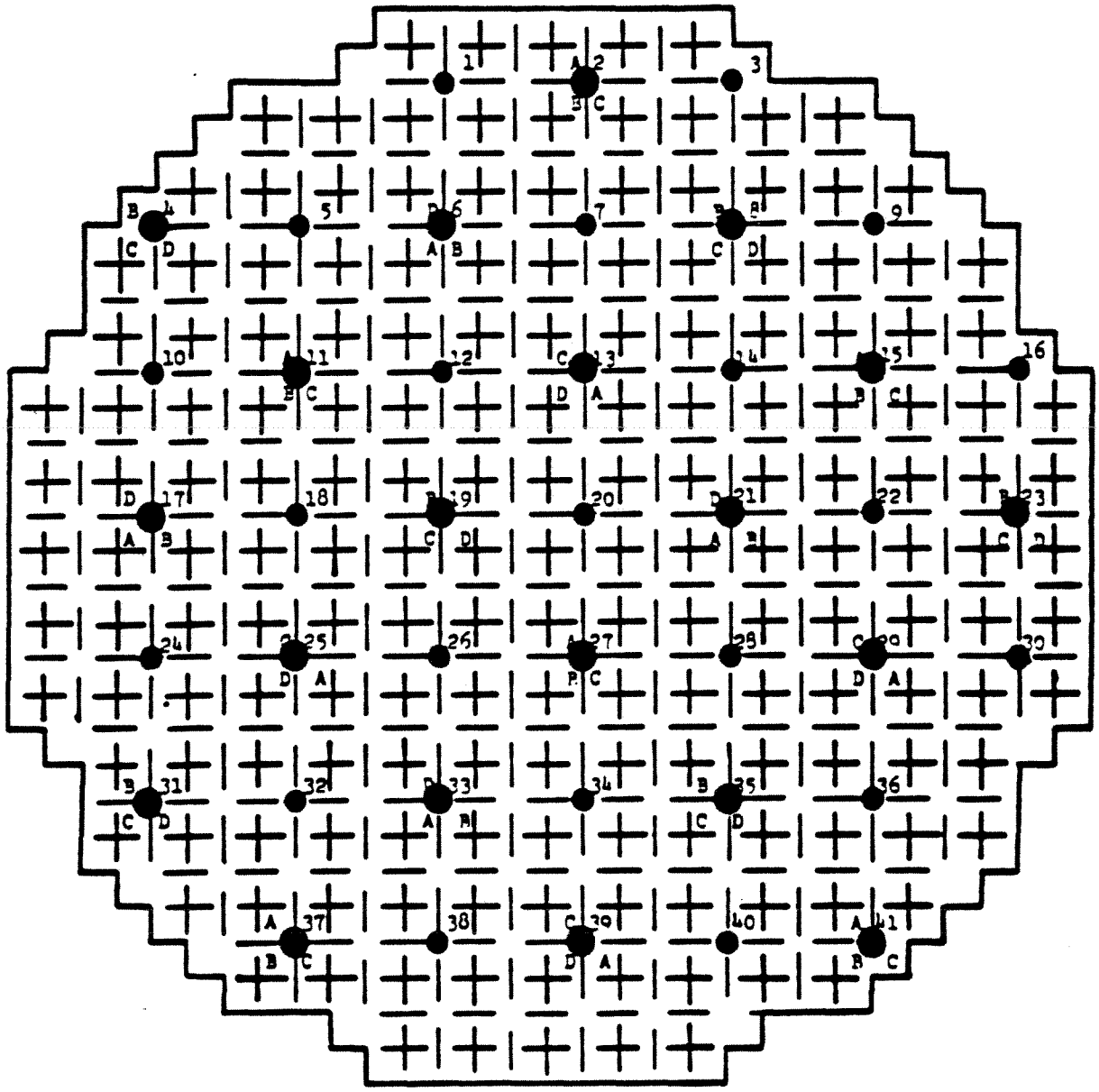


LPRM strings providing input to APRM Channels 1, 2, 3

A 1 B C

Upper right number = LPRM string identification
Upper left letter = LPRM chamber used as input for APRM Channel 1
Lower left letter = LPRM chamber used as input for APRM Channel 2
Lower right letter = LPRM chamber used as input for APRM Channel 3

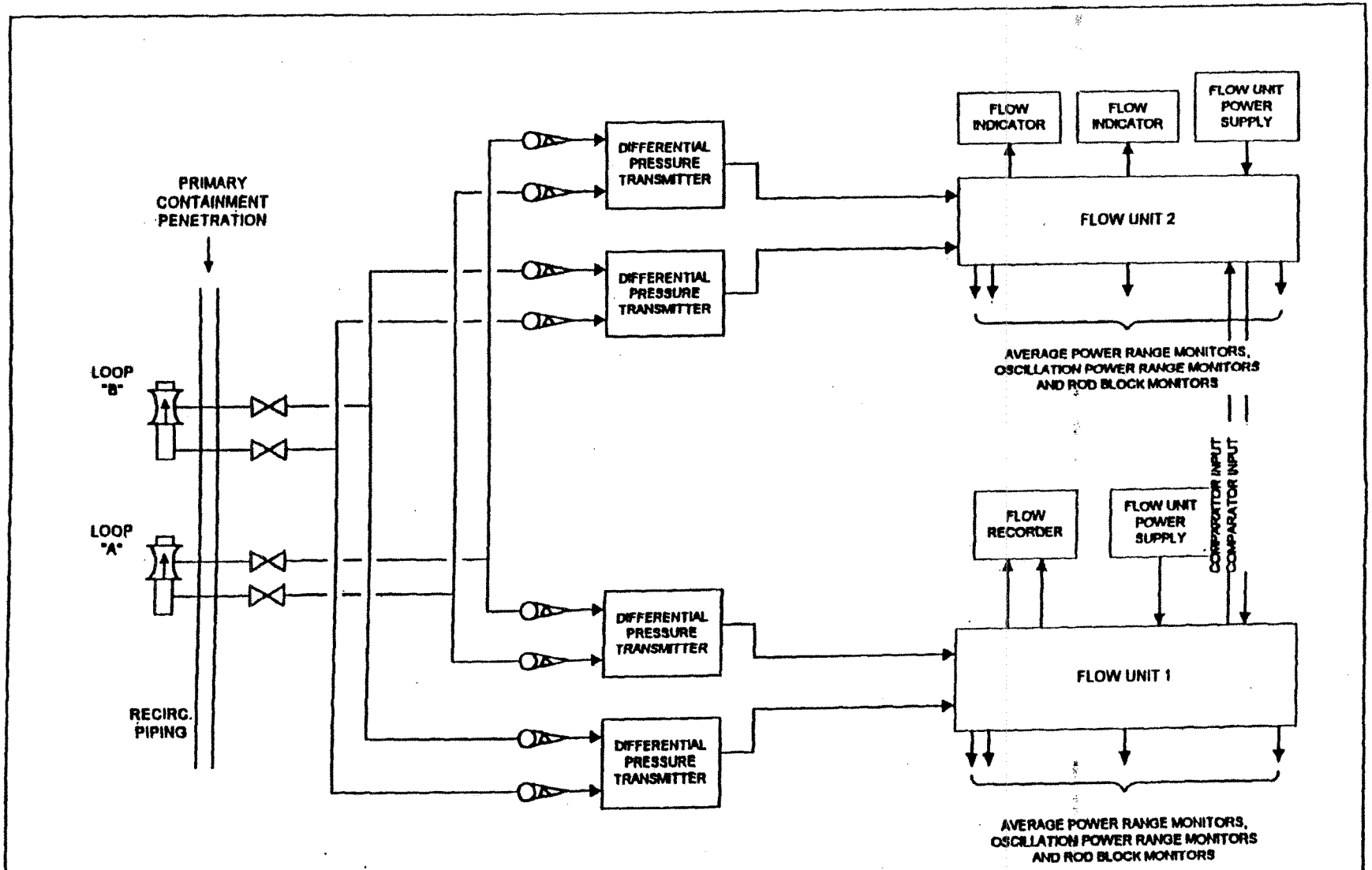
DRESDEN STATION UNITS 2 & 3
APRM LPRM ASSIGNMENTS, CHANNELS 1, 2, 3
FIGURE 7.6-10



LPRM strings providing input to APRM Channels 4, 5, 6

A 2 Upper right number = LPRM string identification
Upper left letter = LPRM chamber used as input for APRM Channel 4
Lower left letter = LPRM chamber used as input for APRM Channel 5
B C Lower right letter = LPRM chamber used as input for APRM Channel 6

DRESDEN STATION UNITS 2 & 3
APRM LPRM ASSIGNMENTS, CHANNELS 4, 5, 6
FIGURE 7.6-11

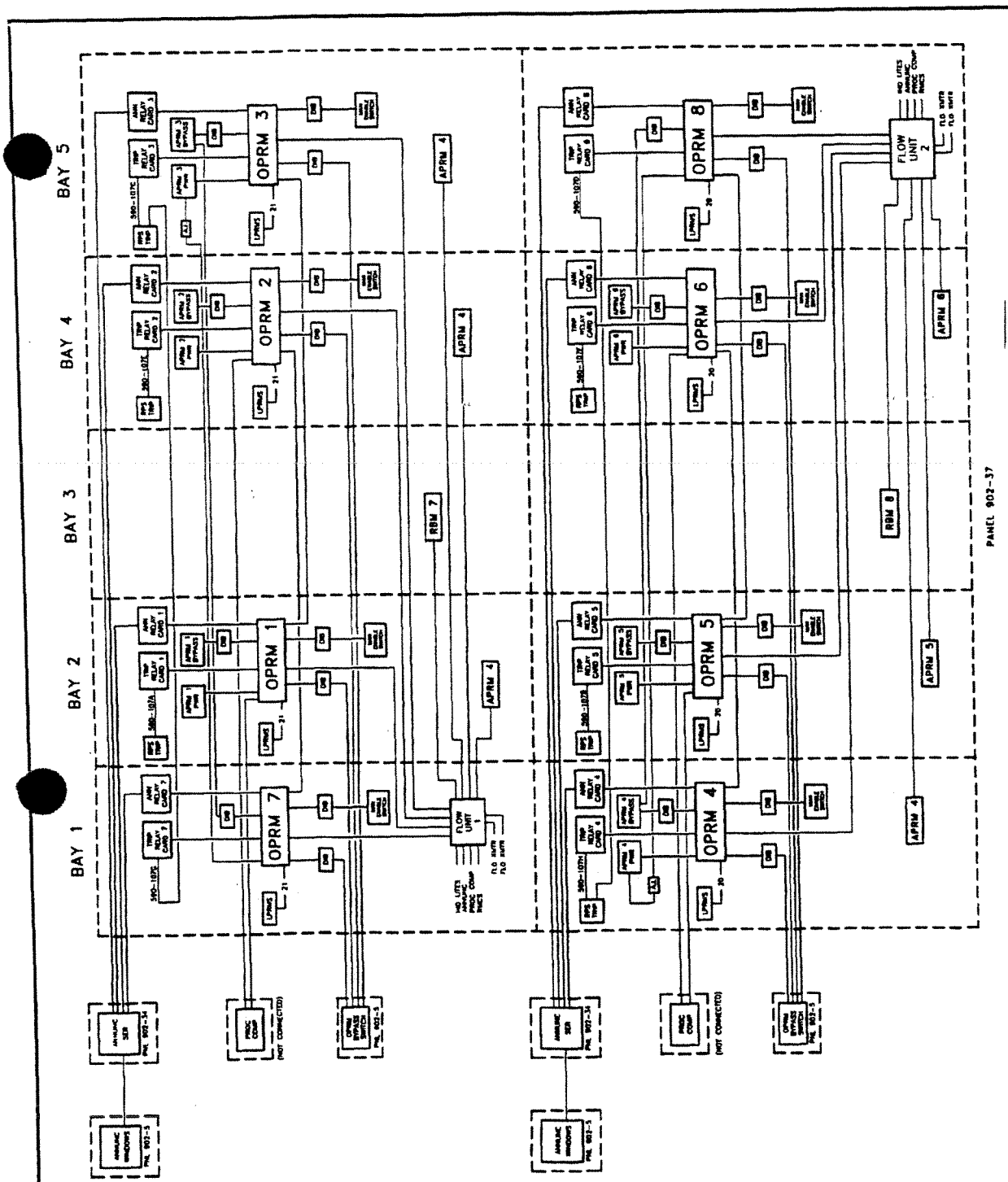


UFSAR REVISION 4, JUNE 2001

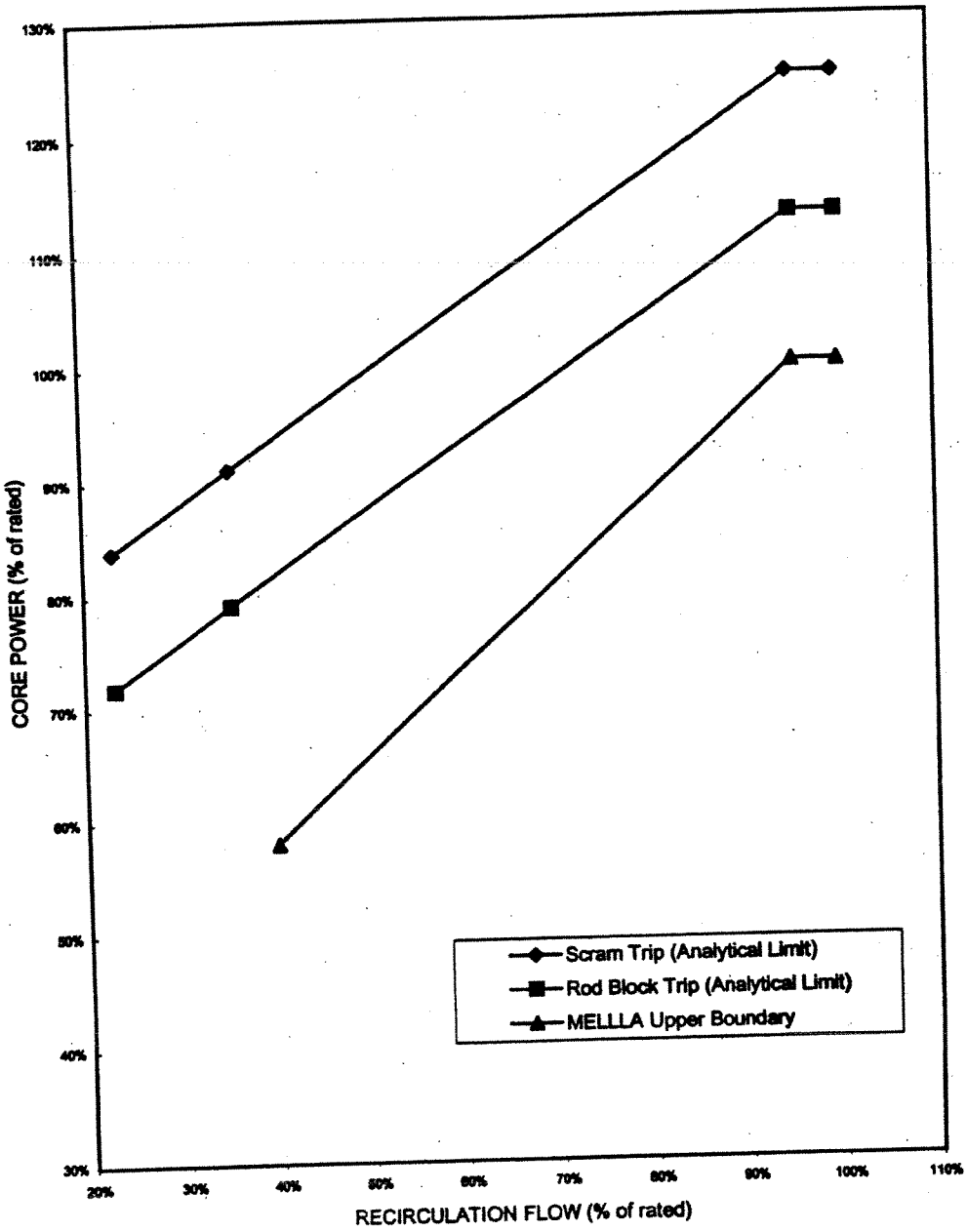
DRESDEN STATION UNITS 2 & 3

FLOW INSTRUMENT FOR APRM, OPRM, AND ROD BLOCK MONITOR

FIGURE 7.6-12



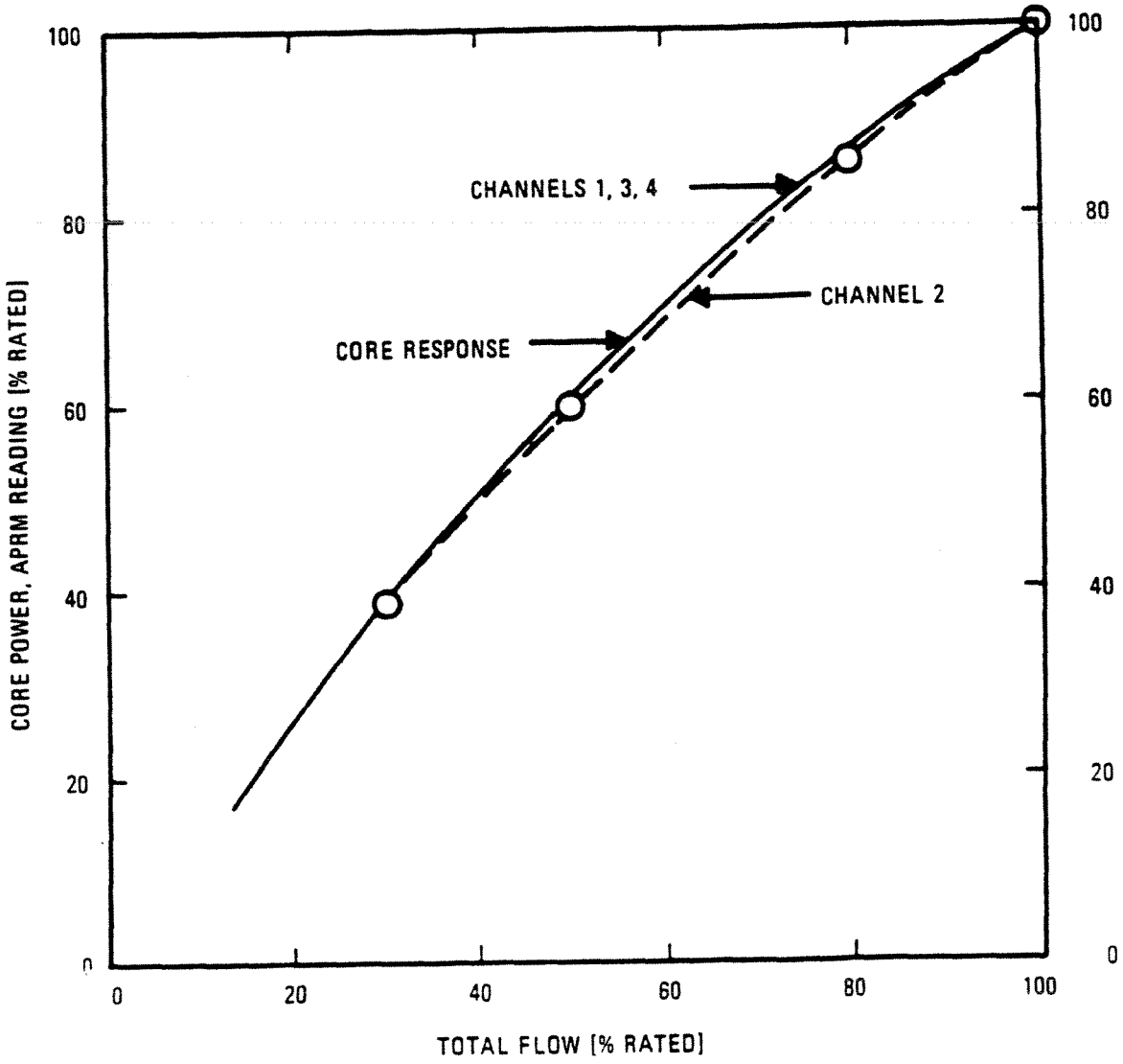
UFSAR REVISION 4, JUNE 2001
DRESDEN STATION UNITS 2 & 3
OPRM INTERCONNECTION BLOCK DIAGRAM
FIGURE 7.6-12A



DRESDEN STATION
UNITS 2 &3

ILLUSTRATIVE APRM SCRAM AND ROD BLOCK TRIPS VS. RECIRCULATION FLOW

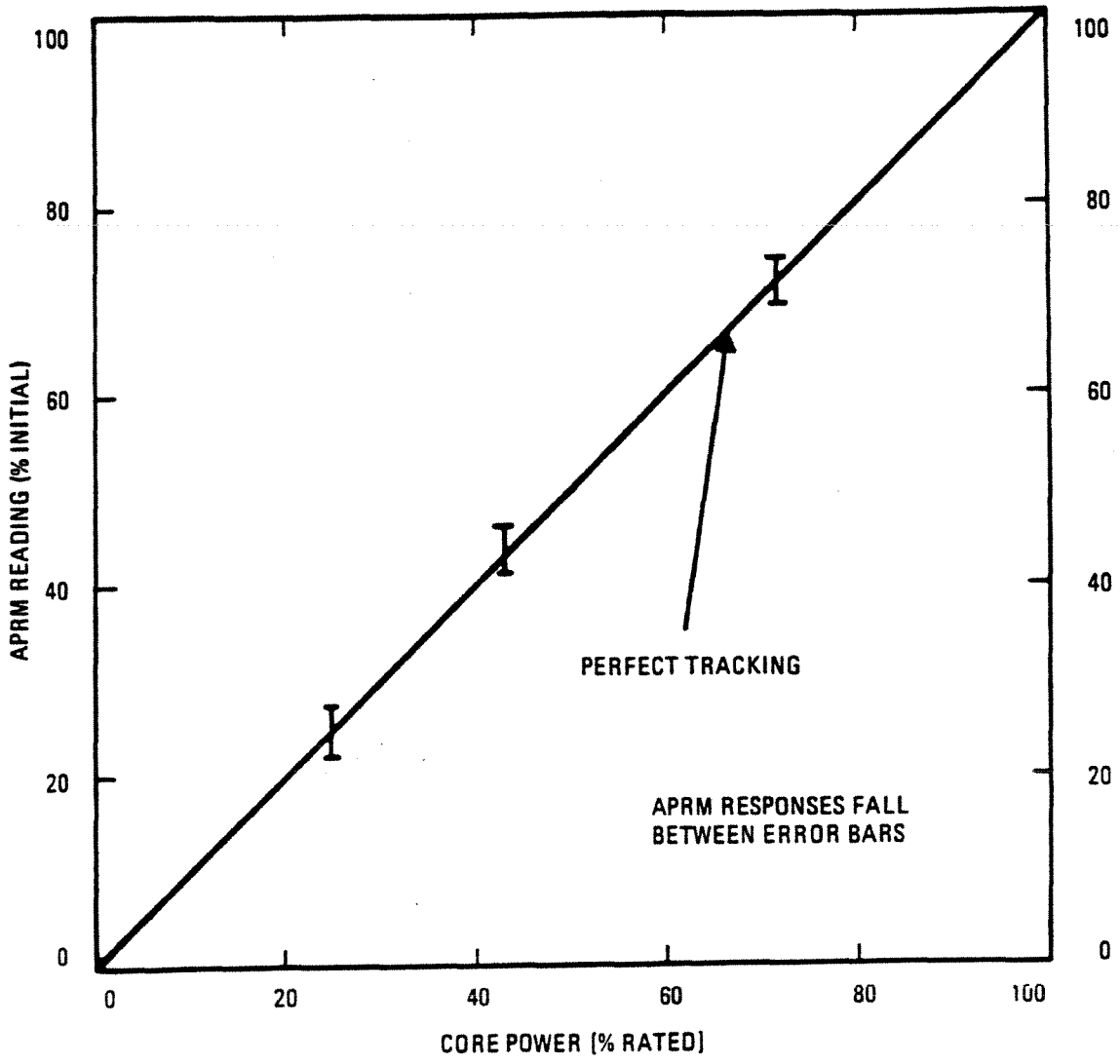
FIGURE 7.6-13



DRESDEN STATION
UNITS 2 & 3

APRM RESPONSE DURING FLOW-INDUCED POWER LEVEL MANEUVERING

FIGURE 7.6-14

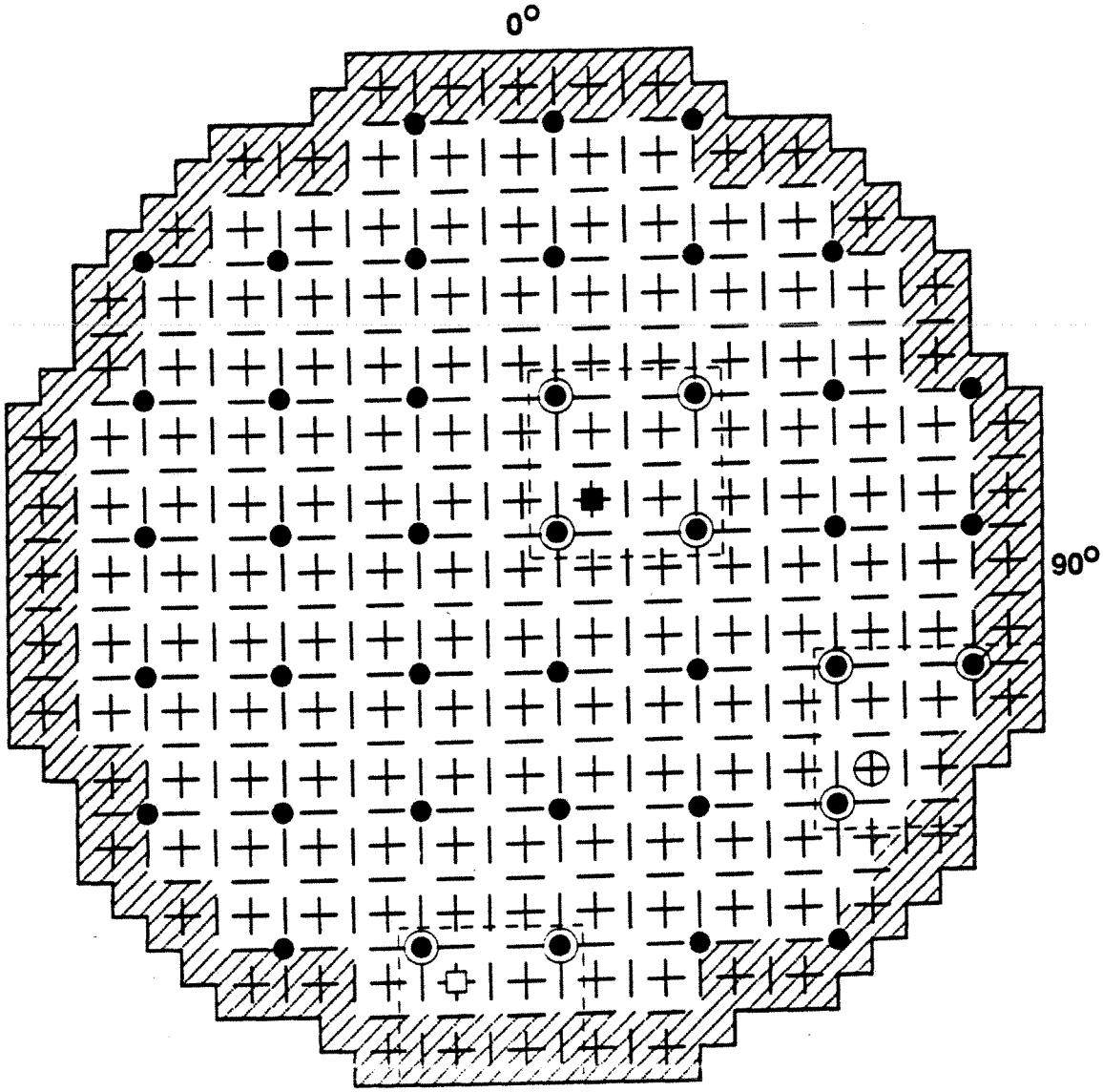


DRESDEN STATION
UNITS 2 & 3

APRM RESPONSE DURING CONTROL ROD-INDUCED POWER LEVEL MANEUVERING

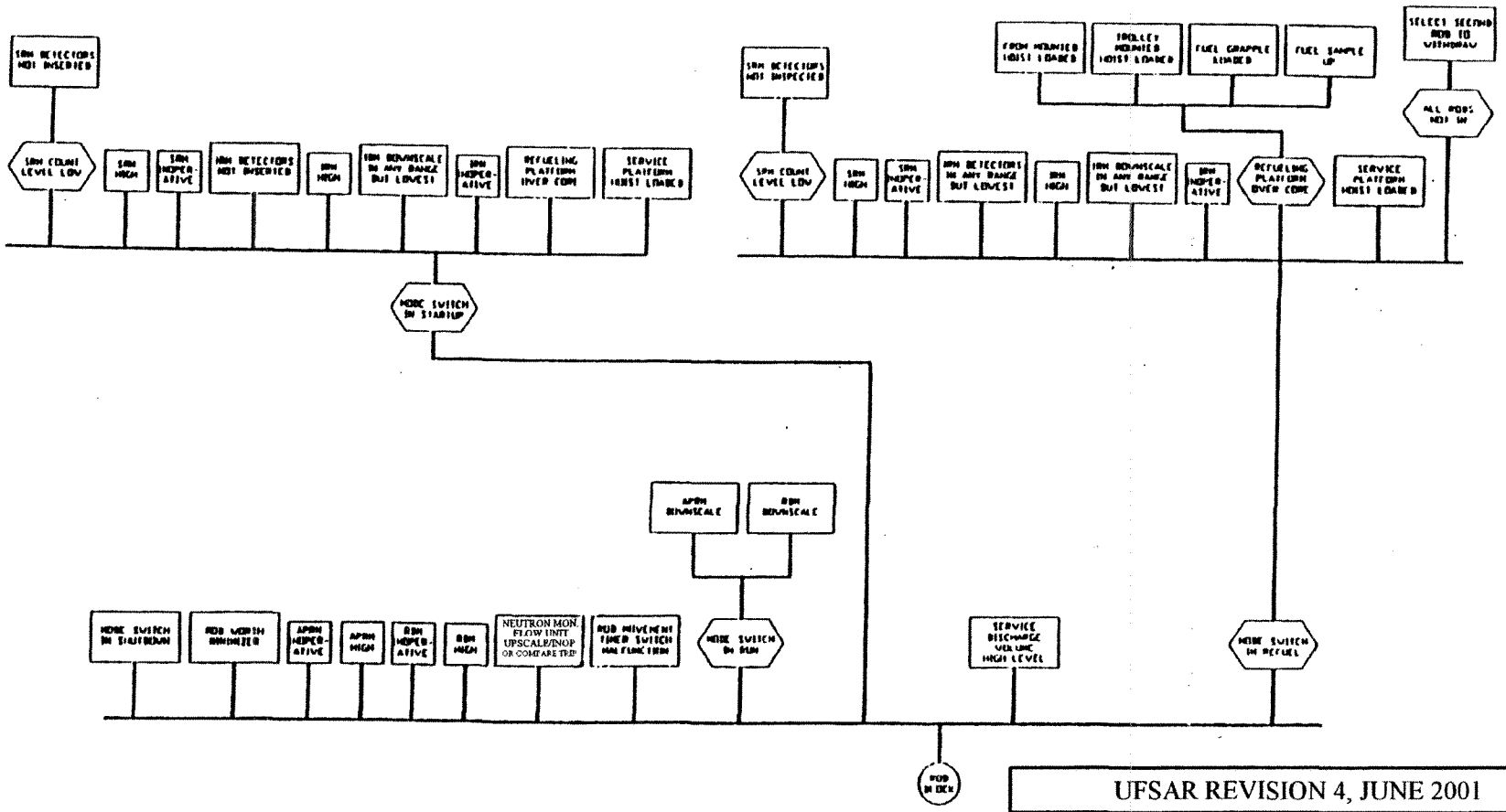
FIGURE 7.6-15

NOTE: ASSIGNMENT IS AUTOMATICALLY
INIATIATED UPON ROD SELECTION



▨ – RBM AUTOMATICALLY BYPASSED (READING ZERO)
□ – TYPICAL ROD YIELDING TWO LPRM STRINGS AS INPUTS
◯ – TYPICAL ROD YIELDING THREE LPRM STRINGS AS INPUTS
■ – TYPICAL ROD YIELDING FOUR LPRM STRINGS AS INPUTS

DRESDEN STATION UNITS 2 & 3
RBM LPRM INPUT ASSIGNMENT
FIGURE 7.6-16

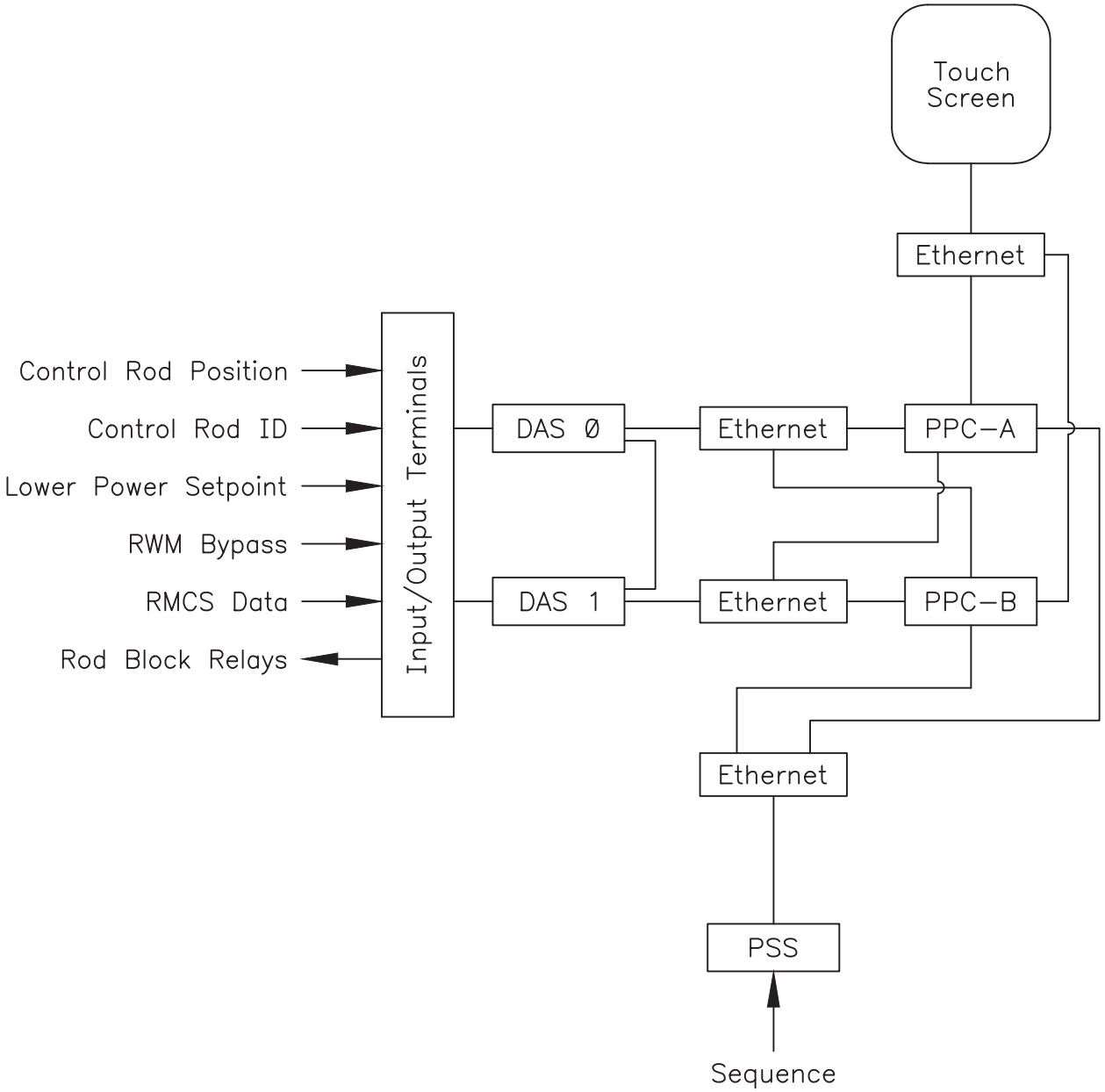


UFSAR REVISION 4, JUNE 2001

DRESDEN STATION
UNITS 2 & 3

CONTROL ROD BLOCK DIAGRAM

FIGURE 7.7-1



UFSAR Revision 11, June 2015
DRESDEN STATION UNIT 2&3
BLOCK DIAGRAM ROD WORTH MINIMAZER SYSTEM
FIGURE 7.7–2

FIGURE DELETED

UFSAR Revision 11, June 2015
DRESDEN STATION UNIT 3
ROD WORTH MINIMAZER SYSTEM BLOCK DIAGRAM
FIGURE 7.7–2A

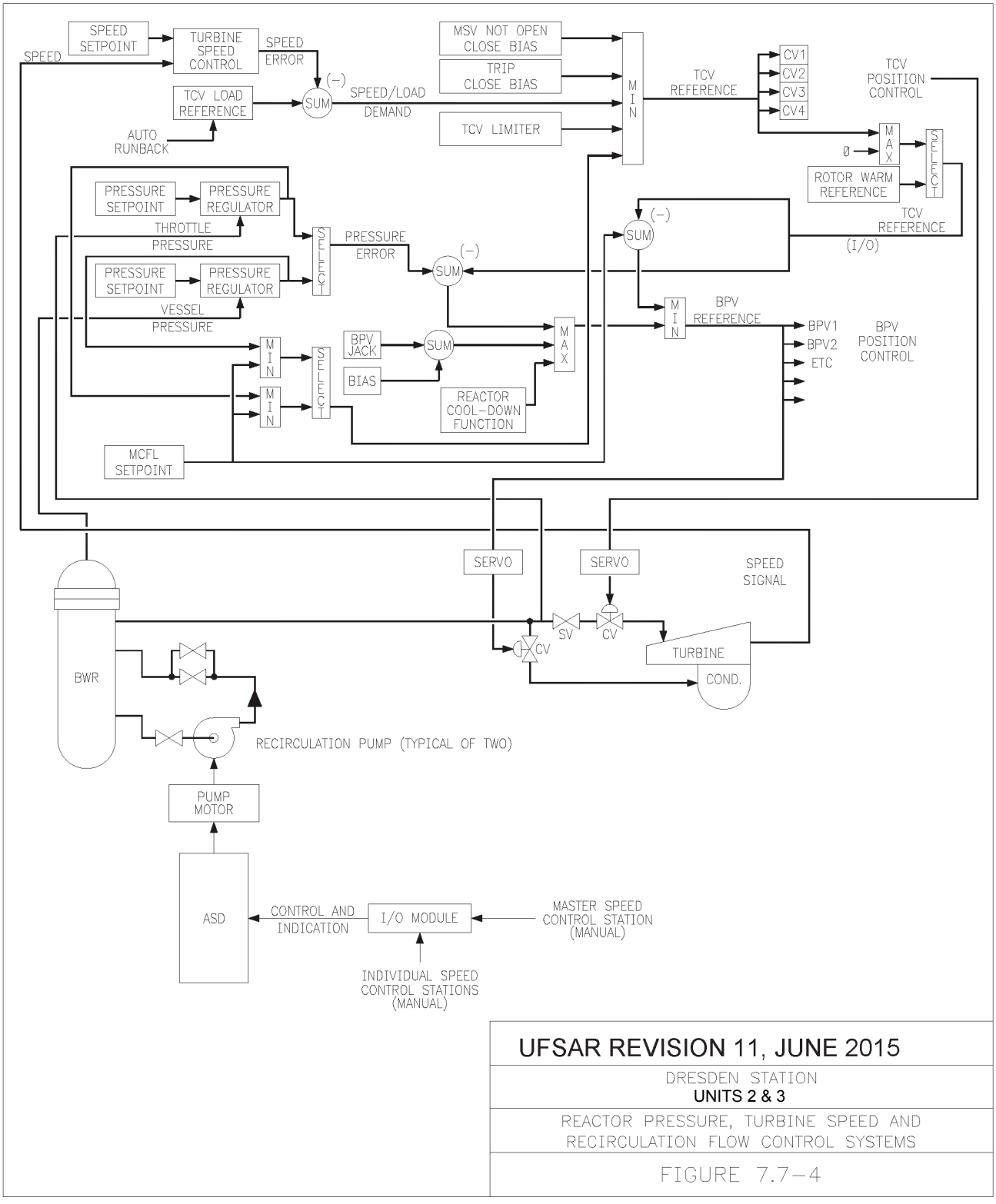
FIGURE DELETED

UFSAR Revision 11, June 2015

DRESDEN STATION
UNITS 2 & 3

RECIRCULATION
SPEED CONTROL NETWORK

FIGURE 7.7-3

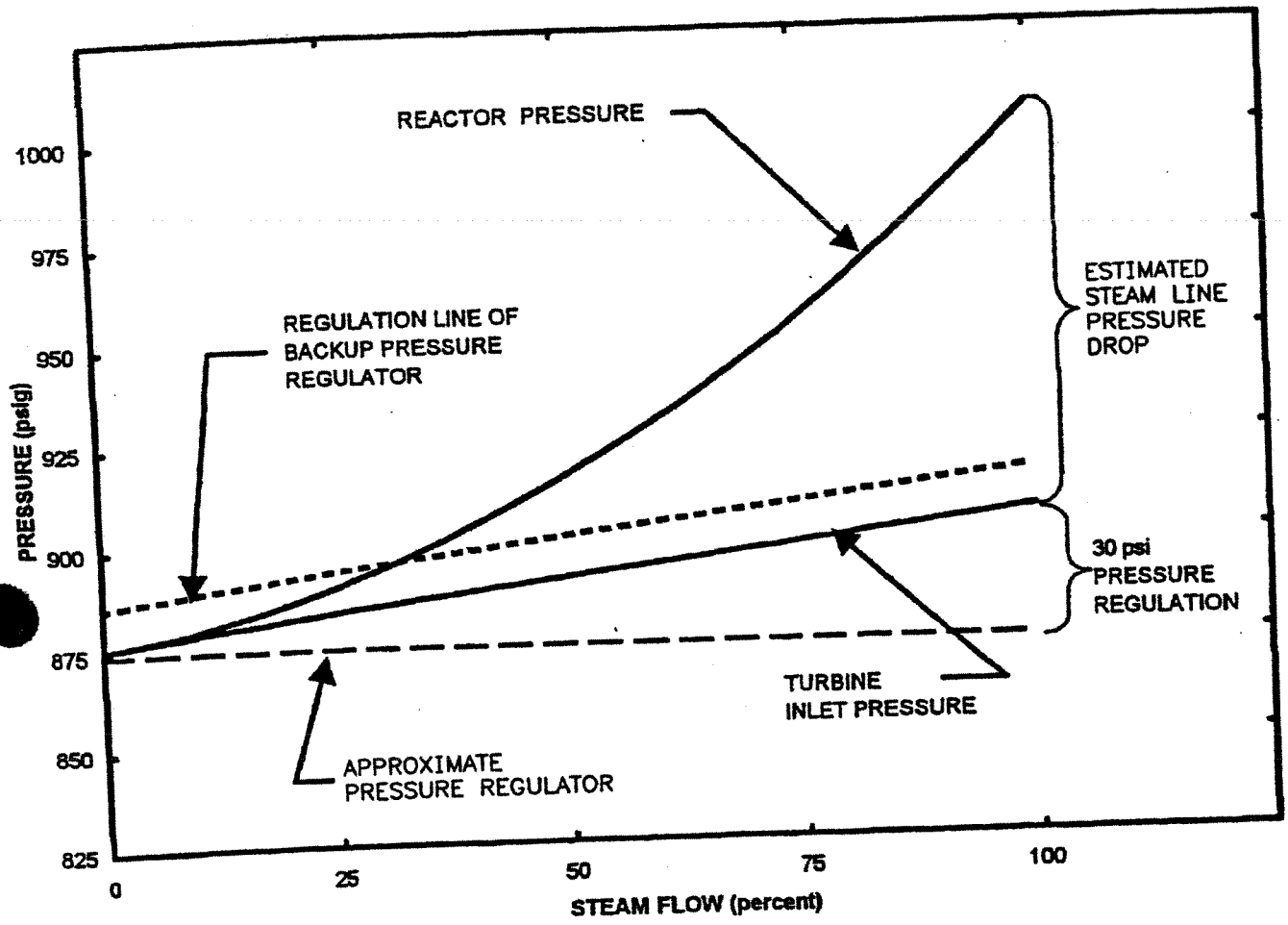


UFSAR REVISION 11, JUNE 2015

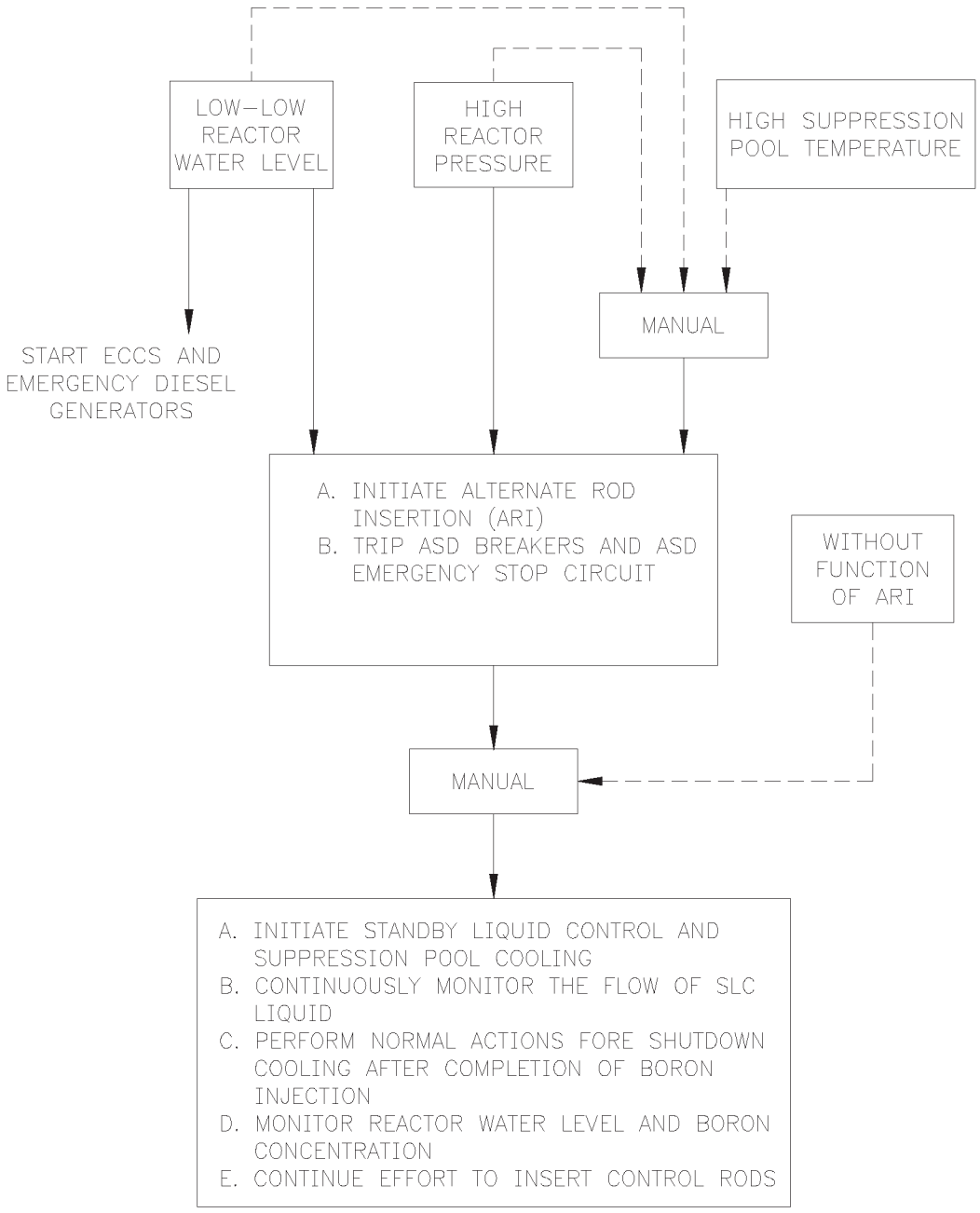
DRESDEN STATION
UNITS 2 & 3

REACTOR PRESSURE, TURBINE SPEED AND RECIRCULATION FLOW CONTROL SYSTEMS

FIGURE 7.7−4



DRESDEN STATION UNIT 2 and 3
TYPICAL VESSEL AND TURBINE INLET PRESSURE VS. STEAM FLOW
FIGURE 7.7-9
REVISION 5, JANUARY 2003



UFSAR REVISION 11, JUNE 2015

DRESDEN STATION
UNIT 2 & 3

ATWS MITIGATION SYSTEM
BLOCK DIAGRAM

FIGURE 7.8–1