7.0 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

The instrumentation and control (I&C) systems presented in this chapter provide protection against improper or unsafe reactor operation during steady-state and transient power operations. They will initiate selected protective functions to mitigate the consequences of design basis accidents. Emphasis is placed on those I&C systems which assure that the reactor can be operated to produce power in a manner that ensures no undue risk to the health and safety of the public. This chapter relates the functional performance requirements, design bases, system descriptions, and safety evaluations for those systems. The safety evaluations show that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

Definitions

Terminology used in this chapter reflect an interdisciplinary approach to safety systems similar to that proposed in Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard 603-1980 "Criteria for Safety Systems for Nuclear Power Generating Stations."

1. Safety System: The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis accidents. The safety system for the Westinghouse nuclear steam supply system (NSSS) is composed of the integrated protection system, the protective action system, safety related display instrumentation, and essential auxiliary supporting systems. The scope of the integrated protection system is shown in Figure 7.1-1.

2. Integrated Protection System: The aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features. (See Figure 7.1-2).

3. Protective Action System: The aggregate of electrical and mechanical equipment which accomplish reactor trip or engineered safety features functions on demand from the integrated protection system.

4. Protective Function: Any one of the functions necessary to mitigate the consequences of a design basis accident. Protective functions will be initiated by the integrated protection system and will be accomplished by the protective action system. Examples of protective functions are reactor trip and engineered safety features (ESF) (such as emergency core cooling, steam line isolation, containment isolation, etc.).

5. Actuated Equipment: The assembly of prime movers and driven equipment used to accomplish a protective function (e.g., motors, shutdown rods, pumps, valves, etc.).

6. Actuation Device: A component that directly controls the motive power for actuated equipment (e.g., circuit breakers, relays, pilot valves, etc.).

7. Channel Set: One of the several separate and redundant segments of the integrated protection system. The channel set will include its associated sensors, field wiring, cabinets, and electronics used to generate one of the redundant actuation signals for a protective function. Channel sets are denoted by Roman numerals I - IV on the figures in this chapter. (See Figures 7.1-1 and 7.1-2).

8. Channel: One of the several separate and redundant measurements of a single variable used by the IPS in generating the signal to initiate a protective function. A channel loses its identity where it is combined with other inputs in the channel set.

9. Actuation Train: One of the several separate and redundant segments of the protective action system. The actuation train will include its associated actuation devices and actuated equipment necessary to accomplish one of the redundant portions of a protective function. This

model will employ 4 reactor trip actuation trains and 2 safeguards actuation trains. Reactor trip actuation trains are denoted by Roman numerals I - IV as dictated by the IPS channel set which originates the command. Fluid systems portions of the safeguards trains use the Train-A, Train-B notation. Train-A equipment is actuated from Train-A logic cabinets, and Train-B equipment is actuated from Train-B logic cabinets. (See Figure 7.1-2).

10. Degree of Redundancy: The number of duplicate channels monitoring a single variable, or the number of duplicate channel sets which can initiate a given protective function, or the number of duplicate actuation trains which can accomplish a given protective function. Redundancy will be employed to maintain protection capability when the safety system is degraded by a single random failure.

7.1.1 Identification of Safety Systems

A summary of the protective functions is given in Subsection 7.1.1.1 while detailed descriptions of the functions are given in Section 7.2 for reactor trip and 7.3 for engineered safety features actuation. Section 7.1 is oriented to the description and analysis of the safety system I&C architecture and hardware. The safety system will be comprised of the following subsystems:

1. The Integrated Protection System (IPS) which will generate the initiation signals for protective functions; i.e., reactor trip and engineered safety features. Components of the IPS are listed in Subsection 7.1.1.2, and the architecture of the IPS is discussed in Subsection 7.1.1.3.

2. The Protective Action System (PAS) which will accomplish reactor trip and engineered safety features functions on demand from the integrated protection system. Components of the PAS are listed in Subsection 7.1.1.4.

3. Safety-related Display Instrumentation which will be needed by the operator is listed in Section 7.5.

4. Essential Auxiliary Supporting Systems which, although they do not perform a safety function directly, will be necessary to operation of the integrated protection system and protective action system. Examples of auxiliary supporting systems are the I&C power supplies and safeguards power supply system. These systems are identified in Subsection 7.1.1.6.

Chapter 7 discusses the instrumentation portions of the safety system which are required to function to achieve the system responses assumed in the accident analyses, and those needed to shutdown the plant safely. Section 7.1 describes the integrated protection system, the protective action system, and those portions of the safety related display instrumentation and auxiliary supporting systems not covered in other sections of this safety analysis report. (Where information is presented in other sections, it is appropriately identified.) Section 7.2 discusses the reactor trip function, and Section 7.3 addresses the engineered safety features. Systems required for safe shutdown are discussed in Section 7.4 in support of other chapters. Safety related display instrumentation is discussed in Section 7.5 and other instrumentation systems required for safety, such as the I&C power distribution system and critical valve interlocks, are presented in Section 7.6. Control systems are discussed in Section 7.7.

7.1.1.1 Protective Functions

Protective Functions are those actions required to achieve the system responses assumed in the safety analyses, and those needed to shutdown the plant safely. As illustrated in Figure 7.1-1, protective functions will be initiated by the Integrated Protection System and will be accomplished by the protective action system. This report has grouped the protective functions into two classes:

1. Reactor Trip
2. Engineered Safety Features (ESF).

Each of these two classes are summarized below and are presented in detail in Sections 7.2 and 7.3 respectively.

7.1.1.1.1 Reactor Trip Function

The safety system will automatically trip the reactor and initiate ESF (if required) whenever predetermined limits are approached. The integrated protection system will maintain surveillance on nuclear and process variables which are related to equipment mechanical limitations, such as pressure, and on variables which directly affect the heat transfer capability of the reactor, such as reactor coolant flow and temperature. When a limit is approached, the Integrated Protection System will initiate the signal to open the reactor trip circuit breakers. This action will remove power to the control rod drive mechanism coils permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will shut down the reactor.

The various parameters which go into generation of a reactor trip are discussed in Section 7.2. The following is a summary listing of the conditions which could cause an automatic reactor trip:

1. Nuclear Startup Conditions:

    a. High source range count rate
    b. High intermediate range current
    c. High power range nuclear power (low setpoint)

2. Nuclear Overpower Conditions:

    a. High power range nuclear power (high setpoint)
    b. High positive nuclear flux rate
    c. High negative nuclear flux rate

3. Core Heat Removal Conditions:

    a. Low Departure from Nucleate Boiling Ratio (DNBR)
    b. High fuel linear heat generation rate (kw/ft)
    c. Low pressurizer pressure
    d. Low reactor coolant pump speed
    e. Low reactor coolant flow

4. Primary System Pressure Conditions:

   a. High pressurizer pressure
   b. High pressurizer water level

5. Heatsink Conditions:

   a. Low steam generator water level
   b. High steam generator water level

6. Turbine tripped condition on plants without full load rejection capability

7. Whenever safety injection is automatically initiated

8. Seismic acceleration (optional)

In addition to the above automatic initiations, reactor trip could be generated directly by manual action (manual reactor trip or manual safety injection). The logic for this function is shown in Figure 7.2-1 (Sheets 2, 12, and 13).

The detailed discussion and evaluation of the reactor trip function is contained in Section 7.2.

7.1.1.1.2 Engineered Safety Features Actuation Functions

The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more engineered safety features (ESF) in order to prevent or mitigate damage to the core and reactor coolant system components, and to ensure containment integrity. The integrated protection system will determine whether or not safety limits are being approached for selected plant parameters. If they are, the integrated protection system will combine the signals through logic functions which respond to combinations indicative of accident situations.

Once the required logic combination is generated, the integrated protection system will send the signals to the appropriate ESF components of the protective action system.

The following is a summary listing of the engineered safety features. The various parameters which will go into actuation of the engineered safety features are discussed in Section 7.3.

1. Safety Injection (includes emergency core cooling and start of supporting systems essential to emergency core cooling - such as diesels, etc.)

2. Steam Line Isolation

3. Containment Spray

4. Containment Isolation:

    a. Phase-A Isolation
    b. Phase-B Isolation
    c. Containment Ventilation Isolation

5. Main Feedwater Isolation

    a. Tripping of Main Feedwater Pumps

    b. Closure of all Feedwater Isolation, Control, and Bypass Valves

6. Emergency Feedwater

    a. Pump Start, Steam Generator Letdown Isolation, and Startup Feedwater Termination

    b. Isolation to a Faulted Steam Generator

7. Block of Boron Dilution

In addition to automatic actuation, engineered safety features can be initiated manually as listed in Subsection 7.3.2.2.8.

The detailed discussion and evaluation of each engineered safety feature is contained in Section 7.3. The logic for their actuation is depicted in Figure 7.2-1.

7.1.1.2 Integrated Protection System Components

The integrated protection system will be the "sense and command" portion of the safety system. It will monitor key plant parameters and will initiate appropriate protective functions when critical limits are approached. Protective functions can also be manually initiated.

The integrated protection system (IPS) will consist of four redundant channel sets (denoted as I - IV) as illustrated in Figure 7.1-2. The system will include instrumentation to monitor process and nuclear variables. It will convert analog inputs to a digital format and will perform any required processing and calculations on the measurements. The results will be combined through coincidence matrices to generate the protective functions previously identified whenever fixed or calculated limits are exceeded. The IPS will also contain built-in test features and will provide information read-out on input parameters and system status. The IPS will also furnish the control system with the protection signals which will be used for plant operational control.

The IPS consists of the following major cabinets:

Integrated Protection Cabinets (IPC)
Engineered Safeguards Features Actuation Cabinets (ESFAC)
Main Control Board Multiplexer (MCB MUX)
Logic Cabinets
Reactor Trip Switchgear (RTS)

This subsection provides a description of the equipment which will make up the integrated protection system. The simplified one line-diagram of the IPS is shown in Figure 7.1-2. The basic elements of the integrated protection system which are described in the following subsections are:

1. Sensors of the Integrated Protection System

    a. Process sensors (flows, levels, pressures, temperatures)
    b. Nuclear instrumentation detectors
    c. Nitrogen-16 (N-16) power monitoring detectors
    d. Equipment status inputs (RCP speed and turbine trip)

2. Integrated Protection Cabinets (Subsection 7.1.1.3.1)

    a. Analog to digital conversion and signal conditioning
    b. Calculations and comparisons to setpoints
    c. Voting matrices and manual inputs
    d. Automatic tester

3. Engineered Safety Features Actuation Cabinets (Subsection 7.1.1.3.2 and 7.1.1.3.3)

    a. ESF System Level Logic
    b. System-level manual actions
    c. Automatic Tester/Data Acquisition

4. Logic Cabinets

    a. Component level logic
    b. Automatic tester
    c. Functional logic computers

In addition to the above listed elements, the following hardware architecture is discussed as it will apply throughout the integrated protection system.

5. Data Link Structures

   a. Isolation Devices
   b. Electrical Data Links
   c. Multiplexing

6. Microprocessors

7. Built-in Test Capabilities

Refer to Section 7.6 for a description of the I&C power distribution system for the integrated protection system.

7.1.1.2.1 Sensors of the Integrated Protection System

The integrated protection system (IPS) will monitor key variables which are related to equipment mechanical limitations and variables which directly affect the heat transfer capability of the reactor. Some limits, such as DNBR, will be calculated in the integrated protection cabinets from other parameters when direct measurement of the variable is not possible. This subsection provides a description of the sensors which monitor the variables for the IPS. For convenience the discussions are grouped into the following 4 categories; a) Process sensors; b) Nuclear instrumentation; c) N-16 power monitoring detectors; d) Status inputs from field equipment. The inputs described are those which will be required by the IPS to generate the initiation signals for the protective functions previously identified. The use of each parameter is discussed in the sections which deal with each protective function and is not repeated here; e.g., reactor trip in Section 7.2 and engineered safety features actuation in Section 7.3.

7.1.1.2.1.1 Process Sensors

The process sensors are devices which measure temperature, pressure, fluid flow, and fluid level. Process instrumentation by definition specifically

excludes nuclear and radiation measurements. The following variables will be measured by process sensors for the Integrated Protection System:

1. Pressures

    a. Pressurizer Pressure
    b. Containment Pressure
    c. Steam Line Pressure

2. Levels

    a. Pressurizer Water Level
    b. Steam Generator Water Level (narrow and wide range)

3. Temperatures

    a. Reactor Coolant Cold Leg Temperature (narrow range)

4. Flow

    a. Reactor Coolant Flow

Pressure transmitters may be force balance and motion balance and could incorporate filled systems. Flows will be measured by using a differential pressure transmitter to measure the differential pressure created across orifices, elbow taps, or venturies. Level measurements will be made using differential pressure transmitters to measure the differential pressure between two vertical taps. Temperatures will be measured using resistance temperature detectors (RTDs).

7.1.1.2.1.2 Nuclear Instrumentation Detectors

Various types of neutron detectors will be used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The power range channels will be capable of recording overpower excursions up to

200 percent of full power. The neutron flux will cover a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation will be necessary.

The lowest range (source range) will cover six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This will generally be greater than two counts per second. The next range (intermediate range) will cover eight decades. Detectors and instrumentation will be chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) will cover approximately two decades of the total instrumentation range. This will be a linear range that will overlap the higher portion of the intermediate range. Detector types for these three ranges will be:

Source Range - proportional counter
Intermediate Range - compensated ionization chamber
Power Range - uncompensated ionization chamber

The power range detectors will be multi-element detectors containing four short separate active volumes spaced uniformally axially. Each section will be surrounded by a controlled neutron environment which will prevent undue influence from neutrons scattered back from surrounding concrete. The neutron detectors will be installed in wells located around the reactor vessel in the primary shield. See Figure 7.1-3.

7.1.1.2.1.3 Nitrogen-16 (N-16) Power Measuring Detectors

The N-16 power monitoring instrumentation will provide an input into calculation of the DNBR and KW/ft reactor trip functions.

The N-16 detectors will monitor the thermal power of the NSSS by detecting the Nitrogen-16 (N-16) content in the coolant system. The N-16 content in the primary coolant is directly proportional to the fission rate in the core and

excludes nuclear and radiation measurements. The following variables will be measured by process sensors for the Integrated Protection System:

1. Pressures

    a. Pressurizer Pressure
    b. Containment Pressure
    c. Steam Line Pressure

2. Levels

    a. Pressurizer Water Level
    b. Steam Generator Water Level (narrow and wide range)

3. Temperatures

    a. Reactor Coolant Cold Leg Temperature (narrow range)

4. Flow

    a. Reactor Coolant Flow

Pressure transmitters may be force balance and motion balance and could incorporate filled systems. Flows will be measured by using a differential pressure transmitter to measure the differential pressure created across orifices, elbow taps, or venturies. Level measurements will be made using differential pressure transmitters to measure the differential pressure between two vertical taps. Temperatures will be measured using resistance temperature detectors (RTDs).

7.1.1.2.1.2 Nuclear Instrumentation Detectors

Various types of neutron detectors will be used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The power range channels will be capable of recording overpower excursions up to

200 percent of full power. The neutron flux will cover a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation will be necessary.

The lowest range (source range) will cover six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This will generally be greater than two counts per second. The next range (intermediate range) will cover eight decades. Detectors and instrumentation will be chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) will cover approximately two decades of the total instrumentation range. This will be a linear range that will overlap the higher portion of the intermediate range. Detector types for these three ranges will be:

Source Range - proportional counter
Intermediate Range - compensated ionization chamber
Power Range - uncompensated ionization chamber

The power range detectors will be multi-element detectors containing four short separate active volumes spaced uniformally axially. Each section will be surrounded by a controlled neutron environment which will prevent undue influence from neutrons scattered back from surrounding concrete. The neutron detectors will be installed in wells located around the reactor vessel in the primary shield. See Figure 7.1-3.

7.1.1.2.1.3 Nitrogen-16 (N-16) Power Measuring Detectors

The N-16 power monitoring instrumentation will provide an input into calculation of the DNBR and KW/ft reactor trip functions.

The N-16 detectors will monitor the thermal power of the NSSS by detecting the Nitrogen-16 (N-16) content in the coolant system. The N-16 content in the primary coolant is directly proportional to the fission rate in the core and

is an isotope of nitrogen generated by neutron activation of oxygen contained in the water. Decay of the N-16 isotope produces high energy gamma rays which will penetrate the wall of the high pressure piping. Therefore the N-16 concentration in the primary coolant can easily be monitored by measuring the gamma radiation outside of the primary coolant piping.

Two N-16 detectors will be mounted externally on the hot leg of each reactor coolant loop. They will be mounted as close as practical to the outside of the primary shield to minimize coolant transit time from the core to the hot leg detectors. The two detectors will be mounted diametrically opposed on the coolant pipe to obtain a more uniform contribution to the total signal from the cross section of fluid in the pipe.

The N-16 gamma detectors will be high sensitivity pressurized gas-filled gamma ionization chambers. They will be shielded from external background radiation by a lead housing to provide a controlled field of view of the pipe section.

7.1.1.2.1.4 Equipment Status Inputs

Some inputs to the integrated protection system will not be measurements of process or nuclear variables, but will be indications of the operational status of certain field-mounted equipment. The IPS will use two such status inputs. These are inputs which will reflect the speed of each reactor coolant pump and when the turbine has been tripped.

RCP speed will be monitored by a speed sensor which produces a digital output representative of the pump speed in revolutions per second. One speed sensor will be mounted on each reactor coolant pump.

The turbine trip is provided by the turbine stop valves position detectors and trip fluid pressure detectors.

7.1.1.2.2 Engineered Safeguards Features Actuation Cabinets

Two ESFAC's are required (assuming a two train design), designated ESFAC A and ESFAC B. Each cabinet is associated with one safeguard train. Major functions of the ESFAC include:

- o Each ESFAC receives bistable trip signals via isolated data links from all four IPC's. These bistable trip signals correspond to the four protection system channels monitoring each process variable.

- o Perform two out of four voting operation on the bistable trip signals and the system level ESF actuation logic. This logic includes the manual system level actuation inputs. The results of this logic are system level ESF actuation signals such as safety injection, containment isolation, and feedwater isolation.

- o Provide sequencer for safety injection and blackout.

- o Provide the system level ESF actuation outputs to the logic cabinets via redundant computer data links.

7.1.1.2.3 Logic Cabinets

There are two sets of logic cabinets in a two train system (one set per train). The number of cabinets in each set is determined by the number and location of the various components (valves and pumps) under the control of the integrated protection system. Figure 7.1-2 shows a typical arrangement of logic cabinets. The logic cabinets provide the following functions:

- o Receives system level ESF actuation signals from the ESFAC and combines these signals with interposing (interlocking) logic specific to each component.

- o Receives component level command signals via redundant data links from the advanced control room, and transmits component status signals to the advanced control room via these same data links.

- Provides the power interface devices to switch control power to the final actuation devices for pump, valves and heaters controlled by the IPS.

7.1.1.2.4 Main Control Board Multiplexers

Two redundant main control board multiplexers are required per safeguards actuation train. These multiplexers provide for the redundant transmission of component level manual actuation signals to the logic cabinets and for reception of component status/position information from the logic cabinets which is used for the display of component status. The data links from the MCB multiplexers to the logic cabinets, shown on Figures 7.1-1 (Sheet 3) and 7.1-2, have the characteristics of a "data highway" in that information may be transmitted and received from multiple drops on the data link.

Two plant safety monitoring system (PSMS) demultiplexers are also required to receive information for the PSMS displays. One is associated with IPC channels I and III. The other is associated with IPC Channels II and IV.

7.1.1.3 IPS Architecture

7.1.1.3.1 Integrated Protection Cabinets (IPC)

Each channel set will be contained in its own integrated protection cabinet, physically separated and electrically isolated from the IPC's of the remaining 3 channel sets.

Major functions of the IPC include the following:

- Input signal conditioning and digitizing of analog process inputs. Each IPC is associated with one protection system set and each receives process inputs from instrumentation associated with that set.

- Performing reactor trip logic and generating a reactor trip output to the reactor trip breakers. Each IPC provides two reactor trip outputs to the two reactor trip breakers in the same set.

- Providing bistable trip outputs from process channels for the engineered safeguards actuation logic in the engineered safeguards features actuation cabinets. Each IPC provides bistable trip outputs to all ESFAC's. (Two ESFAC's exist assuming a two train system). These outputs are transmitted via isolated data links as shown on Figure 7.1-2.

Each integrated protection cabinet consists of a four bay structure containing the following micro-computer subsystems (refer to Figure 7.1-4):

Engineered Safeguards Features	-	ESF 1 and ESF 2
Communications/Automatic Tester	-	C/AT
Trip Bus		
Function Group 1	-	RT Group 1
Function Group 2	-	RT Group 2
Trip Enable	-	TE
Global Trip	-	GT

Figure 7.1-5 shows the IPC functional block diagram.

7.1.1.3.1.1 ESF Subsystem

The ESF subsystem consists of a micro-computer card frame containing micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-6 (There will be two independent ESF subsystems.). This system receives analog (process variable) and digital (manual switch) inputs and performs the ESF logic necessary to the reactor trip system. It also provides the bistable trip signals to the ESFAC's. The ESF subsystem is comprised of the following board types:

- Data Link (receive/transmit) Controller - Provides for all communications with the DA/AT subsystem.

- Central Processing Unit Board (CPU) - Main micro-computer for subsystem and performs all calculations and logic for subsystem functions.

- Non-Volatile Memory (NVRAM) - Provides for storage of constants and setpoints used by subsystem. These constants may be modified by the operator, but are retained upon loss of power.

- Data Link (transmit) - Data link interface for providing bistable trip signals to the ESFAC's.

- Analog I/O - Provides analog input signal conditioning for process inputs to the subsystem. Provides any analog outputs required from the ESF subsystem.

- Digital I/O - Parallel I/O board for processing digital inputs (such as changing from "manual system level actuation" to "operational bypasses") and digital outputs from the subsystem.

7.1.1.3.1.2 Global Trip Subsystem

This subsystem consists of a micro-computer card frame containing micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-7. This system collects the partial block trip and bypass status of the individual trip functions in its channel set and transmits this data to the redundant channel sets. The global trip subsystem also receives the partial trip and bypass status from each of the other three channel sets and uses this information (with its own channel set trips and bypasses) to compute the global trip actuation. For the description of the global trip actuation refer to Reference 1 to Subsection 7.1.3. The global trip subsystem is comprised of the following board types:

- Data Link (transmit) - Sends status information from the global trip subsystem to the data acquisition/auto tester subsystem.

- Central Processing Unit board (CPU) - Main micro-computer for subsystem. Controls all other boards in subsystem and performs all calculations and logic (e.g., 2/4 trip logic) for subsystem functions.

- Digital I/O - Provides global trip signals to the Trip Bus and receives bistable trip signals from other subsystems in the same IPC.

- Data Link (receive/transmit) - Three of these data links are required to send bistable trip signals from one IPC to the three other IPC's. These Data Links also receive bistable trip signals from the three other IPC's.

7.1.1.3.1.3 Trip Enable Subsystem

This subsystem consists of a micro-computer card frame containing micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-8. This system receives data link messages from the three other IPC's containing partial trip and bypass status of individual trip functions. From this data and bypass status information in its own IPC, the trip enable subsystem computes the trip enable actuations for each individual trip function. For the description of the trip enable actuation refer to Reference 1 to Subsection 7.1.3. The trip enable actuations are sent to the trip bus via parallel I/O lines. The trip enable subsystem is comprised of the following board types.

- Data link (transmit) - sends status information from the trip enable subsystem to the data acquisition/auto tester subsystem.

- Central Processing Unit (CPU) - Main micro-computer for subsystem. Controls all other boards in subsystem and performs all calculations and logic for subsystem functions.

- Digital I/O - Provides trip enable signals to the trip bus and receives bistable trip signals from other subsystems in the same IPC.

- Data Link (receive) - Three of these data links are required to receive bistable trip signals and bypass status from the three other IPC's.

7.1.1.3.1.4 Departure from Nucleate Boiling Ratio Subsystem (DNB) (This and FGl are one subsystem.)

This subsystem consists of a micro-computer card frame containing micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-9. This system receives analog process inputs and inputs from the data acquisition subsystem required to perform the DNB reactor trip logic and sends the DNB reactor trip signal to the trip bus. The DNB subsystem is comprised of the following board types.

- Data Link (receive/transmit) - Sends status information from the DNB subsystem to the data acquisition/auto tester subsystem.

- Central Processing Unit (CPU) - Main micro-computer for subsystem. Controls all other boards in the subsystem and performs all calculations and logic for subsystem functions.

- Non-Volatile Memory (NVRAM) - Provides for storage of constants and setpoints used by subsystem. These constants may be modified by the operator, but are retained upon loss of power.

- Analog I/O - Provides analog input signal conditioning for process inputs to the subsystem.

- Digital I/O - Parallel I/O board for processing digital inputs and outputs (such as DNB reactor trip output to trip bus) from the subsystem.

7.1.1.3.1.5 Function Group 1 and 2 Subsystems (FG 1/FG 2)

These subsystems each consist of a micro-computer card frame containing the micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-9.

The function group subsystems provide for the processing of analog inputs to the system that provide direct reactor trip signals to the trip bus. This system also provides status information from these channels to the data acquisition/auto tester subsystem. Each function group subsystem is comprised of the following board types:

- Data Link (receive/transmit) - Sends status information from the function group subsystem to the data acquisition/auto test subsystem.

- Loop Processor - Single board controller that provided analog input signal conditioning, bistable trip comparator function and parallel I/O output of reactor trip signal to trip bus. Independent loop processor boards are provided for each reactor trip function.

7.1.1.3.1.6 Nuclear Instrumentation System Subsystem (NIS) (This and FG2 are one subsystem.)

For installation of the detectors of the NIS, refer to Figure 7.1-3.

The NIS subsystem consists of a micro-computer card frame containing micro-computer cards to perform the required functions. This subsystem provides for the processing of analog process inputs and digital inputs required to generate the neutron flux reactor trip signals. These trip signals are then sent to the trip bus. The NIS subsystem is comprised of the following board types:

- Data Link (receive/transmit) - Sends status information from the NIS subsystem to the data acquisition/auto tester subsystem.

- Central Processing Unit (CPU) - Main micro-computer for subsystem. Controls all other boards in the subsystem and performs all calculations and logic for subsystem functions.

- Non-Volatile Memory (NVRAM) - Provides for storage of constants and setpoints used by subsystem. These constants may be modified by the operator, but are retained upon loss of power.

- Analog I/O - Provides analog input signal conditioning for process inputs to the subsystem.

- Digital I/O - Parallel I/O board for processing digital inputs and outputs (such as neutron flux reactor trip output to Trip Bus) from the subsystem.

7.1.1.3.1.7 Auto Tester and Data Acquisition Subsystem (AT/DA) Architecture

The AT/DA subsystem consists of a micro-computer card frame containing micro-computer cards to perform the functions indicated in the block diagram given in Figure 7.1-11. This subsystem provides a central data collection point. The AT/DA collects and transmits all data that is required by the plant safety monitoring system (PSMS), the integrated control cabinets (ICC), and the ACR computer. Automatic testing of the IPC is performed by this subsystem via data links to all other subsystems in the IPC. The AT/DA subsystem is comprised of the following board types.

- Data Base - Main CPU micro-computer for subsystem during normal operation. This board controls all other data link boards in the subsystem to manage the information collection from subsystems and to transmit the required data to the PSMS, ICC, and ACR computer. During normal operation, the data acquisition subsystem only receives data from the other subsystems in the IPC. No data is transmitted to these other subsystems.

- Test CPU - Main CPU board that controls all other data link boards in the subsystem during testing. This board provides all test features for the IPC. It controls analog and digital I/O to inject test signals into the various subsystems and monitors their response via the data link boards.

- Data Link boards for the following communication links:

  1. External cabinet communications to PSMS, ICC and ACR Computer.

  2. Inter subsystem communications w.thin the IPC.

  3. To simulate data links from the other IPC's during testing of the IPC.

- Digital I/O - Parallel I/O board for processing digital I/O to test panel (operator interface) and for any digital test point monitoring or signal injection.

- Analog I/O - Provides analog input signal conditioning for process inputs to the subsystem (that are being sent to the ICC or PSMS).

The methodology used for test signal injection and analog signal distribution is as follows. The analog input from the transmitter for a typical process input is routed to separate A/D converters for each subsystem that requires the signal. Test injection points are provided upstream of the A/D converters to allow the auto tester to inject simulated analog test inputs to the subsystem being tested without disrupting operation of the remaining subsystems. This method of analog signal distribution assures the functional independence of the various subsystems in the IPC.

7.1.1.3.2 Engineered Safeguards Features Actuation Cabinets

Each ESFAC consists of a two bay cabinet containing the following micro-computer subsystems (refer to Figure 7.1-12):

Engineered Safeguards Features System 1 CPU - ESF 1
Engineered Safeguards Features System 2 CPU - ESF 2
Automatic Tester

Figure 7.1-13 shows the ESFAC architecture.

The two ESF systems (ESF 1 and ESF 2) are redundant computer systems. Each of these receives the four data links from the IPC's via the data link cards shown. Two out of four voting and system level ESF logic is performed by the 2/4 logic CPU boards shown. Hard wired manual system level actuation switch inputs are incorporated into the ESF logic and the resulting system level commands are transmitted to the logic cabinets by means of the redundant data highway controllers. The system is arranged so that the logic cabinets will respond to system level commands from either ESF subsystem in a one out of two fashion. Continuous fault detection ensures that spurious commands are not generated.

The third micro-computer system in the ESFAC is the automatic tester system. This subsystem, under the control of the I&C technician, injects simulated data link signals (via its data link board) into one of the two ESF subsystems. It monitors the output data highways via the data highway control board to verify proper functioning of the ESF subsystem under test. The test CPU board, in addition to controlling this testing, disconnects the data highway signal from the ESF system under test to prevent spurious actuation. The test CPU also controls test computers in the logic cabinets, as slaves, to remotely test those cabinets. Via a separate data link board, the test CPU transmits the status of the ESFAC to the plant computer and post accident monitoring system.

7.1.1.3.3 Logic Cabinets

Each logic cabinet consists of a single bay cabinet containing a single micro-computer card frame and numerous I/O cards as shown in Figure 7.1-14.

The internal architecture of a typical logic cabinet is shown in Figure 7.1-15. Each logic cabinet will be capable of actuating approximately 30 (20 MOV's or 40 AOV's) components, thus seven logic cabinets per train would be required to accommodate the estimated 200 actuations. The actual number of logic cabinets would be determined by the final design of the fluid systems. The modularity of this architecture allows the I&C to be tailored to the specific plant design. The types of components actuated (i.e., switch- gear, MCC, AOV, etc.) could be mixed within any logic cabinet, however, the maximum layout benefit will be achieved if the actuations of a given type are grouped into individual cabinets.

7.1.1.3.4 Main Control Board Multiplexers

The MCB multiplexers consist of multiple micro-computer card frames. Each card frame in the system has redundant counterpart to provide interface to the two redundant data highways in each actuation train. Each card frame should be located in the MCB panel housing the controls it is servicing. This will reduce the amount of hard wiring that must leave each MCB panel since all control pushbutton and status light wiring will be internal wiring to the multiplexer card frame Digital I/O boards. The actual number of card frames will be determined by the number of inputs and outputs and by location in the various MCB panels.

Each MCB multiplexer card frame contains the following board types:

- Central Processing Unit - Main micro-computer board controls all other boards in the card frame.

- Data Highway Control - Provides interface to the data highway for communications with the logic cabinets.

- Digital I/O Cards - Provide for control pushbutton inputs to the system and provide status light outputs to the MCB. The number of cards of this type will be determined by the number of components being serviced by the card frame.

The PSMS multiplexer consists of two single bay cabinets. One receiving information from IPC channels I and III and one receiving information from IPC channels II and IV. Each cabinet contains a micro-computer card frame. This card frame contains the following board types.

- Central Processing Unit - Main micro-computer board controls all other boards in the card frame.

- Data Link (receive) - Three data links are required to receive data from two IPC's and one additional remote data collection point. This remote data collection is for information not used in the IPC, but required in the PSMS (Radiation monitoring for example).

- Digital I/O - These cards provide digital inputs to the System from any control push buttons required and provide digital outputs to drive status lights.

- Analog Output Cards - To drive analog displays in the PSMS.

- CRT Display Generator - To drive any CRT displays used for PSMS.

7.1.1.3.5 Inter Cabinet Communications (Refer to Figure 7.1-10)

A. IPC to IPC

Isolated fiber optic data links (refer to Figure 7.1-18) are used for these communications links. The global trip subsystem in each IPC

controls this communication link. These are standard one way (simplex) communications used to transmit bistable trip status between IPS's for use in two out of four reactor trip logic.

B. IPC to ESFAC

Two isolated fiber optic data links are required in each IPC. One associated with the train A ESFAC and one associated with the train B ESFAC. These data links are part of the ESF subsystem as they transmit bistable trip outputs to the ESFAC for use in safeguards actuation logic. These data links are one way links that only transmit data to the ESFAC's.

C. ESFAC to Logic Cabinets

Two redundant data highways are used for communications from the ESFAC to logic cabinets. Figure 7.1-1 shows this data highway for ESFAC A. This data highway provides for the transmission, by fiber optics, of ESF system level actuation signals to the logic cabinets and for the transmission of component status information back to the ESFAC (as required). The ESF actuation signals to the logic cabinets are transmitted redundantly over the two data highways. The logic cabinets are arranged to respond to an actuation signal from either data highway (one out of two). Extensive testing and error checking on this data highway prevent erroneous ESF actuation.

D. Logic Cabinets to MCB Multiplexer

Two redundant data highways are used for communication of component level switch inputs from the MCB to the logic cabinets. Component status information is transmitted, by fiber optics, from the logic cabinets to the MCB over both of the redundant data highways. These data highways are shown on Figure 7.1-2. Component status information on the data highways is also available to other logic cabinets for interlocking functions. The

logic cabinets are arranged to respond to a component level switch actuation signal from either data highway. Extensive testing and error checking on this data highway prevents erroneous component level actuations.

E. IPC to PSMS, ICC and ACR Computer

A single data link is provided from each IPC to each of these systems. These data links are fiber optic isolated, transmit only, from the IPC to each of the systems listed. These data links provide required information to the PSMS, ICC, and ACR computer such as bistable trips, permissive/trip status, interlocks to ICS, or any other required information.

F. ESFAC to ACR Computer and PSMS

A single data link is provided from each ESFAC to each of these systems. These data links are fiber optic isolated, transmit only, from the ESFAC to each system. They provide required information to the ACR computer and PSMS such as ESF actuation status, component status, or general cabinet operational/test status.

7.1.1.3.6 General Hardware Selection Guidelines

Standard board level products should be used to a great extent, however, some new boards will need to be developed. The output power interface boards in the logic cabinets fall into this new board category. These boards must have the ability to perform two out of three logic at the power interface (output switching) level. This is a new feature not in the old IPS design. This feature does dramatically improve the systems' fault tolerance and is felt to be desirable.

7.1.1.3.7 Off Normal Operation (Failure Tolerance, Maintenance, Test and Bypass)

The WAPWR IPS is designed with a high degree of reliability and fault tolerance. The following design guidelines demonstrate this capability.

- o 2/4 coincidence logic on all reactor trip actuations assures that any failure in a single protection channel cannot cause a spurious reactor trip or prevent a true reactor trip from occurring, if needed. This is true for all failures from the failure of a single instrument or component to the failure (loss of power) of an entire IPC.

- o Reactor trip actuation logic reverts to 2/3 coincidence logic if one channel is bypassed or in test. This assures that a single failure while in test will not cause a spurious reactor trip or prevent a true reactor trip from occurring, if needed. The logic permitting placing of channels in a bypass condition is denoted by "2/4-BYP" on the Logic diagrams. The following table summarizes the automatic voting logic associated with the number of inputs bypassed.

Number of Inputs Bypassed	Number of Remaining Inputs to Result in a Trip
0	two-out-of-four (2/4)
1	two-out-of-three (2/3)
2	one-out-of-two (1/2) (alarmed)
3	automatic trip
4	automatic trip

The bypass logic will be designed to allow the system to meet the single failure criterion while permitting operation for an indefinite period of time with one or two channels bypassed for testing or maintenance. The example of the reactor trip voting logic is shown in Figures 7.1-16 and 7.1-17.

The logic sections of the integrated protection cabinets will also process the manual system-level inputs involved in the reactor trip function. These inputs are listed on Table 7.2-3 and are shown on the functional diagrams, Figure 7.2-1, Sheets 2, 12, and 13. The voting logic for all parameters is shown on the functional diagrams.

The voting logic for reactor trip functions will be contained within each integrated protection cabinet (IPC). The reactor trip breakers operate on a deenergize to trip principle resulting in acceptable consequences of failure modes that deenergize.

- ESF actuation logic in ESFAC's is 2/4 coincidence logic for bistable trip inputs from the IPC's. This assures that a single protection channel failure cannot cause a spurious safeguards actuation or prevent a true safeguards actuation from occurring, if needed.

- ESF actuation logic is performed redundantly in each ESFAC. (Refer to Figure 7.1-13). Separate micro-computer card frames house this redundant logic so that any component failure related to one card frame (i.e., bus fault, board failure) cannot effect the other redundant card frame. The system level ESF actuation outputs are transmitted to the logic cabinets over two redundant data highways. This assures that a single data highway failure will not prevent ESF actuation. Extensive error checking is continuously performed on these data highways to prevent any failures from causing spurious actuation.

- Component level logic, in the logic cabinets, is threefold redundant (see Figure 7.1-15). The three redundant logic computers are contained in a single card frame with the automatic tester and two data highway controller boards. This is to allow each logic computer access to system level ESF actuation signals from both data highways. The logic computers are programmed to respond to ESF actuation signals from either data highway (one out of two logic). This assures that the failure of one data highway will not prevent ESF component level

actuations. The extensive error checking on the data highways will prevent data highway failures from generating spurious ESF component level actuations. The component actuation outputs from the logic computers is combined with the power interface cards in a two out of three voting scheme. This prevents a single failure in the power interface section from causing spurious actuation or preventing a required actuation. Block circuitry (to prevent final component actuation) is not required during testing of the power interface output devices as long as the power interface devices are tested one at a time.

During maintenance, these same features that provide for fault tolerance, allow the system to continue to operate with one channel or certain boards out of service for maintenance. Operation in this mode will, in some instances, increase the chances of a single failure causing a spurious actuation. Any IPC or transmitter associated with one channel set may be taken out of service for maintenance without plant shutdown. The data highways from the ESFAC's to the logic cabinets and from the logic cabinets to the MCB multiplexer's are redundant and one may be out of service, for maintenance, without directly causing plant shutdown. The logic computers in the logic cabinets are threefold redundant with two out of three coincidence logic on their outputs performed on the Power Interface cards. This permits one logic computer to be out of service, for maintenance, while the overall system remains operational operating in a one out of two mode for actuation.

Diverse protective functions in an IPC are implemented in separate subsystems (separate card frames). When the same process input is required by more than one subsystem, the analog signal is split and run separately to A/D inputs of all required subsystems. This design provides functional computer independence (e.g., DNB, ESF, NIS independence) to protect the functional diversity of the entire system.

7.1.1.3.8 Isolation Devices

Data can be multiplexed. Isolation devices will be used to preserve electrical independence of channel sets, and to ensure that no interaction will occur between non-safety systems and the safety system. The following topics are described in this subsection.

1. Isolation devices
2. Multiplexed data links

Isolation devices will be incorporated into selected IPC data links to preserve channel set independence. Isolation devices will serve to prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from being propagated to another circuit where independence of the two circuits will be required.

Optical coupling (see Figure 7.1-18) will offer improved physical and electrical isolation and separation since it will eliminate electrical conductive paths from receiving terminal to transmitting terminal.

Multiplexing

Multiplexing of digital signals offers an approach to reducing the amount of field wiring within and among elements of the integrated protection system, and from the IPS to non-safety areas.

7.1.1.3.9 Microprocessors

Distributed digital processing will be used in the integrated protection system.

Although the number of each type of element may vary, each microprocessor-based subsystem is typically composed of the following basic elements.

1. A Micro-processor-based Bus Controller/Processor
2. Software Programs
3. Memory
4. Interface Elements
5. Data Busses

The bus controller (microprocessor) would direct the data flow on the bus within the subsystem and would execute the program stored in memory. It may perform calculations, comparisons of values against setpoints, or coincidence logic operations. It could read data from memories or input interface devices, and could write data into memories or output devices.

The various program instructions which the microprocessor would execute are collectively referred to as software. The philosophy to be used in building the functional software packages for each microprocessor subsystem is detailed in Appendix 7B. The design approach will maintain strict control over nesting and interrupt levels allowable in each software module. Software modules will have single entry and exit points. Once placed into a read-only memory, these programs will not be alterable.

Memory would be used for data and instruction storage and could be of three types:

1. Read-only Memory (ROM)
2. Volatile Random Access Memory (RAM)
3. Non-volatile Random Access Memory

Read-only memory offers a secure method of storing the system program which would be executed by the microprocessor. It will retain information on loss of power and cannot be altered by electrical noise or by microprocessor malfunctions. The program instructions stored in this type of memory could only be read. The microprocessor will not be able to write data into this memory.

Volatile random access memory offers a read-and-write memory for temporary storage or as a "scratch pad" for calculations. This type of memory may be termed "shared" memory if another subsystem could also read and write into it. In this way, the results of one functional subsystem could be used by another subsystem.

Non-volatile random access memory would be used to hold constants such as fixed setpoints. The microprocessor could only read from the memory, but the constants could be updated locally by using appropriate threshold devices (such as thumbwheel switches) or a portable terminal. It is considered non-volatile since it will retain its information on loss of cabinet power. This permits a secure storage, yet one which is flexible enough to permit field changes for periodic updating.

Interface elements would connect the functional subsystems to specific input or output devices, exclusive of the data transmitters or receivers used in multiplexing. Input interfaces might be analog-to-digital converters, contact interfaces or specialty interfaces. Output interfaces might be undervoltage driver cards for the reactor trip breakers, outputs to integrated logic cabinets, etc.

The data busses would be the lines over which data is moved at the command of the micro-processor bus controller and would connect the various elements of the subsystem together.

Functions performed by the subsystems would be asynchronous in that each would run on its own clock, independent of any other in the system. Communication between subsystems would be through the shared memories. Thus one subsystem could write a result of its calculation into a shared memory to be used at will by a second subsystem. Functions would be performed one at a time by executing, in sequence, program instructions stored in the read-only memory and thereby sampling inputs, performing calculations, manipulating data, and generating outputs.

7.1.1.3.10 Built-in Test Capabilities

The safety system instrumentation will be designed to facilitate periodic testing from the sensor inputs of the integrated protection system through to the actuated equipment of the protective action system. Complete testing will be accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power would upset plant operation or destroy equipment, provisions will be made to test the equipment at reduced power or when the reactor is shut down.

With the exception of operating the final actuators, the test philosophy would be to manually initiate the test sequence, with the test itself proceeding with a minimum of operator intervention. Each integrated protection cabinet will be furnished with an automatic tester (AT/DA) when architecture is discussed in Subsection 7.1.1.3.1.7. This will include injection of reference analog signals into cabinet circuitry, verification of the accuracy of setpoints and other constants, and verification that proper signals appear at other locations in the system. Similar testers will be furnished for the ESFAC and logic cabinets except the test reference signals are all digital.

The test will begin with checking of the analog-to-digital converters over their range of operation, using injected reference signals. Verification of the signal processing algorithms will be made by exercising the test signal sources and observing the results up to and including the attainment of a channel partial trip or actuation signal at the power interface. The tester will automatically place in bypass the voting logic associated with the channel function under test.

The overlapping test sequence will continue by inputting digital test signals at the output side of the threshold functions in combinations necessary to verify the voting logic. Some of the input combinations to the coincidence logic will cause outputs such as reactor trips, safety injection initiation, etc. The reactor trip circuit breaker will be a 2/4 arrangement such that one

channel set tripping will not cause a reactor trip. (See Figure 7.1-17) Therefore, the trip signal generated as the result of the voting logic test could actually open its associated pair of trip breakers. However; to reduce wear on the breakers through excessive tripping and to avoid a single failure causing a plant trip while testing is in progress, the reactor trip channel under test will be bypassed. (The trip breakers will be, by manual means, allowed to be tripped once during the test.) The bypass will cause the trip logic to revert to two-out-of-three in the remaining reactor trip trains.

The automatic tester will not test the ESF actuators. This portion of the test will be accomplished by using the component-level actuation switches at the control board. These signals will enter the integrated logic cabinet at the interposing logic; and, therefore, will overlap the automatic testing of ESF. For those final devices that can be operated at power, without upsetting the plant or damaging equipment, the test will be performed by pressing the manual actuate control which will cause the device to operate. Position switches on the device itself will send a signal back to the integrated logic cabinet where it will be transmitted to the control board for display purposes. The display will verify that the manual command had been successfully completed, thus verifying operability of the final device. For those devices which can not be tested at power without damage or upsetting the plant, the manual test will be conducted from test switches at the ESFAC. These switches will block device actuation but will verify the continuity of the wiring up to the actuation device. Operability of the final equipment would be demonstrated at reduced power or at shutdown, depending on the equipment.

Operation procedures will prohibit testing two channel sets at the same time. There will be no built-in interlocks to prevent simultaneous testing of two integrated protection cabinets. However, the use of bypasses by the tester will ensure that the system could not be placed in an unsafe condition should the procedure prohibiting simultaneous testing be violated. For example, testing two cabinets would amount to two bypasses, which would cause the voting logic to revert to a 1/2 coincidence for the remaining two channels. Attempting to test three or four cabinets at the same time would cause a plant

trip. Therefore, the operational procedure restricting simultaneous testing of two or more cabinets will be made for operability reasons to avoid unnecessary trips.

The built-in on-line testing capabilities of the integrated protection system provisions include complete on-line overlapping testing of the IPS from the sensor inputs, through to the protective action system. In the case of the RCP speed sensor, the on-line test (i.e., the test made during reactor operation) of the input circuitry will be made through the use of the IPS built-in tester, starting from a point as close as practical to the sensor itself. For the front end of the circuit which includes the sensor itself, which is not tested by use of the IPS built-in on-line tester, testing during reactor operation will be accomplished by cross-checking between channels that bear a known relationship to each other and that have read-outs available. Thus the capability for sensor checks and for test and calibration are in accordance with Section 4.9 and 4.10 of IEEE-279-1971.

Periodic testing will be accomplished at a frequency identified in the Technical Specifications, Chapter 16.

In addition to periodic tests, the system will also be designed to perform continuous error detection and data link testing as part of the normal digital processing. Error detection will not involve error correction. Where practical the on-line error detecting features implemented in the IPS will be designed to automatically place the channel in which the error was detected into a trip or bypass mode (either by direct bypass or reconfiguration). In the case of the automatic trip mode the operator shall have the option to place that channel in a bypass mode in a short period of time. If the automatic action is not practical the on-line error detecting feature will be designed to cause alarm annunciation to the operator. The resolution for the specific action for each error detection feature would be determined during the R&D verification program.

Once designed, verified, and placed into read-only memory, the protection system software will be error-free. Therefore, on-line testing of the

software is not meaningful. Errors detected during periodic testing or by on-line diagnostics will have been caused by hardware malfunctions. This position for protection system software is based on two reasons. First, the software verification program will produce error-free software. The tight controls over the software design, implementation, and verification which can ensure that the software will be error-free is detailed in Appendix 7B. Second, the programs will be stored in read-only memory which can not be altered once the bit pattern is fabricated into the memory. Therefore, the software itself could not be altered by hardware malfunctions once placed into the microprocessor subsystem.

7.1.1.4 Protective Action System

The protective action system will be the "execute" portion of the safety system. It will accomplish protective functions on demand from the integrated protection system.

The protective action system will accomplish two types of protective functions; reactor trip and engineered safety features. The functions will be executed by "tripping" actuation devices which in turn will control motive power to the final actuated equipment. The protective action system will also furnish status feedback to the integrated protection system for interlocks and for transmission to the main control board for display.

Redundant segments of the protective action system will be called actuation trains. There will be two engineered safety features actuation trains (I and II), either of which can accomplish the safety feature. Train I will actuate fluid systems Train A components. Train II will interface with Fluid Systems Train B components. There will be four reactor trip actuation trains (I, II, III and IV), any two or more of which can cause reactor trip. The following subsections describe the reactor trip and safeguards actuation trains and their actuation devices and actuated equipment.

7.1.1.4.1 Reactor Trip Actuation Trains

The detailed description of each reactor trip function is given in Section 7.2. Each integrated protection cabinet will generate a reactor trip signal. Each signal will be transmitted over a hard wired data link to two reactor trip circuit breakers in the associated reactor trip actuation train. (See Figure 7.1-17) The eight circuit breakers (two in each of the four trains) will be interconnected in a two-out-of-four configuration. When the reactor trip actuation trains receive trip signals, the respective circuit breakers will open. Opening of the circuit breakers in 2 or more reactor trip actuation trains will interrupt the power from the rod control power supply (motor-generator sets) to the rod control cabinets. Interruption of power will deenergize the control rod mechanism gripper coils, which will release the latches to allow the control and shutdown rods to fall by gravity into the reactor core.

The reactor trip switchgear consists of eight circuit breakers arranged in a two-out-of-four matrix. These circuit breakers are located in two separate cabinets as shown in Figure 7.1-17. The RTS serves to trip the reactor by interrupting power to the control rod drive mechanisms which releases all control rods, thus allowing them to fall by gravity into the reactor core. Each set of two circuit breakers in the RTS receives a trip signal from one integrated protection cabinet. With this arrangement, two IPC's must trip signals to the RTS to cause a reactor trip. The trip is implemented by undervoltage trip attachments and shunt trip devices on the circuit breakers. To generate a reactor trip, the IPC interrupts power to the undervoltage trip attachments of the two circuit breakers under its control, as well as energizing the shunt trip attachment. Either device, UVTA or shunt trip attachment, will trip the breaker.

The RTS may be actuated manually from the main control board via reactor trip switches hard wired to the shunt trip and undervoltage coils on each circuit breaker.

Once tripped, the reactor trip circuit breakers will have to be manually reset before power could be reconnected to the rod control cabinets. The trip breakers can not be reset as long as the trip signals are present from the integrated protection cabinets.

Each reactor trip breaker will be a 3-pole device which can be electrically closed and opened from a remote location. All three poles will operate simultaneously when the breaker is closed or opened. The breaker can be opened by energizing its shunt trip coil or by deenergizing its undervoltage trip coil. During normal plant operation, the undervoltage coil and an interposing relay will be energized by a DC voltage supplied from the integrated protection cabinet. The interposing relay will have a normally closed contact wired in series with the coil of the shunt trip attachment so that the shunt trip opens the breaker when the interposing relay is deenergized. On an automatic reactor trip signal, the IPC will deenergize the undervoltage coil circuit and the interposing relay. This will cause the circuit breaker poles to open. A manual reactor trip initiated from the main control board will deenergize the undervoltage coil through its integrated protection cabinet, and will also separately energize the shunt trip coil directly. This will provide a backup to the undervoltage trip. The main contacts of the reactor trip breaker will be capable of interrupting the short circuit current of the rod control power supply system. Auxiliary switch contacts of the breaker will be used for feedback to the integrated protection cabinet.

The eight breaker logic configuration will permit testing of the reactor trip breakers without the use of auxiliary bypass breakers. The design will be such that the single failure criterion will be met while permitting operation for an indefinite period of time with one or two reactor trip actuation trains bypassed for testing, maintenance, or repair. The automatic tester in each IPC will be able to generate the channel set trip signal without causing a reactor trip. Actual trip of the breakers themselves is accomplished in the overlap portion of the test by operator action of the R.T. control switches in the IPC. During one bypass, the reactor trip logic will revert to a

two-out-of-three to trip design. During two bypasses, the logic will revert to a one-out-of-two design. Single failure criteria will still be met. See Subsection 7.1.2.2.11 for a description of reactor trip bypassing.

7.1.1.4.2 Safeguards Trains

Signals to initiate components of an engineered safety feature will be generated by the logic cabinets. The NSSS design will utilize a two-train safeguards design. The logic cabinets will interface the protection system with the two trains of the ESF protective action system.

The logic cabinets' power switching devices (relays, SCRs, triacs, etc.) will switch control power to the safequards actuation devices, which in turn will control motive power to the safeguards actuated equipment.

The safeguards actuation devices will consist of switchgear for controlling pumps and fan motors, Motor control centers for controlling motor-operated valves (MOVs) and small auxiliary motors, and solenoids for controlling air-operated valves (AOVs) and dampers.

The Switchgear circuit breakers, the motor control center starters and most of the solenoids will operate on an energize-to-actuate principle.

Auxiliary contacts on the actuation devices will provide status feedback to the integrated logic cabinets for providing position information to the control board and for interlocking functions when necessary. Position switches will provide status feedback and interlock information for solenoid-operated and motor-operated valves.

The safeguards actuated equipment will consist of pumps, fans, valves, and dampers as follows:

1. Safety injection pumps and valves

2. Containment isolation valves, Phase-A, which will isolate all non-essential process lines on safety injection.

3. Containment isolation, Phase-B

4. Emergency fan coolers

5. Emergency feedwater pumps

6. Emergency diesel generators

7. Feedwater isolation valves

8. Containment ventilation isolation valves and dampers

9. Steamline isolation valves

10. Containment Spray pumps and valves

11. Valves to terminate boron dilution

Section 7.3 correlates the actuated equipment to the various ESF actuation signals.

Fluid systems equipment in the safeguards trains will normally be labeled Train-A or Train-B. Train-A equipment will be actuated from ILC-A. Train-B equipment will be actuated from ILC-B. Either train alone will meet all the safeguards requirements.

7.1.1.5 Safety-Related Display Instrumentation

Safety related display instrumentation provides the operator with information to enable him to perform required manual safety functions and to determine the effect of manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in Chapter 15. Section 7.5 describes the safety related display instrumentation.

7.1.1.6 Essential Auxiliary Supporting Functions

The following systems will provide services such as cooling, lubrication, and energy supply, which may be required for safety system equipment to accomplish protective functions. The systems are listed here but are described in the referenced sections:

1. Instrument and control system power supply system (See Section 7.6)

2. Safeguards power supply system (See Chapter 8)

3. Emergency backup power supply system, including diesel generator support systems (See Chapter 8 of this module and Chapter 9 of RESAR-SP/90 PDA Module 13, "Auxiliary Systems")

4. Safeguards function portion of the service water system (See Section 9.2 of RESAR-SP/90 PDA Module 13, "Auxiliary Systems")

5. Service water component cooling water system (See Section 9.2 of RESAR-SP/90 PDA Module 13, "Auxiliary Systems")

6. Portions of the chemical and volume control system (CVCS) which will be shared with emergency core cooling (See Section 9.3 of RESAR-SP/90 PDA Module 13, "Auxiliary Systems")

7. Air conditioning, heating, cooling, and ventilation systems which will be necessary to maintain the environment for safety system equipment. (See Section 9.4 of RESAR-SP/90 PDA Module 13, "Auxiliary Systems" and Appendix 7A of this module)

8. Emergency lighting

On the auxiliary systems listed above, only the energy supply systems (1, 2, and 3), will be necessary for actuation of ESF functions. Reactor trip is implemented on a deenergize-to-trip principle. The remaining systems (4 through 7) will not be required for initiation of a protective function.

However, they may be required for proper functioning of actuated equipment some time after the protective function has been initiated.

7.1.1.7 I and C System Designers

Systems discussed in Chapter 7 will be supplied by Westinghouse. Interface information for integration and installation purposes is given in Appendix 7A.

7.1.1.8 Plant Comparison

The majority of functions performed by the RESAR-SP/90 I & C system will be similar to those performed by the Model 414 as documented in RESAR-414. The significant functional difference is Model 414 used a safety-grade RPI input into the DNB module, whereas, RESAR-SP/90 does not have safety-grade RPI input, because in determining radial core peaking factors the conservative assumption for the RESAR-SP/90 is made so that the rods are at their rod insertion limits.

The translation of functions into I & C system hardware does not result in significant differences between RESAR-SP/90 and RESAR-414 because both models employ similar micro-processor based systems.

Adequacy of the hardware and software will be demonstrated for the RESAR-SP/90 through a prototype verification and validation (V & V) program similar to the RESAR-414. Details on the prototype V & V program for RESAR-414 are documented in Reference 3.

7.1.2 Identification of Safety Criteria

7.1.2.1 Design Basis for Safety Systems

The design bases presented in this subsection apply to the safety system instrumentation described in Subsection 7.1.1. Specific design bases information for protective functions are given in Sections 7.2 for reactor trip and 7.3 for ESF. The design bases presented include those required by Section 3 of IEEE 279-1971.

7.1.2.1.1 Design Basis; Generating Station Conditions Requiring Protective Actions (Paragraph 1 of Section 3 of IEEE 279-1971)

The safety system described in Subsection 7.1.1 shall be designed to protect the health and safety of the public by limiting the release of radioactive material during Condition II, III, and IV events to acceptable limits as defined in Chapter 15. The events are summarized below:

Condition II Events

These events (faults of moderate frequency) are expected to occur at least once during the life of the plant and, at most, should result in a reactor trip with the plant being capable of returning to operation when the fault is corrected. These events should not result in any fuel damage. See Chapter 15 for Condition II events.

Condition III Events

These events (infrequent faults) are expected to occur once during the life of several plants. A small amount of fuel damage is acceptable in such an occurrence although the actual release of radioactive material must not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius of the plant. See Chapter 15 for Condition III events.

Condition IV Events

These events (postulated faults) are never expected to occur during the life of any plant. Any release of radioactive material in this type of event must not result in undue risk to the health and safety of the public. See Chapter 15 for Condition IV events.

In order to facilitate the design of the protection system, Westinghouse has chosen a number of specific limits on certain process and design variables which, if met, imply that the radioactive material release limits will be met with a high degree of confidence. These specific limits are defined on an accident by accident basis in Chapter 15.

7.1.2.1.2 Design Basis; Variables Required to be Monitored for Protective Action and Their Minimum Performance Requirements (Paragraphs 2 and 9 of Section 3 of IEEE 279-1971)

The variables required to be monitored for reactor trip and their ranges, accuracies, and response times are discussed in Subsection 7.2.1.2.2 and are listed on Table 7.2-4 and applicability of these trips to design basis transients and accidents is presented in Table 7.2-5.

The variables required to be monitored for engineered safety features actuation and their ranges, accuracies, and response times are discussed in Subsection 7.3.1.2.2 and are listed on Table 7.3-3.

The variables required to be monitored for post accident monitoring and their ranges and accuracies are discussed in Section 7.5.

The design shall conform to the requirements of Paragraph 4.8 of IEEE 279-1971. Conformance is discussed in Subsection 7.1.2.2.8.

7.1.2.1.3 Design Basis; Spatially Dependent Variables (Paragraph 3 of Section 3 of IEEE 279-1971)

The spatially dependent variables required to be monitored for the safety system are discussed in Subsection 7.2.1.2.3.

7.1.2.1.4 Design Basis; Protection During Various Reactor Operating Modes (Paragraph 4 of Section 3 of IEEE 279-1971)

The safety system shall be designed to assure that protective functions can be initiated and accomplished during various reactor operating modes. The following specific design bases apply.

1. Design Basis; Integrated Protection System Channel Bypass During Test of Maintenance.

The safety system shall be designed to permit the bypass - for maintenance, test, or repair - of any one protection channel in the group of channels monitoring a selected variable. The system shall be designed such that this bypass can be accomplished during power operation without causing initiation of a protective function. The system shall be designed to meet the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed.

With one channel bypassed, the system shall be designed to permit the bypass of a second channel in the group monitoring the same variable. In this mode, the failure of a third channel in the group may result in a protective function being initiated. The system shall be designed to meet the single failure criterion while permitting power operation for an indefinite period of time with two channels of the selected variable bypassed. Operation with 2 channels of one variable bypassed shall be alarmed in the control room.

The attempt to bypass three or more channels monitoring the same variable shall result in initiation of the protective functions associated with that variable.

The aspects of the design which permit channel bypass while maintaining immunity to inadvertent initiation of a protective function do not need to be applied to specific channels where the improved reliability is not deemed necessary.

The capability for channel bypass or removal from operation shall conform to the requirements established by Paragraphs 4.11 through 4.14 of IEEE 279-1971. Conformance is discussed in Subsections 7.1.2.2.11 through 7.1.2.2.14.

2. Design Basis; Protection System Blocks, Interlocks, and Permissives for Defined Reactor Operating Modes.

Where operating requirements necessitate automatic or manual block of a protective function, the system shall be designed such that the block will be automatically removed whenever the appropriate permissive conditions are not met. Devices used to achieve automatic removal of the block of a protective function shall be considered part of the safety system and as such shall be designed in accordance with the criteria in this section.

Interlocks are discussed in Sections 7.2, 7.3, and 7.6. The protection (P) interlocks are given on Tables 7.2-2 and 7.3-2. The safety analyses demonstrate that even under conservative critical conditions for either postulated or hypothetical accidents, the protective system will ensure that the NSSS will be put into and maintained in a safe state following an ANS Condition II, III or IV accident commensurate with applicable specifications and pertinent ANS criteria. Therefore, the protective systems will be designed to meet IEEE Standard 279-1971 and will be entirely redundant and separate, including all permissives and blocks. All blocks of a protective function will be automatically cleared whenever the protective function would be required to function in accordance with Paragraphs 4.11, 4.12 and 4.13 of IEEE Standard 279-1971. (See Subsections 7.1.2.2.11 - 7.1.2.2.13).

3. Design Basis; Multiple Setpoints Used During Defined Reactor Operating Modes

It is not necessary that setpoints in the IPS be made more restrictive as a function of operational mode and this subject is, therefore, not applicable to the WAPWR IPS.

4. Design Basis; Access to Protection System Bypasses, Blocks, and Setpoints

The system shall be designed to provide for administrative control over access to the means for manually bypassing protection channels and for manually blocking protective functions. The design shall also provide for administrative control of access to all setpoint adjustments, channel calibration adjustments, and test points.

The system shall be designed to the requirements established by Paragraphs 4.14 and 4.18 of IEEE 279-1971. Conformance to these requirements is discussed in Subsections 7.1.2.2.14 and 7.1.2.2.18.

7.1.2.1.5 Design Basis; Determination of Protective Action Setpoints (Paragraphs 5 and 6 of Section 3 of IEEE 279-1971)

The safety system shall automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset level.

The design shall conform to the requirements established by Paragraph 4.1 of IEEE 279-1971. Conformance to this requirement is discussed in Subsection 7.1.2.2.1.

7.1.2.1.6 Design Basis; Protection Against Natural Phenomena and Unusual Events (Paragraphs 7 and 8 of Section 3 of IEEE 279-1971)

The ability to initiate and accomplish protective functions shall be maintained during and following natural phenomena defined in Chapter 3 as credible to the plant site, such as earthquakes, tornados, hurricanes, floods, winds, etc. The safety system design shall ensure that performance requirements relative to plant safety are met despite degraded conditions in the plant caused by credible events such as fire, flooding, vehicular crashes, explosions, missiles, electrical faults, toxic or corrosive gaseous releases, pipe whip, etc.

Equipment shall be environmentally qualified to meet the accident conditions through which it is required to operate to mitigate the consequences of the accident. The equipment shall be seismically qualified to meet appropriate earthquake levels as described in Chapter 3 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design".

The design shall conform to the requirements established by Paragraphs 4.3, 4.4, and 4.5 of IEEE 279-1971. Conformance to these requirements is discussed in Subsections 7.1.2.2.3 through 7.1.2.2.5.

7.1.2.1.7 Design Basis; Protection Against Equipment Malfunctions

The ability of the safety system to initiate and accomplish protective functions shall be maintained despite credible equipment malfunctions within the safety system. Generally speaking, this basis forms the requirement for the safety system to meet the single failure criterion. To this end, the following specific design bases apply:

1. A single credible failure within the safety system shall not prevent initiation or execution of a protective function, even when channels are intentionally bypassed for test or maintenance for an indefinite period of time.

2. Where signals are derived from protection channels for control, no credible single failure in the protection channel shall cause a control system action requiring protective action by the redundant channels monitoring the same variable.

3. Where signals are derived from protection channels for non-safety systems, no credible failure in the non-safety system shall prevent the protection system from meeting its performance requirements.

4. No single failure within the protection system shall cause a Condition II event (see Chapter 15) to progress to a Condition III event, or a Condition III event to progress to a Condition IV event.

The system shall be designed to meet the single failure criterion, as established by Paragraph 4.2 of IEEE 279-1971. Conformance to this requirement is discussed in Subsection 7.1.2.2.2. Prevention of control system interaction with the protection system shall be designed to the requirements of Paragraph 4.7 of IEEE 279-1971. Conformance is discussed in Subsection 7.1.2.2.7.

7.1.2.1.8 Miscellaneous Design Bases

1. Manual Actuation of Protective Functions

   Means shall be provided in the control room for manual initiation of all protective functions at the system level. Manual actuation shall rely on the minimum of equipment and, once initiated, should go to completion unless deliberate operator intervention is taken. Failure in the automatic initiation portion of a system-level function shall not prevent the manual initiation of that function.

   The system shall be designed to comply with the requirements established by Paragraphs 4.16 and 4.17 of IEEE 279-1971. Conformance to these requirements are discussed in Subsections 7.1.2.2.16 and 7.1.2.2.17.

2. Physical Identification of Protection System Equipment

   In order to provide assurance that the design bases given in this section can be applied in the design, construction, maintenance, and operation of the plant, all safety systems equipment shall be identified distinctly as being in the protection system. Markings shall be different for each redundant division of the safety system.

   The design shall conform to the requirements established by Paragraphs 4.22 of IEEE 279-1971. Conformance to this requirement is discussed in Subsection 7.1.2.2.22.

3. Capability for Checks, Test, Calibration, and System Repair

The system shall be designed to permit checking the operational availability of each input sensor to the integrated protection system during reactor operation.

Capability shall be provided for testing and calibrating the channels and channel set equipment of the integrated protection system.

The system shall be designed to facilitate the diagnosis, location, and repair or adjustment of malfunctioning components.

The system shall be designed to conform to the requirements established by Paragraphhs 4.9, 4.10, and 4.21 of IEEE 279-1971. Conformance to these requirements is discussed in Subsections 7.1.2.2.9, 7.1.2.2.10, and 7.1.2.2.21.

4. Information Read-Out

The system shall be designed to permit identification of protective actions down to the channel level. The system shall be designed to provide the operator with information on the status of safety system equipment.

The design shall conform to the requirements established by Paragraphs 4.19 and 4.20 of IEEE 279-1971. Conformance is discussed in Subsections 7.1.2.2.19 and 20.

7.1.2.2 Conformance of the Safety System Instrumentation to Applicable Criteria

The safety system instrumentation described in Subsection 7.1.1 will be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. Table 7.1-1 lists applicable General Design Criteria, NRC Regulatory Guides and Branch Technical

Positions and Industry Standards. The table also identifies where the subject of the applicable standard or criteria is discussed within the Safety Analysis Report.

The design will conform to the requirements concerned with the I&C portion of the safety system as discussed below. The topics are listed in the order in which they appear in Section 4 of IEEE 279-1971 since that standard umbrellas all requirements of the I&C portion of the safety system. Other criteria related to the IEEE 279-1971 requirements are also identified.

7.1.2.2.1 Conformance to General Functional Requirements (Paragraph 4.1 of IEEE 279-1971, GDC-13, GDC-15, Regulatory Guide 1.105)

The safety system will automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset value. The protective actions are identified in Subsection 7.1.1.1. Reactor trip functions are discussed in detail in Section 7.2 and engineered safety features in Section 7.3. Also provided in those sections are the ranges, accuracies, and typical response times on each variable to be used in generating a protective action.

Westinghouse will use three groups of values in determining reactor trip and engineered safety features actuation setpoints.

The first group of values will be the safety limits assumed in the accident analyses (Chapter 15). These will be the least conservative values.

The second group will consist of limiting values as listed in the Technical Specifications. These will be the maximum/minimum "ALLOWABLE VALUES" for Limiting Safety System Settings (LSSS) and Limiting Conditions for Operation (LCO) given in Chapter 16 of the integrated RESAR-SP/90 PDA document. Limiting values will be obtained by subtracting a safety margin from the accident analysis values. The safety margin will account for instrument error, calibration uncertainties, and process uncertainties such as flow stratification and transport factor effects, etc.

The third group will consist of the nominal values set into the equipment. These values will be obtained by subtracting allowances for instrument drift from the limiting values. The nominal values will allow for normal expected instrument setpoint drift such that the Technical Specification "Allowable Values" will not be exceeded under normal operation. These values are given as the "TRIP SETPOINTS" in Chapter 16 of the integrated RESAR-SP/90 PDA document.

As illustrated above, the trip setpoint will be determined by factors other than the most accurate portion of the instrument's range. The only requirement on the instrument's accuracy value is that over the instrument span, the error must always be less than or equal to that assumed in the accident analyses. The instrument does not need to be the most accurate at the trip setpoint value as long as it meets the minimum accuracy requirements.

Range selection for the instrumentation will cover the expected range of the process variable being monitored consistent with its application. The design of the integrated protection system will be such that trip setpoints will not require process transmitters to operate within 5 percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the integrated protection system stipulate the maximum allowable errors on accuracy, linearity, and reproducibility. The protection channels will have the capability for and will be tested to ascertain that the characteristics throughout the entire span are acceptable and meet functional requirements specifications.

In this regard it should be noted that specific functional requirements for response time, setpoint, and operating span will be finalized contingent on the results and evaluation of safety studies to be carried out using data pertinent to the plant. Emphasis will be placed on establishing adequate performance requirements under both normal and faulted conditions. This will include consideration of process transmitter margins such that even under a highly improbable situation of full power operation at the safety limits that adequate instrumentation response is available to ensure plant safety.

7.1.2.2.2 Conformance to the Single Failure Criterion (Paragraph 4.2 of IEEE 279-1971, IEEE 379-1972, Regulatory Guide 1.53)

Any credible single failure within the integrated protection system will not prevent the initiation or accomplishment of a protective function at the system level.

Redundancy and functional diversity will be designed into the safety system to ensure that system performance requirements can be met even if the safety system is degraded by a single random failure. Redundancy will begin with the sensors monitoring the variables and will be carried through the signal processing and actuation electronics. Redundant actuation trains will also be provided. Subsections 7.1.1.2 and 7.1.1.3 describe the redundant nature of the safety system architecture. In addition, generally two or more diverse functions will initiate most protective actions. Diversity of protective functions is discussed in Section 7.2 for reactor trip, and in Section 7.3 for engineered safety features actuation.

Isolation devices will be incorporated into data links which connect redundant channel sets, or which carry signals to non-safety systems. The isolation devices will be tested to verify that credible faults, such as physical damage, short circuits, open circuits, or the application of credible fault voltages on the devices output terminals, do not propagate back to the isolator's input terminals. The isolation devices provide assurance that, where protection signals are used by non-safety systems, that credible single failures in the non-safety system will not degrade the performance of the safety system.

It is a design goal to minimize inadvertent reactor trips and safeguards actuations. Dual redundancy will be used in critical circuits which could malfunction and give an erroneous trip or ESF initiation signal. The reactor trip circuit breaker arrangement illustrated in Figure 7.1-19 and described in Subsection 7.1.1.3.1 will be designed such that a single failure will not cause a reactor trip. The two-out-of-four actuation train logic for reactor trip will require trip signals from two out of four channels sets. Although

two safeguards actuation trains will be used, the actuation logic for each component will be performed redundantly within each ESFAC and will be "ored" in the logic cabinets. This dual logic is described in Subsection 7.1.1.2.4. It will be provided to minimize the probability of a random single failure causing total loss of an ESF train. It will also enable the ESF actuation logic to meet single failure criterion during periodic testing.

The design approach chosen to reduce the likelihood of inadvertent trips or safeguards actuations will not negate the ability of the safety system to meet the single failure criterion, even when channels are bypassed for test or maintenance. Redundancy of equipment and the design bases applied to bypass capability will ensure compliance to the single failure criterion.

7.1.2.2.3 Conformance to the Requirements for Quality Components and Modules (Paragraph 4.3 of IEEE 279-1971, GDC-1)

Components and modules will be of a quality that is consistent with use in a nuclear generating station protection system. Chapter 17 describes the Westinghouse quality assurance program.

7.1.2.2.4 Conformance to the Requirements for Equipment Qualification (Paragraph 4.4 of IEEE 279-1971, GDC-2, GDC-4, GDC-13, IEEE 323-1974, IEEE 344-1975, Regulatory Guide 1.89, Regulatory Guide 1.100, EICS-10)

Electrical equipment within the safety system will be environmentally qualified to meet the accident conditions through which it must operate to mitigate the consequences of the accident. The environmental qualification program for Class 1E electrical equipment is discussed in Section 3.11 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design".

The equipment will be qualified to the appropriate earthquake intensity as established in Chapter 3 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design". The seismic qualification program is discussed in Section 3.10 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design".

Equipment locations shall be chosen such that the forces to which equipment has been qualified (see Section 3.10 and 3.11 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design") are not exceeded.

7.1.2.2.5 Conformance to the Requirements to Maintain Channel Integrity (Paragraph 4.5 of IEEE 279-1971, GDC-2, GDC-3, GDC-4, Regulatory Guide 1.120)

The safety system instrumentation will be designed to maintain its capability to initiate its protective functions during and following natural phenomena defined in Chapter 3 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design" as credible to the plant site, such as earthquakes, tornados, hurricanes, floods, winds, etc. Functional capability will be maintained despite degraded conditions that may exist in the plant due to credible events such as fires, flooding, vehicular crashes, explosions, missiles, electrical faults, toxic or corrosive gaseous releases, pipe whip etc. The equipment will be environmentally and seismically qualified as discussed in the preceding subsection.

As noted in Chapter 3 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design" and Appendix 7A, the balance of plant applicant will normally be responsible for providing physical protection for Westinghouse supplied safety equipment against damage from natural phenomena or credible events external to the equipment. The NSSS integrated protection system design facilitates such protection by providing the balance of plant designer a defense-in-depth approach in providing protection through a combination of barriers, physical separation, and analyses. For example, safety equipment could be located based on an analysis of potential hazards such that the equipment is outside the zone of influence of the hazard. Or the redundant elements of the safety system might be located in defined zones such that a damaging event in one zone would not affect redundant equipment in other zones. Or, the safety equipment could be bunkered or shielded such that defined potential hazards would not physically damage equipment or wiring. Safety equipment will, of course, be qualified to meet the accident environments for which it is assumed in Chapter 15 to operate. (See Sections 3.10 and 3.11 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design")

Redundancy of equipment will ensure that protective functions can be accomplished despite loss of one of the redundant channel sets or actuation trains due to a credible event.

The integrated protection system will be structured such that the communication between redundant channel sets will occur at the integrated protection cabinets and ESFA cabinets. Cabinets processing low-level signals can be located in well-controlled areas of the plant. Communication among channel sets is over isolated, data links. The isolation devices will prevent credible electrical and physical faults in one channel set from propagating back to another channel set. A description of the isolators is contained in Subsection 7.1.1.2.5. The ESFA cabinets will not communicate with each other but will communicate with each IPC and will interface with high energy source safeguards actuation devices at the power interface for their respective train devices. They, therefore, may normally be located in the more hazardous areas of the plant. Therefore, the design provides for complete physical separation and electrical independence of these cabinets. All signals which leave the integrated protection system from the integrated protection cabinet to non-safety systems are via isolated data links.

Concerning potential hazards that may be caused by supplied equipment, every effort will be made to identify and eliminate potential causes of fire, missiles, etc. that might occur due to postulated faults within the equipment. Equipment will be built to accepted industry codes, standards, and practices aimed at maximizing reliability and safety. For example, wiring used within electrical equipment, and devices used to protect wiring from overcurrent (such as breakers, fuses, and current limiters), will be sized and coordinated according to National Electric Code requirements. Insulation used will be flame retardant and will meet National Electric Code, IEEE, and Underwriter's Laboratory requirements applicable to the environment in which the wiring will be located. Electronics will be housed in cabinets of metal construction coated with intumescent paint. As stated above, isolation devices will be incorporated into wiring leaving the protection cabinets to the other redundant protection cabinets or non-safety area. The independence of electrical equipment will be assured as discussed in Subsection 7.1.2.2.6 below.

7.1.2.2.6 Conformance to the Requirements to Maintain Channel Independence (Paragraph 4.6 of IEEE 279-1971, GDC-22, IEEE 384-1974, Regulatory Guide 1.75)

The flexibility of the IPS will enable the achievement of maximum physical separation of redundant BOP equipment commensurate with the hazard potentials identified for each location.

Where redundant equipment must communicate with each other, such as at the integrated protection cabinets, isolation devices will be employed to preserve physical and electrical independence of the channel sets. These devices are described in Subsections 7.1.1.2.5 and 7.1.2.2.7. They will also be used to preserve the independence of safety equipment from non-safety systems which may use protection signals.

Non-safety wiring will be separated from class 1E wiring by the maximum practical distances. Analyses, tests, or physical barriers will be used to ensure the adequacy of wire routing where separation distances are less than those suggested by Regulatory Guides or industry standards.

The physical separation criteria for IPS cabinets will include the applicable recommendations contained in Paragraph 5.6 of IEEE 384-1974. Specific requirements to be applied will be as follows:

1. Internal separation requirements pertaining to separation between redundant class 1E equipment in accordance with Subparagraph 5.6.2 of IEEE 384-74.

2. Non-class 1E wiring requirements pertaining to separation between class 1E wiring and non-class 1E wiring in accordance with Subparagraph 5.6.5 of IEEE 374-74.

3. Cable entrance requirements of redundant Class 1E cables in accordance with Subparagraph 5.6.6.

It is noted that the application of this criteria to instrumentation cabinets is endorsed by Regulatory Guide 1.75.

Wiring for redundant channel sets and actuation trains will employ physical separation, analyses, isolation, tests, or barriers to ensure independence of the circuits.

Additional physical separation criteria applying to installation of redundant Class 1E wiring is contained in Appendix 7A.

7.1.2.2.7 Conformance to the Requirements Concerning Control and Protection System Interaction (Paragraph 4.7 of IEEE 279-1971, GDC-24)

Conformance to the Requirements on the Use of Isolation Devices

The transmission of signals from protection system equipment for control system use will be through isolation devices. These devices will be classified as part of the protection system and will meet all of the requirements of Section 4 of IEEE 279-1971. The isolation devices will be tested to confirm that credible failures at the output of the isolation device will not prevent the associated protection system channel from meeting the minimum performance requirements.

The isolation device is described in Subsection 7.1.1.2.5. Credible failures to which the devices shall be tested are physical damage, short circuits, open circuits, grounds, and the application of the maximum AC or DC potentials as may be present in any cabinet in which the isolation device is located or in any wireway in which its electrical or optical lines run.

Conformance to Requirements Concerning Control System Failures Interacting with the Protection System

The protection system will be designed to permit margin to safety limits such that an unsafe condition will not be caused by transients induced by normal power plant operation. The plant control system will attempt to keep the

reactor operating away from any safety limit. Should a control system fail and cause a parameter to approach its limit, the protection system will trip the reactor as described in Section 7.2. The setpoints will be chosen to assure that the design bases established for credible events are met (see Subsection 7.1.2.2.1). The accident analyses in Chapter 15 will not assume a control system action to reduce the severity of an accident. Assumptions made on control systems will be worst case assumptions - that their failure will drive the parameters involved toward their worst direction for safety. The safety system setpoints will thus account for these malfunctions.

As previously described, isolation devices will be employed to prevent credible faults in the control system from degrading the functional capability of the protection system.

Conformance to Requirements Concerning Protection System Failures Interacting with Control Systems

It is advantageous to use certain information derived from protection channels to control the plant. This concept reduces the number of penetrations into critical pressure boundaries, such as into the coolant loops, pressurizer, steam generators, etc. It also helps reduce congestion and ease separation in difficult plant areas such as in equipment compartments in the containment and at containment penetrations.

Where protection signals are used for control, functional isolation will be provided between the control and protection systems.

A control system channel selection device will be used to ensure that malfunctioning protection channels will not send erroneous information to the control system. In this way, protection system malfunctions in a channel can not cause a control system action that will result in a protection function actuation using the remaining redundant channels monitoring that variable.

The selection device will continuously monitor the redundant channels which will be sending information to the control systems. The device will only pass

on to the control system those signals which are considered valid. If a signal is determined to be invalid by the channel selection device, it will not be passed on to control.

As long as at least three redundant channels of information are available, an invalid signal can be rejected by the selection device. This is done by comparing the redundant channels to one another and rejecting any one which deviates from the others by more than a reasonable amount, consistent with normal instrument channel drift and calibration tolerances. A detailed discussion of the signal selection algorithm used is made in Reference 2.

7.1.2.2.8 Conformance to Requirements Concerning the Derivation of System Inputs (Paragraph 4.8 of IEEE 279-1971)

To the extent feasible and practical, protection system inputs will be derived from signals that are direct measures of the desired variables. These variables are listed in Table 7.2-4 for reactor trip and Table 7.3-4 for engineered safety features actuation.

The protection system will calculate two variables where direct measurement is not feasible. These are the low DNBR reactor trip and the high Kilowatts per foot (KW/ft) reactor trip. These functions are described in Subsection 7.2.1.1.2.

7.1.2.2.9 Conformance to the Requirements to Provide Capability for Sensor Checks (Paragraphs 4.9 of IEEE 279-1971, IEEE 338-1975, Regulatory Guide 1.118)

Means will be provided for checking with a high degree of confidence the operational availability of each system input sensor during reactor operation. These will be accomplished by one of the following techniques:

1. By perturbing the monitored variable; or

2. By cross checking between channels that bear a known relationship to each other and that have read-outs available; or

3. By introducing any varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable.

7.1.2.2.10 Conformance to the Requirements to Provide Capability for Test and Calibration (Paragraph 4.10 of IEEE 279-1971, GDC-10, GDC-21, IEEE 338-1975, Regulatory Guide 1.22, Regulatory Guide 1.118, EICSB-5, EICSB-22)

Capability will be provided for testing and calibrating channels and devices used to derive the final system output signal from the various channel signals.

Subsection 7.1.1.2.7 describes the built-in testing capabilities of the integrated protection system. These capabilities will provide for complete on-line overlapping testing of the IPS from the inputs to the analog-to-digital converters, through the logic, to the actuation devices in the protective action system.

As permitted by Regulatory Guide 1.22, where actuated equipment is not tested during reactor operation, it will be established that:

1. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant;

2. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation; and

3. The equipment can routinely be tested when the reactor is shutdown.

It is anticipated that the following equipment shall not be tested on-line at full power:

1. Manual system-level actuation switches for protective functions.

2. Actual tripping of the turbine, although one-at-a-time testing of individual trip fluid dump solenoids can be performed on Westinghouse turbines.

3. Closure of main steam isolation valves. (These may be tested at reduced power).

4. Full closure of the feedwater isolation or control valves.

5. Tripping of the main feedwater pumps.

6. Isolation of cooling water services for the reactor coolant pumps.

Where channels are bypassed for the purposes of testing, these will be automatically indicated and removed by the built-in tester. Bypass capability is discussed in Subsection 7.1.2.2.11.

7.1.2.2.11 Conformance to Requirements on Channel Bypass or Removal from Operation (Paragraph 4.11 of IEEE 279-1971)

Provisions will be made within the integrated protection system for the application of bypasses, i.e., blocks of certain protective functions during operational modes such as test and maintenance. The bypass system will be designed in such a way that applicable criteria are met, including the single failure criterion, which is discussed in Subsection 7.1.2.2.2.

Channel Level Bypass Capability

A typical protection channel set will take inputs from one or more process sensors, perform some compensation or other calculation, and will terminate in one or more threshold functions where the process variable will be compared against setpoints. The partial trip outputs from these comparisons will be sent to the logic portion of the protection system where signals will be with the partial trip status of the other system where signals will be combined with the partial trip status of the other channels to initiate a protective

function, such as reactor trip. When a channel is to be tested, the sensor input will be removed and a test signal will be injected in its place, and will be exercised over the range of that input sensor. This method of testing will produce the need for blocking the partial trips to preserve plant availability. The bypass system will provide this plant availability while at the same time it will assure compliance to the single failure criterion. Each comparison function will be provided with a bypass, which will become an additional input to the logic which is downstream of the threshold functions. Interlocks will be provided so that the gate, which will admit the injected test signal to the channel, cannot be closed until all of that channel's threshold functions have been bypassed. The logic which will combine four threshold function outputs and their associated bypasses in a scheme which will always meet the single failure criteria, irrespective of the number of bypasses applied, is considered proprietary by Westinghouse. A description and evaluation of this logic is contained in a separate report (Reference 1). The effect of this logic scheme will be to provide a two-out-of-four coincidence logic which will revert to a two-out-of-three or a one-out-of-two logic when one or two bypasses are applied respectively. If three or more bypasses are simultaneously applied, the logic scheme will provide the necessary output to initiate the protective action in question, generally leading to a plant shutdown.

The bypass status, along with the threshold function outputs, will be transmitted between integrated protection cabinets by means of the isolated data links described in Subsection 7.1.1.2.5.

In addition to using the bypasses during channel test, they will be used while maintenance is being performed on the channel or if the channel sensor is failed and cannot be immediately repaired.

Although there will generally be four protecton channels for each actuation function, all accident analyses or reliability studies will assume that one of these channels is in the bypass mode at the time of the accident. The purpose for this assumption will be to preclude any potential limitations which might have otherwise been placed on the use of the bypass system.

Reactor Trip Breaker Bypass Capability

A reactor trip will be actuated by opening any two of four of the pairs of reactor trip breakers, one pair being associated with each of four integrated protection cabinets. The breakers will be arranged such that the opening of any two pairs of breakers will de-energize the control rod drives, thus causing the reactor trip. See Subsection 7.1.1.4.1. During maintenance or except once during testing of the trip actuation logic, the trip signals going to the undervoltage coils of the reactor trip breakers will be blocked. The logic for performing this bypass function is shown on Figure 7.2-1, Sheet 1. A description and evaluation of the logic is contained in Reference 1. The logic will automatically ensure that no more than one pair (one actuation train) of breakers can be bypassed at any one time. In the event that an attempt to bypass the breakers from one channel set occurs while another channel set is in the bypass mode, those breakers will be tripped rather than bypassed. Then if a trip signal is generated by either of the two remaining channel set (one-out-of-two) the reactor will trip. If more than two bypasses are actuated at a given time, the reactor will be tripped directly. The breaker bypass status will be communicated between the integrated protection cabinets by the same system of isolated data links which carry the partial trip information. If a trip of two remaining pairs occurs while one is in bypass, then that one will be tripped as well.

Bypass of Engineered Safety Features

No ESF system-level actuation logic bypasses (for test or maintenance) will be provided. Instead, all of the actuation logic within the ESFAC cabinet will be in duplicate. Built in test capabilities are discussed in Subsection 7.1.1.3.10.

7.1.2.2.12 Conformance to Requirements on Operating Bypasses (Paragraph 4.12 of IEEE 279-1971)

In addition to the test and maintenance bypasses described in the previous section, several operating bypasses will be provided. These bypasses will

automatically block certain protective actions which would otherwise prevent modes of operations such as start-up, etc. All of the operating bypasses will be automatically removed when the plant moves to an operating regime where the protective action would be required if an accident occurred. These operating bypasses are discussed in more detail in Subsections 7.2.1.1.9 and 7.3.1.1.11.

7.1.2.2.13 Conformance to Requirements to Provide Indication of Bypasses (Paragraph 4.13 of IEEE 279-1971, Regulatory Guide 1.47, EISCB-21)

Status indication for the channel level and the reactor trip breaker bypasses described in Subsection 7.1.2.2.11 will be provided in the control room. The display of the status information will be such that the operator can identify the specific function(s) which is bypassed, and also determine if the logic has reverted to 2/3 or 1/2. In addition to the status indication, an alarm will be sounded in the control room if more than one bypass has been applied to a given protection function, thus causing 1/2 logic. The bypass indication system will be a balance-of-plant design. Westinghouse will supply the necessary IPS bypass status outputs for use by the balance-of-plant designer.

7.1.2.2.14 Conformance to Requirements Controlling Access to the Means for Bypassing (Paragraph 4.14 of IEEE 279-1971)

The bypasses described in Subsection 7.1.2.2.11 could be initiated in either of two ways, automatically via the automatic test system or manually via bypass switches. In either case, the operator will have complete administrative control over bypass actuation. The automatic test sequence bypass will be manually initiated and the manual bypass switches will be located inside the integrated protection cabinets. The IPC doors will be locked under administrative procedures.

7.1.2.2.15 Conformance to the Requirements on the Use of Multiple Setpoints (Paragraph 4.15 of IEEE 279-1971, EICSB-12)

This subject is not applicable to the WAPWR IPS because it is not necessary that setpoints be made more restrictive as a function of operational mode.

The safety system will use two such setpoints; one will be the continuously calculated setpoint for low DNBR reactor trip, and the other will be the continuously calculated KW/ft value which will be compared against a fixed setpoint. Subsection 7.2.1.1.3 provides a discussion of these trips. In each case the value computed will be based on the operating conditions and the protection needed during those operating conditions.

The nuclear channels will use three ranges of instrumentation (source, intermediate, and power range) - each with fixed setpoints. These setpoints will provide protection during startup and could be blocked by manual control as described in Subsections 7.2.1.1.1 and 7.2.1.1.9. Protection will be automatically reinstated when power falls below the applicable permissive levels.

7.1.2.2.16 Conformance to the Requirement for Completion of Protective Action Once it is Initiated (Paragraph 4.16 of IEEE 279-1971, Regulatory Guide 1.62)

Once initiated, protective functions at the system level will go to completion. The action of engineered safety features could be terminated on a component-by-component basis by deliberate operator intervention. Component-level manual reset controls will permit the operator to take this action only after the system-level signal is reset. One of the reasons component reset will be provided is to terminate ESF functions should they be inadvertently actuated. Specific information is provided in Subsections 7.2.2 and 7.3.2 for reactor trip and engineered safety features, respectively.

7.1.2.2.17 Conformance to the Requirements for Manual Initiation of Protective Functions (Paragraph 4.17 of IEEE 279-1971, Regulatory Guide 1.62)

Means will be provided for manual initiation, of protective functions at the system level. Manual initiation circuits will conform to the single failure criterion as described in Subsection 7.1.2.2.2. The specific manual actions are described in Section 7.2 for reactor trip, and in 7.3 for engineered safety features.

The hardware which will be involved in manual actions is discussed in Subsection 7.1.1.2.3 for reactor trip manual actions which will input to the integrated protection cabinet, and in Subsection 7.1.1.2.4 for the safety-level ESF manual actions which will input to the integrated logic cabinets. Table 7.2-3 lists system-level manual actions to the integrated protection cabinets, and Table 7.3-3 lists system-level manual actions relative to engineered safety features.

Manual initiation will depend on the operation of the minimum of equipment. No single failure in either the automatic portion, manual portion, or shared portion will prevent manual or automatic initiation of a protective function at the system level. This capability will be achieved through the redundant structure of the integrated protection system.

7.1.2.2.18 Conformance to Requirements Governing Access to Setpoint Adjustments, Calibration, and Test Points (Paragraph 4.18 of IEEE 279-1971)

Access to all setpoint adjustments, module calibrations, and test points will be under administrative control. Cabinet doors will be locked.

7.1.2.2.19 Conformance to the Requirements on Identification of Protective Actions (Paragraph 4.19 of IEEE 279-1971)

The initiation of a protective action will be identified and indicated down to the channel level. Except for post-accident monitoring information, this status information will not be consider safety-related. As such it will be transmitted to the main control board over isolated, data links from the protection system, for indication and recording.

7.1.2.2.20 Conformance to the Requirements for Information Read-Out (Paragraph 4.20 of IEEE 279-1971, Regulatory Guide 1.97)

The protective system design will provide for status information to be provided to the operator. Status information may be of four types; (a)

parameter values, (b) logic status, (c) equipment status, or (d) actuation device status. Safety relay displays are discussed in Section 7.5.

7.1.2.2.21 Conformance to the Requirement to Facilitate System Repair (Paragraph 4.21 of IEEE 279-1971)

The integrated protection system will be designed to facilitate the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in test capability described in Subsection 7.1.1.2.1 will provide a mechanism for periodically verifying the operability of all modules in the IPS, and of rapidly locating malfunctioning assemblies. Continuous on-line error checking will also detect and locate problem areas. Channel bypass will permit replacement of malfunctioning sensors or channel components without jeopardizing plant availability while still meeting the single failure criterion.

7.1.2.2.22 Conformance to the Requirements for Identification of Redundant Safety System Equipment (Paragraph 4.22 of IEEE 279-1971)

Distinctive markings will be applied to redundant segments of the integrated protection system and protective action system.

The color coded nameplates described below provide identification of equipment associated with protective functions and their channel set or actuation train associations.

Channel Set or Actuation Train	Color Coding
(I); (or Train-A)	RED with WHITE lettering
(II); (or Train-B)	WHITE with BLACK lettering
(III)	BLUE with WHITE lettering
(IV)	YELLOW with BLACK lettering

All non-cabinet mounted protective equipment and components will be provided with an identification tag or nameplate. Small electrical components such as relays will have nameplates on the enclosure which houses them.

Refer to Appendix 7A; Section 7A.2, for interface information.

7.1.3 REFERENCES[1]

1. Cook, B. M. and Rowlins, D. H., "Bypass Logic for the Westinghouse Integrated Protection System", WCAP 8897 (Proprietary) and WCAP 8898 (Non-Proprietary), Revision 1, October 1977.

2. Cook, B. M., "Model 414 Control System Signal Selection Device", WCAP 8899 (Proprietary) and WCAP 8900 (Non-Proprietary), May 1977.

3. Gallagher, J. M. (Jr.) (et. al.), "414 Integrated Protection System Prototype Verification Program", WCAP 9153 (Proprietary) and WCAP 9154 (Non-Proprietary), August, 1977.

---

(1) These topicals are submitted for background information only. Although they are RESAR-414-dependent, the same principles and strategies developed in these topicals will be applied to Model SP/90.

TABLE 7.1-1

LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
1. General Design Criteria (GDC), Appendix A to 10CFR Part 50	General Design Criteria for Nuclear Power Plants	3.1.2, 7, 15
GDC 1	Quality Standards and Records	3, 7.1, 7.5, 17
GDC 2	Design Basis for Protection Against Natural Phenomena	3, 7.1, 7.2, 7.3, 7.5, 7A
GDC 3	Fire Protection	3, 7 9.5
GDC 4	Environmental and Missle Design Bases	3, 7.1, 7.2, 7.3
GDC 5	Sharing of Structures, Systems, and Components	3
GDC 10	Reactor Design	3, 7.1, 7.2, 7.3
GDC 11	Reactor Inherent Protection	3, 15
GDC 12	Suppression of Reactor Power Oscillations	3, 7.7, 15
GDC 13	Instrumentation and Control	3, 7.1, 7.2, 7.3, 7.5

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
GDC 15	Reactor Coolant System Design	3, 7.1
GDC 17	Electric Power Systems	3, 7.6, 8
GDC 18	Inspection and Testing of Electric Power Systems	3, 7.6, 8
GDC 19	Control Room	3, 7.7
GDC 20	Protection System Functions	3, 7.2, 7.3, 7.5
GDC 21	Protection System Reliability and Testability	3, 7.1, 7.2, 7.3
GDC 22	Protection System Independence	3, 7.1, 7A.1
GDC 23	Protection System Failure Modes	3, 7.2, 7.3
GDC 24	Separation of Protection and Control Systems	3, 7.1, 7.2, 7A.1
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	3, 7.7, 15
GDC 26	Reactivity Control System Redundancy and Capability	3, 7.7, 15
GDC 27	Combined Reactivity Control Systems Capability	3, 7.3, 7.7, 15
GDC 28	Reactivity Limits	3, 7.3, 7.7, 15

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
GDC 29	Protection Against Anticipated Operational Occurrences	3, 7.1, 7.2, 7.3, 7.5
GDC 33	Reactor Coolant Makeup	3.1
GDC 34	Residual Heat Removal	3, 7.6.2
GDC 35	Emergency Core Cooling	3, 7.3.1, 7.3.2
GDC 37	Testing of Emergency Core Cooling System	3, 7.3.2.2.6
GDC 38	Containment Heat Removal	3, 7.3.1, 7.3.2
GDC 40	Testing of Containment Heat Removal System	3, 7.3.2
GDC 41	Containment Atmosphere Cleanup	3, 7.3.2
GDC 43	Testing of Containment Atmosphere Cleanup Systems	3, 7.3.2
GDC 44	Cooling Water	3
GDC 46	Testing of Cooling Water System	3, 7.3.2
GDC 50	Containment Design Basis	3
GDC 54	Piping Systems Penetrating Containment	3
GDC 55	Reactor Coolant Pressure Boundary Penetrating Containment	3

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
GDC 56	Primary Containment Isolation	3
GDC 57	Closed Systems Isolation Valves	3
2. Institute of Electrical and Electronics Engineers (IEEE) Standards:		
IEEE Std 279-1971 (ANSI N42.7-1972)	Criteria for Protection Systems for Nuclear Power Generating Stations	7.1, 7.2, 7.3, 7.4, 7.5, 7.6
IEEE Std 308-1974	Criteria for Class 1E Power Systems for Nuclear Power Generating Stations	7.6, 8
IEEE Std 317-1972	Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations	8
IEEE Std 323-1974	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations	3, 7.1.2.2.4
IEEE Std 334-1974	Type Tests of Continuous - Duty Class 1E Motors for Nuclear Power Generating Stations	8
IEEE Std 336-1971 (ANSI N45.2.4-1972)	Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Constructions of Nuclear Power Generating Stations.	7, 8

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
IEEE Std 338-1975	Criteria for the Periodic Testing or Nuclear Power Generating Station Class 1E Power & Protection Systems	7.1, 7.3, 7.5, 7A
IEEE Std 344-1975 (ANSI N41.7)	Recommended Practices for Seismic Qaulification of Class 1E Equipment for Nuclear Power Generating Stations	3, 7.1, 7A
IEEE Std 379-1972 (ANSI N41.2)	Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems	7.1, 7.2, 7.3, 7.5
IEEE Std 382-1972	Type Test of Class 1 Electric Valve Operators	3
IEEE Std 384-1974 (ANSI N41.14)	Criteria for Separation of Class 1E Equipment and Circuits	7.1, 7.3, 7.5, 7A
ANSI/IEEE-ANS-7-4.3.2-1982	Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations	7.1
3. Regulatory Guides (RG)		
RG 1.6	Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems	3, 8
RG 1.9	Selection of Diesel Generator Set Capacity for Standby Power Supplies	3, 8
RG 1.11	Instrument Lines Penetrating Primary Reactor Containment	3

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
RG 1.22	Periodic Testing of Protection System Actuation Functions	3, 7.1, 7.3, 7.5
RG 1.29	Seismic Design Classification	3, 7.1
RG 1.30	Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment	3, 17
RG 1.32	Use of IEEE Std 308-1971, "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations"	3, 8
RG 1.40	Qualification Tests of Continuous Duty Motors Installed inside the Containment of Water-Cooled Nuclear Power Plants	3
RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	3, 7.1, 7A
RG 1.53	Application to the Single-Failure Criterion to Nuclear Power Plant Protection Systems	3, 7.1, 7.3, 7.5
RG 1.59	Design Basis Floods for Nuclear Power Plants	3, 7
RG 1.60	Design Response Spectra for Seismic Design of Nuclear Power Plants	3, 7
RG 1.61	Damping Valves for Seismic Design of Nuclear Power Plants	3, 7

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
RG 1.62	Manual Initiation of Protection Actions	3, 7.1, 7.2, 7.3
RG 1.63	Electric Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plants	3
RG 1.68	Preoperational and Initial Startup Test Programs for Water-Cooled Power Reactors	3, 14
RG 1.70	Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, Rev. 2	3, 7
RG 1.73	Qualification Test of Electric Valve Operators Installed Inside the Containment	3
RG 1.75	Physical Independence of Electric Systems	3, 7.1, 7A
RG 1.78	Assumptions for Evaluating the Habitability of a Nuclear Plant Control Room During a Postulated Chemical Reload	7
RG 1.79	Pre-operational Testing of Emergency Core Cooling Systems for Pressurized Water Reactors	14
RG 1.81	Shared Emergency and Shutdown Electric Systems for multi-unit Nuclear Power Plants	3, 8
RG 1.89	Qualification of Class IE Equipment for Nuclear Power Plants	3

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
RG 1.95	Protection of Nuclear Power Plant Control Room Operators Against an Accidental Chlorine Reload	7
RG 1.97	Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During & Following an Accident	7.1, 7.5
RG 1.100	Seismic Qualification of Electric Equipment for Nuclear Power Plants	3, 7.1
RG 1.105	Instrument Spans and Setpoints	7.1.2.2.1 (Tables 2.2-1 & 3.3-4)
RG 1.106	Thermal Overload Protection for Electric Motors on Motor-Operated Valves	7A.6
RG 1.108	Periodic Testing of Diesel Generators Used as Onsite Electric Power System at Nuclear Power Plants	8
RG 1.118	Periodic Testing of Electric Power & Protection Systems	7.1.2.2.9, 7.1.2.2.10, 7.3.2.2.6, 7.5.3.3.10, 7.5.3.3.17, 7A.9, 8
RG 1.120	Fire Protection Guidelines for Nuclear Power Plants	7.1.2.2.5, 9.5

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

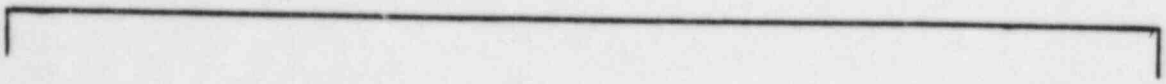
CRITERIA	TITLE	APPLICABLE SECTIONS
4. Branch Technical Positions (BTP) EICSB		
BTP EICSB 3	Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System	7.6.2
BTP EICSB 4	Requirements on Motor-Operated Valves in the ECCS Accumulator Lines	7.3, 7A.6
BTP EICSB 5	Scram Breaker Test Requirements - Technical Specifications	7.1.2.2.11, 16 (Table 4.3-1 Item 21)
BTP EICSB 9	Definition of Use of "Channel-Calibration" - Technical Specifications	(Table 4.3-1, Item 2) of Ch. 16
BTP EICSB 10	Electrical and Mechanical Equipment Seismic Qualification Program	7.1.2.2.4, 3.10
BTP EICSB 12	Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	7.1.2.2.15, 7.2.1.1.1, 7.2.1.1.9 7.2.1.1.2
BTP EICSB 13	Design Criteria for Auxiliary Feedwater Systems	7.3
BTP EICSB 14	Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	7.7.2.2, 15.2.1, 15.2.2, 15.3.6
BTP EICSB 15	Reactor Coolant Pump Breaker Qualification	Not applicable

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
BTP EICSB 16	Control Element Assembly (CEA) Interlocks in Combustion Engineering Reactors	Not applicable
BTP EICSB 18	Application of the Single Failure Criteria to Manually-Controlled Electrically-Operated Valves	TECH. SPEC. 3/4.5 (Ch. 16), 7A.13
BTP EICSB 19	Acceptability of Design Criteria for Hydrogen Mixing and Drywell Vacuum Relief Systems	Not applicable
BTP EICSB 20	Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode	7.6.4, 6.3
BTP EICSB 21	Guidance for Application of Reg. Guide 1.47	3A, 7.1.2.2.13, 7A.5
BTP EICSB 22	Guidance for Application of Reg. Guide 1.22	3A, 7.1.1.2.7, 7.1.2.2.10, 7A.9
BTP EICSB 23	Qualification of Safety-Related Display Instrumentation for Post-Accident Condition Monitoring and Safe Shutdown	3.10, 3.11, 7.5
BTP EICSB 24	Testing of Reactor Trip System and Engineered Safety Feature Actuation System Sensor Response Time	7.1.2.2.9, 7.3.2.2.6, 7.5.3.3.10, 7A.9

TABLE 7.1-1 (Continued)
LISTING OF APPLICABLE CRITERIA

CRITERIA	TITLE	APPLICABLE SECTIONS
BTP EICSB 25	Guidance for the Interpretation of General Design Criterion 37 for Testing the Operability of the Emergency Core Cooling System as a Whole	3.1.2.4, 7.3.2.2.6
BTP EICSB 26	Requirements for Reactor Protection System Anticipatory Trips	7.2.1.1.6
BTP EICSB 27	Design Criteria for Thermal Overload Protection for Motors of Motor-Operated Valves	7A.6, 8



(a,c)

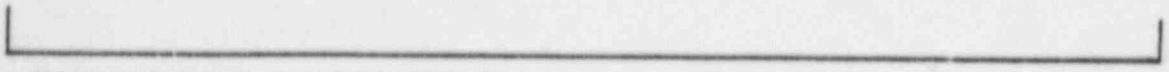
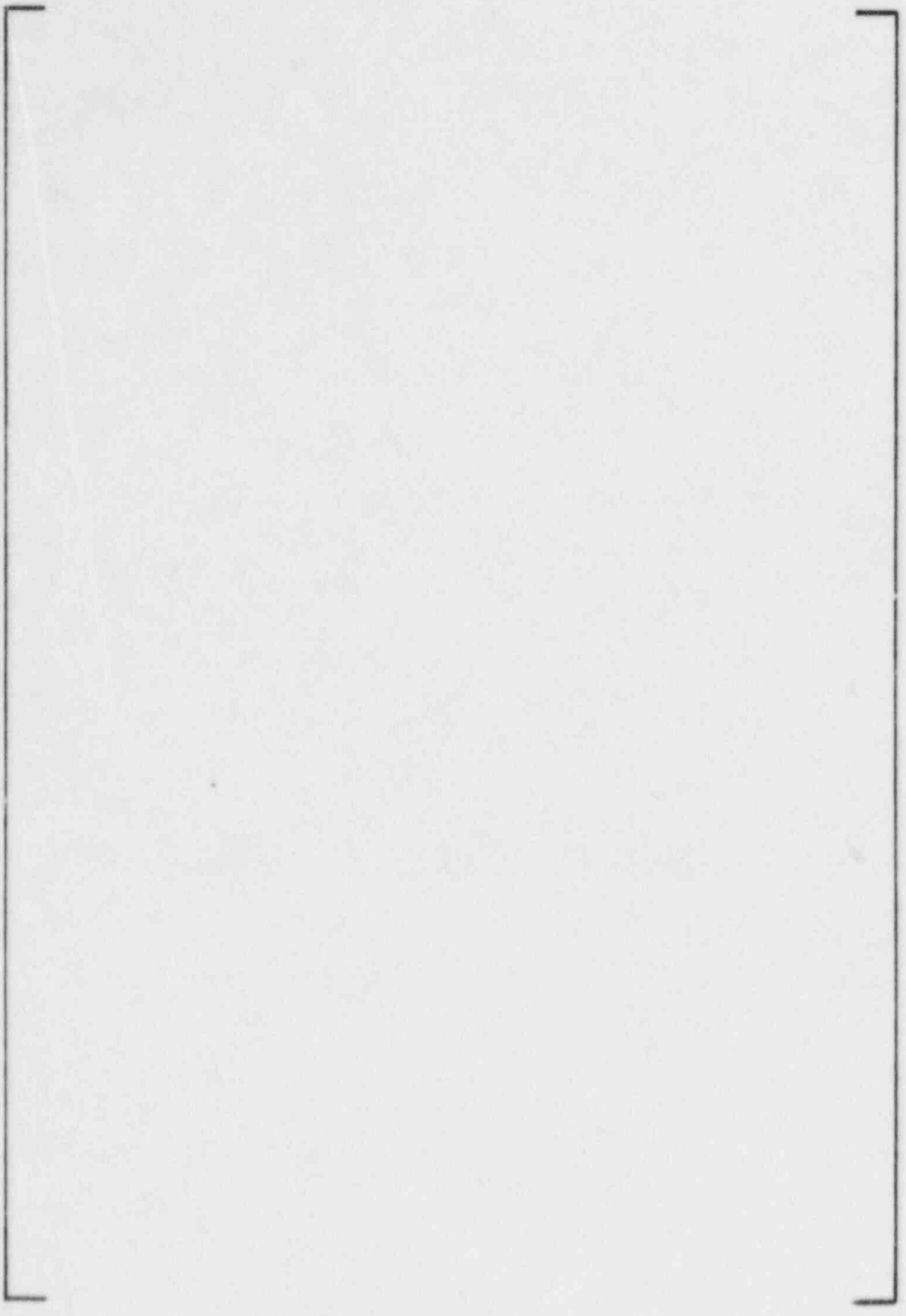


FIGURE 7.1-1 INTEGRATED PROTECTION SYSTEM ARCHITECTURE (SHEET 1 OF 3)



(a,c)

FIGURE 7.1-1 INTEGRATED PROTECTION SYSTEM ARCHITECTURE (SHEET 2 OF 3)

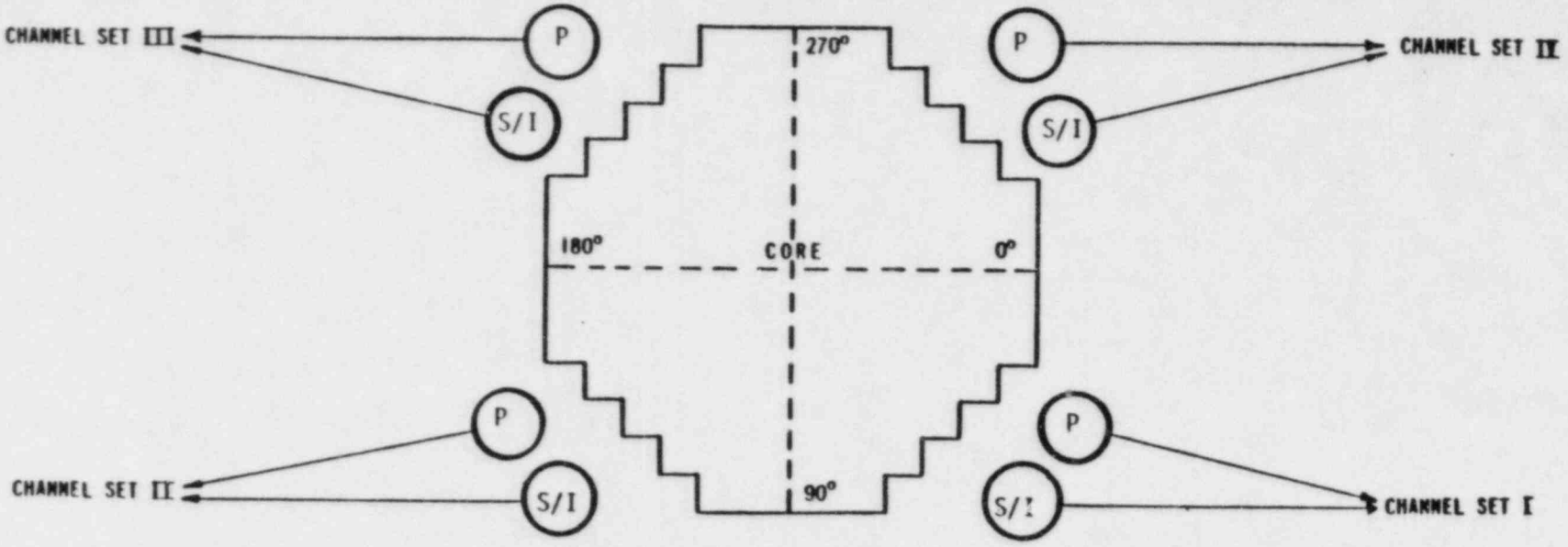
FIGURE 7.1-1 INTEGRATED PROTECTION SYSTEM ARCHITECTURE (SHEET 3 OF 3)

FIGURE 7.1-2

(FOLDOUT)

"IPS SYSTEM BLOCK DIAGRAM"

PROPRIETARY

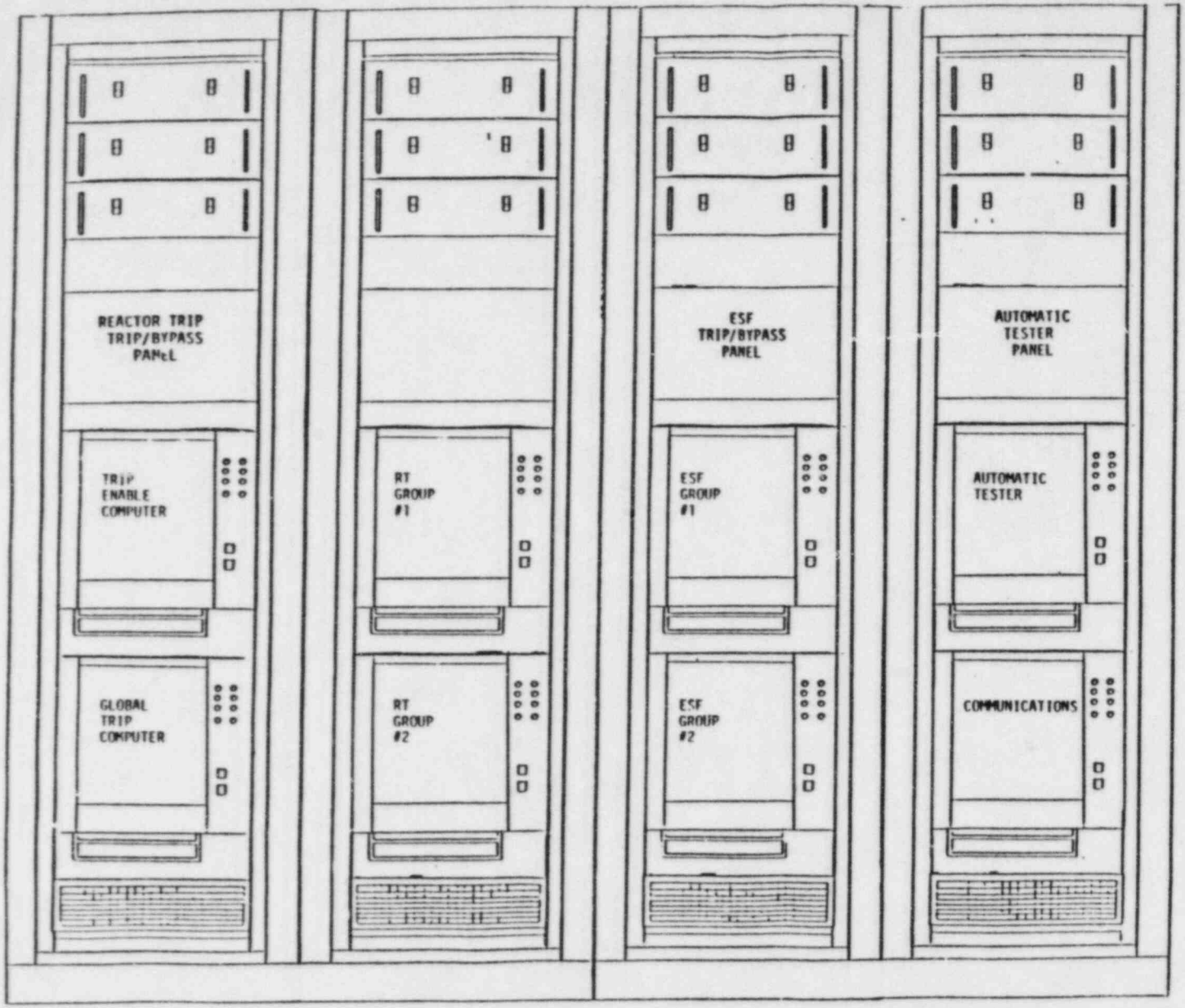


DETECTORS:

P — POWER RANGE MULTI-EXCORE UNCOMPENSATED IONIZATION CHAMBER

S/I — SOURCE RANGE PROPORTIONAL COUNTER AND INTERMEDIATE RANGE COMPENSATED IONIZATION CHAMBER

FIGURE 7.1-3 N.I.S. DETECTOR LOCATIONS



NOTES:

1. THE THREE ASSEMBLIES AT THE TOP OF EACH BAY ARE POWER SUPPLIES.
2. THE ASSEMBLY AT THE BOTTOM OF EACH BAY IS A BLOWER.
3. THE FOUR PANELS LOCATED NEAR THE MIDDLE OF THE FOUR BAYS ARE OPERATOR INTERFACE PANELS. (THE PANEL IN THE SECOND BAY FROM THE LEFT IS CURRENTLY A SPARE PANEL.)

Figure 7.1-4 Integrated Protection System - Cabinet/Subsystem Conceptual Arrangement

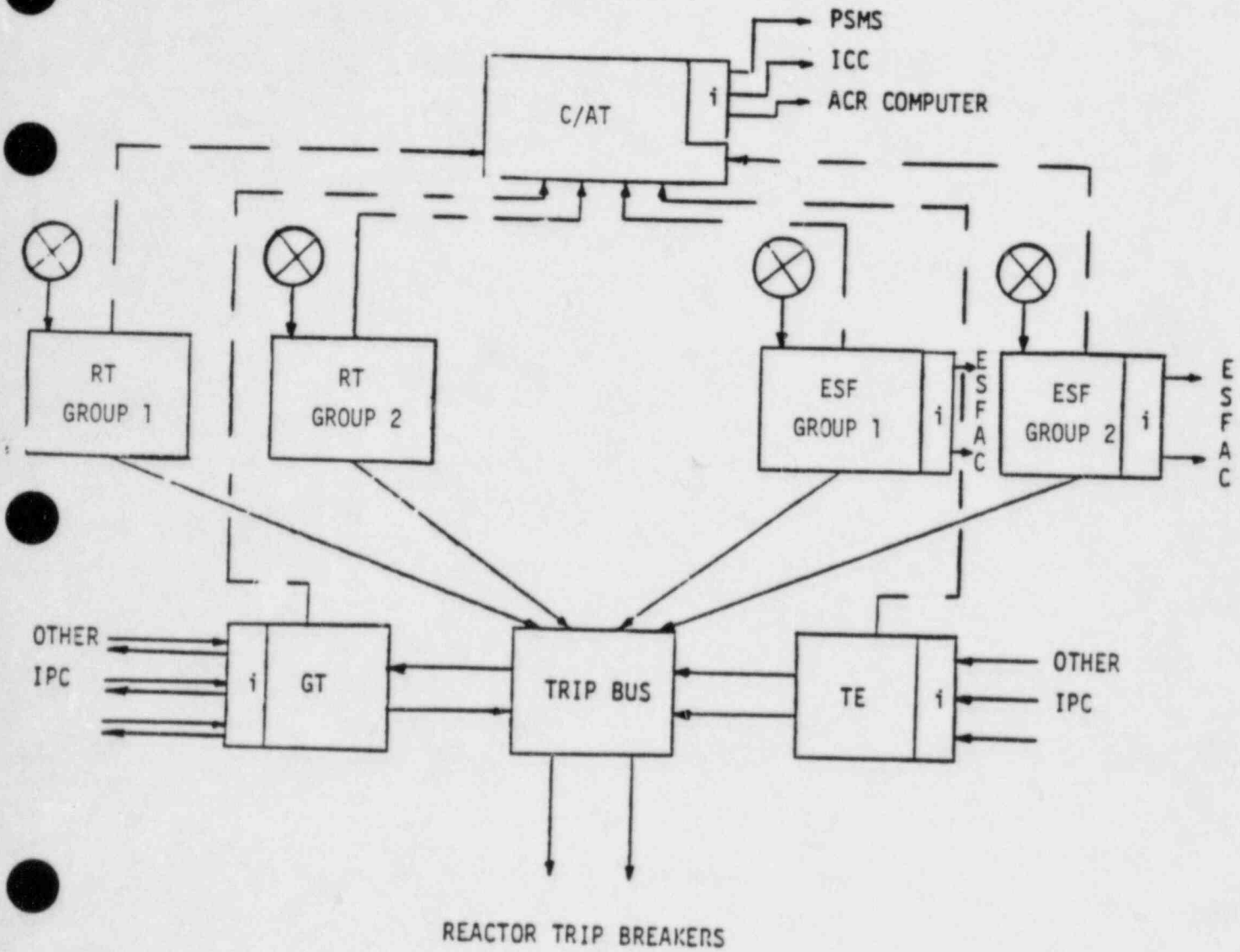


FIGURE 7.1-5 IPC FUNCTIONAL BLOCK DIAGRAM

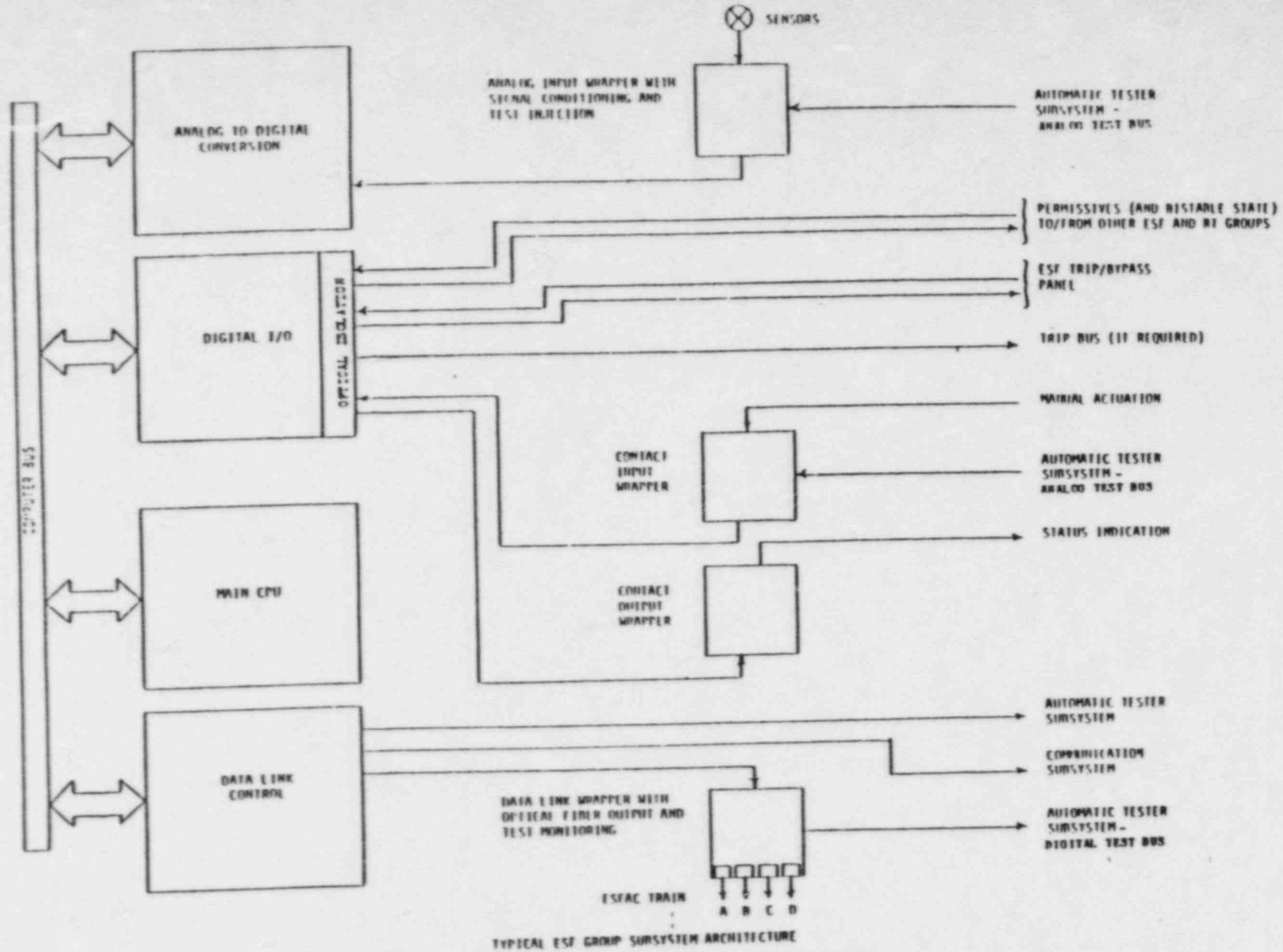


FIGURE 7.1-6 IPC - ESF SUBSYSTEM BLOCK DIAGRAM

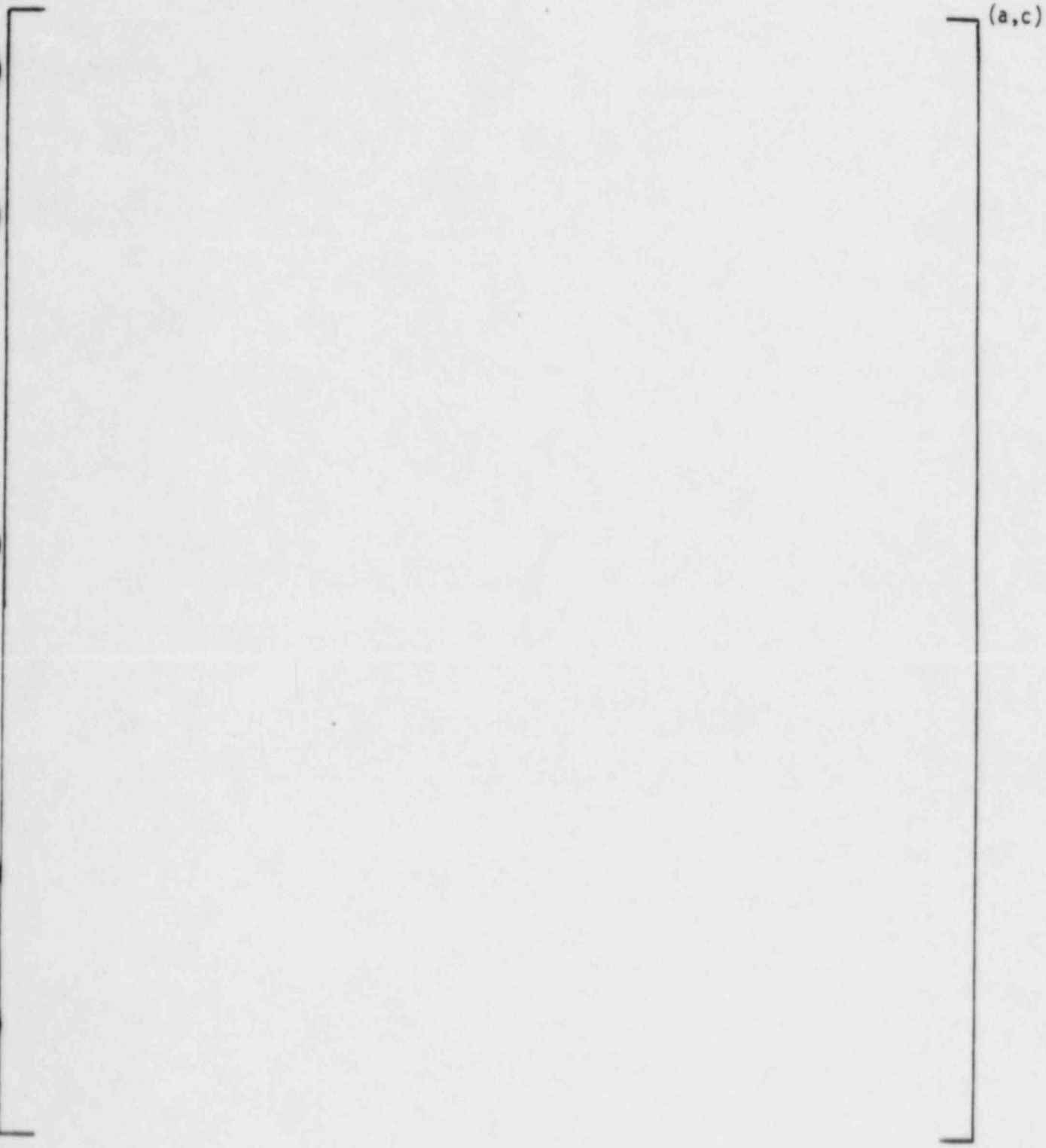
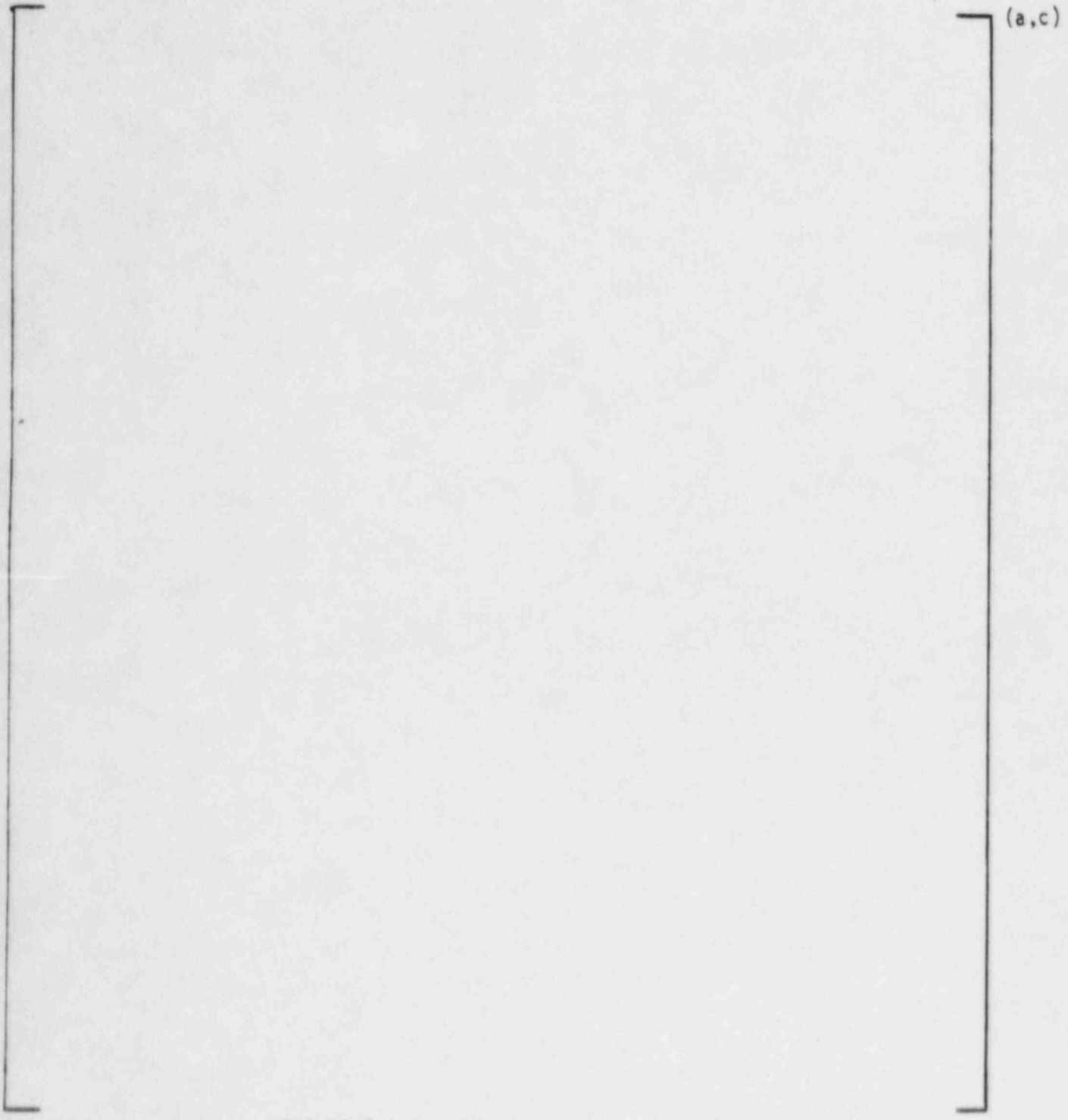
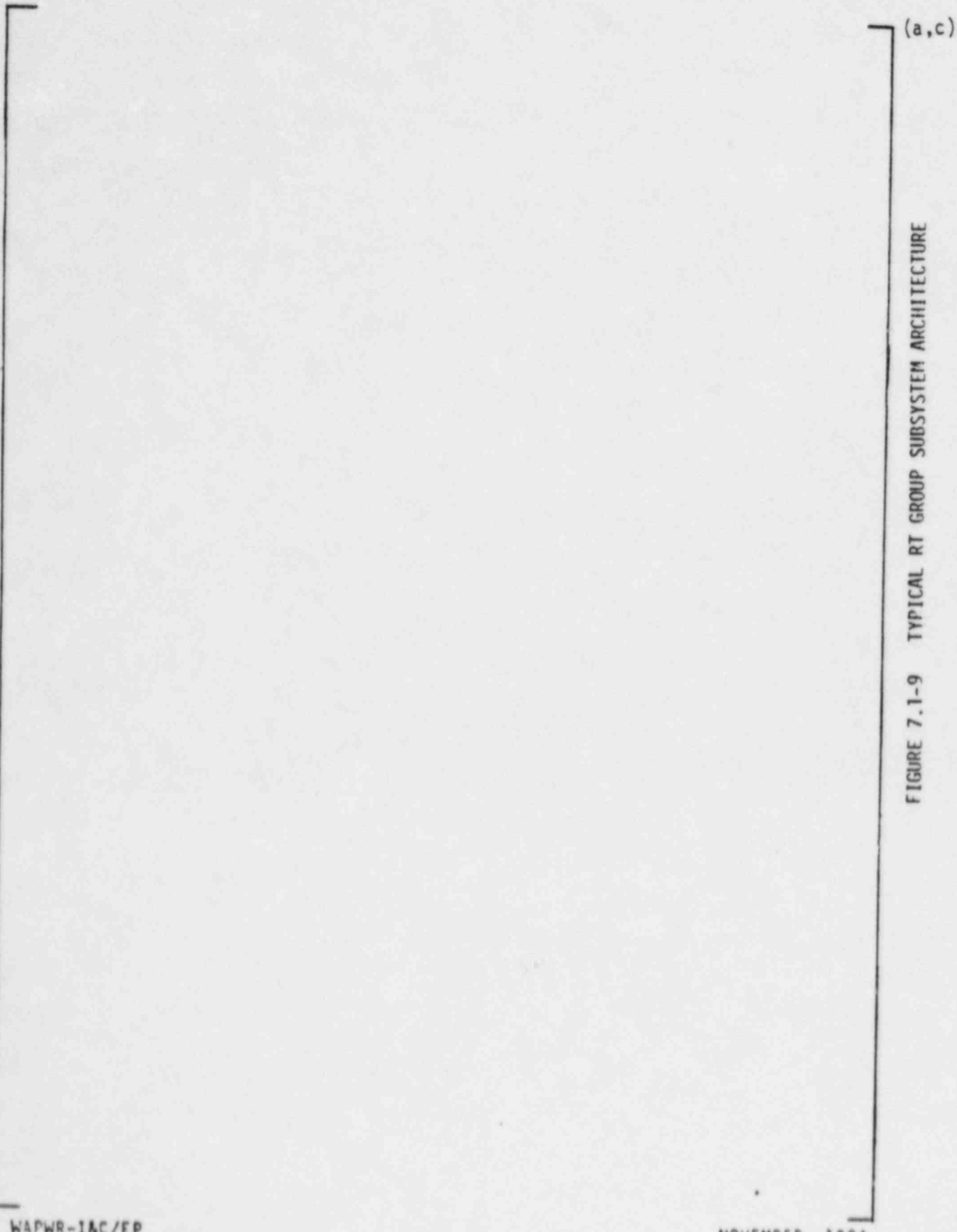


FIGURE 7.1-7 IPC - GLOBAL TRIP SUBSYSTEM BLOCK DIAGRAM (GT)



(a,c)

FIGURE 7.1-8 IPC - TRIP ENABLE SUBSYSTEM BLOCK DIAGRAM



(a,c)

FIGURE 7.1-9 TYPICAL RT GROUP SUBSYSTEM ARCHITECTURE

(a,c)

FIGURE 7.1-10 COMMUNICATION SUBSYSTEM ARCHITECTURE

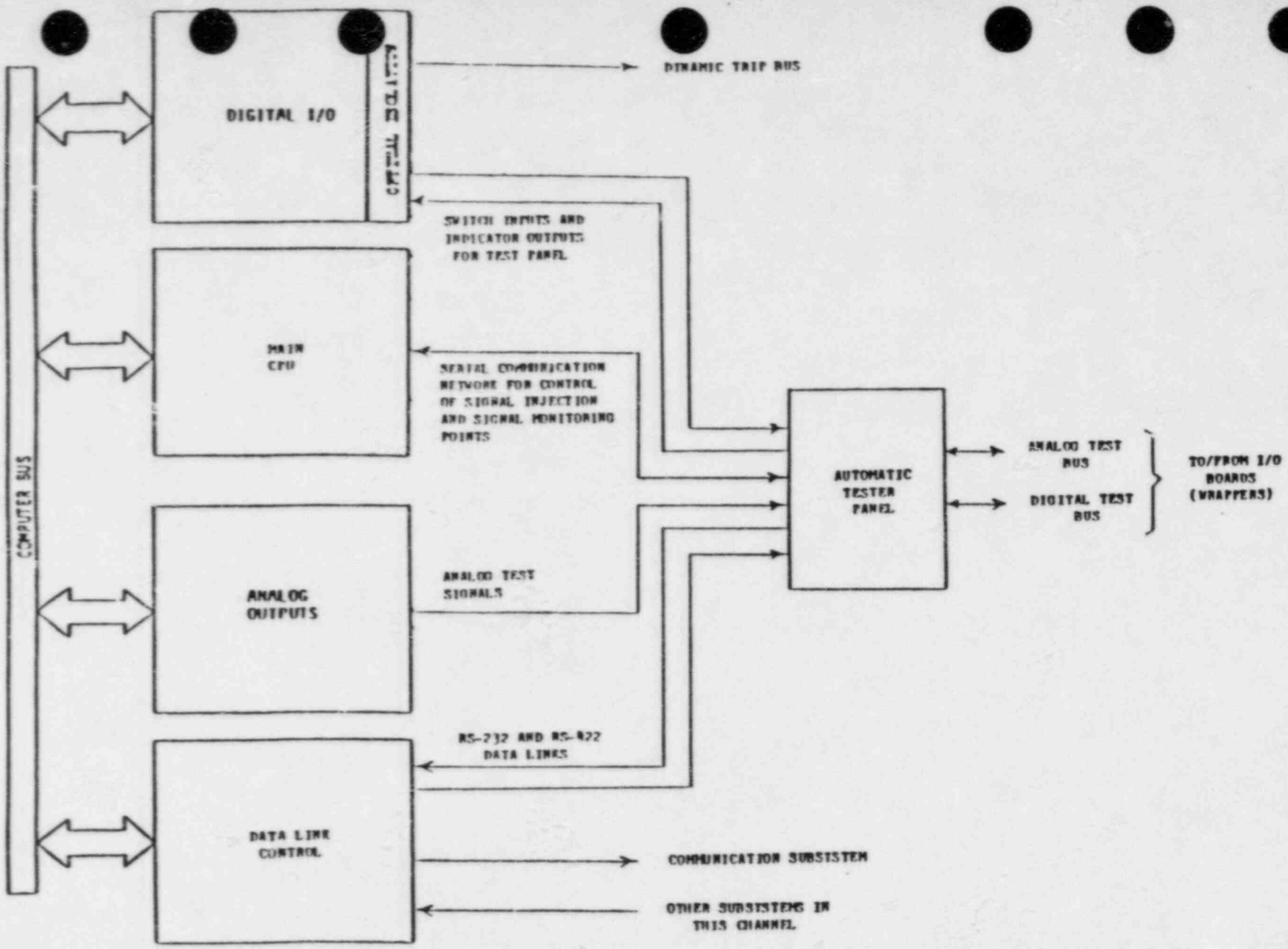


FIGURE 7.1-11 AUTOMATIC TESTER SUBSYSTEM ARCHITECTURE

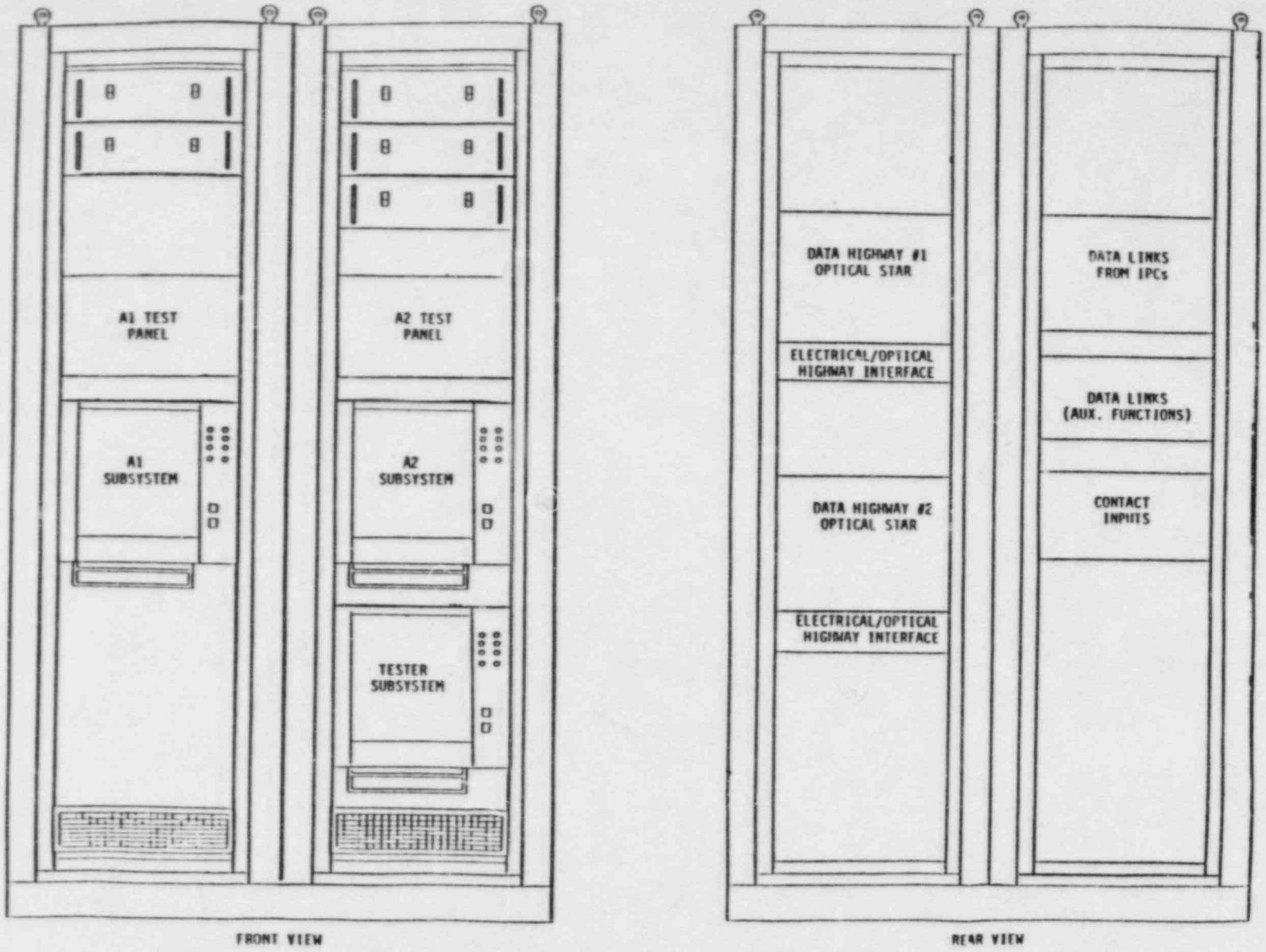


FIGURE 7.1-12 ESFAC EQUIPMENT ARRANGEMENT SKETCH (TRAIN A SHOWN - TYPICAL OF ALL TRAINS)

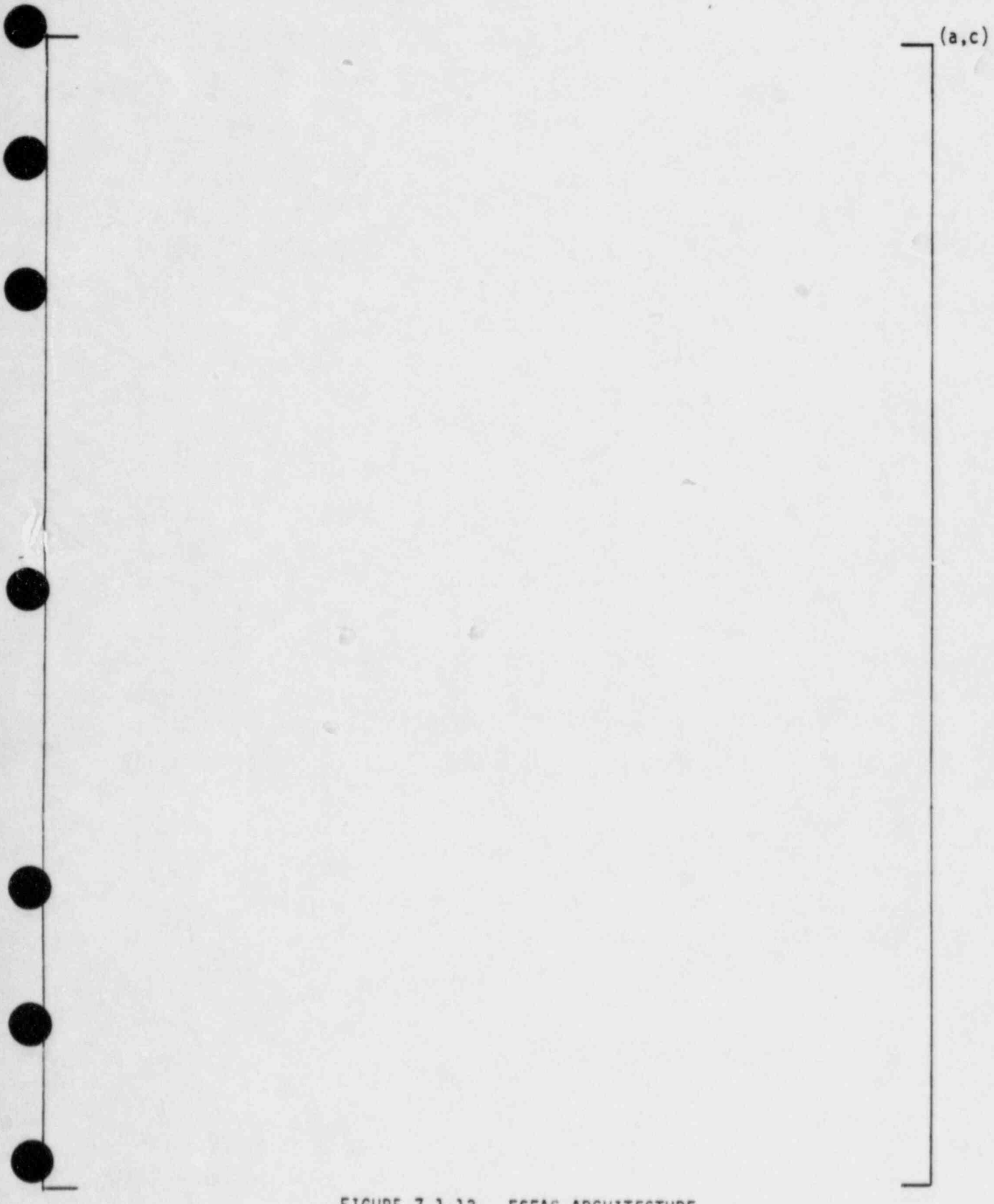
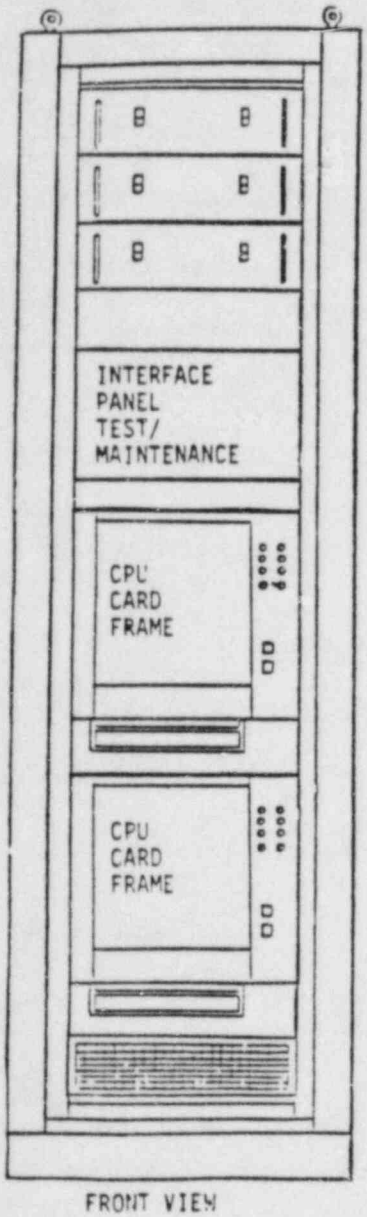
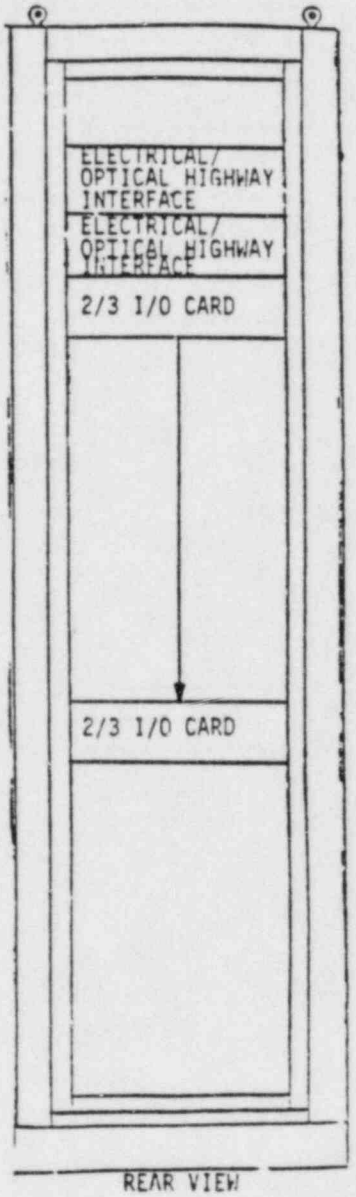


FIGURE 7.1-13 ESFAC ARCHITECTURE

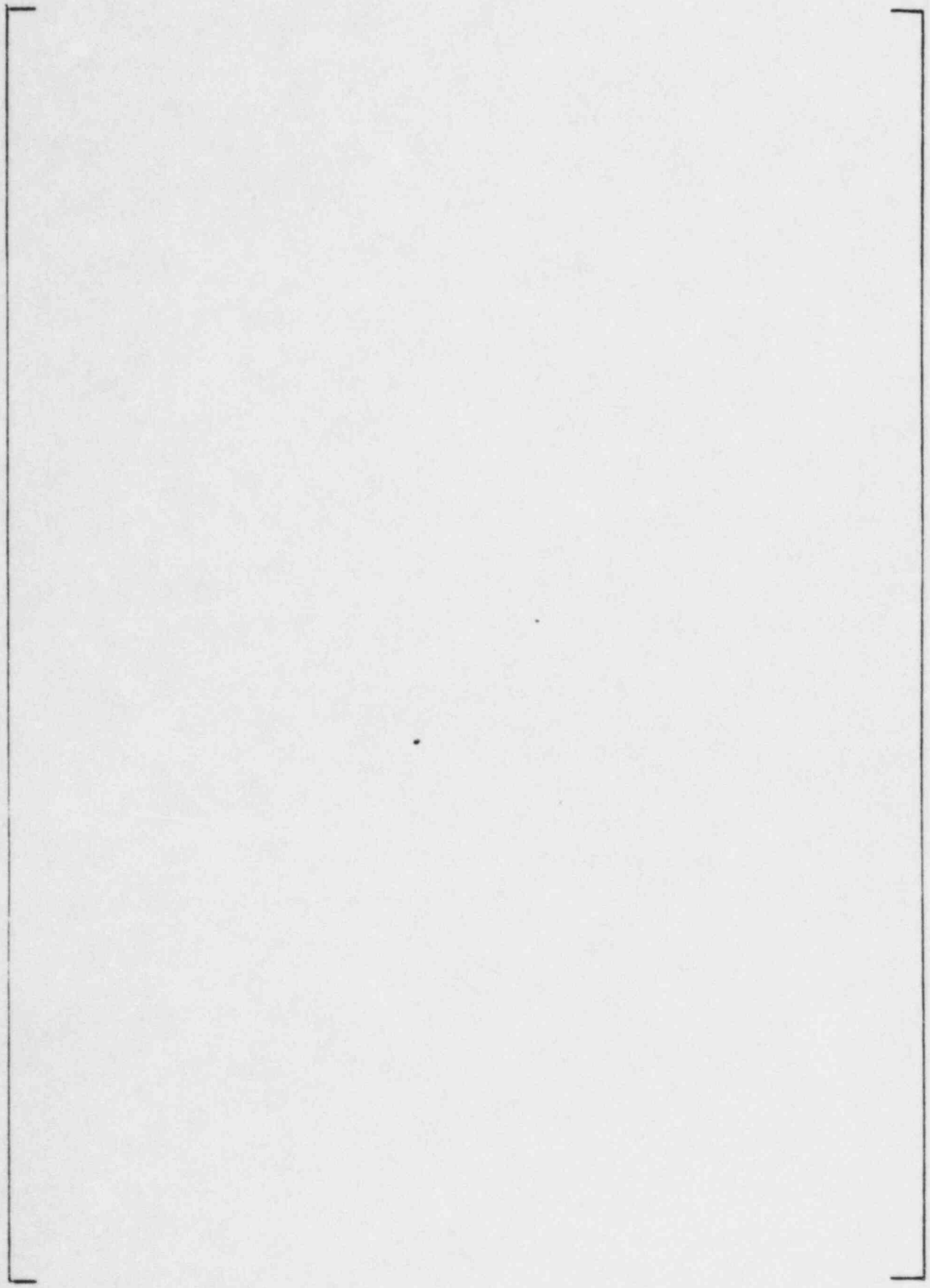


FRONT VIEW



REAR VIEW

FIGURE 7.1-14 FRONT-MOUNTED EQUIPMENT SKETCH



(a,c)

FIGURE 7.1-15 LOGIC CABINET ARCHITECTURE

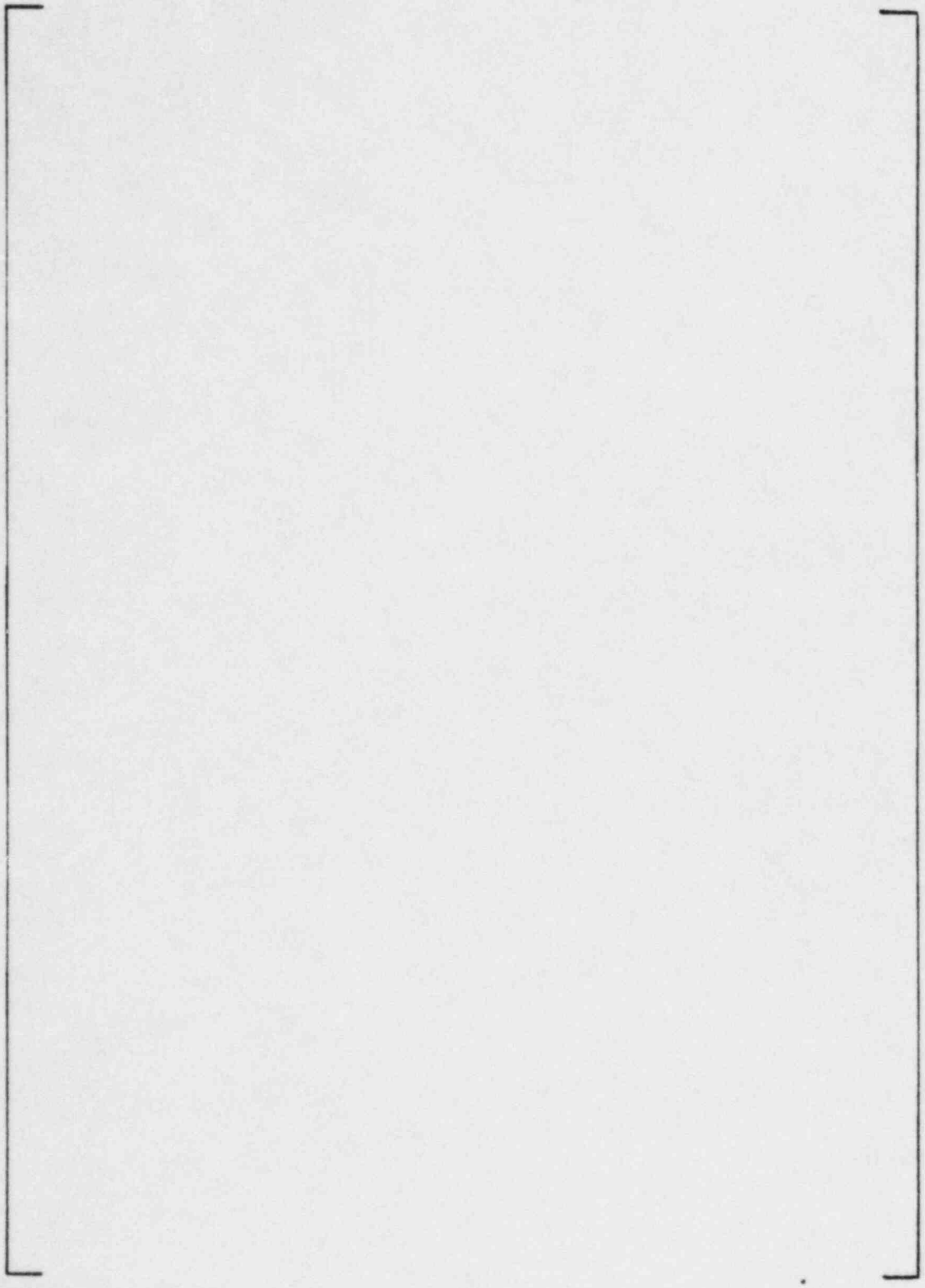


FIGURE 7.1-16 EXAMPLE OF REACTOR TRIP VOTING LOGIC SHOWING CHANNEL PARTIAL TRIPS AND CHANNEL SET TRIPS

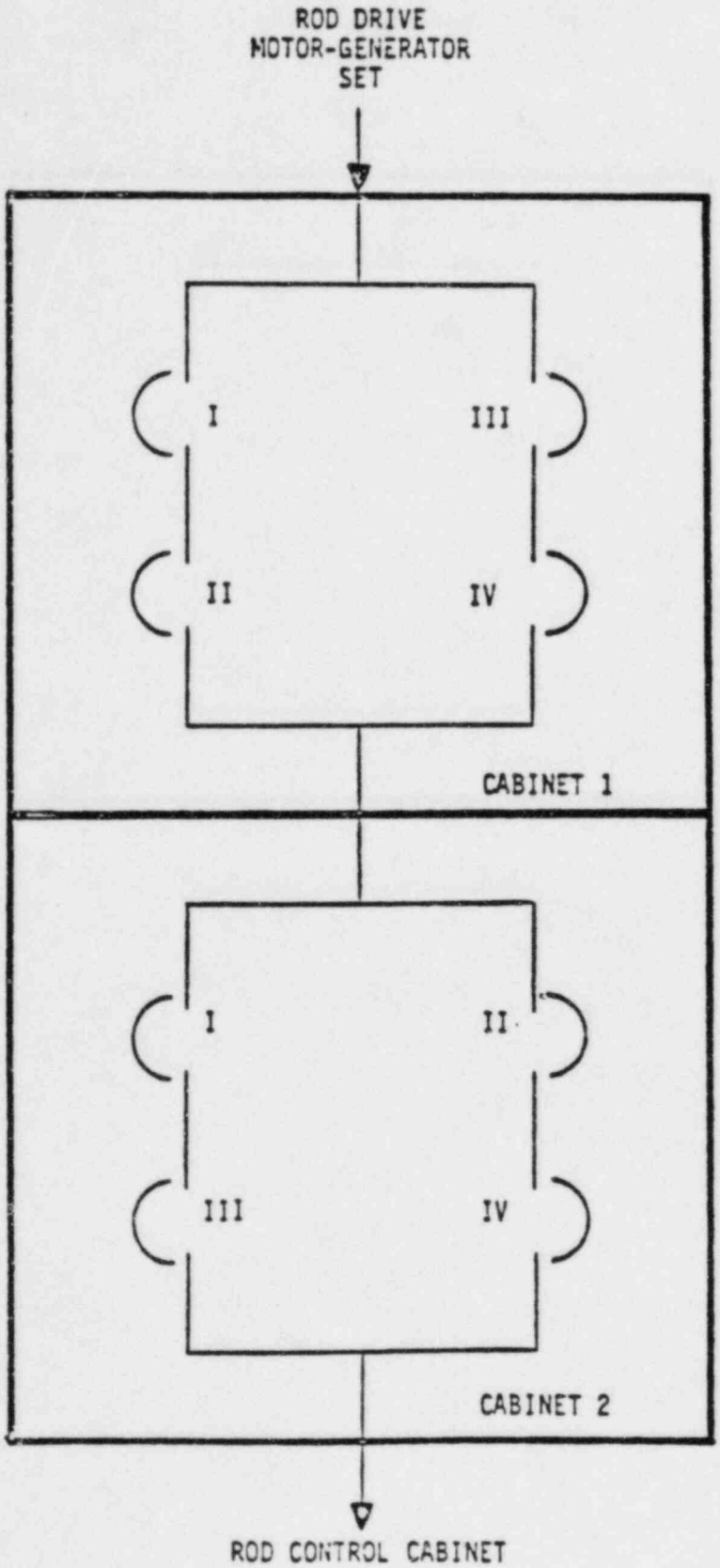


FIGURE 7.1-17 REACTOR TRIP SWITCHGEAR

(a,c)

FIGURE 7.1-18 ALTERNATIVE METHODS - OPTICAL ISOLATION

7.2 REACTOR TRIP

7.2.1 Description

Considerations such as mechanical or hydraulic limitations on equipment or heat transfer requirements on the reactor core define a safe operating region for the nuclear steam supply system (NSSS). Maneuvering of the plant within this safe operating region is permitted in response to normal power generation demands. The NSSS design provides margin to the safety limits such that an unsafe condition is not caused by the transients induced by normal operating changes. The plant control system attempts to keep the reactor operating away from any safety limit. However, excursions toward a limit may occur because of abnormal demands on the generating station, malfunctions in the control system, or by severe transients induced by occurrence of a Condition II or III event (see Chapter 15). Hypothetical events (Condition IV) are analyzed with respect to plant safety limits. The safety system ensures that the reactor is kept operating within the safe region by shutting down the reactor whenever safety limits are approached. Reactor trip is a protective function performed by the integrated protection system when it anticipates an approach of a parameter to its safety limit. Reactor shutdown occurs when electrical power is removed from the shutdown, gray, and control rod drive mechanism coils allowing the rods to fall by gravity into the reactor core.

The equipment involved in reactor trip is listed below and is shown in simplified block diagram form in Figure 7.2-2. Refer to Subsections 7.1.1.2 and 7.1.1.3 for a description of the equipment itself. The equipment involved is:

1. Integrated Protection System (4 redundant channel sets)

    a. Sensors and manual inputs
    b. Integrated protection cabinets (IPCs)

2. Protective Action System (4 redundant reactor trip actuation trains)

a. Reactor trip switchgear
b. Control and shutdown rods

The integrated protection system maintains surveillance on key process variables which are directly related to equipment mechanical limitations, such as pressure, and on variables which directly affect the heat transfer capability of the reactor, such as flow and temperature. Some limits, such as DNBR, are calculated in the integrated protection cabinets from other parameters when direct measurement of the variable is not possible. The variables monitored for reactor trip are listed in Table 7.2-4.

Normally, four redundant measurements using four separate sensors, are made for each variable used for reactor trip. Selected analog measurements are converted to digital form by analog-to-digital converters within the integrated protection cabinets. Signal conditioning may be applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for the given parameter is generated if one channel's measurement exceeds its predetermined or calculation limit. All processing on all variables for reactor trip is duplicated in each of the four redundant segments of the integrated protection system called channel sets. Each channel set sends its channel's partial trip status to each of the other three channel sets over isolated multiplexed links. Each channel set is capable of generating a reactor trip signal if two or more of the redundant channels of a single variable are in the partial trip state.

The reactor trip signal from each of the four integrated protection cabinets is sent to a corresponding reactor trip actuation train of the protective action system. (See Figure 7.1-16)

Each of the 4 reactor trip actuation trains consists of two reactor trip circuit breakers. The reactor is tripped when two or more actuation trains receive a reactor trip signal. This automatic trip demand initiates the following two actions: 1) it deenergizes the undervoltage trip attachments (UVTA's) on the reactor trip breakers, and 2) it energizes the shunt trip devices on the reactor trip breakers. Either action causes the breakers to trip. Opening of the appropriate trip breakers removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion shuts down the reactor.

Bypasses of parameter channels used to generate reactor trip signals and of reactor trip actuation trains are permitted as described in Subsection 7.2.1.1.10. Single failure criterion is met even when one or two channels of reactor trip actuation trains are bypassed. The reactor is automatically tripped if three or four channels or trains are attempted to be bypassed.

Subsection 7.2.1.1 provides a description of each of the reactor trip functions. Subsection 7.2.1.2 provides the design bases information as required by Section 3 of IEEE 279-1971. Subsection 7.2.2 discusses conformance of the reactor trip function to the requirements stated in Section 4 of IEEE 279-1971. The functional diagrams for reactor trips, as well as for other protective functions, are presented in Figure 7.2-1.

7.2.1.1 Functional Description

The following subsections describe the specific reactor trip functions and are grouped according to the following eight conditions:

1. Nuclear Startup Trips (Subsection 7.2.1.1.1)
2. Nuclear Overpower Trips (Subsection 7.2.1.1.2)
3. Core Heat Removal Trips (Subsection 7.2.1.1.3)
4. Primary Overpressure Trips (Subsection 7.2.1.1.4)
5. Loss of Heatsink Trips (Subsection 7.2.1.1.5)

6. Excessive Cooldown Trips (Subsection 7.2.1.1.6)
7. Turbine Trip (Subsection 7.2.1.1.7)

Table 7.2-1 lists the reactor trips and summarizes the coincidence logic to trip. The interlocks for each trip are given on Table 7.2-2. System level manual inputs to reactor trip functions are given on Table 7.2-3.

7.2.1.1.1 Nuclear Startup Trips

1. Source Range High Neutron Flux Trip

Source range high neutron flux trips the reactor when two of the four source range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup and plant shutdown, can be manually blocked when the intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when the intermediate range channels decrease below the P-6 setpoint value. This trip is automatically blocked by the power range protection interlock (P-10) and automatically reinstated below P-6. The source range trip setpoint is set between the P-6 setpoint (source range cutoff power level) and the maximum source range power level. The channels can be individually bypassed at the integrated protection cabinets to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated on the control board.

The logic for this trip is shown on Figure 7.2-1, sheet 3. The development of permissives P-6 is shown on Figure 7.2-1, sheet 3 and P-10 is shown on Figure 7.2-1, sheet 4.

2. Intermediate Range High Neutron Flux Trip

Intermediate range high neutron flux trips the reactor when two of the four intermediate range channels exceed the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked

if the power range channels are above approximately 10 percent power (P-10). The trip is automatically reinstated when the power range channels indicate less than 10 percent power. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the integrated protection cabinets to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated on the control board.

The logic for this trip is shown on Figure 7.2-1, sheet 3. The development of permissive P-10 is shown on Figure 7.2-1, sheet 4.

3. Power Range High Neutron Flux Trip (Low setpoints)

Power range high neutron flux (low setpoint) trips the reactor when two of the four power range channels exceed the trip setpoint.

The trip, which provides protection during startup, can be manually blocked when the power range channels read above approximately 10 percent power (P-10). The trip is automatically reinstated when the power range channels indicate less than 10 percent power.

Channel bypass capability exists for each of the four channels as described in Subsection 7.1.2.2.11.

The logic for this trip is shown on Figure 7.2-1, sheet 3. The development of permissive P-10 is shown on Figure 7.2-1, sheet 4.

7.2.1.1.2 Nuclear Overpower Trips

1. Power Range High Neutron Flux Trip (High Setpoint)

Power range high neutron flux (high setpoint) trips the plant when two of the four power range channels exceed the trip setpoint. It provides

protection against excessive core power generation during normal operation and is always active. The logic for this trip is shown on Figure 7.2-1, sheet 4.

2. High Positive Flux Rate Reactor Trip

This trip protects the reactor when a sudden abnormal increase in power occurs in two out of the four power range channels. It provides DNB protection against ejection accidents of low worth rods from midpower and is always active. A channel is tripped when rate sensitive circuits in the channel detect rates of change in nuclear power above the setpoint value. The channel trip is latched by a memory such that the partial trip signal does not disappear when the rate of change in power goes below the setpoint value. Once, latched, the channel can only be reset from the control board by manual action. The reactor is tripped when two out of the four rate channels have tripped.

Channel bypass capability exists for each of the four channels as described in Subsection 7.1.2.2.11.

The logic for this trip is shown on Figure 7.2-1, sheet 4.

3. High Negative Flux Rate Reactor Trip

This trip protects the reactor when a sudden abnormal decrease in power occurs in two out of the four power range channels. It provides DNB protection against dropped control rods and is always active. A channel is tripped when rate sensitive circuits in the channel detect rates of change in nuclear power above the setpoint value. The channel trip is latched by a memory such that the partial trip signal does not disappear when the rate of change in power goes below the setpoint value. Once, latched, the channel can only be reset from the control board by manual action. The reactor is tripped when two out of the four rate channels have tripped.

Channel bypass capability exists for each of the four channels as described in Subsection 7.1.2.2.11.

The logic for this trip is shown on Figure 7.2-1, sheet 4.

7.2.1.1.3 Core Heat Removal Trips

1. Reactor trip on low DNB Ratio (DNBR)

This function protects the reactor core against departure from nucleate boiling (DNB) by tripping the reactor when the N-16 measured thermal power (Q-16) exceeds the DNB ratio trip setpoint. The setpoint for this trip is calculated continuously by digital processing techniques for each reactor coolant loop as discussed below. Nitrogen-16 (N-16) monitors located on the hot and cold legs of each coolant loop are used to measure the thermal power level. Bypass capability for each channel exists as discussed in Subsection 7.1.2.2.11. The logic for this trip is shown on Figure 7.2-1, sheet 5.

Refer to Figure 7.2-3 for the following discussion. The DNBR trip setpoint (Q_{DNB}) for each channel is determined by selecting the most limiting value of any of the following thermal power limits:

a. the thermal power at which exit boiling begins (Q_1); or

b. the thermal power at which the core hot channel exit quality limit is reached (Q_2); or

c. the thermal power at which the DNBR limit is reached in any of three potentially limiting cells (Q_3, Q_4, Q_5).

The above thermal power values are computed by the following equations:

a. $Q_1 = (Q\ ref_1)$

b. $Q_2 = (Q\ ref_2) * \frac{F^{ref}_{\Delta h}}{F^{N}_{\Delta h}}$

c. $Q_3 = (Q\ ref_3) * \frac{F^{ref}_{\Delta h}}{F^{N}_{\Delta h}} * [f_1\ (Max\ PIP)]$

d. $Q_4 = (Q\ ref_4) * \frac{F^{ref}_{\Delta h}}{F^{N}_{\Delta h}} * [f_2\ (Max\ PIP)]$

e. $Q_5 = (Q\ ref_5) * \frac{F^{ref}_{\Delta h}}{F^{N}_{\Delta h}} * [f_3\ (Max\ PIP)]$

where $Q\ ref_i$ is defined as:

$$Q\ ref_i = \left[A_i \left(\frac{1 + \tau_1 s}{1 + \tau_2 s}\right) T_{in} + B_i P + C_i \left(\frac{1 + \tau_1 s}{1 + \tau_2 s}\right) T_{in}\ P + D_i\right]$$

where i = 1 for use in the Q_1 calculation,
i = 2 for use in the Q_2 calculation,
i = 3 for use in the Q_3 calculation,
i = 4 for use in the Q_4 calculation, and
i = 5 for use in the Q_5 calculation.

The parameters in the above equations are as follows.

A_i, B_i, C_i, and D_i are preset manually-adjustable constants characteristic of the reactor core design. They are based on the effects of coolant inlet temperature-pressure on the thermal power limits. The constants are specified in the Technical Specifications.

T_{in} is the core inlet coolant temperature (°F) and is obtained from the fast response resistance temperature detectors (RTDs) located in the cold leg of each coolant loop.

P is the pressurizer pressure (psia) and is obtained from sensors connected to taps at the top of the pressurizer.

τ_1 and τ_2 are time constants (seconds) and are specified in the Technical Specifications.

s is the Laplace transform operator (seconds $^{-1}$)

$F^{ref}_{\Delta h}$ is a preset constant which is characteristic of the reactor core design. $F^{ref}_{\Delta h}$ is specified in the Technical Specifications.

$F^{N}_{\Delta h}$ is the nuclear enthalpy rise hot channel factor, and is defined as the ratio of the integral of linear power along the rod with the highest integrated power to the average rod power. $F^{N}_{\Delta h}$ is primarily a function of control rod position and reactor power. The insertion limit for the control rods, however, is specified in the Technical Specifications. Therefore, a bounding empirical relationship between power and $F^{N}_{\Delta h}$ can be developed. It is specified in the Technical Specifications. This correlation provides conservatism since the control rods are seldom at or near their rod insertion limits. The power measurement used is the N-16 power monitor input to each protection channel set. No additional compensation is provided in the protection

system calculation of $F^N_{\Delta h}$ to account for operation with a misaligned RCCA. Continued operation with a misaligned RCCA is not considered to be a normal mode of operation.

f_1 (Max PIP) is a function of the parameter Max PIP. Max PIP is the maximum power times integrated power and is the maximum value of:

$$PIP = P_z(J) * \sum_{i=1}^{J} {}_zP\ (i)/J \text{ where J runs from 1 to 26.}$$

P_z in the above equation is a normalized vector containing 26 elements representing the core axial power distribution at 26 equi-spaced points from core bottom to core top. It is continuously computed using core axial power information supplied by the four-section excore neutron detectors. P_z is calculated from:

$$P = A \times D \text{ where}$$

P is the 26-element vector containing the normalized axial flux distribution; A is the 4 by 26 element matrix of conversion coefficients and is calibrated during core life by incore flux maps; and D is a 4-element vector containing the output signals from the four segments of the excore detector.

Max PIP is a measure of the axial power distribution. f_1 (Max PIP) reduces the typical cell thermal power limit (Q_3) when the measured axial power distribution is worse in terms of DNB than the reference axial power distribution which was used in determining the thermal power limits. f_1 (Max PIP) increases Q_3 when the converse is true.

f_2 (Max PIP) is identical to f_1 (Max PIP) except that f_2 defines the axial power distribution effect on the thimble cell thermal power limit (Q_4). Both f_1 and f_2 are determined in the design of the core and are specified in the technical specifications as $Q/Q\ ref_3 = f_1$ (Max PIP) and $Q/Q\ ref_4 = f_2$ (Max PIP).

2. Reactor trip on high KW/ft

This function protects against excessive fuel rod power by tripping the reactor when the peak local power in the core exceeds the kilowatts per foot (Kw/ft) trip setpoint. The peak local power in the core is calculated continuously for each channel set as discussed below. N-16 power monitors located in the hot leg of each coolant loop are employed to measure thermal power. Channel bypass capability exists for each of the four channels. See Figure 7.2-1, sheet 5 for logic for the KW/ft trip.

Refer to Figure 7.2-4 for the following discussion. The KW/ft setpoint is specified in the Technical Specifications. The peak power level in the core is compared against the setpoint value and is calculated by determining the maximum of:

$$Q(J) = Q_{16} * P_z(J) * F_{xy}(J) * U * S(J) \text{ where J runs from 1 to 26}$$

Q_{16} is the core thermal power level as determined by the N-16 power measurements.

$P_z(J)$ is the normalized axial flux distribution vector that was discussed in the DNBR reactor trip in the preceding subsection.

U is a constant for conversion of power to a Kw/ft value and is specified in the Technical Specifications.

S(J) is the densification spike penalty (preset at 26 elevations) and is specified in the Technical Specifications.

$F_{xy}(J)$ is a vector containing the magnitude of the core radial peaking factor at 26 equi-spaced elevations from core bottom to core top. Like $F^N_{\Delta H}$, as described in the DNBR calculation, $F_{xy}(J)$ at elevation "J" is primarily a function of control rod position and core power. Hence a simple correlation between nuclear power and $F_{xy}(J)$ is employed in the

calculation. This correlation is determined based on core flux maps taken at different times during core life. No additional compensation is provided in the protection system calculation of $F_{xy}(J)$ to account for operation with a misaligned RCCA. Continued operation with a misaligned RCCA is not considered to be a normal mode of operation.

3. Reactor Trip Low Pressurizer Pressure

The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-10 the reactor is tripped when the pressurizer pressure measurements (compensated for rate of change) fall below preset limits. This trip is blocked below P-10 to permit startup.

The logic for this trip is shown on Figure 7.2-1, sheet 5. The development of the P-7 permissive is shown on Figure 7.2-1, sheet 4.

4. Reactor Trip on Low Reactor Coolant Flow

The parameter sensed is reactor coolant flow. Four elbow taps in each coolant loop are used as a flow device that indicates the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. A partial trip signal from two out of the four channels in a loop would indicate a low flow in that loop. Below P-7 the reactor trips on this function are blocked. Above P-7, but below the P-8 setpoint, reactor trip will occur if two out of the four loops have a low flow condition. Above the P-8 setpoint, low flow in any one loop will cause a reactor trip.

Bypass capability exists for each of the four channels in each of the four loops, as discussed in Subsection 7.1.2.2.11.

The logic for this trip is shown on Figure 7.2-1, sheet 5. The development of permissives P-7 and P-8 are shown on Figure 7.2-1, sheet 4.

5. Reactor Trip on Reactor Coolant Pump Underspeed

This function protects the reactor core from DNB in the event of loss of flow in more than one loop by tripping the reactor when the speed on two out of the four reactor coolant pumps fall below the setpoints. Loss of flow in more than one loop could be caused by a voltage or frequency transient in the plant power supply such as would occur during a station blackout, or by accidental opening of more than one RCP circuit breaker. There is one speed detector mounted on each reactor coolant pump. The trip is blocked below P-10 to permit plant startup.

Bypass capability exists for the four RCP underspeed channels as described in Subsection 7.1.2.2.11.

The logic for this trip is shown on Figure 7.2-1, sheet 5. The development of P-7 is shown on Figure 7.2-1, sheet 4.

RCP speed is detected by a probe mounted on the reactor coolant pump frame. The speed signal is transmitted to the integrated protection system to provide the trip logic function described above.

The RCP underspeed trip replaces the undervoltage and underfrequency reactor trips used previously. The principle reason for this change is to improve plant availability during voltage dip transients which do not result in violations of plant safety limits. The undervoltage trip setpoint was chosen to trip the reactor if the RCP motor pull out torque dropped below nominal due to low voltage. This event could cause a pump speed decrease and a consequent flow reduction. The basis for the undervoltage trip setpoint and time response was the demonstration of acceptable results for the complete loss of flow accident. Transient voltage reductions below the undervoltage trip setpoint followed by subsequent voltage recovery could result in an undervoltage reactor trip even though pump speed and flow reductions would not violate safety limits.

The RCP underspeed trip provides a more direct measurement of the parameter of interest, and will permit the plant to ride through many postulated voltage dip transients without reactor trip if safety limits are not violated. Selection of the underspeed trip setpoint and time response provide for the timely initiation of reactor trip during the complete loss of flow accident and the limiting frequency decay event, consistent with the analysis results reported in Chapter 15.

The built-in on-line testing capabilities of the integrated protection system provisions include complete on-line overlapping testing of the IPS from the sensor inputs, through to the protective action system. For the RCP speed sensor, the on-line test is discussed in Subsection 7.1.1.3.10.

The basis for environmental qualification of the RCP speed detectors is that they will be required to perform their protective function (during the complete loss of flow accident and the limiting frequency decay event) in an environment (i.e., temperature, humidity, pressure, chemical, and radiation) no more severe than the environment in which they are required to perform their normal function. Therefore, it is not necessary to impose environmental qualification requirements on these detectors that are more restrictive than those imposed for use under rated conditions. The RCP speed detectors will be qualified for use under rated conditions with their performance verified by actual on-line operation in the plant. The RCP speed detectors will also require qualification to the worst vibrations to which they could be subjected and be required to operate.

7.2.1.1.4 Primary Overpressure Trips

1. Pressurizer High Pressure Reactor Trip

The purpose of this trip is to protect the reactor coolant system against system overpressure. The same sensors used for the pressurizer low pressure reactor trip are used for the high pressure trip except that

separate setpoints are used for trip. The high pressure channel trips when an uncompensated pressurizer pressure signal exceeds a preset limit. There are no interlocks or permissives associated with this trip function.

Bypass capability exists for each channel as described in Subsection 7.1.2.2.11.

The logic for this trip is shown in Figure 7.2-1, sheet 6.

2. Pressurizer High Water Level Reactor Trip

This trip is provided as backup to the high pressurizer pressure reactor trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup.

Bypass capability exists for the four channels as described in Subsection 7.1.2.2.11.

The logic for the trip is shown on Figure 7.2-1, sheet 6. The development of P-7 is shown on Figure 7.2-1, sheet 4.

7.2 1.1.5 Loss of Heatsink Trips

Reactor Trip on Low Water in any Steam Generator

This trip protects the reactor from loss of heat sink in the event of a loss of feedwater to the steam generators. The reactor is tripped when two out of the four water level sensors in any steam generator produce signals below the setpoint value. Bypass capability exists for the four channels in each steam generator.

The logic for the trip is shown on Figure 7.2-1, sheet 7. There are no interlocks or permissives to this trip.

7.2.1.1.6 Excessive Cooldown Trips

Reactor Trip on High Water Level in any Steam Generator

This trip protects the reactor from loss of heat sink in the event of a high level in the steam generators. The reactor is tripped when two out of the four water level sensors in any steam generator produce signals above the setpoint value. Bypass capability exists for the four channels in each steam generator.

The logic for this trip is shown on Figure 7.2-1, sheet 7. There are no interlocks or permissives for this trip.

7.2.1.1.7 Reactor Trip/Turbine Trip

7.2.1.1.7.1 Reactor Trip on a Turbine Trip [Anticipatory]

This trip is actuated on two out of four protection channels indicating a turbine trip condition. A turbine trip condition in a channel is defined as closing of one of the four turbine throttle valves or low pressure of the turbine stop emergency trip fluid. As an option, the trip may be blocked by P-9 on plants without full load rejection capability.

The reactor trip on turbine trip provides additional protection and conservatism beyond that required for the health and safety of the public.

This trip is included as part of good engineering practice and prudent design. No credit is taken in any of the safety analyses (Chapter 15) for this trip.

The turbine provides anticipatory trips to the reactor protection system from contacts which change position when the turbine stop valves close or when the turbine autostop oil pressure goes below its setpoint.

One of the design bases considered in the protection system is the possibility of an earthquake. With respect to these contacts, their functioning is unrelated to a seismic event in that they are anticipatory to other diverse parameters which cause reactor trip. The contacts are shut during plant operation and open to cause reactor trip when the turbine is tripped. This design functions in a de-energize-to-trip fashion to cause a plant trip if power is interrupted in the trip circuitry. This ensures that the protection system will not be degraded by this anticipatory trip because seismic design considerations do not form part of the design bases for anticipatory trip sensors. (The integrated protection cabinets which receive the inputs from the anticipatory trip sensors are, of course, seismically qualified as discussed in Section 3.10 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design"). The anticipatory trips thus meet IEEE-279-1971, including redundancy, separation, single failure, etc. Seismic qualification of the contacts sensors is not required.

Bypass capability exists for the four channels, as described in Subsection 7.1.2.2.11.

The logic for these trips is shown on Figure 7.2-1, sheet 14. The development of the P-9 block is shown on Figure 7.2-1, sheet 4.

7.2.1.1.7.2 Turbine Trip on a Reactor Trip

In implementing this function (TT-O-RT) it is recognized that full conformance to IEEE 279 and associated standards is not possible due to the fact that the turbine building is expected to not be in a seismic category I structure. If qualification of the turbine trip equipment (EHC solenoids) cannot be demonstrated, other applicable Sections of IEEE 279 (refer to 4.2, 4.3, 4.5 excluding seismic, 4.6, and 4.10) are criteria for which conformance is to be provided. Although the power source for tripping the turbine need not to be Class 1E, it will use a highly reliable power supply. Furthermore the turbine trip on reactor trip will employ a deenergize to trip principle. The redundant trip paths between the protection system and the EHC will satisfy

separation-by-potential-and-by-space requirements. The installation of components will be done in a manner as reliable as reasonably achievable without reliance on electrical isolation. For the functional logic refer to Figure 7.2-1 (sheet 14).

7.2.1.1.8 Reactor Trip on Safety Injection

A reactor trip will be initiated if safety injection is actuated either automatically or manually. The means for actuating safety injection automatically are described in Section 7.3. This trip protects the core against a loss of reactor coolant or a steamline rupture.

Manual safety injection can be initiated from either of two controls on the control board. Operating either of the two controls will actuate safety injection and will give a reactor trip signal to the reactor trip actuation train from two different means. Outputs on each switch, each separated by a barrier and electrically separated, send their position status to the integrated protection system. These inputs will de-energize the under-voltage trip attachments (UVTA) on the reactor trip breakers, causing them to trip open. Additional outputs on each switch send their position status directly to the shunt trip coil on each reactor trip circuit breaker. These provide a backup to the under-voltage coil trip of the breakers.

The logic for this trip is shown on Figure 7.2-1, sheets 2 and 12.

7.2.1.1.9 Manual Reactor Trip

The manual reactor trip consists of two switches on the main control board, either of which will open all eight of the reactor trip circuit breakers. Outputs on each switch, each separated by a barrier and electrically separated, send their position status to the integrated protection cabinets. These inputs will de-energize the under-voltage coils on the reactor trip circuit breakers, causing them to open. Additional outputs send their status

information directly to the shunt trip attachment UVTA of each breaker. Energizing the shunt trip coil opens the breaker contacts. This acts as a backup to the under-voltage coil trip of the breakers.

The logic for the manual trip is shown on Figure 7.2-1, Sheets 2 and 13. There are no interlocks or bypasses associated with this trip.

7.2.1.1.10 Reactor Trip System Interlocks

The interlocks used in the reactor trip functions are designated as P-xx permissives and are listed on Table 7.2-2. These permissives are implemented at the channel level rather than at the logic train level.

The logic architecture of the IPS does not lend itself to bringing the permissive function to a lower logic level in the creation of a trip function. Also the plant availability has been determined to be improved using the present technique because permissives are integrated to each channel.

Manual blocks to reactor trip are listed on Table 7.2-3 and are described below:

1. Source Range Block (One control for each channel set)

   This block can only be instituted above the P-6 setpoint, and is automatically removed below P-6. The channel is automatically bypassed above P-10, with bypass removed below P-10. See Figure 7.2-1, Sheet 3.

2. Intermediate Range Block (One control for each channel set)

   This block can only be instituted above the P-10 setpoint and is automatically removed below P-10. See Figure 7.2-1, sheet 3.

3. Power Range (low setpoint) block (One control for each channel set)

This block can only be instituted above the P-10 setpoint and is automatically removed below P-10. See Figure 7.2-1, sheet 3.

The above three manual blocks, when used in conjunction with the applicable permissives, are used during startup.

7.2.1.1.11 Bypasses of Reactor Trip Functions

Each channel used in reactor trip can be bypassed, as discussed in Subsection 7.1.2.2.11, except for manual reactor trip, and reactor trips on safety injection. One channel can be bypassed for an indefinite period of time with the trip logic automatically reverting to a two-out-of-three to trip. Two channels can be bypassed for an indefinite period of time with the trip logic reverting to a one-out-of-two to trip. Attempting to bypass more than two channels will result in a reactor trip. The single failure criterion is met during bypasses.

The bypass is implemented automatically during on-line testing. Manual bypass is used during repair or maintenance of sensors or channel electronics.

7.2.1.2 Design Bases For Reactor Trips

This section provides the design bases information on the reactor trip function, including the information required by Section 3 of IEEE-279-1971. Reactor trip is a protective function generated as part of the integrated protection system. As such, there is no "reactor trip system" per se. Those design bases which relate to the equipment which initiate and accomplish reactor trips are contained in Subsection 7.1.2.1 and are not repeated here. The design bases presented here are concerned with the variables monitored for reactor trips, the minimum performance requirements in generating the trips, and the requirements placed on reactor trips during various reactor operating modes.

7.2.1.2.1 Design Basis; Generating Station Conditions Requiring Reactor Trip (Paragraph 1 of Section 3 of IEEE-279-1971)

The generating station conditions requiring protective actions are analyzed in Chapter 15. Those conditions which would typically result in a reactor trip are listed on Table 7.2-5. This table correlates the accident conditions (II, III, or IV events) to each reactor trip.

7.2.1.2.2 Design Basis; Variables, Levels, Ranges, and Accuracies used in Reactor Trip Functions (Paragraphs 2, 5, 6, and 9 of Section 3 of IEEE-279-1971)

The variables required to be monitored for reactor trips are:

1. Neutron flux
2. Nitrogen-16 (N-16) in each loop
3. Pressurizer pressure
4. Water level in the pressurizer
5. Reactor coolant flow in each loop
6. Speed of each reactor coolant pump
7. Water level in each steam generator
8. Reactor coolant inlet temperature (T_{cold}) in each loop
9. Position of each turbine throttle stop valve
10. Pressure of the turbine stop emergency trip fluid
11. Position of each manual safety injection switch
12. Position of each manual reactor trip switch

The typical ranges, accuracies, and response times for each variable are listed on Table 7.2-4.

A discussion on levels that, when reached, will require reactor trip is contained in Subsection 7.1.2.2.1.

The "ALLOWABLE VALUES" for the Limiting Safety System Settings (LSSS) and the "TRIP SETPOINT" for reactor trips are in the Technical Specifications.

7.2.1.2.3 Design Basis; Spatially Dependent Parameters used in Reactor Trip (Paragraph 3 of Section 3 of IEEE-279-1971)

The parameter used for reactor trip which has a spatial dependence is the N-16 power measurement. The N-16 signals from the hot leg of each coolant loop are dependent on coolant density. In order to account for variations on coolant density in the hot leg piping, two N-16 power monitors are located 180 degrees apart on each hot leg. A representative hot leg N-16 signal from each loop is determined by averaging the signals from the two monitors.

Radially varying coolant inlet temperature is not a concern since the resistant temperature detectors (RTDs) are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant such that radial temperature variations do not exist.

Neutron flux is not a spatially dependent concern because of core radial symmetry. The variable is used for axial calculations involving neutron flux. Four-element multi-excore detectors furnish this axially-dependent information to the DNBR and KW/ft calculators as previously described. Each of the four detectors is a four-sectioned detector vertically-oriented, which is referred to herein as a multi-sectional detector.

7.2.1.2.4 Design Basis; Operational Limits for Variables in Various Reactor Operating Modes (Paragraph 4 of Section 3 of IEEE-279-1971)

During start-up or shutdown, reactor trips are provided for three ranges of neutron flux (source, intermediate, and power range). The source range, intermediate range, and power range (low setpoint) trips can be manually blocked when the appropriate power escalation permissives are present. The trips are automatically re-instated during power de-escalation. Subsection 7.2.1.1 describes these reactor trips. Their interlocks are described in Subsection 7.2.1.1.9.

During testing or maintenance, it is advantageous to be able to bypass a channel monitoring a variable for reactor trip. Although no setpoints need to be changed for bypassing, the coincidence logic is automatically adjusted as described in Subsections 7.2.1.1.10 and 7.1.2.2.11. The logic assures that the remaining redundant channels for that variable will meet this single failure criterion. The logic is automatically reinstated when the bypass is removed.

7.2.1.2.5 Design Basis; Reactor Trips for Malfunctions, Accidents, Natural Phenomena, or Credible Events: (Paragraph 8 of Section 3 of IEEE-279-1971)

There are no reactor trip functions which directly shut down the reactor on occurrence of either natural phenomena (such as flood, wind, etc.) or credible events (such as fire, pipe whip, etc.). A seismic trip is provided as an option, however. The operator can, of course, trip the reactor at any time by pressing the manual reactor trip button. The safety system normally relies on provisions made by the owner to protect equipment against damage from events. (See Subsection 7.1.2.2.5).

Functional diversity is employed in determining the reactor trips for accident conditions. Generally, two or more reactor trips will occur for the transients analyzed in the accident analyses.

For example, protection is provided for the complete loss of coolant flow event by low RCP speed and by low coolant flow reactor trips. Therefore, complete reliance is not made on a single reactor trip terminating a given accident. Table 7.2-5 lists the reactor trips and the conditions which will normally result in each trip.

Redundancy is employed to provide assurance that reactor trips will be generated on demand, even when the protection system is degraded by a single random failure within the equipment. All reactor trips are four-way

redundant. The single failure criterion is met even if one or two channels are bypassed, as discussed in Subsection 7.1.2.2.11. The reactor is tripped automatically if an attempt is made to bypass three or more channels.

7.2.1.3 Final System Drawings

Preliminary functional diagrams are provided in Figure 7.2-1, sheets 1-14. Final functional diagrams, block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review will be provided in the plant specific applicant's Final Safety Analysis Report.

7.2.2 Analyses

7.2.2.1 Failure Mode and Effects Analysis (FMEA)

Failure mode and effects analyses will be performed on the integrated protection system which initiates the reactor trip. Results of this study will be documented in a separate report for reference in the plant specific applicant's Preliminary Safety Analysis Report prior to issuance of the Construction Permit.

7.2.2.2 Conformance of the Reactor Trip Function to Applicable Criteria

This section discusses conformance of the reactor trip function to applicable requirements as summarized in Table 7.1-1. Reactor trip is a protective function generated by the Westinghouse integrated protection system. Consequently there is no "reactor trip system" per se. Requirements which address equipment in the protection system are presented in Subsection 7.1.2.2 and are not repeated here. The discussions presented in this section address only the functional aspects of reactor trip.

7.2.2.2.1 Conformance to the General Functional Requirement for Reactor Trip (Paragraph 4.1 of IEEE-279-1971, GDC-13, GDC-20)

Refer also to Subsection 7.1.2.2.1.

The integrated protection system will initiate a reactor trip whenever a condition monitored by the system reaches a preset level. The reactor trips are listed on Table 7.2-1 and are discussed in detail in Subsection 7.2.1.1. The variables which are required to be monitored for these trips are listed in Subsection 7.2.1.2.2. Table 7.2-4 lists the typical ranges, accuracies, and response times for these variables. The levels which, when reached, requiring reactor trips are listed in the Technical Specifications.

As discussed in Subsection 7.1.2.2.1, the setpoints actually set into the equipment provide a margin to the safety limits which are assumed in the accident analyses. The safety limits are based on mechanical or hydraulic limitations of equipment or on heat transfer characteristics on the reactor core. While most setpoints used for reactor trip are fixed, there are continuously calculated setpoints for the DNBR trips. All setpoints for reactor trip have been selected on the basis or engineering design or safety studies. As previously stated, the setpoints all provide a margin before reactor trip is actually required to allow for uncertainties and instrument errors.

The DNBR and KW/ft existing at any point in the core design is not a directly measurable quantity; however, the process variables that determine DNBR are sensed and evaluated. Small isolated changes in various process variables may not individually result in violation of a core safety limit; whereas the combined variations over sufficient time may cause the DNBR or KW/ft limit to be exceeded. The design concept for reactor trips takes cognizance of this situation by providing reactor trips associated with individual process variables in addition to the DNBR and KW/ft safety limit trips. Process variable trips prevent reactor operation whenever a change in the monitored value is such that a core or safety limit is in danger should operation

continue. Basically, DNBR and KW/ft trips provide protection for slow transients. Other trips such as low flow or high flux will trip the reactor for rapid changes in flow or flux respectively. This prevents fuel damage before actuation of the slower responding DNBR and KW/ft trips could be effected.

Table 7.2-5 summarizes the events which will normally result in reactor trips.

7.2.2.2.2 Conformance to the Single Failure Criterion for Reactor Trip (Paragraph 4.2 of IEEE 279-1971, IEEE 379-1972)

Refer also to Subsection 7.1.2.2.2.

A single failure in the integrated protection system or the reactor trip actuation trains will not prevent a reactor trip, even when the reactor trip channels are bypassed for test or maintenance. Conformance of the equipment to this requirement is discussed in Subsection 7.1.2.2.2. In addition to the redundancy of equipment, diversity of reactor trip functions is incorporated. Each Condition II, III, or IV event requiring a reactor trip will typically result in a trip from diverse parameters. Examples of these can be gained from correlating the events listed on Table 7.2-5 to the various reactor trips. For example, reactor trip because of an uncontrolled rod cluster control assembly bank withdrawal at power may occur on power range high neutron flux, low DNBR, high KW/ft, pressurizer high pressure or pressurizer high water level. Reactor trip on complete loss of reactor coolant flow may occur on low flow or from the diverse parameter of low RCP pump speed. The accident analyses may ignore reactor trips from some parameters to intentionally allow the simulation of the event to proceed farther than will actually happen. These worst case assumptions provide additional conservatism to the results.

7.2.2.2.3 Conformance to the Requirements Covering Control and Reactor Trip Interactions (Paragraph 4.7 of IEEE 279-1971, GDC-24)

Refer also to Subsection 7.1.2.2.7.

The Westinghouse nuclear steam supply system (NSSS) is designed to permit maneuvering of the plant in response to normal power generation demands without causing a reactor trip. The plant control system will attempt to keep the reactor operating away from any safety limit; however, the selection of the reactor trip setpoints does not assume such control actions. The accident analyses in Chapter 15 will usually assume that the plant is at normal operation commensurate with the operating mode at the onset of the accident. That is, if a control system action leads to more conservative results, that assumption will be made. If, on the other hand, failure of a control system to work leads to more conservative results, that assumption will be made. In this way, reactor trips do not depend on control system actions.

As stated in Subsection 7.1.2.2.7, Westinghouse considers it advantageous to use certain protection channels for control. Isolation devices are incorporated into these data links to prevent control system failures from degrading the performance of the protection system.

Failures in a protection channel monitoring a variable which is also used for control will not result in control system actions requiring protection by the redundant channels monitoring that variable. This is discussed in Subsection 7.1.2.2.7.

7.2.2.2.4 Conformance to Requirements on the Derivation of System Inputs for Reactor Trip (Paragraph 4.8 of IEEE 279-1971)

Refer also to Subsection 7.1.2.2.8.

To the extent feasible, inputs used for reactor trip are derived from signals that are direct measurements of the desired variables. Two exceptions exist,

DNBR and KW/ft which cannot be directly measured. The process variables that do affect these parameters can be measured and they are used to calculate continuously the DNBR setpoint and the KW/ft values.

The DNBR trip setpoint is calculated from pressurizer pressure, reactor coolant inlet temperature, N-16, and nuclear axial power shape. Normal flow is assumed in the calculation. The setpoint is compared against N-16.

KW/ft is calculated from N-16, and the nuclear axial power shape in the core. This value is compared against a fixed setpoint.

The DNBR and KW/ft trips are described in detail in Subsection 7.2.1.1.2.

7.2.2.2.5 Conformance to Requirements on Bypassing of Reactor Trip Functions (Paragraph 4.11, 4.12, 4.13, and 4.14 of IEEE 279-1971)

With the exception of the manual reactor trips, all reactor trips channels and the reactor trip actuation trains can be bypassed as described in Subsections 7.1.2.2.11 through 7.1.2.2.14. The requirements of paragraphs 4.12 through 4.14 of IEEE 279-1971 are discussed in those subsections.

Operating bypasses for reactor trips are described in Subsection 7.2.1.1.9.

7.2.2.2.6 Conformance to Requirements on Multiple Setpoints used for Reactor Trips: (Paragraph 4.15 of IEEE 279-1971)

Conformance of the design for reactor trips to this requirement of IEEE 279-1971 is discussed in Subsection 7.2.1.2.4. Refer also to Subsection 7.1.2.2.15.

7.2.2.2.7 Conformance to the Requirement for Completion of Reactor Trip Once it is Initiated: (Paragraph 4.16 of IEEE 279-1971, Regulatory Guide 1.62)

Once initiated, all reactor trips will go to completion. Return to operation requires deliberate operator action to reset the reactor trip circuit breakers which were opened to trip the reactor. The circuit breakers cannot be closed while the reactor trip signals are present from the respective integrated protection cabinets. A manual control is provided on the main control board for resetting the reactor trip signals in each integrated protection cabinet following a reactor trip. Refer also to Subsection 7.1.2.2.16.

7.2.2.2.8 Conformance to the Requirement to Provide for Manual Initiation of Reactor Trip: (Paragraph 4.17 of IEEE 279-1971, Regulatory Guide 1.62)

The reactor can be tripped by actuating one of two manual reactor trip controls from the main control board. The reactor can also be tripped by actuating one of two manual safety injection controls on the main control board. Both of these trips are described in detail in Subsections 7.2.1.1.7 and 7.2.1.1.8. Refer also to Subsection 7.1.2.2.17.

TABLE 7.2-1
REACTOR TRIPS

Reactor Trip**	* of Channels	Channel Set Trip Logic:	Bypass Logic:	Permissives & Interlocks (See Table 7.2-2)
1. Source Range Reactor Trip	4	2/4	Yes*	P-6, P-10
2. Intermediate Range Reactor	4	2/4	Yes*	P-10
3. Power Range (Low Setpoint) Trip	4	2/4	Yes*	P-10
4. Power Range (High Setpoint) Trip	4	2/4	Yes*	----
5. High Positive Flux Rate Trip	4	2/4	Yes*	----
6. High Negative Flux Rate Trip	4	2/4	Yes*	----
7. Low DNBR (N-16) Reactor Trip	4 (1/loop)	2/4	Yes*	----
8. High KW/ft Reactor Trip	4 (1/loop)	2/4	Yes*	----
9. Pressurizer Low Pressure Trip	4	2/4	Yes*	P-7
10. Pressurizer High Pressure Trip	4	2/4	Yes*	----
11. Pressurizer High Water Level Trip	4	2/4	Yes*	P-7
12. Low Reactor Coolant Flow	(a) 4/Loop (b) 4/Loop	2/4 In any loop 2/4 In 2/4 loops	Yes* Yes*	P-8 P-7
13. Reactor Coolant Pump Underspeed	4 (1/RCP)	2/4	Yes*	P-7
14. Low Steam Generator Water Level	4/S.G.	2/4 In any S.G.	Yes*	----

*Bypass Logic = 2/4 with no bypasses; 2/3 with 1 bypass; 1/2 alarmed with 2 bypasses; automatic trip with three or four bypasses.
**Reactor Trip Actuation Trains can also be bypassed with the logic as defined in "*" above.

TABLE 7.2-1 (Cont.)

REACTOR TRIPS

Reactor Trip**	* of Channels	Channel Set Trip Logic:	Bypass Logic:	Permissives & Interlocks (See Table 7.2-2)
15. High Steam Generator Water Level	4/S.G.	2/4 In any S.G.	Yes*	----
16. Closed Turbine Throttle Stop Valves (not provided on plants with full load rejection capability)	1/valve	2/4 valves	Yes*	P-9 (optional on plants without full load rejection)
17. Low Stop Emerg. Trip Fluid Pressure (not provided on plants with full load rejection capability)	4	2/4	Yes*	P-9 (optional on plants without full load rejection)
18. Automatic Safety Injection	4	2/4	Yes*	----
19. Manual Safety Injection	2 switches	1/2 switches	No	----
20. Manual Reactor Trip	2 switches	1/2 switches	No	----

*Bypass Logic = 2/4 with no bypasses; 2/3 with 1 bypass; 1/2 alarmed with 2 bypasses; automatic trip with three or four bypasses.

**Reactor Trip Actuation Trains can also be bypassed with the logic as defined in "*" above.

TABLE 7.2-2

REACTOR TRIP PERMISSIVES & INTERLOCKS

Designation	Derivation	Function
P-6	intermediate range neutron flux above setpoint	Allows manual block of source range reactor trip.
$\overline{\text{P-6}}$	intermediate range neutron flux below setpoint.	Automatically defeats any block of source range reactor trip
P-7	power range nuclear power above setpoint	Permits reactor trips on low flow in more than one coolant loop, RCP under speed, pressurizer low pressure, and pressurizer high water level.
$\overline{\text{P-7}}$	power range nuclear power below setpoint	Blocks reactor trips on low coolant flow in more than 1 loop, RCP under-speed, pressurizer low pressure, and pressurizer high water level.
P-8	power range nuclear power above setpoint	Permits reactor trip on low flow in any loop.
$\overline{\text{P-8}}$	power range nuclear power below setpoint	Blocks reactor trip on low coolant flow in any single loop.
P-9*	power range nuclear power above setpoint	Permits reactor trip on a turbine trip.
$\overline{\text{P-9*}}$	power range nuclear power below setpoint	Blocks reactor trip on a turbine trip.
P-10	power range nuclear power above setpoint	(a) Allows manual block of power range (low setpoint) reactor trip.

* P-9 is an option on those plants that do not have full load rejection capability. Plants with full load rejection do not incorporate a reactor trip on turbine trip.

TABLE 7.2-2 (Cont.)

REACTOR TRIP PERMISSIVES & INTERLOCKS

Designation	Derivation	Function
		(b) Allows manual block of intermediate range reactor trip and C-1. (See Table 7.7-1)
		(c) Automatically blocks source range reactor trip (back-up to P-6)
P-10	power range nuclear power below setpoint	(a) Defeats the block of power range (low setpoint) reactor trip.
		(b) Defeats the block of intermediate range reactor trip and C-1. (See Table 7.7-1)
		(c) Permits manual reset of each source range channel reactor trip.

TABLE 7.2-3

SYSTEM-LEVEL MANUAL INPUTS TO THE REACTOR TRIP FUNCTIONS

	MANUAL CONTROL	TO CHANNEL SET				FIGURE 7.2-1 SHEET:
(1)	Manual Reactor Trip Control #1	I	II	III	IV	(2&13)
(2)	Manual Reactor Trip Control #2	I	II	III	IV	(2&13)
(3)	Reactor Trip Reset	I	II	III	IV	(13)
(4)	Source Range Block, Ch. Set I	I				(3)
(5)	Source Range Block, Ch. Set II		II			(3)
(6)	Source Range Block, Ch. Set III			III		(3)
(7)	Source Range Block, Ch. Set IV				IV	(3)
(8)	Intermediate Range Block, Ch. Set I	I				(3)
(9)	Intermediate Range Block, Ch. Set II		II			(3)
(10)	Intermediate Range Block, Ch. Set III			III		(3)
(11)	Intermediate Range Block, Ch. Set IV				IV	(3)
(12)	Power Range Block (Low Setpoint), Ch. Set I	I				(3)
(13)	Power Range Block (Low Setpoint), Ch. Set II		II			(3)
(14)	Power Range Block (Low Setpoint), Ch. Set III			III		(3)
(15)	Power Range Block (Low Setpoint), Ch. Set IV				IV	(3)
(16)	Manual Safety Injection #1	I	II	III	IV	(2&12)
(17)	Manual Safety Injection #2	I	II	III	IV	(2&12)

Note: All controls are located on the control board except as noted on the applicable sheet of Figure 7.2-1.

TABLE 7.2-4

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES
[DESIGN BASIS FOR REACTOR TRIP]

PROTECTIVE FUNCTIONS	VARIABLES TO BE MONITORED	RANGE OF VARIABLES (TYPICAL)	PROTECTION SYSTEM ACCURACY (TYPICAL) (NOMINAL)	RESPONSE TIME (SEC)*
A. Reactor Trips				
1. Source Range High Neutron Flux	Neutron Flux	6 Decades of Neutron Flux 1 to 10^6 C/S	±5% of full power	0.5
2. Interm. Range High Neutron Flux	Neutron Flux	8 Decades of Neutron Flux Overlapping Source Range by 2 Decades and Including 100% Power	±5% of full scale ±1% of full scale From 10^{-4} to 10^{-3} amp	0.5
3. Power Range High Neutron Flux (Low Setting)	Neutron Flux	1 to 120% Full Power	±1% of Full Power	0.5
4. Power Range High Neutron Flux (Hi-Setting)	Neutron Flux	1 to 120% of Full Power	±1% of Full Power	0.5
5. High Positive Flux Rate	Neutron Flux	1 to 120% of Full Power	±5% of Span	0.5
6. High Negative Flux Rate	Neutron Flux	1 to 120% of Full Power	±5% of Span	0.5
7. Low DNBR			±5% of Rated Core Power	6.0
	Reactor Coolant Inlet Temp. (T_{COLD})	510 to 630°F		
	Pressurizer Pressure	1700 to 2500 psig		

TABLE 7.2-4 (Cont.)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES

[DESIGN BASIS FOR REACTOR TRIP]

PROTECTIVE FUNCTIONS	VARIABLES TO BE MONITORED	RANGE OF VARIABLES (TYPICAL)	PROTECTION SYSTEM ACCURACY (TYPICAL) (NOMINAL)	RESPONSE TIME (SEC)*
	N-16 Power	0 to 150% of Rated Core Power		
	Excore Detector Flux (Power Range)	0 to 120% of Rated Core Power		
8. High KW/ft			±10% of Rated Core Power	2.5
	N-16 Power	0 to 150% of Rated Core Power		
	Excore Detector Flux (Power Range)	0 to 120% of Rated Core Power		
9. Pressurizer Low Pressure	Pressurizer Pressure	1700 to 2500 psig	±18 psi (Compensated Signal)	2.0
10. Pressurizer High Pressure	Pressurizer Pressure	1700 to 2500 psig	±14 psi (Uncompensated Signal)	2.0
11. Pressurizer High Water Level	Water Level	Entire Cylindrical Portion of Pressurizer	±2.3% of Full Range ΔP Between Taps At Design Temp Pressure	2.0
12. Low Reactor Coolant Flow	Coolant Flow	0 to 120% of Rated Flow	±2.5% of Full Flow Within Range of 70% to 100% of Full Power	1.0

TABLE 7.2-4 (Cont.)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES

[DESIGN BASIS FOR REACTOR TRIP]

PROTECTIVE FUNCTIONS	VARIABLES TO BE MONITORED	RANGE OF VARIABLES (TYPICAL)	PROTECTION SYSTEM ACCURACY (TYPICAL) (NOMINAL)	RESPONSE TIME (SEC)*
13. Low Reactor Coolant Pump Speed	Pump Speed	0 to 120% of Rated Speed	±1.0%	0.6
14. Low Water Level in Any Steam Generator	Water Level	~8 ft. Below Nominal Full Load Water Level	±2.3% of ΔP Signal Over Pressure Range of 700 to 1200 psig	2.0
15. High Water Level In Any Steam Generator	Water Level	~ 6 ft. Above Nominal Full Load Water Level	±2.3% of ΔP Signal Over Pressure Range of 700 to 1200 psig	2.0
16. Turbine Trip A. Closure of Turbine Throttle/Stop Valves	Valve Position	N.A.	N.A.	2.0
B. Low Stop Emergency Trip Fluid Pressure	Fluid Pressure	N.A.	N.A.	2.0
17. Safety Injection	See Section B1 ESF	See Section B1 ESF	See Section B1 ESF	See Section B1 ESF
18. Manual Reactor Trip	N.A.	N.A.	N.A.	N.A.

*Time from step change of the variable being monitored from 5% below to 5% above the setpoint. Value until the rods are free to fall.

TABLE 7.2-5

PROTECTIVE FUNCTIONS FOR CONDITION II, III, AND IV EVENTS

NOTES:
1. ○ Indicates where this protective function (e.g. a trip - may occur during the course of the accident (see chapter 15 subsections 2 through 4) but this protective function by itself does not necessarily impose functional requirements on this function.
2. ① Indicates initial protective function, that generates a trip signal for the design condition.

	ACCIDENTS	7.2 REACTOR TRIPS (SEE TABLE 7.2-5)																				7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (ESFAS) (SEE TABLE 7.3-5)									
		1. SOURCE RANGE HIGH NEUTRON FLUX	2. INTERMEDIATE RANGE HIGH NEUTRON FLUX	3. POWER RANGE HIGH NEUTRON FLUX (LOW SETTING)	4. POWER RANGE HIGH NEUTRON FLUX (HIGH SETTING)	5. HIGH POSITIVE FLUX RATE	6. HIGH NEGATIVE FLUX RATE	7. LOW DNBR	8. HIGH KW/FT	9. PRESSURIZER LOW PRESSURE	10. PRESSURIZER HIGH PRESSURE	11. PRESSURIZER HIGH WATER LEVEL	12. LOW REACTOR COOLANT FLOW	13. REACTOR COOLANT PUMP UNDERSPEED	14. LOW WATER LEVEL IN ANY STEAM GENERATOR	15. HIGH WATER LEVEL IN ANY STEAM GENERATOR	16. TURBINE TRIP (ANTICIPATORY)	17. SAFETY INJECTION	18. MANUAL REACTOR TRIP	1. SAFETY INJECTION	2. CONTAINMENT SPRAY	3. CONTAINMENT ISOLATION $\phi\phi$	4. $\phi\phi$	5. CONTAINMENT VENTILATION ISOLATION	6. STEAM LINE ISOLATION	7. FEEDWATER LINE ISOLATION	8. STARTUP OF EMERGENCY FEEDWATER PUMPS	9. TURBINE TRIP	10. BLOCK BORON DILUTION
15.2 CONDITION II EVENTS	2.1 UNCONTROLLED ROD CLUSTER CONTROL ASSEMBLY BANK WITHDRAWAL FROM A SUBCRITICAL CONDITION	○	○	①	○	○																								
	2.2 UNCONTROLLED ROD CLUSTER CONTROL ASSEMBLY BANK WITHDRAWAL AT POWER				①			①	○		○	○																	○	
	2.3 ROD CLUSTER CONTROL ASSEMBLY MISALIGNMENT						①																						○	
	2.4 UNCONTROLLED BORON DILUTION	①			①			①	○		○	○																	○	①
	2.5 PARTIAL LOSS OF FORCED REACTOR COOLANT FLOW												①																○	
	2.6 START-UP OF AN INACTIVE REACTOR COOLANT LOOP				○								①																○	
	2.7 LOSS OF EXTERNAL ELECTRICAL LOAD AND/OR TURBINE TRIP							○			①	○					○												○	
	2.8 LOSS OF NORMAL FEEDWATER										○	○			①														○	
	2.9 LOSS OF OFF-SITE POWER TO THE STATION AUXILIARIES (STATION BLACKOUT)										○	○	○		①		○											○	○	
	2.10 EXCESSIVE HEAT REMOVAL DUE TO FEEDWATER SYSTEM MALFUNCTION			○	○			○	○							①				○						○			○	
	2.11 EXCESSIVE LOAD INCREASE INCIDENT				○			○	○	○																			○	
	2.12 ACCIDENTAL DEPRESSURIZATION OF THE REACTOR COOLANT SYSTEM							○		①																			○	
	2.13 ACCIDENTAL DEPRESSURIZATION OF THE MAIN STEAM SYSTEM									○								①		①					①	①	○	○		
15.3 CONDITIONS III EVENTS	3.1 LOSS OF REACTOR COOLANT FROM SMALL RUPTURED PIPES OR FROM CRACKS IN LARGE PIPES WHICH ACTUATES THE ECCS									①								○		①						○	○			
	3.2 MINOR SECONDARY STEAM PIPE BREAKS (ANALYSIS COVERED BY LARGE BREAKS)																													
	3.3 INADVERTENT LOADING OF A FUEL ASSEMBLY INTO AN IMPROPER POSITION																													
	3.4 COMPLETE LOSS OF FORCED REACTOR COOLANT FLOW												○	①															○	
	3.5 SINGLE ROD CLUSTER CONTROL ASSEMBLY WITHDRAWAL AT FULL POWER							○																					○	
15.4 CONDITION IV EVENTS	4.1 MAJOR REACTOR COOLANT SYSTEM PIPE RUPTURE (LOCA)									①								○		①	○								○	
	4.2.1 MAJOR SECONDARY SYSTEM PIPE RUPTURE MAIN STEAM LINE RUPTURE				○			○	○	○								○		①					①	①	○	○		
	4.2.2 MAJOR SECONDARY SYSTEM PIPE RUPTURE MAIN FEEDWATER LINE RUPTURE							○			○				①			○		○					○		○	○		
	4.3 STEAM GENERATOR TUBE RUPTURE							○		①						○		○		①									○	
	4.4 SINGLE REACTOR COOLANT PUMP LOCKED ROTOR												①																○	
	4.5 FUEL HANDLING ACCIDENT																													
	4.6 RUPTURE OF A CONTROL ROD DRIVE MECHANISM HOUSING (ROD CLUSTER CONTROL ASSEMBLY EJECTION)			①	①	○																							○	

FIGURE 7.2-1

(SHEETS 1 THROUGH 14)

"WAPWR STANDARD FUNCTIONAL DIAGRAMS"

(FOLDOUT)

PROPRIETARY

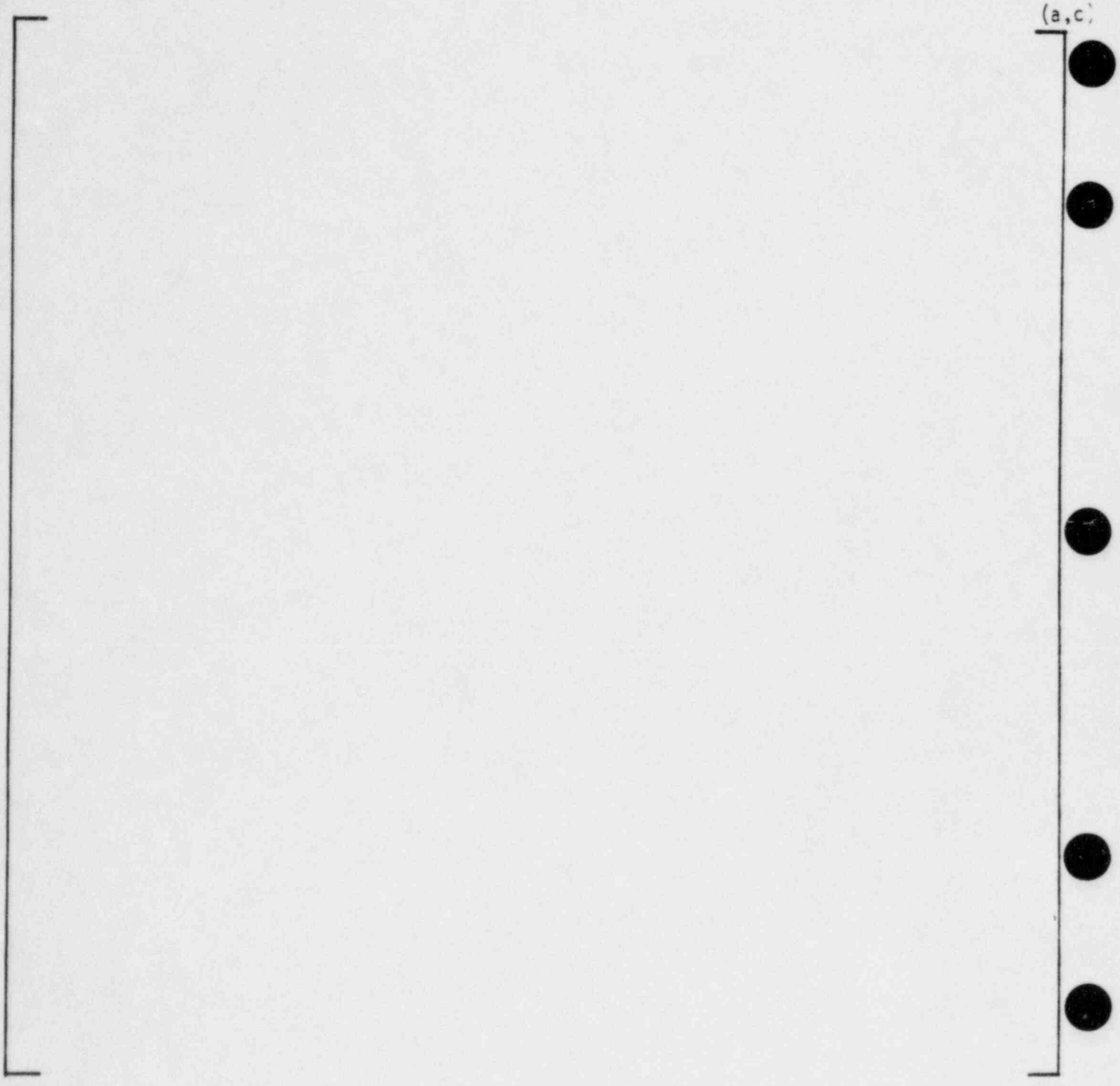


Figure 7.2-2. Generation of a Typical Reactor Trip Function

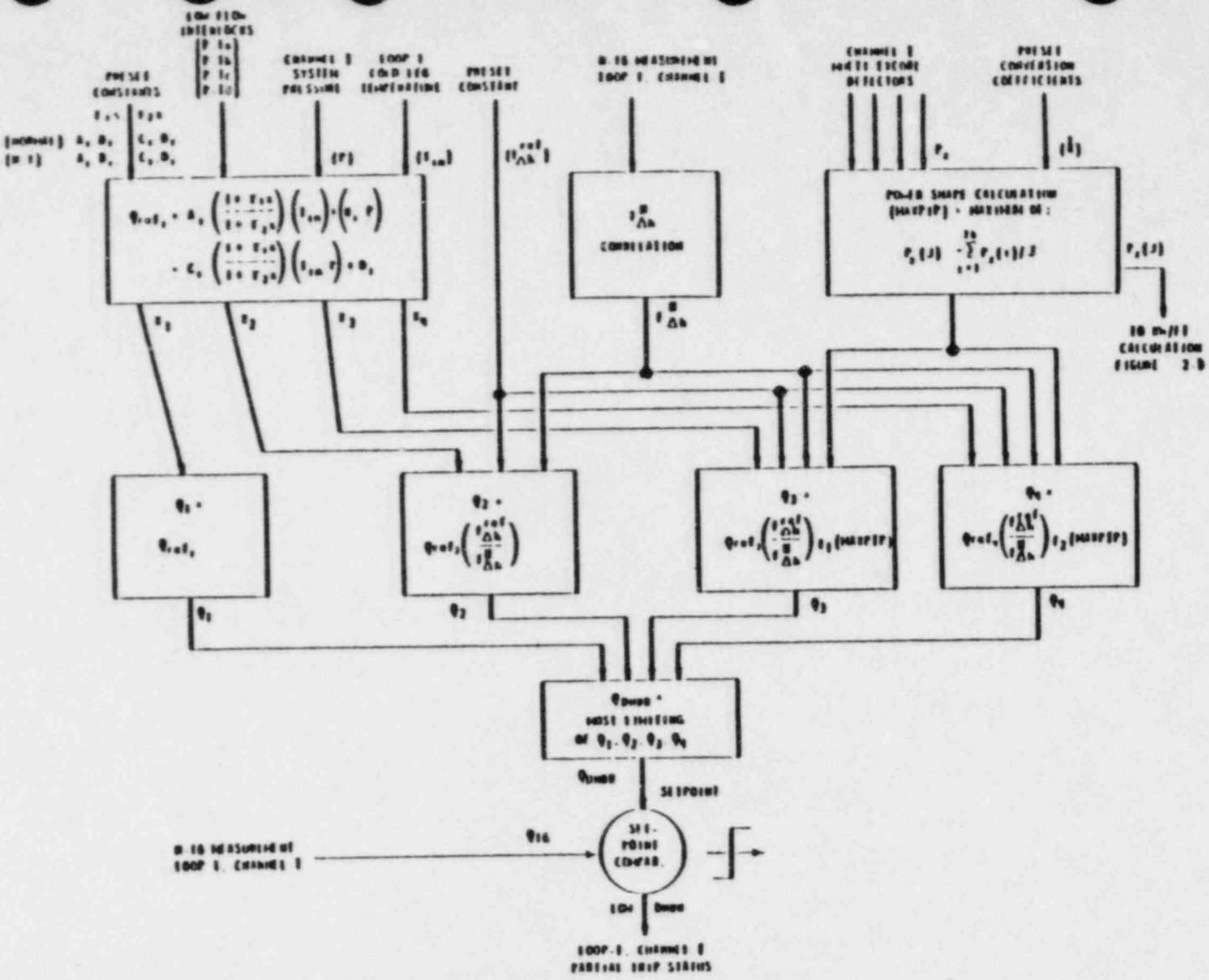


FIGURE 7.2-3 BLOCK DIAGRAM OF DNBR CALCULATIONS

FIGURE 7.2-4 BLOCK DIAGRAM OF HIGH KW/FT CALCULATIONS

7.3 ENGINEERED SAFETY FEATURES (ESF)

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility shall be provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary engineered safety features. The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the engineered safety features in order to prevent or mitigate damage to the core and reactor coolant system components, and ensure containment integrity.

7.3.1 Description

The integrated protection system (IPS) determines whether or not safety limits are being approached for selected plant parameters. If they are, the IPS combines the signals through logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures. Once the required logic combination is generated, the IPS will send the signals to actuate appropriate engineered safety features components in the protective action system. A block diagram of the IPS is given in Figure 7.1-2.

The equipment involved in engineered safety features actuation is listed below. (Refer to Subsections 7.1.1.2.2 and 7.1.1.2.3 for descriptions of the equipment.)

1. Integrated Protection System (4 redundant channel sets)

    a. Sensors
    b. Integrated Protection Cabinets (4 Cabinets)
    c. Engineered Safety Features Actuation Cabinets (2 Cabinets)
    d. Integrated Logic Cabinets
    e. Manual Inputs and Status Indication

2. Protective Action System (2 redundant safeguards trains)

   a. Actuation Devices (e.g., switchgear, motor control centers, auxiliary motors, and solenoids)

   b. Actuated Equipment (e.g., valves, pumps, etc. - see Subsection 7.1.1.3.2)

The following paragraphs summarize the major functional elements of the IPS which are involved in generating an ESF actuation signal to a safeguards component. Refer to Subsection 7.1.1.1.2 for detailed explanations of the functions.

Refer to Figure 7.1-2 for the following description.

Four sensors normally monitor each variable which is used for an engineered safety feature actuation. (These sensors may be monitoring the same variable for a reactor trip function as well.) Analog measurements are converted to digital form by analog-to-digital (A-D) converters within each of the 4 integrated protection cabinets (IPC's). Following any required signal conditioning or processing, the measurements are compared against applicable setpoints for the ESF function to be generated. When the measurement exceeds the setpoint, the output of the comparison results in a channel "partial trip" condition. The partial trip information for all channels is transmitted over isolated data links to engineered safety features actuation cabinets (ESFAC's) I and II to form the basic signals which will eventually result in a safeguards Train-A or Train-B actuation. The voting logic is performed twice within each ESFAC. Each voting logic element will generate an actuation signal if the required coincidence of partial trips exist at its inputs.

Within each ESFAC, the signals are combined through ESF logic sensitive to accident situations to generate a system-level ESF signal. For example, a safety injection signal will be generated on coincidence of low-3 T_{cold} and P-15, or on low pressurizer pressure, or on high-1 containment pressure, etc. System-level ESF manual actions are also processed by the ESF logic in each ESFAC.

The system-level signals must then be broken down to the individual signals through the logic cabinets to start each component associated with an engineered safety feature. For example, a single safety injection signal must start pumps, align valves, start diesel generators, etc. The interposing logic within each logic cabinet accomplishes this function and also performs necessary interlocking to ensure that components are properly aligned for safety. Component-level manual actions are also processed in the interposing logic. Since each logic cabinet computer signal is triplicated for reliability and to prevent inadvertent actuation, the triplicated component-level signals must be "voted" in the power interface. The power interface also transforms the low level signals to voltages and currents commensurate with the actuation devices which they must operate. The actuation devices in turn control motive power to the final safeguards component. The logic cabinets thus interface the integrated protection system to the 2 safeguards trains of the protective action system.

Subsection 7.3.1.1 provides a description of each of the engineered safety features. Subsection 7.3.1.2 provides the design bases information as required by Section 3 of IEEE 279-1971. Subsection 7.3.2 discusses conformance of the engineered safety features to the requirements stated in Section 4 of IEEE 279-1971. The functional diagrams for engineered safety features actuation are presented in Figure 7.2-1.

7.3.1.1 Functional Description

The following subsections describe the specific engineered safety features and are grouped into the following categories of actuation signals:

1. Safety Injection (Subsection 7.3.1.1.1)
2. Steamline Isolation (Subsection 7.3.1.1.2)
3. Containment Spray (Subsection 7.3.1.1.3)
4. Containment Isolation (Subsection 7.3.1.1.4)
5. Main Feedwater Isolation (Subsection 7.3.1.1.5)
6. Emergency Feedwater (Subsection 7.3.1.1.6)
7. Blocking Boron Dilution (Subsection 7.3.1.1.7)

Table 7.3-1 lists the engineered safety features actuation signals and summarizes the coincidence logic that will actuate these functions. The permissives and interlocks for the functions are given on Table 7.3-3. System-level manual inputs to ESF are listed on Table 7.3-4.

7.3.1.1.1 Engineered Safety Features Actuated on a Safety Injection (SI) Signal (See Figure 7.2-1, Sheet 12)

The safety injection signal will be derived from one or more of the following initiating means:

1. Manual Initiation of Safety Injection; or
2. High (Hi-1) Containment Pressure; or
3. Pressurizer Low Pressure; or
4. Low Compensated Steamline Pressure in any Steamline; or
5. Low-3 T_{cold} in 2/4 loops.

To permit startup and cooldown, the safety injection signals on low compensated steamline pressure, low pressurizer pressure, or low-3 T_{cold} may be manually blocked when pressurizer pressure is below the P-11 setpoint. To permit operation below normal operating temperatures for at power reactivity control, the safety injection signal on low-3 T_{cold} is automatically blocked whenever nuclear power is above the P-15 setpoint.

The safety injection signal may be manually reset after 30 to 750 seconds following initiation. It will remain reset until the reactor trip breakers are closed. The time delay assures that, on a blackout, the diesel generators have been brought up to speed and all the required loads sequenced on before permitting the operator to reset safety injection signal. Resetting the signal does not turn off any safeguards equipment, since individual components are required to latch in and seal on the SI signal. (See note 5 on Figure 7.2-1, Sheet 12). However, the operator cannot take manual control of any safeguards component actuated by the safety injection signal, until the SI signal is first reset.

The safety injection signal will actuate the following engineered safety features:

1. Startup of emergency feedwater pumps, steam generator letdown isolation, and startup feedwater termination;

2. Startup of emergency diesels;

3. Start of service-water pumps and isolation of non-essential service water, if required;

4. Start of other pumps (e.g., component cooling);

5. Start of emergency fan coolers;

6. Emergency Core Cooling System and alignment of it to the safety injection mode.

7. Safety injection diesel loading sequence when and if sequencing is necessary;

8. Reactor trip, provided one has not been generated by one of the reactor trip functions identified in Section 7.2;

9. Phase-A containment isolation to prevent fission product release; i.e., isolation of all lines not essential to safety injection;

10. Containment ventilation isolation;

11. Control room isolation;

12. Feedwater isolation.

7.3.1.1.2 Engineered Safety Features Actuated on a Steamline Isolation Signal (See Figure 7.2-1, Sheet 10)

A steamline isolation signal will be derived from any one of the following conditions:

1. Manual initiation of steamline isolation; or
2. High steamline negative pressure rate; or
3. Low compensated steamline pressure or
4. High (Hi-2) containment pressure; or
5. Low-3 T_{cold}

Steamline isolation on conditions 3 or 5 above may be manually blocked when pressurizer pressure is below the P-11 setpoint. Steamline isolation on condition 5 is automatically blocked when nuclear power is above the P-15 setpoint.

The steamline isolation signal will close all steamline isolation valves and bypass valves which are in parallel with the associated steamline isolation valves. In addition to manual system-level steamline isolation, each steamline isolation valve can be individually closed.

7.3.1.1.3 Engineered Safety Features Actuated on a Containment Spray Signal (See Figure 7.2-1, Sheet 13)

A signal to actuate containment spray will be generated from any of the following conditions:

1. Manual actuation of 1 pair out of the 2 pairs of manual spray switches; or

2. High (Hi-3) containment pressure.

The containment spray signal may be manually reset from the main control board. This resets the signal but will not terminate spray.

The containment spray signal will actuate the following safeguards features:

1. Start of containment spray to reduce containment pressure and temperature following a loss of coolant accident or steamline break inside containment.

2. Containment isolation (Phase B) following a LOCA, steamline or feedline break accident inside containment, to limit radioactive releases. (Phase B isolation together with Phase A isolation results in isolation of all but the safety injection and containment spray lines penetrating the containment.)

In addition to the above, manual initiation of spray will cause containment ventilation isolation if not already actuated by safety injection.

7.3.1.1.4 Engineered Safety Features Actuated on a Containment Isolation Signal (See Figure 7.2-1, Sheet 13)

Phase A containment isolation will be generated on a safety injection signal (manual or automatic) as described in Subsection 7.3.1.1.1. It can also be initiated by one of two Phase A controls on the main control board.

Phase B containment isolation will be initiated on high (Hi-3) containment pressure or on manual initiation of containment spray, as described in Subsection 7.3.1.1.3.

Containment ventilation isolation will occur on a safety injection signal (automatic or manual) as described in Subsection 7.3.1.1.1 or by manual initiation of Phase A isolation or by manual initiation of containment spray, as described in Subsection 7.3.1.1.3.

7.3.1.1.5 Engineered Safety Features Actuated on a Feedwater Isolation Signal (See Figure 7.2-1, Sheets 2, 8, 10)

A feedwater isolation signal will be generated under any of the following conditions:

1. High water level in any steam generator; or
2. Safety injection (automatic or manual) see Subsection 7.3.1.1.1; or
3. Low-2 T_{cold} in any 2/4 loops; or
4. Low pressurizer water level if the reactor has been tripped.

Condition 4 above will cause closure of all main feedwater control valves. Conditions 1 through 3 above will cause tripping of all main feedwater pumps and closure of all feedwater isolation valves, main feedwater control valves and bypass valves.

Feedwater isolation on low-2 T_{cold} may be manually blocked when the pressurizer pressure is below the P-11 setpoint. Feedwater isolation on low-2 T_{cold} is automatically blocked whenever nuclear power is above the P-15 setpoint.

7.3.1.1.6 Engineered Safety Features Actuated on a Signal to Actuate the Emergency Feedwater System (See Figure 7.2-1, Sheets 7, 8)

The Emergency Feedwater System will be actuated on any of the following conditions:

1. Low-1 water level (narrow range instrumentation) in any steam generator coincident with the failure of the startup feedwater system to deliver adequate cooling flow to the same steam generator; or

2. Low-2 water level (wide range instrumentation) in any steam generator coincident with reactor trip; or

3. Safety injection (automatic or manual) - see Subsection 7.3.1.1.1; or

4. Manual.

The following events occur on conditions 1-4 above:

1. Both motor and turbine driven emergency feedwater pumps are started.

2. The startup feedwater pump is stopped and startup feedwater flow control valves are closed.

3. Blowdown isolation and sample line valves are closed. They are also closed on low-1 water level in any steam generator.

The emergency feedwater isolation valves between either pair of steam generators, which have normally interconnected emergency feedwater lines, will close when an excessive pressure differential exists between them.

7.3.1.1.7 Engineered Safety Features Actuated on a Signal to Block Boron Dilution (See Figure 7.2-1, Sheet 3)

A signal to block boron dilution will be derived from source range neutron flux increasing at an excessive rate (source range flux doubling). The source range flux doubling signal may be blocked manually above the P-6 power level. It is automatically reinstated below P-6. The block of boron dilution is required if the source range flux doubling count rises during startup or shutdown, indicating an unplanned boron dilution. A signal to block boron dilution will close the volume control tank (VCT) outlet isolation valves and open the makeup valves from the spent fuel pit.

7.3.1.1.8 Blocks, Permissives, and Interlocks for ESF Actuation

The interlocks used for engineered safety features actuation are designated as P-xx permissives and are listed on Table 7.3-3.

Manual blocks to engineered safety features actuations are described below:

1. Safety Injection on pressurizer low pressure, low compensated steamline pressure, or low-3 T_{cold} (when nuclear power is below the P-15 setpoint) can be manually blocked when pressurizer pressure is below the P-11 setpoint.

2. Steamline Isolation on low compensated steamline pressure, high negative steam pressure rate, or low-3 T_{cold} (when nuclear power is below the P-15 setpoint) can be manually blocked when pressurizer is below the P-11 setpoint

3. Feedwater isolation on low-2 T_{cold} (when nuclear power is below the P15 setpoint) can be manually blocked when pressurizer pressure is below the P-11 setpoint.

4. Tripping of the turbine on low-2 compensated T_{cold} (when nuclear power is below the P-15 setpoint) can be manually blocked when pressurizer pressure is below the P-11 setpoint.

5. The block of boron dilution source range flux doubling can be manually defeated above the P-6 intermediate range power level.

7.3.1.1.9 Bypasses of Engineered Safety Features Actuations

The channels used in engineered safety features actuation which can be manually bypassed in the integrated protection system are indicated on Table 7.3-1. A description of this bypass capability is given in Subsection 7.1.2.2.11. The actuation logic for ESF which is contained in the ESFAC and

logic cabinets will not be bypassed for test. Instead, the output of one of the two ESF logic trains in a cabinet in test will be placed in a trip condition.

7.3.1.1.10 Sequencing of ESF Loads

See Chapter 8.

7.3.1.2 Design Bases for Engineered Safety Features Actuation

This section provides the design bases information for engineered safety features actuation, including the information required by Section 3 of IEEE 279-1971. Engineered safety features are protective functions initiated by the integrated protection system. Consequently, there is no ESF actuation system per se. Those design bases which relate to the equipment which initiate and accomplish engineered safety features are given in Subsection 7.1.2.1 and are not repeated here. The design bases presented here are concerned with the variables monitored for ESF actuation and the minimum performance requirements in generating the actuation signals.

7.3.1.2.1 Design Basis; Generating Station Conditions Requiring ESF Actuation (Paragraph 1 of Section 3 of IEEE 279-1971)

The following is a summary of those generating station conditions requiring protective action:

1. Primary System

    a. Rupture in small pipes or cracks in large pipes
    b. Rupture of a reactor coolant pipe (loss of coolant accident)
    c. Steam generator tube rupture.

2. Secondary System

   a. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief or safety valve

   b. Rupture of a major steamline pipe

   c. Rupture in feedline pipe

Table 7.2-4 summarizes the engineered safety features as they relate to Condition II, III, or IV events as analyzed in Chapter 15.

7.3.1.2.2 Design Basis; Variables, Ranges, Accuracies, and Typical Response Times Used in ESF Actuation (Paragraphs 2, 5, 6, and 9 of Section 3 of IEEE 279-1971)

The variables required to be monitored for engineered safety features acutations are:

1. Pressurizer Pressure
2. Reactor Coolant Inlet Temperature (T_{cold}) in each loop
3. Steamline Pressure in each steamline
4. Containment Pressure
5. Water level in each Steam Generator (Narrow and Wide Ranges)
6. Startup feedwater flow to each steam generator
7. Source Range neutron flux
8. Pressurizer Water Level

A discussion on levels that, when reached, will result in engineered safety features actuation, is given in Subsection 7.1.2.2.1. The "ALLOWABLE VALUES" for the Limiting Conditions for Operation (LCO) and the "TRIP SETPOINTS" for ESF actuations are given in the Technical Specifications.

Typical ranges, accuracies, and response times for the variables used in ESF actuations are listed in Table 7.3-2.

The response time of engineered safety features actuation is defined as the interval required for the engineered safety features sequence to be initiated subsequent to the point in time that the appropriate variable(s) exceed setpoints. The response time includes sensor/process (analog) and logic (digital) delay plus the time delay associated with tripping open the reactor trip breakers and control and latching mechanisms, although the engineered safety features actuation signal occurs before or simultaneously with engineered safety features sequence initiation (See Figure 7.2-1, Sheet 12). Therefore, the response times to initiate engineered safety features presented on Table 7.3-2 are conservative. The values listed are maximum allowable times consistent with the safety analyses and are systematically verified during plant pre-operational startup tests. These maximum delay times thus include all compensation and therefore require that any such network be aligned and operating during verification testing.

The integrated protection system associated with engineered safeguards actuation is always capable of having response time tests performed using the same methods as those tests performed during the preoperational test program or following significant component changes.

7.3.1.2.3 Design Basis; Spatially Dependent Variables Used for ESF Actuation (Paragraph 3 of Section 3 of IEEE 279-1971)

No spatially dependent variables are used for engineered safety features actuation.

7.3.1.2.4 Design Basis; Limits for ESF Parameters in Various Reactor Operating Modes (Paragraph 4 of Section 3 of IEEE 279-1971)

During startup or shutdown, various ESF actuations can be manually blocked if the pressurizer pressure is below the P-11 setpoint. These functions are listed in Subsection 7.3.1.1.8.

During testing or maintenance of the integrated protection cabinets, certain channels used for ESF may be bypassed. Although no setpoints are changed for bypassing, the logic is automatically adjusted as described in Subsection 7.1.2.2.8. the ESF channels which can be bypassed in the integrated protection system (IPS) are listed on Table 7.3-1.

7.3.1.2.5 Design Basis; ESF Functions for Malfunctions, Accidents, Natural Phenomena, or Credible Events (Paragraph 8 of Section 3 of IEEE 279-1971)

The accidents which the various ESF functions are designed to mitigate are detailed in Chapter 15. Table 7.2-5 contains a summary listing of the engineered safety features which will typically be actuated for various Condition II, III, or IV events.

The safety system is qualified as discussed in Sections 3.10 and 3.11. It also normally relies on provisions made by the owner to protect equipment against damage from natural phenomena and credible events (See Subsection 7.1.2.2.5). Consequently there are no engineered safety features actuated by the integrated protection system to mitigate the consequences of these types of events; e.g., extinguishing fires, etc.

Functional diversity is employed in determining the actuation signals for engineered safety features. For example, a safety injection signal will be generated from high containment pressure, low pressurizer pressure, low compensated steamline pressure, etc. Therefore, complete reliance is not normally made on a single signal actuating ESF functions. The extent of this diversity can be seen from the initiating signals presented in Subsection 7.3.1.1. Table 7.3-1 also lists the ESF signals, and the conditions which will result at their actuation.

Redundancy will be employed to provide assurance that engineered safety features will be actuated on demand, even when the protection system is degraded by a single random failure. This redundancy is described in Subsections 7.1.1.2 and 7.1.1.3. The single-failure criterion is met even when ESF channels are bypassed as previously described.

7.3.1.3 Final System Drawings

Functional block diagrams, electrical elementaries and other drawings as required to assure electrical separation and to perform a safety review will be provided in the plant specific applicant's final safety analysis report. Preliminary drawings for the instrumentation and control systems are included at the end of Sections 7.2, 7.3, 7.6, and 7.7.

7.3.2 Analysis for Engineered Safety Features Actuation

7.3.2.1 Failure Mode and Effects Analyses

The failure mode and effects analyses that will be performed on the integrated protection system, as discussed in Subsection 7.2.2.1, will include analysis of the equipment which generates the actuation signals for engineered safety features. Results of this study will be documented in a separate report for reference in the plant specific applicant's preliminary safety analysis report prior to issuance of the construction permit.

7.3.2.2 Conformance of Engineered Safety Features to the Requirements of IEEE 279-1971

This section discusses conformance of engineered safety features actuation to the requirements of Section 4 of IEEE 279-1971. Engineered safety features accomplish a protective function when each ESF component receives an initiation signal from the integrated protection system. Consequently there is no physically identifiable engineered safety features actuation system per se. Those requirements of Section 4 of IEEE 279-1971 which address equipment in the integrated protection system are presented in Subsection 7.1.2.2 and are not repeated here. The discussions presented in this section address only the functional aspects of actuating engineered safety features.

7.3.2.2.1 Conformance to the General Functional Requirements for Engineered Safety Features Actuation (Paragraph 4.1 of IEEE 279-1971)

The integrated protection system (IPS) will automatically generate an actuation signal for an engineered safety feature whenever a condition monitored by the IPS reaches a preset value. The specific engineered safety features actuation functions are listed in Table 7.3-1 and are discussed in detail in Subsection 7.3.1.1

Table 7.3-2 lists the typical ranges, accuracies, and response times of the parameters being monitored. The engineered safety features, in conjunction with a reactor trip, protects against damage to the core and reactor coolant system components, as well as to ensure containment integrity following a condition II, III, or IV event. Table 7.2-4 summarizes the events which will normally result in the initiation of engineered safety features. The setpoints which, when reached, actuate engineered safety features are listed in the Technical Specifications.

7.3.2.2.2 Conformance to the Single Failure Criterion for Engineered Safety Features Actuation (Paragraph 4.2 of IEEE 279-1971)

A single failure in the integrated protection system (IPS), will not prevent an actuation of the engineered safety features when the condition monitored by the IPS reaches the preset value that requires the initiation of an actuation signal. The single failure criterion is met even when one of the engineered safety features actuation cabinets is being tested, as discussed in Subsection 7.1.1.2.7, or when there is a bypass condition in connection with test or maintenance of channel set(s) in the integrated protection system.

7.3.2.2.3 Conformance to the Requirements for Channel Independence of the Engineered Safety Features Actuation (Paragraph 4.6 of IEEE 279-1971)

The discussion presented in Subsection 7.1.2.2.6 is applicable. The signals to initiate Train A of the engineered safety features are electrically

isolated from the signals to initiate the redundant train (Train B). Both safeguard trains of the safeguards protection action system are electrically independent and redundant, as well as the power supplies for the trains up to and including the final actuated equipment.

7.3.2.2.4 Conformance to the Requirements Governing Control and Protection System Interaction of the Engineered Safety Features Actuation (Paragraph 4.7 of IEEE 279-1971)

The discussions presented in Subsection 7.1.2.2.7 are applicable.

7.3.2.2.5 Derivation of System Inputs for Engineered Safety Features Actuation (Paragraph 4.8 of IEEE 279-1971)

To the extent feasible and practical, the integrated protection system inputs are derived from signals that are direct measures of the desired parameters. The parameters are listed in Table 7.3-2.

7.3.2.2.6 Capability for Sensor Checks and Equipment Test and Calibration of the Engineered Safety Features Actuation (Paragraph 4.9 and 4.10 of IEEE 279-1971)

The discussions of system testability in Section 7.1 is applicable to the sensors, signal processing, and actuation logic that initiate engineered safety features actuation.

The following discussions cover those areas in which the testing provisions differ from those used to generate a reactor trip.

Testing of Engineered Safety Features Actuation

The testing program meets the requirements of Regulatory Guide 1.22 as discussed in Subsection 7.1.2.2.10. The program is as follows:

1. Prior to initial plant operations, engineered safety features tests will be conducted.

2. Subsequent to initial startup, engineered safety features tests will be conducted during each regularly scheduled refueling outage.

3. During on-line operation of the reactor, the integrated protection system will be fully tested as described. In addition, essentially all of the engineered safety features final actuators will be fully tested. The remaining few final actuators whose operation is not compatible with continued on-line plant operation will be tested at refueling shutdown.

4. During normal operation, the operability of testable final actuation devices of the engineered safety features will be tested by manual initiation from the control room.

During reactor operation, the basis for acceptability of engineered safety features actuation will be the successful completion of the overlapping tests performed on the integrated protection system. Process indications are used to verify operability of sensors.

The basis for acceptability for the engineered safety features interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground of signal cables in radiation environments are based on qualification test data which identifies what constitutes acceptable radiation, thermal, etc. degradation.

Frequency of Performance of Engineered Safety Features Actuation Tests

During reactor operation, complete integrated protection system testing (excluding sensors or those devices whose operation would cause plant upset)

is performed on a basis as specified in the Technical Specifications. Testing is also performed during scheduled plant shutdown for refueling.

Engineered Safety Features Actuation Test Description

The guidelines used in developing the testing circuitry and procedures are:

1. The test procedures must not involve the potential for damage to any plant equipment.

2. The test procedures must minimize the potential for accidental tripping.

3. The provisions for on-line testing must minimize complication of engineered safety features actuation circuits so that their reliability is not degraded.

Testing During Shutdown

Emergency core cooling system tests will be performed at each major fuel reloading with the reactor coolant system isolated from the ECCS by closing the appropriate valves. This is in compliance with (1971) GDC-37.

Containment spray system tests will be performed at each major fuel reloading. The tests will be performed with the isolation valves in the spray supply lines at the containment and spray additive tank blocked closed and are initiated by tripping the normal actuation instrumentation.

Periodic Maintenance Inspections

The maintenance procedures which follow may be accomplished in any order. The frequency will depend on the operating conditions and requirements of the reactor power plant. If any degradation of equipment operation is noted,

either mechanically or electrically, remedial action is taken to repair, replace, or readjust the equipment. Optimum operating performance must be achieved at all times.

Typical maintenance procedures include the following:

1. Check cleanliness of all exterior and interior surfaces.

2. Check all fuses for corrosion.

3. Inspect for loss or broken control knobs and burned out indicator lamps.

4. Inspect for moisture and condition of cables and wiring.

5. Mechanically check all connectors and terminal boards for looseness, poor connection, or corrosion.

6. Inspect the components of each assembly for signs of overheating or component deterioration.

7. Perform complete system operating check.

7.3.2.2.7 Conformance to Requirements on Bypassing of Engineered Safety Features Actuation Functions (Paragraph 4.11, 4.12, 4.13, and 4.14 of IEEE 279-1971)

The discussions of Subsections 7.1.2.2.8 through 7.1.2.2.14 and 7.3.1.1.9 are applicable.

7.3.2.2.8 Conformance to the Requirement for Completion of Engineered Safety Features Actuation Once Initiated (Paragraph 4.16 of IEEE 279-1971)

Once initiated, engineered safety features will go to completion unless deliberate operator action is taken to terminate the function on a component-

by-component basis. The ability to terminate operation of ESF components is necessary for several reasons. For example, components must be turned off and properly aligned if inadvertently actuated. Also, a component may have to be removed from operation for repair or maintenance.

Equipment actuated on a safety injection (SI) cannot be turned off for 30 to 120 seconds following initiation of the SI signal. This assures that the diesel generator will have attained its speed and that all required loads have been sequenced onto the generator before the SI signal can be reset. This interlock is shown on Figure 7.2-1, Sheet 12. Once reset, the safety injection signal will not be reinitiated as long as the reactor trip circuit breakers are open.

Resetting a system-level ESF signal does not terminate any ESF function. Rather, it permits the operator to individually turn off equipment. Equipment cannot be reset until the system-level signal is reset.

7.3.2.2.9 Conformance to the Requirement to Provide Manual Initiation At the System-Level for All ESF Actuations (Paragraph 4.17 of IEEE 279-1971)

Manual initiation at the system-level exists for all engineered safety features actuations. Specifically these are:

1. Safety Injection	2 SI switches
2. Steamline Isolation	2 Steamline Isolation Switches
3. Containment Spray	2 pairs of 2 Spray Switches
4. Phase-A Isolation	2 Phase-A Isolation Switches
5. Phase-B Isolation	Manual Spray actuates Phase-B Isolation

6.	Containment Vent. Isolation	Manual Spray or Manual Phase-A Isolation actuates Containment Ventilation Isolation.
7.	Feedwater Isolation	2 Manual Feedwater Isolation Switches
8.	Emergency Feedwater	Manual Safety Injection, 2 manual start switches in control room, or 2 local manual start switches

As a minimum, two switches are provided to assure that the protective function can be manually initiated at the system-level despite a single random failure in one switch. In certain applications, e.g., containment spray, two pairs of switches are provided. One pair must be actuated simultaneously to actuate spray. This reduces the likelihood of inadvertent spray while still assuring that the single failure criterion is met.

7.3.2.3 Summary

The effectiveness of the integrated protection system in initiating engineered safety features is evaluated in Chapter 15, based on the ability of the system to contain the effects of Condition III and IV faults, including loss of coolant and steamline break accidents.

The integrated protection system, in order to initiate engineered safety features actuation, must detect Condition III and IV faults and generate signals which actuate the engineered safety features. The system must sense the accident condition and generate the signal actuating the protection function reliably and within a time consistent with that determined by the accident analyses in Chapter 15.

Longer times are associated with the actuation of the mechanical and fluid system equipment associated with engineered safety features. This includes the time required for switching, bringing pumps and other equipment to speed,

and the time required for them to take load. Evaluation of engineered safety features in mitigating consequences of breaks in the primary and secondary systems is as follows:

Loss of Coolant Protection

By analysis of loss of coolant accident and in system tests it has been verified that, except for very small coolant system breaks which can be protected against by the charging pumps followed by an orderly shutdown, the effects of various loss of coolant accidents are reliably detected by the low pressurizer pressure signal; the emergency core cooling system (safety injection) is actuated in time to prevent or limit core damage.

For large coolant system breaks, the passive accumulators inject first because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active emergency core cooling system phase.

High containment pressure also actuates the steamline isolation and safety injection systems. Therefore, emergency core cooling actuation can be brought about by sensing this other direct consequence of a primary system break, that is, the engineered safety features actuation system detects the leakage of the coolant into the containment. The generation time of the actuation signal as given in Table 7.3-2 is adequate.

Containment spray will provide additional emergency cooling of containment and also limit fission product release upon sensing elevated containment pressure (Hi-3) to mitigate the effects of a loss of coolant accident.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is in Table 7.3-2 and is well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the required fluid and supporting systems.

The analyses in Chapter 15 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss of coolant.

Steamline Break Protection

The emergency core cooling system is also actuated in order to protect against a steamline break. Table 7.3-1 gives the signals that make up the excessive cooldown protection function. Table 7.3-2 gives the time between occurrence of the signals that make up the excessive cooldown protection signal and high containment pressure (for breaks in containment), and generation of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the safety injection system is actuated for a steam break in time to limit or prevent further core damage. There is a reactor trip and the core reactivity is further reduced by the highly borated water injected by the safety injection system.

Additional protection against the effects of a steamline break is provided by feedwater isolation which occurs upon initiation of the functions shown in Table 7.3-1.

Additional protection against a steamline break accident is provided by steamline isolation; i.e., closure of all steamline isolation valves in order to prevent uncontrolled blowdown of all steam generators. Table 7.3-1 gives the signals that make up the steamline isolation function. The generation of the steamline isolation signals, as given in Table 7.3-2, is again short compared to the time to trip the fast-acting steamline isolation valves which are designed to close in less than approximately 5 seconds.

The analyses in Chapter 15 of steamline break accidents (see RESAR-SP/90 PDA Module 6/8, "Secondary Side Safeguards System/Steam and Power Conversion System") and an evaluation of the integrated protection system design shows that the engineered safety features actuations are effective in preventing or mitigating the effects of a steamline break accident.

Feedline Break Protection

Engineered safety features are actuated in order to protect against a feedline break. Following reactor trip due to a low steam generator water level trip setpoint, a steamline isolation signal is obtained when the pressure in the steamlines falls below a given setpoint. When the setpoint is reached, all main steam isolation valves are closed which guarantees a steam supply for the turbine driven emergency feedwater pumps.

Assurance that adequate feedwater is available for the feedline break is provided by the emergency feedwater system which includes two motors driven pumps and two turbine driven pumps. The emergency feedwater pumps are initiated automatically by the signals identified in Table 7.3-1.

Analysis of the feedline break accident shows that minimum emergency feedwater capacity is adequate to remove decay heat, to prevent overpressurization of the reactor coolant system, and to prevent uncovering the reactor core. Minimum emergency feedwater capacity is that capacity available following a feedline break event assuming the worst single failure. The analysis in Chapter 15 of the feedline break accident (see RESAR-SP/90 PDA Module 6/8, "Secondary Side Safeguards System/Steam and Power Conversion System") shows that the engineered safety features actuations are effective in mitigating the effects of a feedline break accident.

TABLE 7.3-1

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

ESF Actuation Signal	# of Channels	Channel Set Trip Logic	Permissives & Interlocks
1. SAFETY INJECTION (Figure 7.2-1, Sheets 7, 9, 10)			
a. Manual Safety Injection	2 switches	1/2 switches	----
b. High (Hi-1) Containment Pressure	4	2/4-BYP*	----
c. Pressurizer Low Pressure	4	2/4-BYP*	Manual block permitted below P-
d. Low Compensated Steamline Pressure	4/steamline	2/4-BYP* in any st. line	Manual block permitted below P-
e. Low-3 T_{cold}	1/loop	2/4 loops	P-15; Manual block permi below P-11
2. STEAMLINE ISOLATION (Figure 7.2-1, Sheets 7, 8, 9, 10)			
a. High Steamline Negative Pressure Rate	4/steamline	2/4-BYP in any steamline*	Manual block permitted below P
b. Low Pressurizer Pressure	4	2/4-BYP*	Manual block permitted below P
c. High (Hi-2) Containment Pressure	4	2/4-BYP*	----
d. Low Compensated Steamline Pressure	4/steamline	2/4-BYP in any steamline*	Manual block permitted below P-1
e. Low-3 T_{cold}	1/loop	2/4 loops	P-15; Manual block permitt below P-11
f. Manual Steamline Isolation	2 switches	1/2 switches	----

* 2/4-BYP indicates automatic bypass logic. The logic is 2/4 with no bypasses; 2/3 with one bypass; 1/2 with two bypasses; and automatically actuated with three or four bypasses.

TABLE 7.3-1 (Cont.)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

ESF Actuation Signal	# of Channels	Channel Set Trip Logic	Permissives & Interlocks
3. CONTAINMENT SPRAY			
(Figure 7.2-1, Sheet 13)			
a. Manual Containment Spray	4 switches	2/4 switches	----
b. High (Hi-3) Containment Pressure	4	2/4-BYP*	
4. CONTAINMENT ISOLATION (PHASE-A)			
a. Safety Injection Signal (Auto and Manual)	See item Number 1(a) through (e)		
b. Manual Phase-A Isolation	2 switches	1/2 switches	----
CONTAINMENT ISOLATION (PHASE-B)			
a. High (Hi-3) Containment Pressure	4	2/4-BYP*	----
b. Manual Containment Spray	4 switches	2/4 switches	----
CONTAINMENT VENTILATION ISOLATION			
a. Safety Injection (Auto or Manual)	See item Number 1(a) through (e)		
b. Manual Phase-A Isolation	2 switches	1/2 switches	----
c. Manual Containment Spray	4 switches	2/4 switches	----

* 2/4-BYP indicates automatic bypass logic. The logic is 2/4 with no bypasses; 2/3 with one bypass; 1/2 with two bypasses; and automatically actuated with three or four bypasses.

TABLE 7.3-1 (Cont.)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

ESF Actuation Signal	# of Channels	Channel Set Trip Logic	Permissives & Interlocks
5. FEEDWATER LINE ISOLATION (Closure of Isolation and Modulating Valves) (Figure 7.2-1, Sheets 2, 5, 8, 11, 16)			
a. Steam Generator High Water Level	4/St. Gen.	2/4-BYP in any steam generator*	----
b. Safety Injection Signal (Auto and Manual	See Item Number 1(a) through (e)		
c. Manual Feedwater Isolation	2 switches	1/2 switches	----
d. Low-2 T_{cold}	1/loop	2/4 loops	P-16
FEEDWATER ISOLATION (Trip of all Main F/w Pumps)			
a. Steam Generator High Water Level	4/St. Gen.	2/4-BYP in any steam generator*	----
b. Manual Feedwater Isolation	2 switches	1/2 switches	----
c. Safety Injection Signal (Auto and Manual)	See Items Number 1(a) through (e)		

* 2/4-BYP indicates automatic bypass logic. The logic is 2/4 with no bypasses; 2/3 with one bypass; 1/2 with two bypasses; and automatically actuated with three or four bypasses.

TABLE 7.3-1 (Cont.)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

ESF Actuation Signal	# of Channels	Channel Set Trip Logic	Permissives & Interlocks
6. EMERGENCY FEEDWATER			
(Figure 7.2-1 Sheet 8)			
a. Low-1 Steam Generator Water Level Coincident With Low SFWS Flow	4/St. Gen. 1/Injection Line	2/4-BYP in any steam generator* 1/2 assigned channels per steam generator	----
b. Low-2 Water Level Coincident With Reactor Trip	2/St. Gen.	1/2	----
c. Safety Injection Actuation	See Item Number 1		
d. Manual	2	1	
7. BLOCK OF BORON DILUTION			
(Figure 7.2-1, Sheet 3)			
a. Flux Doubling Calculation	4	2/4-BYP	

* 2/4-BYP indicates automatic bypass logic. The logic is 2/4 with no bypasses; 2/3 with one bypass; 1/2 with two bypasses; and automatically actuated with three or four bypasses.

TABLE 7.3-2

ESFAS VARIABLES, LIMITS, RANGES AND ACCURACIES

Protective Functions	Variables to be Monitored	Conditions of the Variable or Other ESF Actuation Signals That Initiate Protective Action	Range of Variables (Typical) (Nominal)	Protection System Accuracy (Typical)	Response Time (Sec)
B. ESF					
1. Safety Injection (S.I.)					
	Containment pressure	Containment pressure-Hi-1	-5 to 60 psig	±1.8% of span	1.6
	Pressurizer pressure	Pressurizer pressure-low	1700 to 2500 psig	± 14 psi (uncompensated signal)	1.0
2. S.I. Portion of Excessive Cooldown Protection					
	Reactor coolant inlet temperature (T_{cold})	Low -3 T-cold	510 to 630°F	±2.5°F	6.0
	Steamline pressure	Low compensated steamline pressure	0 to 1400 psig	±2.3% of Span	1.0

TABLE 7.3-2 (continued)

ESFAS VARIABLES, LIMITS, RANGES AND ACCURACIES

Protective Functions	Variables to be Monitored	Conditions of the Variable or Other ESF Actuation Signals That Initiate Protective Action	Range of Variables (Typical) (Nominal)	Protection System Accuracy (Typical)	Response Time (Sec)
3. Containment Spray	Containment pressure	Containment pressure Hi-3	-5 to 60 psig	±1.8% of span	1.5
4. Containment Isolation					
A. Phase A	See 1 & 2 above	Safety injection	See 1 & 2 above	See 1 & 2 above	See 1 & 2 ab
B. Phase B	Containment pressure	Containment pressure Hi-3	-5 to 60 psig	±1.8% of span	1.5
C. Containment Vent. Isolation	See 1 & 2 above	Safety injection	See 1 & 2 above	See 1 & 2 above	See 1 & 2 ab
	Radiation Level	Containment radioactivity-Hi			
5. Steamline Isolation					
	Containment pressure	Containment pressure - Hi-2	-5 to 60 psig	±1.8% of span	1.5
	See 2 above	Excessive cooldown	See 2 above	See 2 above	See 2 above
	Steam pressure rate	Negative steam pressure rate - high	0 to 1400 psig	±2.3% of span	1.0

TABLE 7.3-2 (continued)

ESFAS VARIABLES, LIMITS, RANGES AND ACCURACIES

Protective Functions	Variables to be Monitored	Conditions of the Variable or Other ESF Actuation Signals That Initiate Protective Action	Range of Variables (Typical) (Nominal)	Protection System Accuracy (Typical)	Response Time (Sec)
6. Feedwater Line Isolation					
	Pressurizer water level	Pressurizer water level coincident with reactor trip	Cylindrical portion of PRZ	±2.3% of Full range ΔP between taps at design temp/ press	2.0
	See 2 above	Excessive cooldown	See 2 above	See 2 above	See 2 above
	Reactor coolant inlet temperature (T-cold)	Low 2 T-cold	510 to 630°F	±2.5% F	6.0
	Water level in steam generator	High steam generator water level	8 feet below nominal level to 6 feet above nominal level	±2.3% of ΔP span over pressure range from 700 to 1400 psig	2.0

TABLE 7.3-2 (continued)

ESFAS VARIABLES, LIMITS, RANGES AND ACCURACIES

Protective Functions	Variables to be Monitored	Conditions of the Variable or Other ESF Actuation Signals That Initiate Protective Action	Range of Variables (Typical) (Nominal)	Protection System Accuracy (Typical)	Response Time (Sec)
7. Startup of emergency feedwater pumps					
	Water level in steam generator	Low SFWS flow in coincidence with low-1 level in any SG	8 feet below nominal level to 6 feet above nominal level	±2.3% of ΔP span over pressure range from 700 to 1400 psig	2.0
	See 1 & 2 above	Safety injection	See 1 & 2 above	See 1 & 2 above	See 1 & 2 ab
	Water level in steam generator	Low-2 W. R. level in coincidence with reactor trip	8 feet below nominal level to 6 feet above nominal level	±2.3% of ΔP span over pressure range from 700 to 1400 psig	2.0
8. Turbine trip					
	Water level in steam generator	High water level in steam generator	-42 feet below nominal level to 6.5 feet above	±2.3% of ΔP span over pressure range from 700 to 1400 psig	2.0

TABLE 7.3-2 (continued)

ESFAS VARIABLES, LIMITS, RANGES AND ACCURACIES

Protective Functions	Variables to be Monitored	Conditions of the Variable or Other ESF Actuation Signals That Initiate Protective Action	Range of Variables (Typical) (Nominal)	Protection System Accuracy (Typical)	Response Time (Sec)
	See 2 above	Excessive cooldown Reactor trip-circuit-breaker open in 2 or more actuation trains	See 2 above	See 2 above	See 2 above
	Reactor coolant inlet temp T-cold	Low-2 T_{cold}	510-630°F	±2.5°F	6.0
9. Block steam dump					
	Reactor coolant inlet temperature (T-cold)	Low-1 T-cold	510 to 630°F	±2.5°F	6.0
10. Block boron dilution					
	Neutron flux	High source range neutron flux	1 to 10^6 c/sec	±5% of equiv. linear full scale output	0.5

TABLE 7.3-3

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation*	Derivation	Function Performed
P-6	Intermediate range neutron flux channels above setpoint	Allows manual block of source range channels thus permitting boron dilution
$\overline{\text{P-6}}$	Intermediate range neutron flux channels below setpoint	Defeats any manual block of source range channels permitting source block of boron dilution
P-11	Pressurizer pressure below setpoint	(a) Permits manual block of safety injection on low pressurizer pressure, low steamline pressure, or low 3 T-cold (b) Permits manual block of steamline isolation on low steamline pressure, or low 3 T-cold (c) Permits manual block of feedwater isolation on low 2 T-cold (d) Permits manual unblock of steamline isolation on high negative steamline pressure rate.

TABLE 7.3-3 (Cont.)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation*	Derivation	Function Performed
$\overline{\text{P-11}}$	Pressurizer pressure above setpoint	(a) Defeats manual block of safety injection on low pressurizer pressure, low steamline pressure, or low 3 T-cold
		(b) Defeats manual block of steamline isolation on low steamline pressure, or low 3 T-cold
		(c) Defeats manual block of feedwater isolation on low 2 T-cold
		(d) Defeats manual unblock of steamline isolation on high negative steamline pressure rate
		(e) Opens all accumulator isolation valves
P-15	Power range nuclear power below setpoint	(a) Permits safety injection and steamline isolation on low 3 T-cold

TABLE 7.3-3 (Cont.)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation*	Derivation	Function Performed
		(b) Permits feedwater isolation on low 2 T-cold
$\overline{\text{P-15}}$	Power range nuclear power above setpoint	(a) Blocks safety injection and steamline isolation on low 3 T-cold
		(b) Blocks feedwater isolation on low 2 T-cold
P-16	Reactor trip breakers open or reactor trip signal present	(a) Trips turbine
		(b) Permits closure of main feedwater control valves on low pressurizer water level
		(c) Prevents opening of the feedwater system valves which are closed on high steam generator water level or low 2 T-cold
		(d) Prevents automatic re-activation of safety injection after a delayed manual reset of safety injection

TABLE 7.3-3 (Cont.)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation*	Derivation	Function Performed
$\overline{\text{P-16}}$	Reactor trip breakers closed and no trip signal present	(a) Prevents closure of main feed-control valves on low pressurizer water level
		(b) Permits opening of the feedwater system valves which are closed on high steam generator water level or low 2 T-cold
		(c) Permits automatic re-activation of safety injection after a delayed manual reset of safety injection

NOTES:

*(P-XX) = presence of the P-XX signal

($\overline{\text{P-XX}}$) = absence of the P-XX signal

TABLE 7.3-4

SYSTEM-LEVEL MANUAL INPUTS TO THE INTEGRATED LOGIC CABINETS (ILC)

	INPUT	TO CHANNEL SET			
1.	Emergency Cooldown Protection Block - I	I			
2.	Emergency Cooldown Protection Block - II		II		
3.	Emergency Cooldown Protection Block - III			III	
4.	Emergency Cooldown Protection Block - IV				IV
5.	Emergency Cooldown Protection Reset - I	I			
6.	Emergency Cooldown Protection Reset - II		II		
7.	Emergency Cooldown Protection Reset - III			III	
8.	Emergency Cooldown Protection Reset - IV				IV
9.	Safety Injection Actuation 1	I	II		
10.	Safety Injection Actuation 2	I	II		
11.	Containment Spray #1	I	II		
12.	Containment Spray #2	I	II		
13.	Containment Spray #3	I	II		
14.	Containment Spray #4	I	II		
15.	Containment Isol. - φA #1	I	II		
16.	Containment Isol. - φA #2	I	II		
17.	Steamline Isolation #1	I	II		
18.	Steamline Isolation #2	I	II		
19.	SI Reset & Block - CH I	I			
20.	SI Reset & Block - CH II		II		
21.	Cont. Spray Reset - CH I	I			
22.	Cont. Spray Reset - CH II		II		
23.	Cont. Isol. φA Reset - CH I	I			
24.	Cont. Isol. φA Reset - CH II		II		
25.	Cont. Isol. φB Reset - CH I	I			
26.	Cont. Isol. φB Reset - CH II		II		

TABLE 7.3-4 (Cont.)

SYSTEM-LEVEL MANUAL INPUTS TO THE INTEGRATED LOGIC CABINETS (ILC)

	INPUT	TO CHANNEL			
27.	Contain. Vent Isol. Reset I	I			
28.	Contain. Vent Isol. Reset II		II		
29.	Steamline Isol. Reset - CH I	I			
30.	Steamline Isol. Reset - CH II		II		
31.	Feedwater Isolation Reset - I	I			
32.	Feedwater Isolation Reset - II		II		
33.	Block Boron Dilution Block - I	I			
34.	Block Boron Dilution Block - II		II		
35.	Block Boron Dilution Block - III			III	
36.	Block Boron Dilution Block - IV				IV
37.	Block Boron Dilution Reset - I	I			
38.	Block Boron Dilution Reset - II		II		
39.	Block Boron Dilution Reset - III			III	
40.	Block Boron Dilution Reset - IV				IV

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

The functions necessary for safe shutdown are available from instrumentation channels that are associated with the major systems in both the primary and secondary systems of the nuclear steam supply system (NSSS). These channels are normally aligned to serve a variety of operational functions, including startup and shutdown as well as protective functions.

However, prescribed procedures for securing and maintaining the plant in a safe condition can be instituted by appropriate alignment of selected systems in the NSSS. The discussion of these systems together with the applicable codes, criteria and guidelines is found in other RESAR-SP/90 PDA modules, as appropriate. In addition, the alignment of shutdown functions associated with the engineered safety features (ESF) which are invoked under postulating limiting fault situations is discussed in Chapter 6 of the integrated RESAR-SP/90 PDA document and Section 7.3.

Two kinds of shutdown conditions, both capable of being achieved with or without offsite power, are addressed in this section: hot standby and cold shutdown. Hot standby is a stable condition of the reactor achieved shortly after a programmed or emergency shutdown of the plant. Cold shutdown is a stable condition of the plant achieved after the residual heat removal process has brought the primary coolant temperature below 200°F. A description of systems required to achieve and maintain cold shutdown are described in Subsection 5.4.7 of RESAR-SP/90 PDA Module 1, "Primary Side Safeguards System".

For either case of safe shutdown, i.e., hot standby or cold shutdown, the reactivity control systems maintain a subcritical condition of the core. The plant technical specifications explicitly define both hot standby and cold shutdown conditions.

As a minimum, the electrically powered equipment necessary to be aligned for achieving and maintaining safety grade cold shutdown without offsite power, and with an event initiated by a single random failure, with limited operator action outside the control room, are:

1. Emergency Class 1E electrical power supply

2. Emergency feedwater system

3. Residual heat removal (and isolation) system

4. Borated EWST water inventory supply to the suction of the high head safety injection (HHSI) pumps

5. Redundant discharge system from and including the HHSI pump system supplying RCS

6. Pressure relief system for RCS

7. Decay heat removal using steam generator PORVs and bypass

8. Emergency letdown system

9. Reactor protection system

10. Component cooling water

11. Service water

The instrumentation and functions which are required to be aligned for maintaining hot standby are:

1. Prevent the reactor from achieving criticality in violation of the technical specifications

2. Provide an adequate heat sink such that design and safety limits are not exceeded

3. Pressurizer pressure control

4. Reactor coolant system inventory control

7.4.1 Description

The hot standby systems are identified in the following lists together with the associated instrumentation and controls provisions. The identification of the monitoring indicators (Subsection 7.4.1.1) and controls (Subsection 7.4.1.2) are those necessary for maintaining a hot standby. The equipment and services for a cold shutdown are identified in Subsection 7.4.1.4. Loss of the local controls and normal automatic control systems are not assumed coincident with evacuation.

7.4.1.1 Monitoring Indicators

The characteristics of these indicators, which are provided outside as well as inside the control room, are described in Section 7.5. The necessary indicators are as follows:

1. Water level indicator for each steam generator

2. Pressure indicator for each steam generator by means of steamline pressure indicator

3. Pressurizer water level indicator

4. Pressurizer pressure indicator

7.4.1.2 Controls

7.4.1.2.1 General Considerations

1. The turbine is tripped. This can be accomplished at the turbine as well as in the control room.

2. The reactor is tripped. This can be accomplished at the reactor trip switchgear as well as in the control room.

3. Safety related manual controls for hot standby shutdown are located inside as well as outside the main control room. These controls are provided with REMOTE/LOCAL selector switches located outside the main control room. An annunciator is alarmed in the main control room and the indicator lights in the main control room are turned off when LOCAL CONTROL is selected; and control of the switchgear is transferred from the control room to a local station(s).

4. All automatic systems continue functioning.

7.4.1.2.2 Pumps and Fans

1. Start-up feedwater pump

   Normally on a loss of electrical power, the start-up feedwater pump would come on as part of the blackout sequence. The emergency feedwater pumps start automatically on an accident sequence or can be started manually. START/STOP controls located outside as well as inside the control room are provided.

2. HHSI pumps

   START/STOP motor controls for these pumps are located outside, as well as inside the control room.

3. Service water pumps

   These pumps will start automatically following a loss of normal electrical power. START/STOP motor controls are located outside as well as inside the control room.

4. Component cooling water pumps

   These pumps, energized from the emergency generator, start automatically following a loss of normal electrical power. START/STOP controls are located outside as well as inside the control room.

5. Control room ventilation units including the control room air inlet dampers.

   The control room ventilation units have START/STOP controls and LOCAL/REMOTE switches.

7.4.1.2.3 Emergency Generators

These units start automatically following a loss of normal AC power. However, manual controls for diesel startup are provided locally at the emergency generator as well as within the control room. For a description of Class 1E power supplies, refer to Section 8.3.

7.4.1.2.4 Valves and Heaters

1. HHSI flow control

   Flow control valves fail open. Subsequent control can be maintained by the use of solenoid valves described in Subsection 5.4.7 of RESAR-SP/90 PDA Module 1, "Primary Side Safeguards System" controlled manually from both inside and outside the control room.

2. Letdown valves

   Letdown can be established through the emergency letdown line, if normal letdown is unavailable, by manual control from both inside and outside the control room.

3. Emergency feedwater control valves

   Manual control with transfer switches for these valves are located locally. These controls duplicate functions that are inside the control room.

4. Steam generator safety valves

5. Pressurizer heater control

   ON/OFF control with selector switch is provided for two backup heater groups outside the control room. The heater groups are connected to separate buses, such that each can be connected to separate emergency generators in the event of loss of outside power. The controls are grouped with the charging flow controls and duplicate functions available in the control room.

7.4.1.3 Control Room Evacuation

It is noted that the instrumentation and controls listed in Subsections 7.4.1.1 and 7.4.1.2 which are used to achieve and maintain a safe shutdown are available in the event that an evacuation of the control room is required. These controls and instrumentation channels together with the equipment identified in Subsection 7.4.1.4 identify the potential capability for cold shutdown of the reactor subsequent to a control room evacuation through the use of suitable procedures. The control room evacuation shall not occur simultaneously or coincident with an abnormal operating condition (ANS Condition II, III, or IV), except the loss of offsite power which would be coincident. Normal controls from the control room would be expected to function under all conceivable events.

7.4.1.4 Equipment and Systems Necessary for Cold Shutdown

1. Emergency feedwater pumps (See RESAR-SP/90 PDA Module 6, "Secondary Side Safeguards System").

2. Boration capability

3. HHSI pumps

4. Service water pumps

5. Control room ventilation

6. Component cooling pumps

7. Residual heat removal pumps (Subsection 5.4.7 of RESAR-SP/90 PDA Module 1, "Primary Side Safeguards System")

8. Certain motor control center and switchgear (Section 8.3)

9. Controlled steam release

10. Nuclear instrumentation system (NIS); source range or intermediate range (Section 7.2). For a more complete description of the NIS, refer to WCAP 8255.

11. Reactor coolant inventory control (HHSI pumps and emergency letdown)

12. Pressurizer pressure control including opening control for pressurizer relief valves and heater control

13. Accumulator piping and valving for isolation and venting

In addition, the pressurizer pressure and steam line pressure safety injection trip signals must be blocked and the accumulator isolation valves closed.

Controls are provided to block the steamline low pressure and pressurizer low pressure signals. These controls prevent an SIS provided that the pressure within the pressurizer is less than a predetermined design level.

7.4.1.5 Other Considerations

1. Additional shutdown air compressors are powered from Class 1E buses and are provided to increase availability of normal controls and minimize operator actions.

2. Other equipment supplied from Class 1E buses to minimize impact on nonsafety equipment in containment include:

   a. Containment recirculation coolers

   b. CRDM air cooling fans

3. Loss of instrument air does not prevent the operation of the minimum systems necessary for hot standby or cold shutdown described in Subsection 7.4.1.

7.4.2 Analysis

Hot standby is a safe stable plant condition, automatically reached following a reactor trip from power. The plant design features also permit the achievement of cold shutdown as referred to in Subsection 7.4.1.2 and described in Subsection 5.4.7 of RESAR-SP/90 PDA Module 1, "Primary Side Safeguards System". In the unlikely event that access to the control room is restricted, the plant can be safely kept at a hot standby by the use of the monitoring indicators and the controls listed in Subsections 7.4.1.1 and 7.4.1.2, and described in Subsection 7.4.1.3, until the control room can be re-entered.

Cold shutdown conditions can be achieved from outside the control room through the use of suitable procedures and by virtue of local control of the equipment listed in Subsection 7.4.1.2, in conjunction with the instrumentation and controls provided external to the control room.

The controls available external to the control room provide the capabilities of achieving and maintaining a safe shutdown when the main control room is inaccessible. The controls necessary for immediate operator action to establish a stable plant condition are available on the ASP or in adjacent emergency switchgear rooms. The controls provide a means of sustaining the capability for boration, letdown, residual heat removal, natural circulation, continuing reactor coolant pump seal injection and for thermal barrier cooling water flow, and depressurization.

The instrumentation and control functions which are required to be aligned for maintaining safe shutdown of the reactor that are discussed above are the minimum number of instrumentation and control functions.

Proper operation of other nonsafety related systems will allow a more normal shutdown to be made and maintained by preventing a transient (Section 7.7).

In considering more restrictive conditions than those discussed in Section 7.4, certain accidents and transients are postulated in the safety analyses which take credit for safe shutdown when the protection systems reactor trip terminates the transients and the engineered safety features system mitigates the consequences of the accident. In these transients, in general, no credit is taken for the control system operation should such operation mitigate the consequences of a transient. Should such operation not mitigate the consequences of a transient, no penalties are taken in the analyses for incorrect control system actions over and above the incorrect action of the control system, whose equipment failure was assumed to have initiated the transient. These analyses presented in Chapter 15.0 of various PDA modules show that safety is not adversely affected when such transients include the following:

1. Inadvertent boron dilution

2. Loss of normal feedwater

3. Loss of external electrical load and/or turbine trip

4. Loss of AC power to the station auxiliaries (station blackout)

The results of the analysis which determined the applicability of the nuclear steam supply system safe shutdown systems to the NRC General Design Criteria, IEEE Standard 279-1971, applicable NRC Regulatory Guides and other industry standards are presented in Table 7.1-1. The functions considered and listed below include both safety-related and nonsafety-related equipment.

1. Reactor trip system

2. Engineered safety features actuation system

3. Safety-related display instrumentation for post-accident monitoring

4. Main control board

5. Controls & instrumentation external to the control room

6. Residual heat removal

7. Instrument power supply

8. Control systems

7.5 INSTRUMENTATION IMPORTANT TO SAFETY

7.5.1 Introduction

An analysis was conducted to identify the appropriate variables and to establish the appropriate design bases and qualification criteria for instrumentation employed by the operator for monitoring conditions in the reactor coolant system, the secondary heat removal system, and the containment, including engineered safety functions and the systems employed for attaining a safe shutdown condition.

The instrumentation is used by the operator to monitor the WAPWR throughout all operating conditions including anticipated operational occurrences and accident and post-accident conditions.

7.5.2 Variable Classifications and Requirements

The plant safety analyses and evaluations define the design basis accident (DBA) event scenarios for which preplanned operator actions are required. Accident monitoring instrumentation is necessary to permit the operator to take required actions to address these analyzed situations. However, instrumentation is also necessary for unforeseen situations (i.e., to ensure that, should plant conditions evolve differently than predicted by the safety analyses, the control room operating staff has sufficient information to evaluate and monitor the course of the event). Additional instrumentation is also needed to indicate to the operating staff whether the integrity of the fuel cladding, the reactor coolant pressure boundary (RCPB), or the reactor containment has degraded beyond the prescribed limits defined as a result of the plant safety analyses and other evaluations.

Five classifications of variables have been identified to provide this instrumentation:

A. Those variables that provide information needed by the operator to perform manual actions identified in the operating procedures and associated with DBA events are designated type A. These variables are restricted to preplanned actions for DBA events. The basis for selecting type A variables is given in Subsection 7.5.2.2.1.

B. Those variables needed to assess that the plant critical safety functions are being accomplished or maintained, as identified in the plant safety analysis and other evaluations, are designated type B.

C. Those variables used to monitor for the gross breach or the potential for gross breach of the fuel cladding, the RCPB, or the containment are designated type C.

D. Those variables needed to assess the operation of individual safety systems and other systems important to safety are designated type D.

E. Those variables that are required for use in determining the magnitude of the postulated releases and continually assessing any such releases of radioactive materials are designated type E.

The five classifications of variables are not mutually exclusive, in that a given variable (or instrument) may be included in one or more types. When a variable is included in one or more of the five classifications, the equipment monitoring this variable meets the requirements of the highest category identified.

Three categories of design and qualification criteria are used. This classification is made in order to identify the importance of the information and to specify the requirements placed on the accident monitoring instrumentation. Category 1 instrumentation has the highest performance requirements and should be utilized for information which cannot be lost under any circumstances. Category 2 and Category 3 instruments are of lesser importance in determining the state of the plant and do not require the same level of operational assurance.

The primary differences between category requirements are in qualification, application of single failure, power supply, and display requirements. Category 1 requires seismic and environmental qualification, the application of a single failure criteria, utilization of emergency power, and an immediately accessible display. Category 2 requires environmental and seismic qualification commensurate with the required function but does not require the single failure criteria, emergency power, or an immediately accessible display. Category 2 requires, in effect, a rigorous performance verification for a single instrument channel. Category 3, which is high quality commercial grade, does not require qualification, single failure criteria, emergency power, or an immediately accessible display.

Table 7.5-1 summarizes the following information for each variable identified:

A. Instrument range or status.
B. Type and category.
C. Environmental qualification.
D. Seismic qualification.
E. Number of channels.
F. Power supply.

7.5.2.1 Definitions

7.5.2.1.1 Design Basis Accident Events

Those events, any one of which could occur during the lifetime of a particular unit, and those events not expected to occur but postulated because their consequences would include the potential for release of significant amounts of radioactive gaseous, liquid, or particulate material to the environment are DBA events. Excluded are those events (defined as normal and anticipated operational occurrences in 10 CFR 50) expected to occur more frequently than once during the lifetime of a particular unit.

The limiting accidents that were used to determine instrument functions are:

- o Loss-of-coolant accident (LOCA).
- o Steam line break.
- o Feedwater line break
- o Steam generator tube rupture.

7.5.2.1.2 Hot Standby

Hot standby is the state of the plant in which the reactor is subcritical such that k_{eff} is less than or equal to 0.99 and the reactor coolant system (RCS) temperature is greater than or equal to 350°F.

7.5.2.1.3 Cold Shutdown

Cold shutdown is the state of the plant in which the reactor is subcritical such that k_{eff} is less than or equal to 0.99, the RCS temperature is less than 200°F, and the RCS pressure is less than or equal to 10 CFR 50, Appendix G limits.

7.5.2.1.4 Controlled Condition

A controlled condition is the state of the plant that is achieved when the "subsequent action" portion of the plant emergency procedures is implemented and the critical safety functions are being accomplished or maintained by the control room operating staff.

7.5.2.1.5 Critical Safety Functions

Critical safety functions are those safety functions that are essential to prevent a direct and immediate threat to the health and safety of the public. These are the accomplishing or maintaining of:

- o Reactivity control
- o Reactor coolant system integrity

- o Reactor coolant inventory control
- o Reactor core cooling.
- o Heat sink maintenance.
- o Reactor containment environment.

7.5.2.1.6 Immediately Accessible Information

Immediately accessible information is information that is visually available to the control room operating staff immediately (i.e., within human response time requirements), once they have made the decision that the information is needed.

7.5.2.1.7 Primary Information

Primary information is information that is essential for the direct accomplishment of the preplanned manual actions necessary to bring the plant into a safe condition in the event of a DBA event; it does not include those variables that are associated with contingency actions.

7.5.2.1.8 Contingency Actions

Contingency actions are those manual actions that address conditions beyond the DBA events.

7.5.2.1.9 Key Variables

Key variables are those variables which provide the most direct measure of the information required.

7.5.2.1.10 Backup Information

Backup information is that information, made up of additional variables beyond those classified as key, that provide supplemental and/or confirmatory information to the control room operating staff. Backup variables do not

provide indication which is as reliable or complete as that provided by primary variables and are not usually relied upon as the sole source of information.

7.5.2.2 Variable Types

These accident monitoring variables and information display channels are those that are required to enable the control room operating staff to perform the functions defined by type A, B, C, D, and E classifications as follows.

7.5.2.2.1 Type A

Type A variables provide the primary information required to permit the control room operating staff to:

A. Perform the diagnosis to be specified in the WAPWR emergency operating instructions.

B. Take the specified, preplanned, manually controlled actions for which no automatic control is provided that are required for safety systems to accomplish their safety function in order to recover from the DBA.

C. Attain and maintain a cold shutdown condition.

The verification of the actuation of safety-related systems has been excluded from the type A definition. The variables which provide this verification are included in the definition of type D.

Type A variables are restricted to preplanned actions for DBA events. Variables used for contingency actions and additional variables which might be utilized are of types B, C, D, and E.

7.5.2.2.2 Type B

Type B variables provide to the control room operating staff information to assess the process of accomplishing or maintaining critical integrity safety functions (i.e., reactivity control, RCS integrity, RCS inventory control, reactor core cooling, heat sink maintenance, and reactor containment environment).

7.5.2.2.3 Type C

Type C variables provide the control room operating staff information to monitor:

A. The extent to which variables that indicate the potential for causing a gross breach of a fission product barrier have exceeded the design basis values.

B. The incore fuel cladding, the RCPB, or the primary reactor containment which may have been subject to gross breach.

These variables include those required to initiate the early phases of an emergency plan. Excluded are those associated with monitoring of radiological release from the plant which are included in type E.

Type C variables used to monitor the potential for breach of a fission product barrier have an arbitrarily determined extended range. The extended range was chosen to minimize the probability of instrument saturation even if conditions exceed those predicted by the safety analysis.

Although variables selected to fulfill type C functions may rapidly approach the values that indicate an actual gross failure, it is the final steady-state value reached that is important. Therefore, a high degree of accuracy and a rapid response time are not necessary for type C information display channels.

7.5.2.2.4 Type D

Type D variables provide the control room operating staff sufficient information to monitor the performance of:

A. Plant safety systems employed for mitigating the consequences of an accident and subsequent plant recovery to attain a cold shutdown condition. These include verification of the automatic actuation of safety systems.

B. Other systems normally employed for attaining a cold shutdown condition.

7.5.2.2.5 Type E

Type E variables provide the control room operating staff information to:

A. Monitor the habitability of the control room.

B. Monitor the plant areas where access may be required to service equipment necessary to monitor or mitigate the consequences of an accident.

C. Estimate the magnitude of release of radioactive material through identified pathways and continually assess such releases.

D. Monitor radiation levels and radioactivity in the environment surrounding the plant.

7.5.2.3 Variable Categories

The qualification requirements of the type A, B, C, D, and E accident monitoring instrumentation are subdivided into three categories. Descriptions of the three categories are given below. Table 7.5-2 briefly summarizes the selection criteria for type A, B, C, D, and E variables into each of the three categories. Table 7.5-3 briefly summarizes the design and qualification requirements of the three designated categories.

7.5.2.3.1 Category 1

7.5.2.3.1.1 Selection Criteria for Category 1

The selection criteria for Category 1 variables have been subdivided according to the variable type. For type A, those key variables used for diagnosis or providing information for necessary operator action have been designated Category 1. For type B, those key variables used for monitoring the process of accomplishing or maintaining critical safety functions have been designated Category 1. For type C, those key variables used for monitoring the potential for breach of a fission product barrier have been designated Category 1. There are no type D or type E Category 1 variables.

7.5.2.3.1.2 Qualification Criteria for Category 1

The instrumentation is seismically and environmentally qualified in accordance with Sections 3.10 and 3.11, respectively, of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design". Instrumentation shall continue to read within the required accuracy following but not necessarily during a seismic event.

At least one instrumentation channel is qualified from the sensor up to and including the display. For the other instrumentation channels, qualification as a minimum is applied up to and includes the channel isolation device. (Refer to Subsection 7.5.2.3.4. in regards to extended range instrumentation qualification.)

7.5.2.3.1.3 Design Criteria for Category 1

A. No single failure within either the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources, concurrent with the failures that are a cause of or result from a specific accident, will prevent the control room operating staff from being presented the required information. Where failure of one accident-monitoring channel results in information ambiguity (e.g., the redundant displays disagree), the

additional information is provided to allow the control room operating staff to analyze the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the same variable (addition of an identical channel) or by providing independent channels which monitor different variables which bear known relationships to the channels (addition of a diverse channel(s)). Redundant or diverse channels are electrically independent and physically separated from each other with two-train separation and from equipment not classified important to safety in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems".

If ambiguity does not result from failure of the channel, then a third redundant or diverse channel is not required.

B. The instrumentation is energized from station emergency standby power sources, battery backed where momentary interruption is not tolerable, as discussed in Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants".

C. The out-of-service interval will be based on normal Technical Specification requirements for the system it serves where applicable or where specified by other requirements.

D. Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal time interval between generating station shutdowns, a capability for testing during power operation is provided.

E. Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.

F. The design facilitates administrative control of the access to all setpoint adjustments, module calibration adjustments, and test points.

G. The monitoring instrumentation design minimizes the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications that could be potentially confusing to the control room operating staff.

H. The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

I. To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.

J. Periodic checking, testing, calibration, and calibration verification will be performed in accordance with the applicable portions of Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems".

K. The range selected for the instrumentation encompasses the expected operating range of the variable being monitored to the extent that saturation does not negate the required action of the instrument in accordance with the applicable portions of Regulatory Guide 1.105, "Instrument Setpoints".

7.5.2.3.1.4 Information Processing and Display Interface Criteria for Category 1

The interface criteria specified here provide requirements to be implemented in the processing and displaying of the information.

A. The control room operating staff has immediate access to the information from redundant or diverse channels in units of measure familiar to the staff; i.e. for temperature readings, degrees should be used, not volts. Where two or more instruments are needed to cover a particular range, overlapping instrument spans are provided.

B. A historical record of at least one instrumentation channel for each process variable is maintained. A recorded pre-event history for these channels is required for a minimum of 1 h, and continuous recording of these channels is required following an accident until continuous recording of such information is no longer deemed necessary. The term "continuous recording" is not intended to exclude the use of discrete time sample data storage systems. This recording is available when required and does not need to be immediately accessible.

7.5.2.3.2 Category 2

7.5.2.3.2.1 Selection Criteria for Category 2

The selection criteria for Category 2 variables are subdivided according to the variable type. For types A, B, and C, those variables which provide preferred backup information are designated Category 2. For type D, those key variables that are used for monitoring the performance of safety systems have been designated Category 2. For type E, those key parameters to be monitored for use in determining the magnitude of the release of radioactive materials and for continuously assessing such releases have been designated Category 2.

7.5.2.3.2.2 Qualification Criteria for Category 2

Category 2 instrumentation is qualified from the sensor up to and including the channel isolate device for at least the environment (seismic and/or environmental) in which it must operate to serve its intended function.

7.5.2.3.2.3 Design Criteria for Category 2

A. Category 2 instrumentation associated with those safety-related systems that are required to operate following a safe shutdown earthquake to mitigate a consequential plant incident are energized from a seismically qualified power source, which is battery backed where momentary interruption is not tolerable. Otherwise, the instrumentation is

energized from a highly reliable onsite power source, not necessarily the emergency standby power, which is battery backed where momentary interruption is not tolerable.

B. The out-of-service interval will be based on normal Technical Specification requirements for the system it serves where applicable or where specified by other requirements.

C. Servicing, testing, and calibration programs will be specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal time interval between generating station shutdowns, a capability for testing during power operation is provided.

D. Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.

E. The design facilitates administrative control of the access to all setpoint adjustments, module calibration adjustments, and test points.

F. The monitoring instrumentation design minimizes the potential for the development of conditions that would cause meters, annunciators, recorders, and alarms, etc., to give anomalous indications that could be potentially confusing to the operator.

G. The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

H. To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.

I. Periodic checking, testing, calibration, and calibration verification will be in accordance with applicable portions of Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems".

J. The range selected for the instrumentation encompasses the expected operating range of the variable being monitored to the extent that saturation does not negate the required action of the instrument in accordance with the applicable portions of Regulatory Guide 1.105, "Instrument Setpoints".

7.5.2.3.2.4 Information Processing and Display Interface Criteria for Category 2

The instrumentation signal is, as a minimum, processed for display on demand. Recording requirements are variable specific and are determined on a case-by-case basis.

7.5.2.3.3 Category 3

7.5,2.3.3.1 Selection Criteria for Category 3

The selection criteria for Category 3 variables have been subdivided according to the variable type. For types B and C, those variables which provide backup information have been designated Category 3. For types D and E, those variables which provide preferred backup information have been designated Category 3. There are no Category 3 type A variables.

7.5.2.3.3.2 Qualification Criteria for Category 3

The instrumentation is high quality, commercial grade which is not required to provide information when exposed to a post-accident adverse environment.

7.5.2.3.3.3 Design Criteria for Category 3

A. Servicing, testing, and calibration programs will be specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal time interval between generating station shutdown, a capability for testing during power operation is provided.

B. Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.

C. The design facilitates administrative control of the access to all setpoint adjustments, module calibration adjustments, and test points.

D. The monitoring instrumentation design minimizes the potential for the development of conditions that would cause meters, annunciators, recorders, and alarms, etc., to give anomalous indications that could be potentially confusing to the operator.

E. The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

F. To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.

7.5.2.3.3.4 Information Processing and Display Interface Criteria for Category 3

The instrumentation signal is, as a minimum, processed for display on demand. Recording requirements are variable specific and have been determined on a case-by-case basis.

7.5.2.3.4 Extended Range Instrumentation Qualification Criteria

The qualification environment for extended range instrumentation is based on the DBA events; the assumed maximum qualification value of the monitored variable shall be equal to the specified maximum range for the variable. The monitored variable is assumed to approach this peak by extrapolating the most severe initial ramp associated with the DBA events. The decay is considered proportional to the decay for this variable associated with the DBA events. No additional qualification margin needs to be added to the extended range variable. All environmental envelopes, except those pertaining to the variable measured by the information display channel, are those associated with the DBA events. The environmental qualification requirement for extended range instrument does not account for steady-state elevated levels that may occur in other environmental parameters associated with the extended range variable. For example, a sensor measuring containment pressure must be qualified for the measured process variable range (i.e., three times design pressure for concrete containments), but the corresponding ambient temperature is not mechanistically linked to that pressure. Rather, the ambient temperature value is the bounding value for DBA events analyzed in Chapter 15. The extended range requirement is to ensure that the instrument will continue to provide information if conditions degrade beyond those postulated in the safety analysis. Since extended variable ranges are nonmechanistically determined, extension of associated parameter levels is not justifiable and is therefore not required.

7.5.3 Description of Variables

7.5.3.1 Type A Variables

Type A variables are defined in Subsection 7.5.2.2.1. They are the variables which provide primary information required to permit the control room operating staff to:

A. Perform the diagnosis to be specified in the WAPWR emergency operating procedures

B. Take specified preplanned manually controlled actions for which no automatic control is provided that are required for safety systems to accomplish their safety function to recover from a design basis accident (DBA) event. (Verification of actuation of safety systems is excluded from type A and is included as type D.)

C. Attain and maintain a cold shutdown condition.

Key type A variables have been designated Category 1. These are the variables which provide the most direct measure of the information required. The key type A variables are:

- o Reactor coolant system (RCS) upper- and lower- range pressure.
- o WR hot leg reactor coolant temperature (T_{hot}).
- o WR cold leg reactor coolant temperature (T_{cold}).
- o WR steam generator level.
- o Pressurizer level.
- o Containment pressure.
- o Steam line pressure.
- o Containment sump water level.
- o Emergency feedwater storage tank level.
- o Emergency feedwater flow.
- o Containment radiation level.
- o Steamline radiation.
- o Core exit temperature.
- o RCS subcooling.

No type A backup variables have been identified. Therefore, no Category 2 or 3 variables have been designated. A summary of type A variables is provided in Table 7.5-4.

7.5.3.2 Type B Variables

Type B variables are defined in Subsection 7.5.2.2.2. They are the variables that provide information to the control room operating staff to assess the process of accomplishing or maintaining critical safety functions, i.e.:

- o Reactivity control.
- o RCS pressure control.
- o Reactor coolant inventory control.
- o Reactor core cooling.
- o Heat sink maintenance.
- o Primary reactor containment environment.

Variables which provide the most direct indication (i.e., key variable) to assess each of the six critical safety functions have been designated Category 1. Preferred backup variables have been designated Category 2. All other backup variables have been designated Category 3. These are listed in Table 7.5-5.

7.5.3.3 Type C Variables

Type C variables are defined in Subsection 7.5.2.2.3. Basically, they are the variables that provide to the control room operating staff information to monitor the potential for breach or actual gross breach of:

- o Incore fuel clad.
- o RCS boundary.
- o Containment boundary.

(Variables associated with monitoring of radiological release from the plant are included in type E.)

Those type C key variables which provide the most direct measure of the potential for breach of one of the three fission product boundaries have been designated Category 1. Backup information indicating potential for breach is designated Category 2. Variables which indicate actual breach have been designated as preferred backup information and are designated Category 2.

Table 7.5-6 summarizes the selection of type C variables.

7.5.3.4 Type D Variables

Type D variables are defined in Subsection 7.5.2.2.4. They are those variables that provide sufficient information to the control room operating staff to monitor the performance of:

A. Plant safety systems employed for mitigating the consequences of an accident and subsequent plant recovery to attain a safe shutdown condition, including verification of the automatic actuation of safety systems.

B. Other systems normally employed for attaining a cold shutdown condition.

Type D key variables are designated Category 2. Preferred backup information is designated type D Category 3.

The following systems or major components have been identified as requiring type D information to be monitored:

A. Reactivity control (employed for verifying that the reactor has tripped and that adequate negative reactivity has been added to the core to prevent a return to criticality).

B. Pressurizer level and pressure control (assess status of the RCS following return to normal pressure and level control under certain post-accident conditions).

C. Chemical and volume control system (CVCS) (employed for attaining a safe shutdown under certain post-accident conditions).

D. Secondary pressure and level control (employed for restoring/maintaining a secondary heat srink under post-accident conditions).

E. Integrated safeguards system (ISS) including the containment systems and residual heat removal system (RHRS).

F. Emergency feedwater system (EFWS).

G. Component cooling water system (CCWS).

H. Essential service water system (ESWS).

I. Heating, ventilation, and air conditioning (HVAC).

J. Electric power to vital safety systems.

K. Verification of automatic actuation of safety systems.

Table 7.5-7 lists the key variables identified for each system listed above.

For the purpose of specifying seismic qualification for type D Category 2 variables, it is assumed that a seismic event and a break in Seismic Category 1 piping will not occur concurrently. As a result, the limiting event is an unisolated (single failure of a main steam isolation valve) break in Nuclear Safety Class 2 main steam piping. Instrumentation necessary to monitor this event and associated with the safety systems which are required to mitigate it should be seismically qualified. Similarly, the environmental qualification of type D Category 2 variables depends on whether the instrumentation is subject to a high-energy line break when required to provide information.

7.5.3.5 Type E Variables

Type E variables are defined in Subsection 7.5.2.2.5. They are those variables that provide the control room operating staff with information to:

A. Monitor the habitability of control room.

B. Monitor the plant areas where access may be required to service equipment necessary to monitor or mitigate the consequences of an accident.

C. Estimate the magnitude of release of radioactive materials through identified pathways.

D. Monitor radiation levels and radioactivity in the environment surrounding the plant.

Key type E variables are qualified to Category 2 requirements. Preferred backup type E variables are qualified to Category 3 requirements.

Table 7.5-8 lists the key type E variables.

7.5.4 Bypassed and Inoperable Status Indication for Engineered Safety Features Systems

7.5.4.1 Description

For a description of the Bypassed and Inoperable Status Indication (BISI) System and compliances to Regulatory Guide 1.47, refer to RESAR-SP/90 PDA Module 15, "ACR/Human Factors".

TABLE 7.5-1
(Sheet 1 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Reactor coolant pressure (upper range	1200-3600	A1, B1, B2, C1 C2, D2	Yes	Yes	3 per unit	1E	Transmitters locate outside of contain
Reactor coolant pressure (lower range)	0-1400	A1, B1, B2, D2	Yes	Yes	3 per unit	1E	Transmitters loc outside of conta
RCS wide range T_{hot}	50° to 700°F	A1, B1, B2	Yes	Yes	2 per loop	1E	
RCS wide range T_{cold}	50° to 700°F	A1, B1, B2, C1	Yes	Yes	2 per loop	1E	
Wide range steam generator water level	0 to 100 percent of span	A1, B1, B2, D2	Yes	Yes	3 per steam generator	1E	Temperature comp
Pressurizer level	0 to 100 percent of span	A1, B1, D2	Yes	Yes	3 per unit	1E	
Containment pressure	0 to 53 psig	A1, B1, C2, D2	Yes	Yes	3 per unit	1E	
Steamline pressure	0 to 1350 psig	A1, B1, D2	Yes	Yes	3 per loop	1E	

TABLE 7.5-1
(Sheet 2 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Containment water level	0 to 100% level	A1, B1, B2, C2	Yes	Yes	3 per unit	1E	
Emergency feed-water storage tank level	0 to 100 percent of span	A1, D2	Yes	Yes	3 per tank	1E	
Total emergency feedwater flow	0 to max. runout flow	A1, B1, D2	yes	Yes	2 per loop	1E	
Containment radiation level	10^{-4} 10^{8} R/hr	A1, B1 E2	Yes	Yes	2 per unit	1E	
Steamline radiation monitor	10^{-1} to 10^{3} $\mu Ci/cm^3$	A1	Yes	Yes	1 per loop	1E	
Core exit temperature	100 to 2200°F	A1, B1, C1	Yes	Yes	4 per core quadrant per train	1E	
RCS subcooling	200°F sub-cooling to 35°F super-heat	A1, B1	Yes	Yes	3 per unit	1E	
Neutron flux	10^{-8} to 100 percent of full power	B1	Yes	Yes	2 per unit	1E	

TABLE 7.5-1
(Sheet 3 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Reactor vessel water level	0 to 100 percent plenum height; 0 to 100 percent reactor vessel height	B1, C1	Yes	Yes	2 per unit	1E	
Containment hydrogen concentration	0 to 10 percent partial pressure	B1, C1	Yes	Yes	2 per unit	1E	
Control rod position indication	0 to 228 steps	B3, D3	No	No	2 per control rod	Non-1E	
Containment pressure (extended range)	-5 to 140 psig	C1, C2	Yes	Yes	3 per unit	1E	
Plant vent radiation level	10^{-6} to 10^{4} $\mu Ci/cm^3$	C2, E2	No	Yes	1 per unit	1E	
Site environmental radiation level	NA	C3, E3	No	No	NA	NA	

TABLE 7.5-1
(Sheet 4 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
RCS activity (post-accident sampling)	NA	C3	No	No	1	NA	
Containment isolation valve status	Closed/ Not Closed	C2, D2	Yes	Yes	1 per valve	1E	
Power-operated relief (PORV) valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Primary safety valve status	Closed/not closed	D2	yes	Yes	1 per valve	1E	
Pressurizer heater power availability	On/off	D2	Yes	Yes	2 per unit	1E	
Charging system flow	0 to 110 percent design flow	D2	Yes	Yes	1 per path	1E	
Letdown flow	0 to 110 percent design flow	D2	Yes	Yes	1 per path	1E	
Volume control tank level	0 to 100 percent of span	D2	No	Yes	1 per tank	1E	

TABLE 7.5.2-1
(Sheet 5 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Chemical and volume control system valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Chemical and volume control system pump status	On/off	D2	Yes	Yes	1 per pump	1E	
Reactor coolant pump seal injection flow	0 to 20 gal/min	D2	No	Yes	1 per pump	1E	
Steam generator atmospheric PORV status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Steam generator safety valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Main steam line isolation valve status	Closed/ Not closed	B2, D2	Yes	Yes	1 per valve	1E	
Main steamline isolation bypass valve status	Closed/ Not closed	B2, D2	Yes	Yes	1 per valve	1E	
Main feedwater control valve status	Closed/ Not closed	D2	Yes	Yes	1 per loop	1E	

TABLE 7.5.2-1
(Sheet 6 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Main feedwater bypass valve status	Closed/ Not closed	D2	Yes	Yes	1 per loop	1E	
Main feedwater isolation valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Main feedwater flow	0 to 110 percent design flow	D2	No	No	1 per loop	Non-1E	
Startup feedwater control valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Startup feedwater flow	0 to 110 percent design flow	D2	No	No	1 per loop	Non-1E	
Steam generator overflow valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Steam generator blowdown isolation valve status	Closed/ Not closed	D2	Yes	Yes	1 per valve	1E	
Safety injection flow	0 to 110 percent design flow	D2	Yes	Yes	1 per train	1E	

TABLE 7.5-1
(Sheet 7 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
RHR/containment spray flow	0 to 110 percent design flow	D2	Yes	Yes	1 per train	1E	
EWST level	0 to 100 percent	D2	Yes	Yes	1 per tank	1E	
ISS valve status (SI, RHR/ CS, accumulators, core reflood tanks)	Open/closed	D2	Yes	Yes	1 per valve	1E	
Accumulator pressure	0 to 750 psig	D2	Yes	Yes	1 per accumulator	1E	
Core reflood tank pressure psig	0 to 300 psig	D2	Yes	Yes	1 per tank	1E	
RHR heat exchanger inlet temperature	50 to 400 °F	D2	Yes	Yes	1 per exchanger	1E	
RHR heat exchanger outlet temperature	50 to 400 °F	D2	Yes	Yes	1 per exchanger	1E	
Fan cooler motor speed	0 to 110 percent design speed	D2	Yes	No	1 per cooler	1E	

TABLE 7.5-1
(Sheet 8 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Emergency feed-water valve status	Open/closed	D2	Yes	Yes	1 per valve	1E	
Component cooling water header pressure	0 to 200 psig	D2	No	Yes	1 per train	1E	
Component cooling water header temperature	0 to 300°F	D2	No	Yes	1 per train	1E	
Component cooling water surge tank level	0 to 100 percent	D2	No	Yes	1 per train	1E	
Component cooling water flow to engineered safety features com-ponents	0 to 110 percent design flow	D2	Yes	Yes	1 per component	1E	
Component cooling water valve status	Open/closed	D2	Yes/No	Yes	1 per valve	1E	
Essential service water header pressure	0 to 200 psi	D2	No	Yes	1 per header	1E	

TABLE 7.5-1
(Sheet 9 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Essential service water flow	0 to 110 percent design flow	D2	No	Yes	1 per header	1E	
RCS boron concentration	0 to 2000 ppm	D3	No	No	1 per unit	Non-1E	
Heating, ventilation, and air-conditioning system status	Open/closed	D2	Yes	Yes	1 per damper	1E	
Engineered safety features (ESF) environment temperature	High/low	D2	Yes	Yes	1 per ESF component	1E	
Ac, dc, vital instrument voltage	Bus specific	D2	No	Yes	1 per bus	1E	
Reactor trip breaker position	Open/ Closed	D2	No	Yes	1 per breaker	1E	
Turbine stop valve status	Closed/ Not closed	D2	No	No	1 per valve	Non-1E	
Turbine control valve status	Closed/ Not closed	D2	No	No	1 per valve	Non-1E	
Emergency feedwater pump status (motor-driven)	On/off	D2	No	Yes	1 per pump	1E	

TABLE 7.5.2-1
(Sheet 10 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Turbine driven emergency feed-water pump supply valve status	Open/closed	D2	Yes	Yes	1 per pump	1E	
Safety injection pump status	On/off	D2	Yes	Yes	1 per pump	1E	
RHR/containment spray pump status	On/off	D2	Yes	Yes	1 per pump	1E	
Component cooling water pump status	On/off	D2	No	Yes	1 per pump	1E	
Essential service water system pump status	On/off	D2	No	Yes	1 per pump	1E	
Reactor vessel head vent valve status	Open/closed	D2	Yes	Yes	1 per valve	1E	
Control room radiation level	10^{-5} to 1 R/hr	E2	No	Yes	1 per control room	1E	
Plant vent air flow rate		E2	No	Yes	1 per plant vent	1E	
Condenser air ejector radia-tion level	10^{-6} to 10^{5} µCi/cc	E2	No	Yes	1 per ejector	1E	

TABLE 7.5-1
(Sheet 11 of 11)

POST-ACCIDENT MONITORING INSTRUMENTATION

Variable	Range/ Status	Type/ Category	Qualification		Required Number of Instruments	Power Supply	Notes
			Environ-mental	Seismic			
Condenser air ejector flow rate		E2	No	Yes	1 per ejector	1E	
Steam generator safety relief valve radiation level	10^{-1} to 10^{3} µCi/cc	E2	Yes	Yes	1 per valve or header	1E	
Steam generator safety/relief valve flow rate		E2	Yes	Yes	1 per valve or header	1E	
Radiation level from liquid pathways	10^{-6} to 10^{-1} µCi/cc	E2	No	Yes	1 per pathway	1E	
Liquid pathways flow rate		E2	No	Yes	1 per pathway	1E	
Other potential sources of radiation release	10^{-6} to 10^{4} µCi/cc	E2	No	Yes	1 per source	1E	
Other potential source flow rate		E2	No	Yes	1 per source	1E	
Area radiation	10^{-4} to 10^{8} R/hr	E2	No	Yes	Site specific	1E	
Environs radiation level		E3	No	No	Site specific	Non-1E	
Meteorological parameters	Site specific	E3	No	No	Site specific	Non-1E	

TABLE 7.5-2

SUMMARY OF SELECTION OF CRITERIA

Type	Category 1	Category 2	Category 3
A	Key variables that are used for diagnosis or providing information necessary for operator action	Variables which provide preferred backup information	None
B	Key variables that are used for monitoring the process of accomplishing or maintaining critical safety functions	Variables which provide preferred backup information	Variables which provide backup information
C	Key variables that are used for monitoring the potential for breach of a fission product barrier	Variables which provide preferred backup information	Variables which provide backup information
D	None	Key variables which are used for monitoring the performance of plant systems	Variables which provide preferre backup information which are use for monitoring the performance c plant systems
E	None	Key variables to be monitored for use in determining the magnitude of the release of radioactive materials and for continuously assessing such releases.	Variables to be monitoried whicl provide preferred backup informa tion for use in determining the magnitude of the release of radio- active materials and for continu- ously assessing such releases.

TABLE 7.5-3

SUMMARY OF DESIGN, QUALIFICATION, AND INTERFACE REQUIREMENTS

Qualification	Category 1	Category 2	Category 3
Environmental	Yes	As appropriate (See Subsection 7.5.2.3.2.2)	No
Seismic	Yes	As appropriate (See Subsection 7.5.2.3.2.2.)	No
Design			
Single failure	Yes	No	No
Power supply	Emergency diesel generator	Emergency diesel generator/onsite (as appropriate, see Subsection 7.5.2.3.2.3.A)	As required
Channel out of service	Technical Specifications	Technical Specifications	As required
Testability	Yes	Yes	As required
Interface			
Minimum indication	Immediately accessible	Demand	Demand
Recording	Yes	As required (See Subsection 7.5.2.3.2.4.)	As required (See Subsection 7.5.2.3.3.

TABLE 7.5-4

SUMMARY OF TYPE A VARIABLES

Variable	Variable Function	Type/ Category
RCS pressure (lower- and upper-range)	Key	A1
T_{hot} (WR)	Key	A1
T_{cold} (WR)	Key	A1
Steam generator level (temperature compensated WR)	Key	A1
Pressurizer level	Key	A1
Containment pressure	Key	A1
Steamline pressure	Key	A1
Containment water level	Key	A1
Emergency feedwater storage tank level	Key	A1
Emergency feedwater flow	Key	A1
Containment radiation level	Key	A1
Steamline radiation monitor	Key	A1
Core exit temperature	Key	A1
RCS subcooling	Key	A1

TABLE 7.5-5

SUMMARY OF TYPE B VARIABLES

Function Monitored	Variable	Variable Function	Type/ Category
Reactivity control	Neutron Flux	Key	B1
	WR T_{hot}	Backup (P)*	B2
	WR T_{cold}	Backup (P)	B2
	Control rod position	Backup	B3
RCS Integrity	RCS pressure (lower and upper range)	Key	B1
	WR T_{hot}	Key	B1
	WR T_{cold}	Key	B1
Reactor coolant inventory control	Pressurizer level	Key	B1
	Reactor vessel water level	Key	B1
	Containment water level	Backup (P)	B2
	WR steam generator level	Backup (P)	B2
Reactor core cooling	Core exit temperature	Key	B1
	Reactor vessel water level	Key	B1
	RCS subcooling	Key	B1
	WR T_{hot}	Backup (P)	B2
	WR T_{cold}	Backup (P)	B2
	RCS pressure (WR)	Backup (P)	B2
Heat sink maintenance	Steam generator level (WR)	Key	B1
	Emergency feedwater flow	Key	B1
	Steamline pressure	Key	B1
	Main steamline isolation and bypass valve status	Backup(P)*	B2
Containment environment	Containment pressure	Key	B1
	Containment area radiation	Key	B1
	Containment water level	Key	B1
	Containment hydrogen concentration	Key	B1

* P = preferred

TABLE 7.5-6
(Sheet 1 of 2)

SUMMARY OF TYPE C VARIABLES

Function Monitored	Variable	Condition	Variable Function	Type/ Category
Incore fuel clad	Core exit temperature	Potential for breach	Key	C1
	Reactor vessel water level	Potential for breach	Key	C1
	RCS activity	Actual breach	Backup	C3
RCS boundary	RCS pressure (upper range)	Potential for breach	Key	C1
	RCS temperature (wide range)	Potential for breach	Key	C1
	RCS pressure (upper range)	Actual breach	Backup (P)*	C2
	Containment pressure	Actual breach	Backup (P)	C2
	Containment water level	Actual breach	Backup (P)	C2
Containment boundary	Containment pressure (extended range)	Potential for breach	Key	C1
	Containment hydrogen concentration	Potential for breach	Key	C1
	Plant vent radiation level	Actual breach	Backup (P)	C2

* P = preferred

TABLE 7.5-6
(Sheet 2 of 2)

SUMMARY OF TYPE C VARIABLES

Function Monitored	Variable	Condition	Variable Function	Type/ Category
	Containment isolation valve status	Actual breach	Backup (P)	C2
	Containment pressure (extended range)	Actual breach	Backup (P)	C2
	Site environmental radiation	Actual breach	Backup	C3

TABLE 7.5-7
(Sheet 1 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Variable Function	Type/ Category
Reactivity Control System	Reactor trip breaker position	Key	D2
	Control Rod Position	Backup	D3
	Turbine Stop Valve Status	Key	D2
	Turbine Control Valve Position	Key	D2
	RCS Boron Concentration	Backup	D3
Pressurizer level and pressure control	Power-operated relief valve (PORV) status	Key	D2
	Safety valve status	Key	D2
	Pressurizer level	Key	D2
	RCS pressure (WR)	Key	D2
	Pressurizer heater power availability	Key	D2
CVCS	Charging system flow	Key	D2
	Letdown flow	Key	D2
	Volume control tank level	Key	D2
	Seal injection flow	Key	D2
	CVCS valve status	Key	D2
	Head vent valve status	Key	D2
Secondary pressure and level control	Steam generator atmospheric steam dump valve status	Key	D2
	Steam generator safety valve status	Key	D2
	Main steam isolation valve and bypass valve status	Key	D2
	Main feedwater control and bypass status	Key	D2

TABLE 7.5-7
(Sheet 2 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Variable Function	Type/ Category
	Main feedwater isolation valve status	Key	D2
	Startup feedwater control valve status	Key	D2
	Main feedwater flow	Key	D2
	Startup feedwater flow	Key	D2
	Emergency feedwater flow	Key	D2
	Steam generator level (WR)	Key	D2
	Steam generator overflow valve status	Key	D2
	Steam generator blowdown isolation valve status	Key	D2
	Steamline pressure	Key	D2
ISS (including containment spray and residual heat removal)	Emergency water storage tank level	Key	D2
	Total SIS flow	Key	D2
	Total RHR/containment spray flow	Key	D2
	EWST level	Key	D2
	ISS valve status	Key	D2
	Accumulator pressure	Key	D2
	Core reflood tank pressure	Key	D2
	RHR heat exchanger inlet and outlet temperature	Key	D2
	Fan cooler motor speed	Key	D2
	Containment pressure	Key	D2
Emergency feedwater system	Emergency feedwater flow	Key	D2
	Emergency feedwater valve status	Key	D2
	Emergency feedwater storage tank level	Key	D2

TABLE 7.5-7
(Sheet 3 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Variable Function	Type/ Category
Component cooling water system	CCWS header pressure	Key	D2
	CCWS header temperature	Key	D2
	CCWS surge tank level	Key	D2
	Flow to ESF components	Key	D2
	CCWS valve status	Key	D2
Essential service water system	ESWS header pressure	Key	D2
	ESWS flow	Key	D2
HVAC	Environmental for ESF components	Key	D2
	System status	Key	D2
Electric power	AC/DC vital instrument voltage	Key	D2
Verification of automatic actuation's of safety systems	Reactor trip breaker position	Key	D2
	Turbine stop valve position	Key	D2
	Turbine control valve position	Key	D2
	ac/dc vital bus voltage	Key	D2
	Main feedwater control valve status	Key	D2
	Main feedwater bypass valve status	Key	D2
	Main feedwater isolation valve status	Key	D2
	Containment isolation valve status	Key	D2
	Emergency feedwater valve alignment	Key	D2
	Emergency feedwater pump start (motor-driven)	Key	D2
	Emergency feedwater pump supply valve status (turbine-driven)	Key	D2

TABLE 7.5-7
(Sheet 4 of 4)

SUMMARY OF TYPE D VARIABLES

System	Variable	Variable Function	Type/ Category
	SI pump start	Key	D2
	CCWS pump start	Key	D2
	ESWS pump start	Key	D2
	RHR/containment spray pump start	Key	D2
	CVCS pump status	Key	D2
	SI valve alignment	Key	D2
	Containment spray valve alignment	Key	D2
	SI flow	Key	D2
	RHR/containment spray flow	Key	D2
	Emergency feedwater flow	Key	D2

TABLE 7.5-8
SUMMARY OF TYPE E VARIABLES

Variable	Variable Function	Type/ Category
Control room radiation level	Key	E2
Plant vent radiation level	Key	E2
Plant vent air flow rate	Key	E2
Condenser air ejector radiation level	Key	E2
Condenser air ejector flow rate	Key	E2
Steam generator safety/refuel valve radiation level	Key	E2
Steam generator safety/relief valve flow rate	Key	E2
Radiation level of material discharged from liquid pathways	Key	E2
Liquid pathways flow rate	Key	E2
Other potential sources of radiation release	Key	E2
Other potential source flow rate	Key	E2
Environs radiation level	Backup (P)*	E3
Meteorological parameters	Backup (P)*	E3
Containment radiation level	Key	E2
Area radiation in areas requiring accessibility	Key	E2

* P = preferred

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

7.6.1 Instrumentation and Control System Power Supplies

7.6.1.1 Description

Each of the four channels of the integrated protection system (IPS) has its own dedicated 120V AC vital instrumentation and control power supply. Each of the four sets of 120V AC electrical power supply distribution panels (2 panels per set) receives its power from either of two 120V AC sources. The primary panel is fed from two interlocked circuit breakers, each with a separate source. Refer to the one line diagram shown in Figure 7.6-1. One source is a regulating stepdown transformer; the other source, an instrument inverter. The interlock on the primary panel is such that only one of the two circuit breakers may be closed at one time. Each of the four inverters can receive its power from either of two sources: one a 480V 3-phase AC source; the other, a 125V battery source. The inverter can use either the 125V DC source or the 480V 3-phase AC source to make 120V AC instrument power. The 480V 3-phase AC power is rectified to become 120V DC. This rectified DC is auctioneered with the DC from the battery to automatically select the source that powers the inverter. The back-up panel receives power from the regulating transformer source. Although generically a two battery supply for four vital instrument inverters has been used satisfactorily on many Westinghouse plants, in a previous Westinghouse submittal for review of an IPS plant (see RESAR 414) the NRC Staff has required four independent Class 1E batteries and battery chargers for the four vital instrument inverters. Although the Westinghouse evaluation of the two battery systems for the IPS has indicated that adverse interactions between control and protection cannot result due to the loss of a single power source, Westinghouse requires a four battery system for current IPS in the interest of increased conservatism and to acknowledge previously expressed NRC requests.

7.6.1.2 Analysis

It can, therefore, be more readily concluded that no single failure of a power source will prevent a required protection function to occur, or create an adverse interaction between the control and protection systems as a result of the loss of a single power source.

Based on the scope definitions presented in IEEE-308, Sept. 1971, IEEE-279, 1971, and IEEE-338, 1971, the criterion which is applicable to the instrumentation and control power supply system is IEEE-308 (Sept. 1971). The design will be in compliance with IEEE-308 (Sept. 1971) and Safety Guide 6. Availability of this system will be verified by periodic testing performed on the served systems and by checking the inverter output and auctioneering circuit by alternately deenergizing one input at a time. The Inverters will be seismically qualified.

7.6.2 Residual Heat Removal Isolation Valves - Interlocks and Actuation

7.6.2.1 Description

The residual heat removal isolation valves will normally be closed and will be only opened for residual heat removal after system pressure has been reduced to low RCS pressure 550 psig and temperature conditions.

1. Each residual heat removal valve will be provided with red (open) and green (closed) position indicating lights located in the main Control Room at the control switch for each valve. The valve position sensing for the valve position readout in the control room is by means of the cam operated switch within the motor operator of the valve.

2. The interlock and actuation logic functions will be as shown in the logic diagram of Figure 7.6-2.

This interlock is provided for the normally closed, motor operated RHR inner and outer suction isolation valves (9000A, B, C, D and 9001A, B, C, D) to

prevent the suction valves for a specific RHR subsystem from being opened by operator action unless the RCS pressure, as measured by the appropriate RCS wide-range pressure channel, is less than 550 psig and the following corresponding valves are in a closed position:

-- Spray additive isolation valves (9112, 9212, 9213, 9113)

-- RHR/EWST suction isolation valves (9007A, B, C, D)

-- Containment spray header isolation valves (9011A, B, C, D; 9009A, B, C, D)

-- System test line isolation valves (8813A, B, C, D; 8814A, B, C, D)

-- High head pump discharge isolation valves (8803A, B, C, D)

-- RHR to CVCS letdown isolation valve (where applicable) (9018A, B)

This prevent-open feature ensures that each of the four RHR subsystems are properly aligned for normal cooldown operations. The closed valves, listed above, provide a double barrier against leakage from the RHR subsystems either in conjunction with a series check valve or by providing two closed series motor-operated valves.

The interlock also automatically closes the inner and outer RHR suction isolation valves in the event that the RCS pressure were to increase to a value greater than 750 psig. This automatic closing feature ensures that both valves will be closed during a plant startup prior to reaching operating conditions, should one have been inadvertently left open by operator omission. The valves may be closed by operator action from the main control board at any time.

The wide-range RCS pressure interlock for both the prevent open and the autoclosure features on the inner isolation valves is independent and diverse from that provided to the outer isolation valves. Diversity is provided by

use of the set of wide range pressure inner transmitters of a model different than the set of outer transmitters.

7.6.2.2 Analysis of Residual Heat Removal Valves - Interlocks and Actuation

Based on the scope definitions presented in IEEE 279-1971 and IEEE 338-1971, these criteria do not apply to the residual heat removal isolation valve interlocks, because their function is not required during or after a design basis event. However, in order to meet NRC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE Standard 279-1971 will be applied with the following comments.

1. For the purpose of applying IEEE Standard 279-1971, to this circuit, the following definitions will be used.

   a. Protection System

      The two valves in series in each of the four lines and all components of their interlocking and closure circuits. (Note that the RHRS consists of four subsystems, each consisting of pump, a heat exchanger and valving to control the cooldown and isolate the system as necessary.)

   b. Protective Action

      The automatic initiation and maintenance of residual heat removal system isolation from the reactor coolant system when reactor coolant system pressures are above the preset value.

2. On-line Testability; IEEE Standard 279-1971, Paragraph 4.10: The above mentioned pressure interlock signals and logic will be tested on line to the maximum extent possible without adversely affecting safety. This test will include the initiating signals from which are derived the actuation and interlocking signals through to the actuation and interlocking signals available from the train oriented

integrated logic cabinets. This is done in the best interests of safety since an actual actuation to permit opening the valve could potentially leave only one remaining valve to isolate the low pressure Residual Heat Removal System from the Reactor Coolant System.

3. IEEE Standard 279-1971, Paragraph 4.15: This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring are discussed in Section 3.11 of RESAR-SP/90 PDA Module 7, "Structural/Equipment Design". The safety-grade cold shutdown concept imposes a conflicting requirement to provide a single failure RHRS initiation function along with the classical single failure autoclose function. The WAPWR design for cold shutdown is based on no operator action outside of the control room. Therefore, the WAPWR design with two electrical trains incorporates an RHRS suction valve arrangement with four way independence. Each RHRS suction valve is powered by a separate power supply and interlocked with a separate RCS pressure transmitter. RHR subsystems "A" and "D" have one suction valve powered by train "A" and one suction valve powered by "battery train A". "Battery train A" includes one battery, inverter (or motor-generator), and circuitry. The battery is continually charged by vital bus "A". RHR subsystems "B" and "C" have one suction valve powered by train "B". Battery train "B" is similar to battery train "A" except that battery train "B" constitute independent power supplies and provide the single failure autoclosure capability not provided by two electrical sources. Single failure initiation capability is provided by the two totally redundant pairs of RHR subsystems.

7.6.3 Critical Function Isolation Motor Operated Valve Interlocks

The control circuits for the accumulator and core reflood tank discharge isolation valves designated "critical function valves", are shown in Figure 7.6-3. The accumulator and core reflood tank discharge isolation valves are motor operated, normally open valves which are controlled from the MCP.

These valves are interlocked such that:

a) They open automatically on receipt of an "S" signal with the MCP switch in either the "AUTO" or "CLOSE" position.

b) They open automatically whenever the RCS pressure is above the SI unblock pressure (P-11) specified in the Technical Specifications only when the MCP switch is in the "AUTO" position.

c) They cannot be closed as long as an "S" signal is present.

The MCP switches for these valves are three position switches which provide a "spring return to AUTO" from the OPEN position and a "maintain position" from the CLOSE position.

The "maintain in CLOSE" is required to provide an administratively controlled manual block of the automatic opening of the valve at RCS pressure above the SI unblock pressure (P-11). The manual block or "maintain in CLOSE" position may be required in order to perform check valve leak tests or other anticipated operations.

Administrative control is required to ensure that any accumulator valve, which has been closed at pressures above the SI unblock pressure, is returned to the "AUTO" position. Verification that the valve automatically returns to its normal full open position would also be required.

During plant shutdown, the accumulator valves are in a closed position. To prevent an inadvertent opening of these valves during that period, the accumulator valve breakers should be opened or removed. Administrative control is again required to ensure that these valve breakers are closed during the pre-startup procedures.

These normally open, motor operated valves have been identified as "critical function" valves, and alarms indicating a mispositioning (with regard to their ECCS function) are provided. The alarms sound in the main control room.

Refer to Figure 7.6-4 for the logic diagram for the critical function valve alarm.

An alarm will sound for any critical-function valve for the following conditions when the RCS pressure is above the "SI unblocking pressure":

a) Valve motor operator limit switch indicates valve is not fully open, or

b) Valve stem mounted limit switch indicates valve is not fully open.

The valve stem limit switch shall repeat itself at given intervals.

In addition, each critical function valve will be provided with red (open) and green (closed) position indicating lights located in the main Control Room at the control switch for each valve. The valve position sensing for the valve position readout in the control room is by means of the cam operated switch within the motor operator of the valve.

It has been shown, in discussing the foregoing features of the control and indication for the critical function valves that the instrumentation and control for these valves complies with Branch Technical Position ICSB 3.

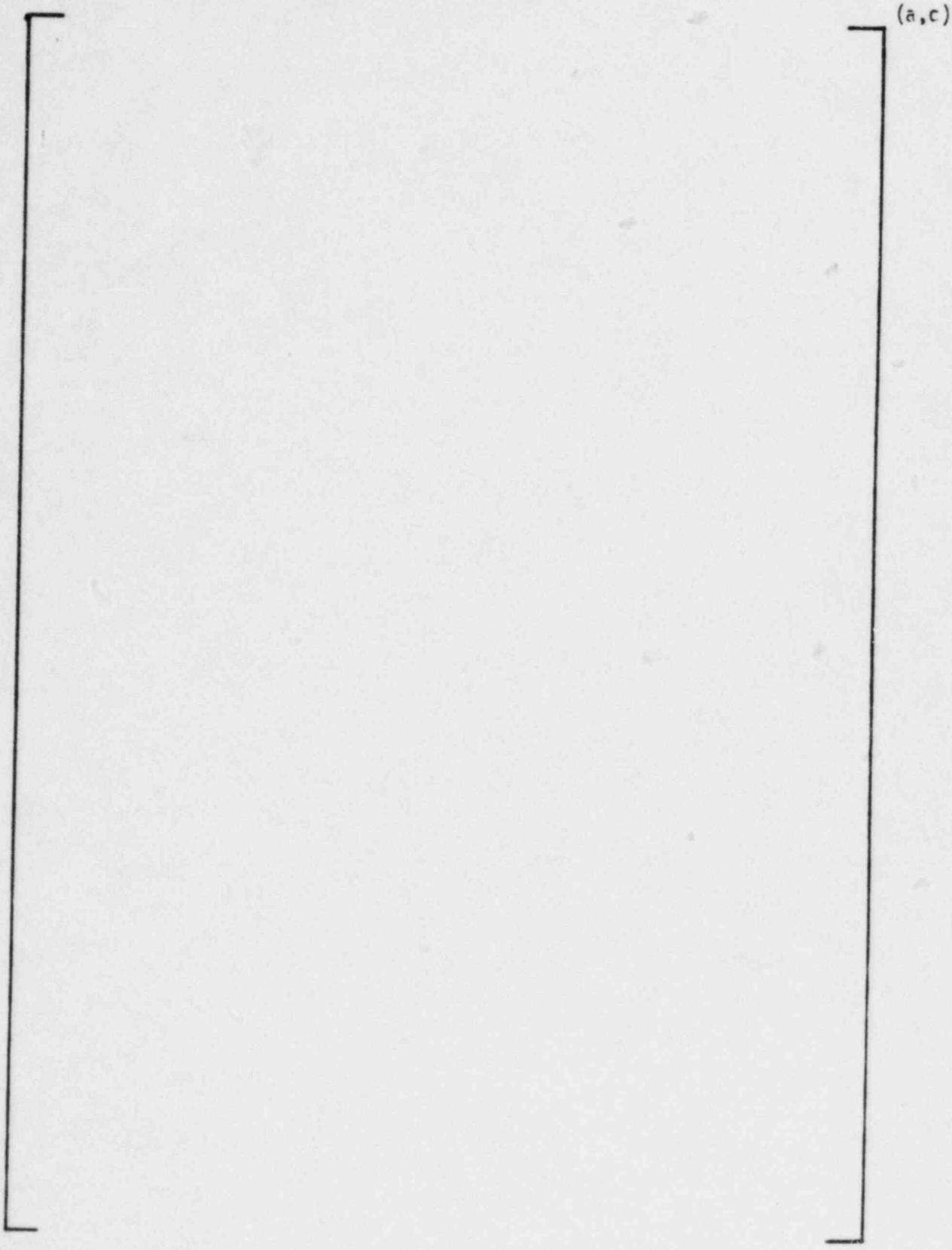


FIGURE 7.6-1 TYPICAL I&C ELECTRICAL POWER DISTRIBUTION SYSTEM - 118 VAC

(a,c)

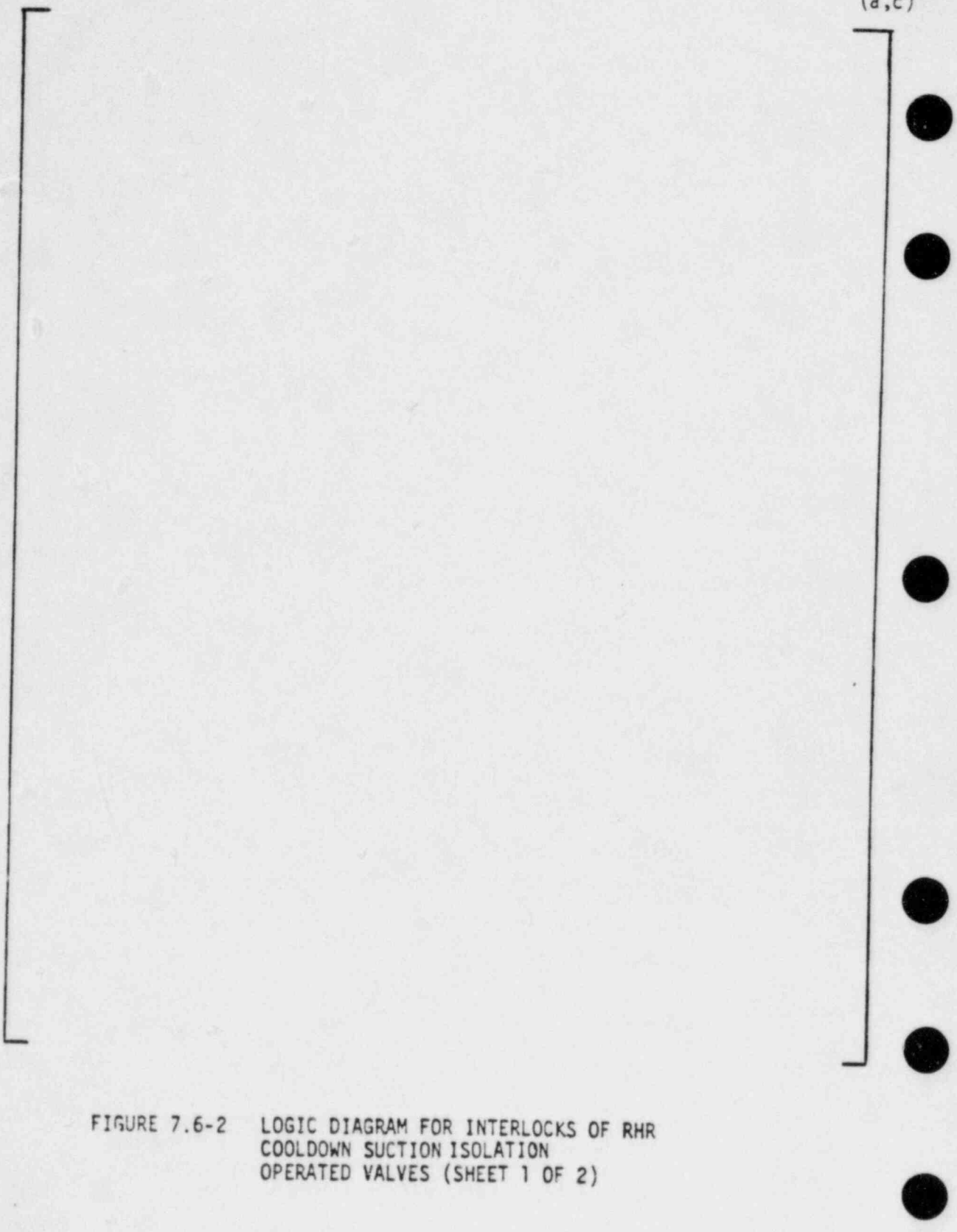


FIGURE 7.6-2 LOGIC DIAGRAM FOR INTERLOCKS OF RHR COOLDOWN SUCTION ISOLATION OPERATED VALVES (SHEET 1 OF 2)

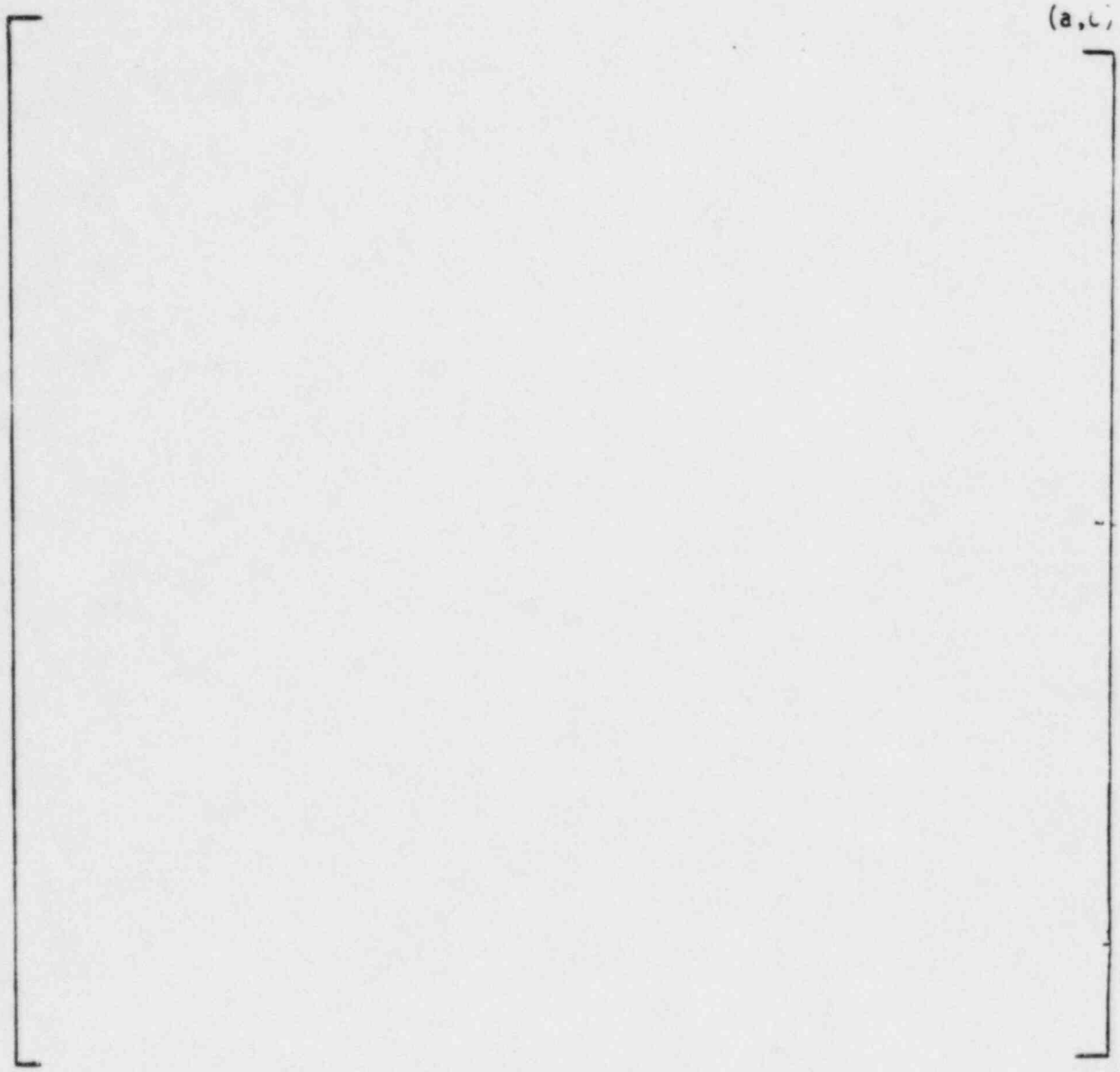


FIGURE 7.6-2 LOGIC DIAGRAMS FOR INTERLOCKS OF RHR COOLDOWN SUCTION ISOLATION MOTOR OPERATED VALVES (SHEET 2 OF 2)

(a,c)

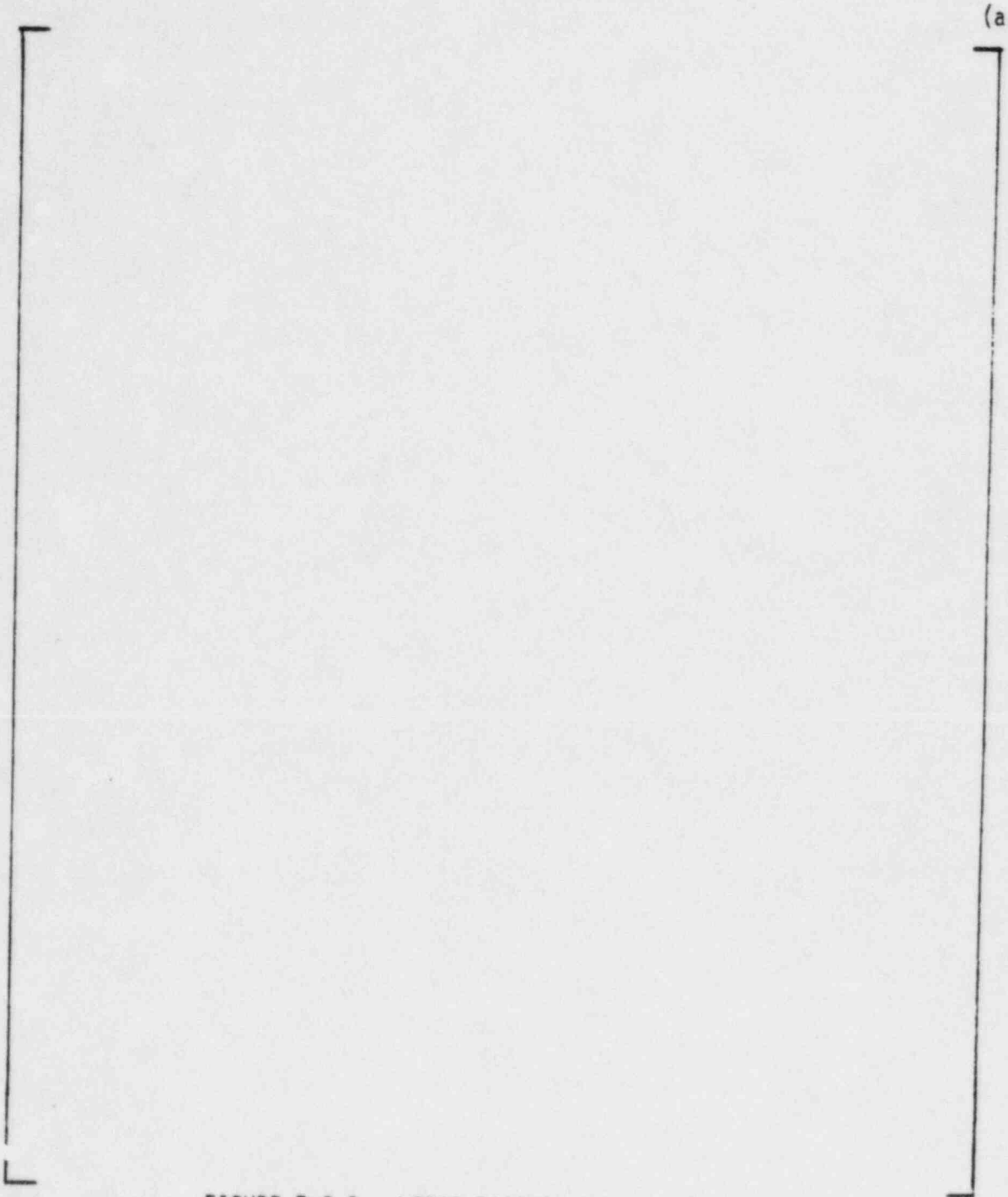


FIGURE 7.6-3 LOGIC DIAGRAM FOR MOTOR OPERATED VALVE INTERLOCKS FOR ACCUMULATOR AND CORE REFLOOD TANK DISCHARGE ISOLATION VALVES

(a,c)

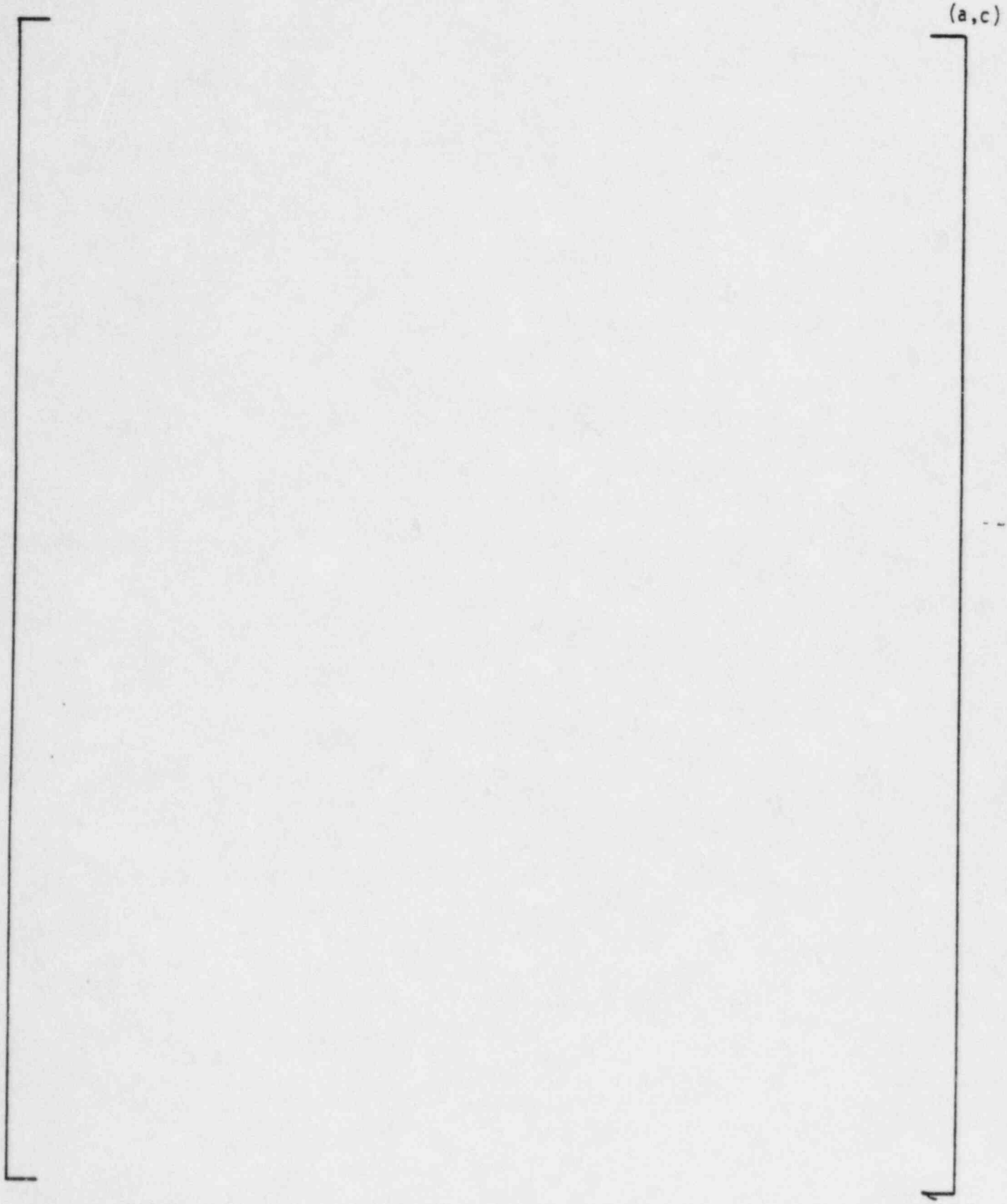


FIGURE 7.6-4 LOGIC DIAGRAM FOR CRITICAL FUNCTION VALVE ALARM

7.7 CONTROL AND INSTRUMENTATION SYSTEMS

The purpose of the WAPWR control systems is to establish and maintain the plant (especially the nuclear steam supply system) operating conditions within prescribed limits. A well designed control system can improve plant safety by minimizing the number of situations for which some protective response must be initiated. A well designed system should also relieve the operator from routine tasks, so that he can maintain a more global perspective of the plant conditions.

The WAPWR control systems are referred to as integrated, because they share a commonality of hardware design and implementation philosophy. They will also be designed to be functionally integrated so as to provide enhanced responsiveness during plant transients. The term integrated should not be construed as having all the control functions performed in a single piece of hardware. In fact, specific design requirements are imposed which limit the impact of individual equipment failures.

The NSSS control systems regulate the operating conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

- o RCS Temperature

  The NSSS control systems function to maintain the reactor coolant system (RCS) temperature at or near a programmed value which may be a function of plant load or other operating conditions. Steam conditions for the turbine will depend strongly on the temperature maintained in the reactor coolant. RCS temperature may also be used as a mechanism for maintaining core reactivity.

- Nuclear Power Distribution

  Operating limits include the distribution of nuclear energy production within the core as well as its average value. The axial distribution of the nuclear power will be maintained within prescribed limits.

- RCS Pressure

  The RCS coolant must be pressurized to prevent significant boiling at the high operating temperatures required for good plant performance. This pressure must be controlled within limits which prevent reductions which would expose the fuel to possible DNB or from increases which would challenge the RCS design pressure.

- Pressurizer Water Level

  In order to provide a sufficient buffer for plant transients, the RCS pressurizer contains a prescribed volume of water and steam which depends on plant load and operating temperature.

- Steam Generator Water Level

  The steam generator water level must be maintained within limits which are set to assure adequate energy removal capability and to avoid moisture carryover.

- Steam Dump

  For very fast and large transients such as load rejections, an additional thermal load (steam dump) must function until nuclear power can be reduced. This steam dump is also used to maintain hot no load or hot low load conditions prior to turbine loading. It also provides a means for plant cooldown.

7.7.1 Description

The plant control and instrumentation systems described in this section will perform the following functions:

1. Automatic Power Control System (APCS)

   The APCS will coordinate the responses of the various reactivity control mechanisms so as to provide an enhanced reactor performance. The APCS will enable daily load follow operation with a minimum of manual control required by the operator. Load regulation and frequency control will be compatible with the APCS operation.

2. Rod Control System

   The Rod Control System is designed to maintain nuclear power and reactor coolant temperature, without challenges to the protection systems, during normal operating transients.

3. Boron Control System

   The boron control system will change the reactor coolant boron concentration as directed by the APCS in such a manner that the axial nuclear power distribution and other operating conditions are maintained.

4. Pressurizer Pressure Control

   The pressurizer pressure control system will act to maintain or restore the pressurizer pressure to the nominal operating value following normal operating transients. The control system will react to avoid any challenges to the protection systems during these operatin transients. The necessity for pressure relief via the power operated relief valves (PORVs) should be minimized.

5. Pressurizer Water Level Control

The pressurizer water level control system will establish and maintain or restore pressurizer water level to its required value. The required water level will be programmed as a function of reactor coolant system temperature and power generation to minimize charging and letdown requirements. No challenges to the protection system are to result from normal operational transients.

6. Steam Generator Water Level Control System

The purpose of the steam generator water level control system is to maintain the steam generator water level at a predetermined setpoint during steady state operation, and to maintain the water level within operating limits during normal transient operation. The water level control system will act to restore normal water level following a unit trip. The various modes of feedwater addition will be automated to require a minimum of operator involvement.

7. Steam Dump Control

The steam dump control system will react to prevent a reactor trip following a sudden loss of electrical load. The steam dump control system will also ensure that stored energy and residual heat are removed following a reactor trip so that the plant can be brought to equilibrium no-load conditions without actuation of the steam generator safety valves. The steam dump control system is also to provide for maintaining the plant at no-load or low load conditions and should facilitate a controlled cooldown of the plant.

7.7.1.1 Automatic Power Control System (APCS)

The APCS is a direct extension of the core reactivity control systems. It is intended to provide an integrated control of these systems such that the core

axial power distribution and other parameters are maintained in a automatic and prescribed manner. Rather than controlling just a single mechanism such as boron concentration, or control rod position, this control system will provide a integrated response to reactivity control.

The APCS is designed to relieve the operator from the difficult and time consuming duty of manipulating the reactivity control mechanisms during periods of time in which the power level or power distribution is changing. The APCS should be capable of providing control in the load range from 15% to 100% power. The APCS will allow daily load follow operation on a 14-1-8-1 hr. cycle from 100-50% power subject only to core power distribution limits. The APCS will also facilitate concurrent load regulation and frequency control.

Each of the control systems with which the APCS interfaces must be capable of being operated independently. Although this mode of operation is intended for those infrequent times that the APCS is not available.

The inputs to the APCS will consist of those parameters necessary to describe the current state of the NSSS:

- Current power level
- Power distribution (axial offset)
- Cold leg temperature (T_{COLD})
- Boron concentration
- Control rod position
- Gray rod position
- Water displacer rod positions

The operating constraints will include such items as control rod insertion and withdrawal limits, the range of allowable operating temperatures, and the range of allowable power distributions.

Power distribution is characterized in terms of an axial offset (A.O.) parameter which is obtained from the power range multi-section excore neutron detectors. Axial offset is computed as:

$$A.O. = \frac{\text{power in top of core - power in bottom of core}}{\text{power in top of core + power in bottom of core}}$$

As in the Model 414 reactor, the thermodynamic state will be measured and controlled in terms of the cold leg temperature, T_{cold}. Since the operating power level is also available from compensated N-16 measurements in the hot leg, the temperature rise across the reactor can be inferred. Control rod and gray rod positions will be supplied to the APCS via the appropriate position monitoring system.

The APCS will enable the NSSS to follow turbine load changes without requiring operator actions. This capability will make possible the use of remote dispatching, i.e., setting the turbine load from the economic dispatch center rather than locally at the plant site. The use of remote dispatching will allow the unit to be fully integrated into the economic dispatch and load follow requirements of the utility, and help to maintain grid fault security. The APCS will provide, as an optional output, data on how large a power change the plant can safely accept while maintaining automatic control, and how quickly it can make the change. The operator will be provided with manual overrides to restrict or prohibit altogether the remote dispatching.

7.7.1.2 Rod Control System

A PWR is inherently stable due to negative temperature and power reactivity feedback effects. However, in order to maintain the temperature within the desired control band, neutron absorbing control rods are inserted into the core. By adjusting control rod insertion in conjunction with other reactivity control mechanisms such as soluble boron concentration or gray rod position, additional operating goals can be achieved (e.g., minimizing axial power peaking, maximizing spinning reserve capability, etc.).

Automatic rod control will be available over the entire range of power operation, including power escalation for turbine synchronization and loading. Stable and accurate control of RCS temperature is provided within an

established control deadband. Deadband for temperature control is provided to eliminate unnecessary rod motion and to allow greater flexibility of reactivity control through variations in moderator temperature. The rod control system must be responsive to plant transients to maximize the margins to plant safety actuation setpoints, and yet must not result in excessive rod motion for automatic frequency control and load regulation operation.

In order to allow the elimination of the RCS hot leg narrow range temperature measurement and the associated bypass line piping, the control system will be designed to operate on the basis of the cold leg temperature. Control performance with this modification will be designed to be at least comparable to previous performance based on control of average core temperature.

Rod control will be provided by two distinct, but integrated, control systems. The first of these systems will be designed to provide rod control at low power levels and is shown in Figure 7.7-1. This system will be designed to provide direct control of nuclear power. In order to assure that RCS temperature is maintained at the proper value, this operation must be applied in conjunction with automatic steam pressure control by the steam dump control system. The low power rod control system will receive a nuclear power demand signal in terms of the power which is to be attained, and the rate at which power is to be increased/decreased. Control logic will be supplied to coordinate this controller with the control for the high power range and to prevent automatic low power rod control if automatic steam dump pressure control is unavailable. Control action will be taken based on the difference between demanded nuclear power and measured nuclear power.

The rod control in the high power range (15-100% power) is shown in Figure 7.7-2. The purpose of this control system is to maintain the RCS coolant temperature within a specified range (deadband) of a setpoint value which is a function of power level and possibly other operating parameters. Reactor coolant system temperature is established by measurement of the cold leg temperature, since an accurate measurement of this value is possible without complex and costly sampling scoops and bypass piping. The reference T_{cold} is a programmed function of turbine power. To provide responsive transient

performance, control action will also be provided based on the difference between power extracted by the turbine and that supplied by the reactor. The power difference is passed through a high pass filter to eliminate any long term offsets due to errors in measurement of nuclear or turbine power.

Both rod control systems generate direction and speed demand signals for the control rods only. The direction of rod movement is based on the sign of the control error, and the speed demand is based on its magnitude. The rod speed signal will vary between a minimum speed of 3.75 inches/minute and a maximum speed of 45 inches/minute (60 to 72 steps/minute). Manual control will be provided which will move the control rods at a prescribed fixed speed.

Each control bank will be subdivided into two groups to obtain smaller incremental reactivity changes/step. All rod control cluster assemblies in a group will be electrically parallel to move simultaneously. There will be individual position indication for each rod cluster control assembly.

A summary of the rod cluster control assembly sequencing characteristics is given below:

1. Two groups within the same bank will be stepped such that the relative position of the group will not differ by more than one step.

2. The control banks will be programmed such that withdrawal of the banks will be sequenced in the following order; control bank A, control bank B, control bank C and control bank D. The programmed insertion sequence will be the opposite of the withdrawal sequence, i.e., the last control bank withdrawn (bank D) with be the first control bank inserted.

3. The control bank withdrawals will be programmed such that when the first bank has reached a preset position, the second bank will begin to move out simultaneously with the first bank. When the first bank has reached the top of the core, it will stop, while the second bank will continue to move toward its fully withdrawn position. When the second bank has reached a

preset position, the third bank will begin to move out. This withdrawal sequence will continue until the unit has reached the desired power level. The control bank insertion sequence will be the opposite.

4. Overlap between successive control banks will be adjustable between 0 to 80 percent with an accuracy of ±1 step.

5. Rod speed for the control banks will be capable of being controlled between a minimum of 6 steps per minute and a maximum 72 steps per minute.

7.7.1.3 Control Rod Position Monitoring

1. Digital Rod Position

The digital rod position indication system will measure the actual position of each rod using a detector which will consist of discrete coils mounted concentric with the rod drive pressure housing. The coils will be located axially along the pressure housing and will magnetically sense the entry and presence of the rod drive shaft through its center line.

2. Demand Position System

The demand position system will count the pulses generated in the rod drive control system to provide a digital readout of the demanded bank position.

The demanded and measured rod position signals will be displayed on the control board. The plant computer will provide an audible alarm whenever an individual rod position signal has deviated from the other rods in the bank by a preset limit. The alarm will be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors.

Alarms will also be generated if any shutdown rod is detected to have left its fully withdrawn position, or if any control rod is detected at the bottom position except as part of the normal insertion sequence.

7.7.1.4 Control Rod Insertion and Withdrawal Limits

With the reactor critical, the normal indication of reactivity status in the core will be the position of the control bank in relation to reactor power (as indicated by the N-16 power monitors). The N-16 power signal will be used to calculate insertion limits for the control banks. Two alarms will be provided for each control bank.

1. A "low" alarm will alert the operator of an approach to the rod insertion limits which will require boron addition by following normal procedures with the chemical and volume control system, or gray rod insertion.

2. A "low-low" alarm will alert the operator to take immediate action to add boron to the reactor coolant system by any one of several alternate methods, or to insert gray rods.

The purpose of the control bank rod insertion alarms is to give warning to the operator of excessive rod insertion. The insertion limit will maintain sufficient core reactivity shutdown margin following reactor trip and will provide a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection. Insertion limits will ensure that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip will increase with increasing power, the allowable rod insertion limits must be decreased (the rods must be withdrawn further) with increasing power. The insertion limit will be calculated from the reactor power as measured by the N-16 power monitor according to the following equation:

$$Z_{LL} = A \cdot (Q_{N-16})_{auct} + B$$

where

Z_{LL}	=	Maximum permissible insertion limit for the affected control bank
$(Q_{N-16})_{auct}$	=	Highest reactor power signal of all N-16 power monitors
A,B	=	Constants chosen to maintain $Z_{LL} \geq$ the actual limit based on physics calculations

The control rod bank demand position (Z) will be compared to Z_{LL} as follows:

If $Z - Z_{LL} \leq D$ a low alarm will be actuated
If $Z - Z_{LL} \leq E$ a low-low alarm will be actuated

7.7.1.5 Control Rod Stops and Turbine Runbacks

Rod stops will be provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Automatic turbine load runback will be initiated by an approach to DNB or high kw/ft conditions. This will prevent high power operation that might lead to an undesirable condition. However, the limit, if reached, will be protected by reactor trip.

In addition to the turbine runbacks, the turbine load reference will be frozen during ramp load increases if the reactor coolant cold leg temperature is below the programmed reference by an excessive amount. The ramp load increase will automatically resume when the excessive temperature deviation no longer exists.

7.7.1.6 Boron Control System

Soluble boron concentration represents one of the mechanisms for maintaining core reactivity. It is used in conjunction with additional reactivity control

mechanisms such as control rods, and moderator temperature to meet reactor operating goals (e.g., axial offset, spinning reserve, water processing requirements) as directed by the APCS. The boron recycle system (BRS) will provide either highly borated or demineralized water for the RCS makeup depending on whether boration or dilution is required.

Under normal operation, the boron control system will respond to changes in Boron concentration demand as dictated by the APCS. The boron control system in conjunction with the BRS must be capable of changing the RCS boron concentration as required to follow the reference 14-1-8-1, 100%-50%-100% load follow cycle, when RCS boron concentration is sufficiently high.

7.7.1.7 Gray Rod Control System

In addition to high worth control rods, the WAPWR will accommodate relatively low worth gray rods. The gray rods assemblies will be either fully inserted or fully withdrawn. They will be operated in conjunction with the control rods, and other mechanisms for controlling reactivity, in such a manner as to meet overall plant operating objectives.

Automatic control of the gray rods will be provided by the APCS. The APCS will determine when gray rod insertion or withdrawal will be advantageous in meeting the plant performance requirements. Only one group of gray rod assemblies will be allowed to be in motion at any particular time. The gray rod control system will compare the actual and demanded positions of the gray rods and will alert the operator if any discrepancies occur. The gray rods will be inserted and withdrawn in a pre-selected sequence where the sequence for withdrawal is opposite that of insertion. Gray rods will be utilized for power distribution control during those periods of reactor operation with low boron concentration. They also serve as a backup to the BRS during operation with high boron concentration.

7.7.1.8 Pressurizer Pressure Control System

The NSSS pressure must be closely regulated during operation to prevent pressure from increasing to the point where a safeguards actuation is required to prevent overstressing the pressure boundary; or from decreasing to a condition where safeguards actuation is required to prevent the possibility of DNB. Fine control of pressure to the desired setpoint is accomplished by regulating the output of a group of variable heaters. Large decreases in pressure are accommodated by actuation of on/off heaters and by the inherent flashing from the water mass in the pressurizer which is at saturation. Large pressure increases are controlled by actuating pressurizer spray to condense steam.

Pressurizer pressure control must be designed to provide stable and accurate control of pressure to its predetermined setpoint. Automatic pressure control is to be available from the point at which nominal pressure is established in the startup cycle to 100% power. During steady state operating conditions, the heater output must be regulated to make up for pressurizer heat loss and a small continuous pressurizer spray. During normal transient operation, the pressure must be regulated to provide adequate margin to safety systems actuation or reactor trip. Pressurizer PORV operation should not be required for all normal transients including full load rejection. The control system is designed so as to minimize equipment duty (e.g., spray nozzle thermal cycling due to spray actuation) due to automatic frequency control operation.

The design for control of pressurizer pressure is shown in Figures 7.7-3 and 7.7-4. Because of the different dynamic characteristics of the heaters and spray; separate control algorithms are provided for each.

Small and/or slowly varying changes in pressure will be regulated by modulation of the proportional heaters. Reset (integral) action is included to maintain pressure at its setpoint. Decreases in pressure larger than that which can be accommodated by the proportional heaters will result in the actuation of the backup heaters. The backup heaters will be deactivated when

the proportional heaters alone are capable of restoring pressure. Large increases in the pressurizer water level will also result in activation of the backup heaters. The purpose of this action is to avoid the accumulation of subcooled fluid in the pressurizer, so that flashing of the pressurizer fluid will act to limit the pressure decrease on any subsequent outsurge.

Pressure increases too large and fast to be handled by reducing the proportional heater output will result in spray actuation. Spray action will continue until pressure has decreased to the point at which the proportional heaters can again regulate pressure. The control system is designed so that spray is not actuated unless it is required, in order to minimize the spray nozzle duty. The system should not keep spray on any longer than is required so that any subsequent depressurization is not made worse. For normal transients including a full load rejection, this control system must act promptly to prevent opening of the PORVs.

7.7.1.9 Pressurizer Level Control System

The pressurizer water inventory or level control is designed to provide a reservoir for the RCS inventory changes which occur due to changes in RCS density. As the RCS temperature is increased from hot zero load to full load values, the RCS fluid expands. To minimize the duty on the water handling systems, the pressurizer level is programmed to absorb this change. The pressurizer level control regulates charging flow to the RCS to compensate for any differences between letdown and charging flow so as to maintain the programmed level.

Pressurizer level control is designed to provide stable and accurate control of pressurizer level to its programmed value as derived from the current operating parameters. Automatic level control is supplied from the point in the startup cycle where the hot zero load Level is established through 100% power. In addition to power, the reference water level is also compensated for changes in operating temperature that result from such things as rod control deadband, or reduced T_{avg} return to power operation.

The design for the pressurizer level control system is shown in Figure 7.7-5. The reference level for the pressurizer is characterized in terms of N-16 derived power (Q_{N-16}), and RCS cold leg temperature (T_{cold}). During startup, the reference water level is held at the hot zero power value. The error between the measured level and the computed reference level is used in the control algorithm to provide a modulating signal for charging flow. The level control system must be responsive enough to accommodate the RCS inventory shrink and swell for the maximum heatup and cooldown during startup and shutdown.

7.7.1.10 Steam Generator Water Level Control System

Steam generator water level control maintains a reservoir or heat sink for the power generated by the reactor. Safety and/or operational concerns establish a range within which water level must be maintained. Steam generator water level is controlled by adjusting the feedwater flow in relation to the steam flow. Control of level during a disturbance is complicated by a phenomenon referred to as "shrink and swell". A change in steam flow, with feedwater flow held constant, will give rise to a short term level effect which is opposite that of the long term effect of the flow change. This shrink or swell arises from a hydraulic force and mass redistribution within the steam generator downcomer and the tube bundle.

The design of the steam generator water level control system must provide for stable and accurate control of water level over a wide range of operating conditions. Automatic water level control is to be available as soon as narrow range water level control is called for in the startup sequence. Automatic water level control must remain available through 100% power with a minimum of requirements for operator input. Water level control is to encompass initial feeding of the steam generator using the startup feedwater system, as well as feeding of the steam generator by the main feedwater system using the main and bypass feedwater valves. Continuous feedwater control is to be provided between these modes.

The feedwater control system is to be responsive to changes in plant parameters to minimize the likelihood of normal transients producing undesirable operating conditions. The control is compensated for the effects of shrink and swell on water level to provide improved control action.

The three distinct, but integrated, modes of feedwater control are indicated in Figures 7.7-6 to 7.7-8. Main feedwater valve control will employ measurement of steam flow and feedwater flow since large and rapid changes in steam flow are likely to occur during high power operation. Steam generator level measurement will be used with integral action to insure that the reference level is maintained even in the event of steam and feedwater flow measurement errors. Steam pressure changes are included in the control algorithm to provide improved transient responsiveness to shrink and swell. The control logic signals are used to effect the transition between control modes (i.e., main, bypass, startup).

The control of the bypass feedwater valve will be utilized for low power operation. Steam and feedwater flow measurements are not useful for this mode, because they tend to be noisy and inaccurate at low power. Reset action will be provided on water level to maintain the required setpoint. Control logic signals will be used to direct a smooth transition between control modes. Steam dump in the pressure control mode should be used in conjunction with low power feedwater control to minimize the impact of any operating disturbances.

Startup feedwater control will be used to maintain the steam generator water level during the steaming phases of plant heatup and cooldown. This control will be based on maintaining water level at an adjustable setpoint.

7.7.1.11 Steam Dump Control System

Steam dump provides an auxiliary heat removal capability from the NSSS. Steam dump is utilized when there is a sudden decrease in the power being supplied to the turbine, and when that decrease is larger than that which can be

accommodated by the other NSSS control systems. Steam dump is also used to provide a regulated heat removal during startup and cooldown and when maintaining the plant in a hot standby condition. This steam flow is taken directly from the steam header to the turbine condenser (or to atmosphere if so designed).

The steam dump control system must be able to very rapidly detect any large mismatch between power delivered to the turbine and power produced by the reactor, and initiate the proper steam dump to prevent a reactor trip or safeguards initiation. Steam dump should, in conjunction with pressurizer pressure control, prevent actuation of the pressurizer PORVs following a full load rejection.

The steam dump control system must be able to regulate steam flow in order to maintain a reference plant condition (steam pressure) during low power and standby operating conditions. In addition, the steam dump control system should be able to gradually reduce the steam generator saturation temperature to provide a programmed plant cooldown rate as part of the plant cooldown procedure.

The steam dump control system will be composed of two control systems. The first of these is shown in Figure 7.7-9. This is a power mismatch control system which is designed to detect substantial primary/secondary load imbalances due to a load rejection or trip. The controller is designed to provide trip open logic to the appropriate steam dump valves to compensate for this power difference. Compensated turbine power (turbine first stage pressure) and nuclear (N-16) power are used to provide the power mismatch signal. The error between the reference T_{cold} and measured T_{cold} is used to return the plant to the proper operating point.

The second control system, shown in Figure 7.7-10, is a steam pressure controller. This control system is applied when the NSSS is being maintained in a hot, low power condition prior to turbine loading. It is also used to provide a controlled cooldown, the controller will translate the decreasing

temperature demand to a steam pressure setpoint using saturated water property tables. After compensation, this signal will be used to provide the pressure control setpoint.

Interlocks are provided to minimize the possibility of inadvertent or unwarranted operation of the steam dump valves.

7.7.1.12 Signal Selector

The integrated control system for the WAPWR will derive certain of its control inputs from signals which are also utilized in the integrated protection system. A number of advantages accrue from this design philosophy:

i) The NSSS will be controlled from the same measurements with which it is protected, thereby assuring the control system will function to maintain margins between operating conditions and safety limits, and reduce the likelihood of spurious trips.

ii) Reducing the number of redundant measurements for any single process variable reduces the overall plant complexity at critical pressure boundary penetrations. This leads to a reduction is separation requirements within the containment as well as to a decrease in plant cost and maintenance requirements.

In order to obtain these advantages, certain measures must be taken to ensure the independence of the protection and control systems. The criteria for these measures are contained in the Standard IEEE-279-1971 (specifically Section 4.7). In addition to specifying that isolation devices must be provided to guard the protection system against possible electrical faults in the control system, this standard contains the following paragraphs which describe the functional independence that must exist for control and protection system actions;

"4.7.3 Single Random Failure. Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.

Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action for the bypassed channel."

In designs previous to the Model 414 Westinghouse met this criteria by providing a two-out-of-four (2/4) logic on protection variables which were also used for control, and reverting to one-out-of-three (1/3) protection by initiating a protection action(s) when that channel was taken out of service for test or maintenance. The disadvantage of this procedure was that while plants were operated in this 1/3 mode, they were exposed to the possibility that a single component failure or spurious signal could cause an inadvertent plant trip. The Westinghouse integrated protection system avoids this exposure by using a bypass logic during test and maintenance wherein the 2/4 logic reverts to 2/3 logic. This action necessitates a different mechanism for complying with the functional independence of control and protection as required by IEEE-279.

In the integrated control and protection system, functional independence of control and protection is obtained by providing a signal selection device for those signals which are also utilized in the protection system. The purpose of the signal selection device is to ensure that a failed signal which could result in failure of a protection channel will not result in a control action that could result in a plant condition requiring that protective action. The signal selection device will provide this capability by comparing all of the redundant signals and automatically eliminating an aberant signal from use in

the control system. This capability will exist for bypassed sensors or for sensors whose signals have diverted from the expected error tolerance.

The redundant signal selector subsystems receive identical data from the IPC's and perform identical selection algorithms. Both subsystems provide validated data to both redundant highways of the process bus. When there is no failure of either signal selector or either highway, the control subsystems are free to use data from either of the signal selectors via either of the highways. The redundancy serves two purposes; it protects against a failure disrupting the control system, and it provides the capability to remove one of the selectors from service for automatic testing while maintaining normal control using data from the other selector.

7.7.2 Analysis

The plant control systems will be designed to assure high reliability in any anticipated operational occurrence as well as to meet the following objectives which will be considered in the design process insofar as it is practical.

7.7.2.1 Performance

The control system shall be capable of manuevering the plant through the reference transients below. This maneuvering shall be done without the need for manual intervention and without violating plant protection or component limits, even with expected adverse instrument errors.

1) The capability to accept 10% step load decreases from any initial power level between 100% and 25% of full power, and step load increase of 10% from any initial power level between 15% and 90% of full power without reactor trip or steam dump actuation.

2) The capability to accept ramp load changes at 5% power per minute while operating in the range of 15% to 100% of full power without reactor trip or steam dump system actuation, subject to core power distribution limits.

3) The capability to accept the design full load rejection without reactor trip.

4) The capability to accept a turbine trip from full power operation with reactor trip but without actuation of any of the emergency safeguards systems.

5) The capability to follow the design basis net load follow pattern for 95% of the fuel cycle. The design basis load follow pattern is defined as the daily (24 hour period) cycle consisting of 14 hours operation at 100% power, followed by 1 hour linear ramp to 50% power, followed by 8 hours of operation at 50% power and then a 1 hour linear ramp back to 100% power. The ICS shall not be limiting in providing this capability.

6) The capability to return to at least 90% power from part power operation during the daily load follow cycle at a rate of 5% power per minute. The capability should be maintained for at least 85% of the fuel cycle length.

7) The capability to perform the design basis load regulation during steady state operation, or during the design basis load follow cycle. The design basis load regulation operation consists of unplanned, random load changes as often as every 3 minutes with a maximum value of $\pm$5% power from the long term average value.

8) Frequency control capability will be accommodated in the design of the ICS.

The control system shall permit manuevering the plant through the transients described above without actuation of any of the following:

1) Steam generator safety valves
2) Steam generator power operated relief valves
3) Pressurizer safety valves
4) Pressurizer power operated relief valves

In addition, these valves shall not be actuated during a normal plant trip.

7.7.2.2 Availability/Operability

The impact of the ICS on plant unavailability or inoperability should be minimized. The probability of a failure in the ICS resulting in plant unavailability during the eighteen (18) month fuel cycle should be reasonably small. The plant is defined to be unavailable if the failure(s) result in the plant being unable to achieve and/or maintain all steady state operating points within the warranted plant output.

Both automatic and manual control are provided for each of the control functions identified here. Manual control will override automatic control. While in the manual mode, the automatic system will track the manual system so that upon transfer to the automatic mode, the transfer will be bumpless. (A bumpless transfer is defined as a transfer between modes which maintains a continuous and smooth control signal). Sufficient information will be supplied to the operator to allow manual operation in a safe and efficient manner.

The ICS design should minimize the time required for startup following a reactor trip or load rejection, it should also minimize any requirements for setpoint changes due to changes in plant operations (e.g., water displacer rod withdrawal).

The ICS should reduce the requirements for complex operator actions during normal operation. Automatic control systems are used where practical.

7.7.2.3 Safety

No single failure at the component level within the ICS or its supporting systems, should be able to initiate an event so rapid that an operator could not reasonably intervene to prevent reactor trip or ESF actuation. This criterion is not meant to be applicable during maintenance of the ICS.

Consequences of credible failures in control system are to be no greater than the maximum failure of a single system.

The ICS design should reduce the number of possible interactions between control and protection systems which could lead to a degraded accident condition, and reduce the probability and consequence of failures in the control systems on plant safety and operability.

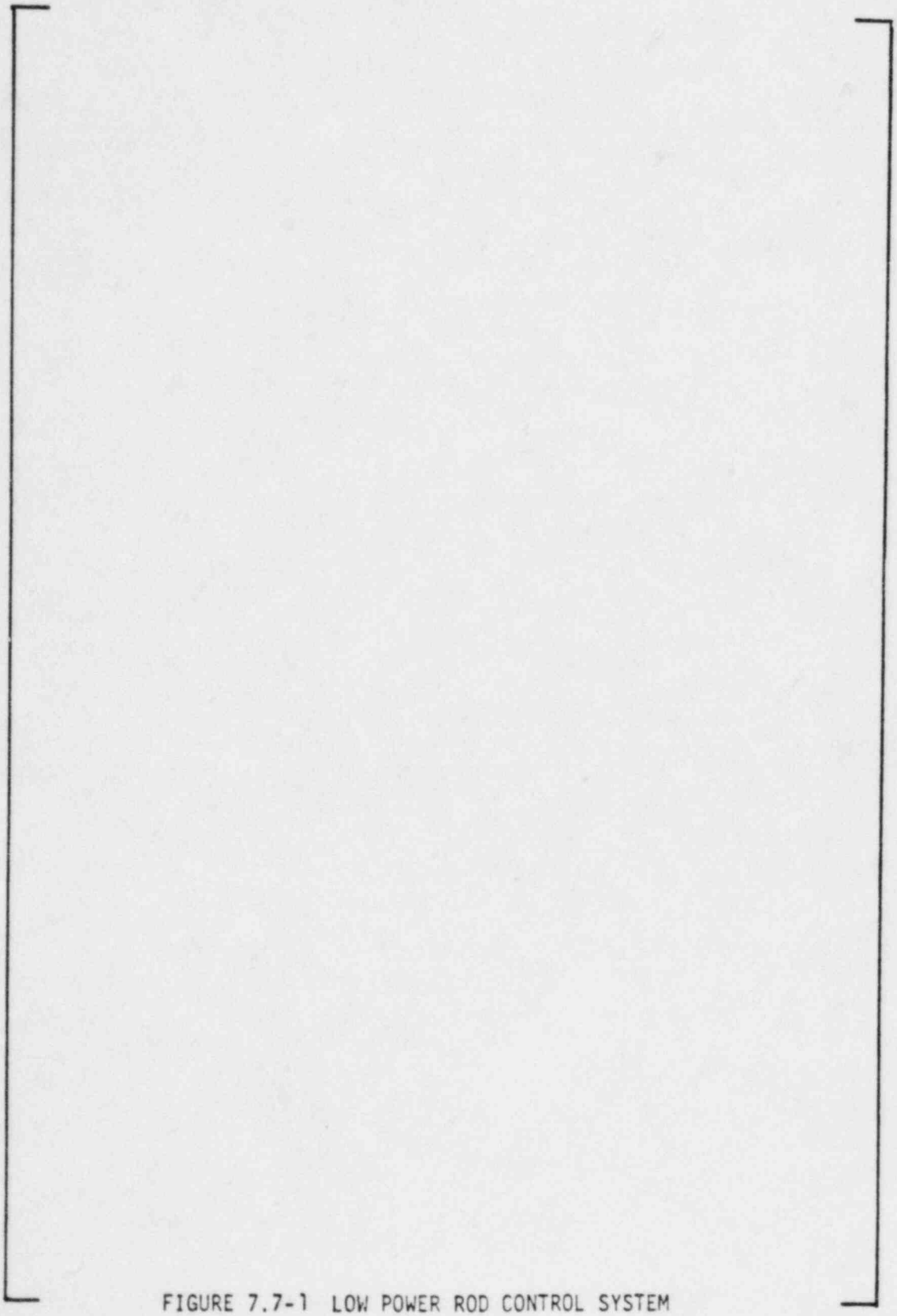


FIGURE 7.7-1 LOW POWER ROD CONTROL SYSTEM

(a,c)

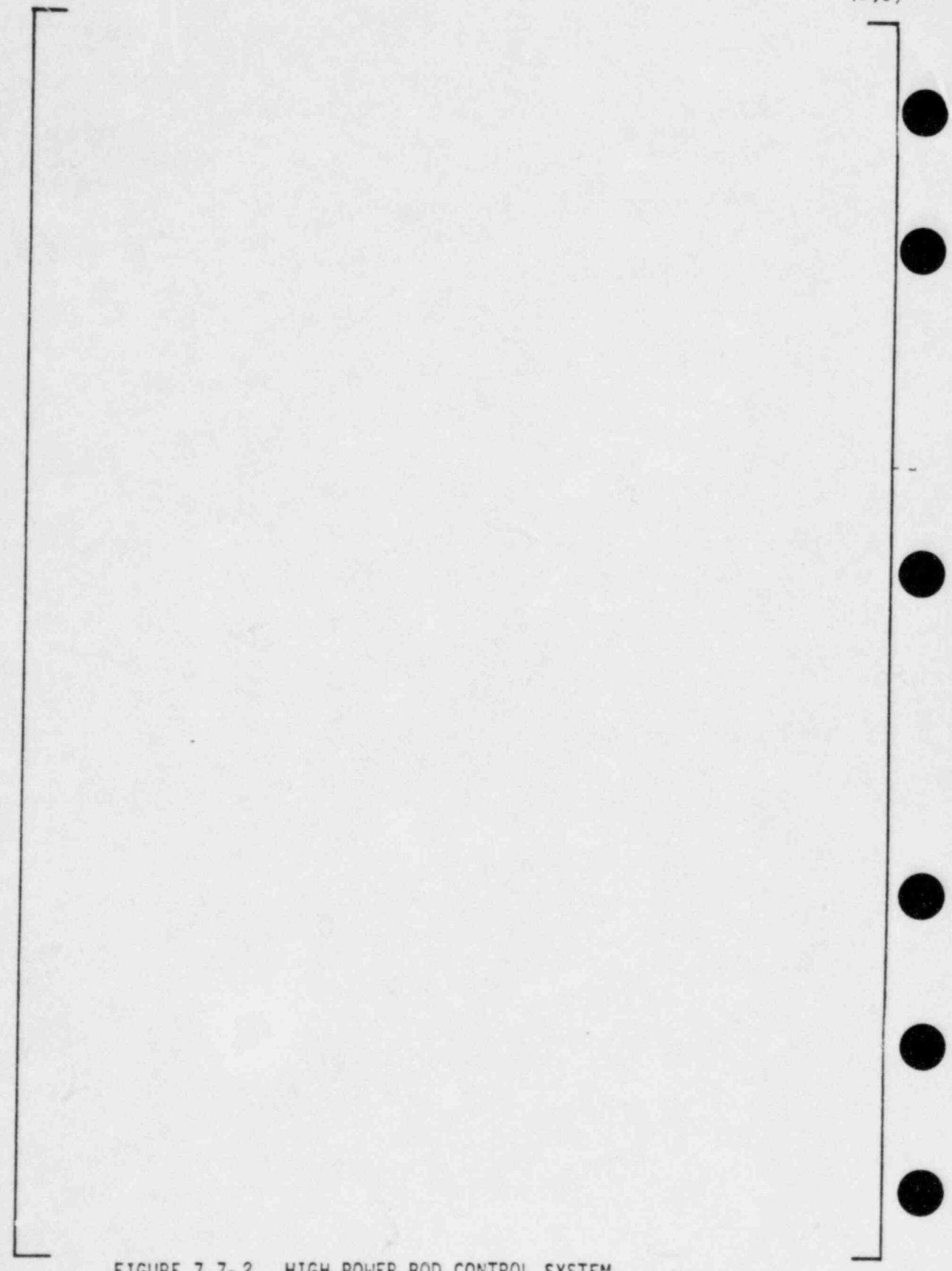


FIGURE 7.7-2 HIGH POWER ROD CONTROL SYSTEM

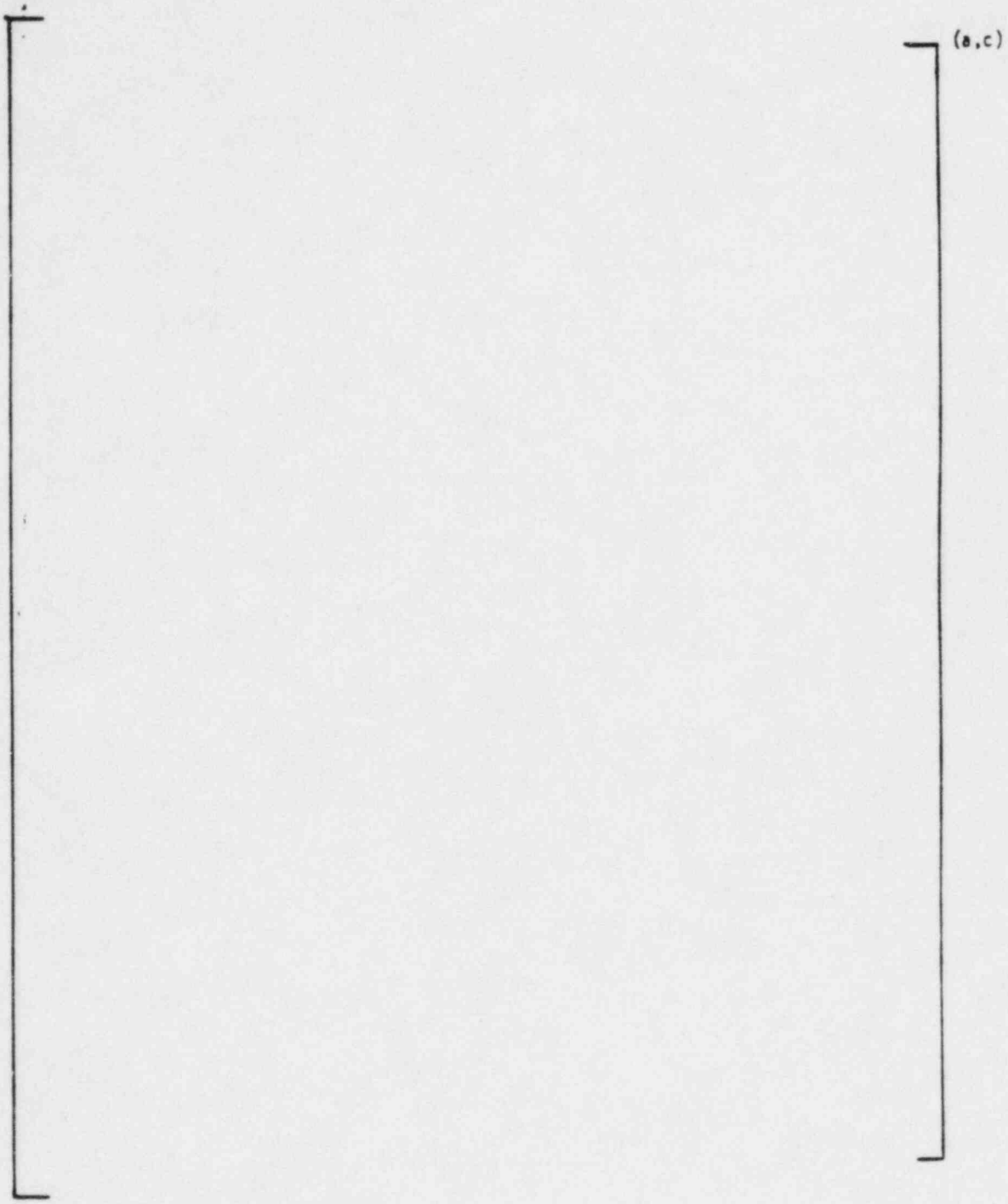


FIGURE 7.7-3 PRESSURIZER HEATER CONTROL

FIGURE 7.7-4 PRESSURIZER SPRAY CONTROL

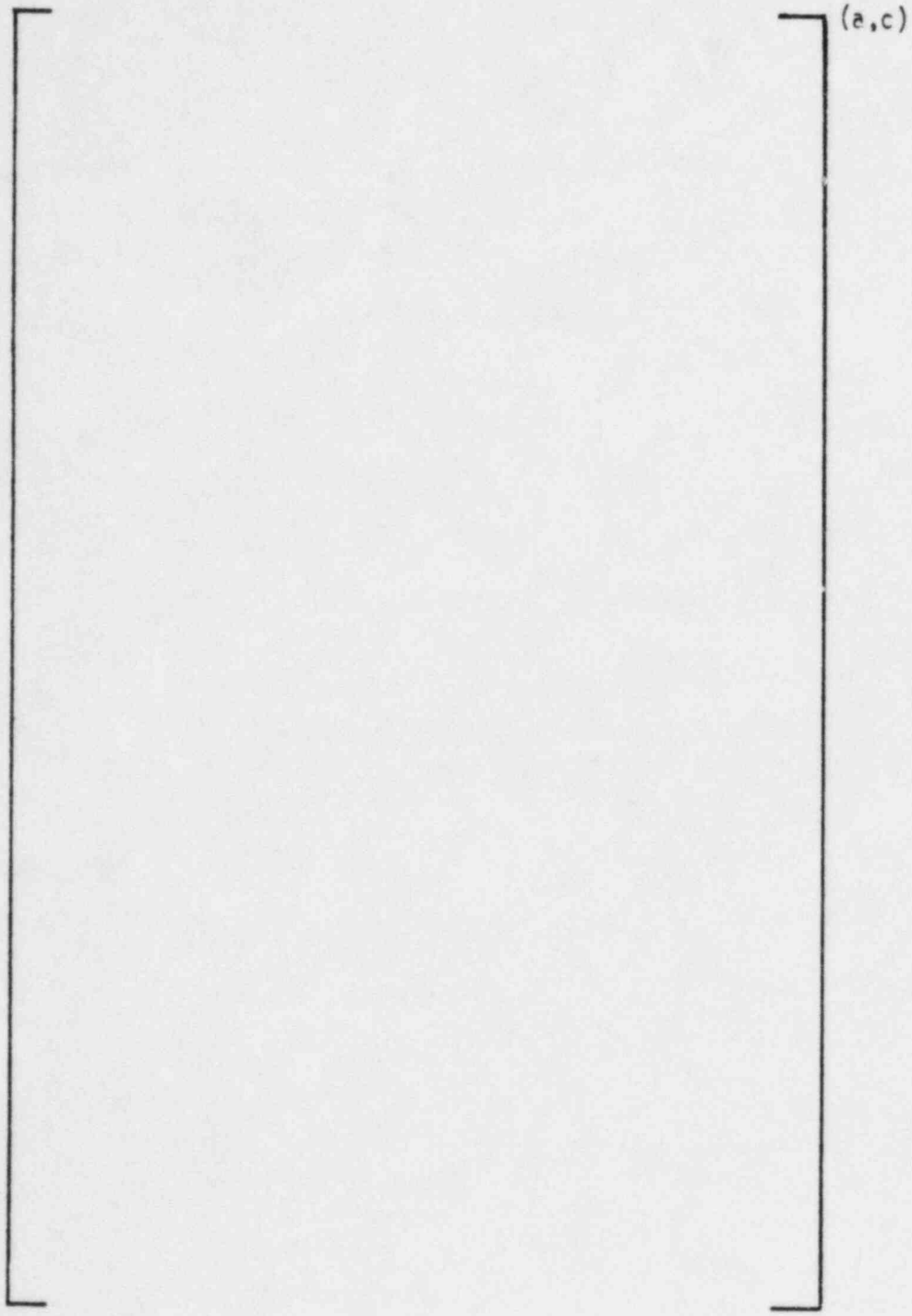


FIGURE 7.7-5 PRESSURIZER WATER LEVEL CONTROL

(a,c)

FIGURE 7.7-6 SG LEVEL CONTROL - NORMAL POWER

(a,c)

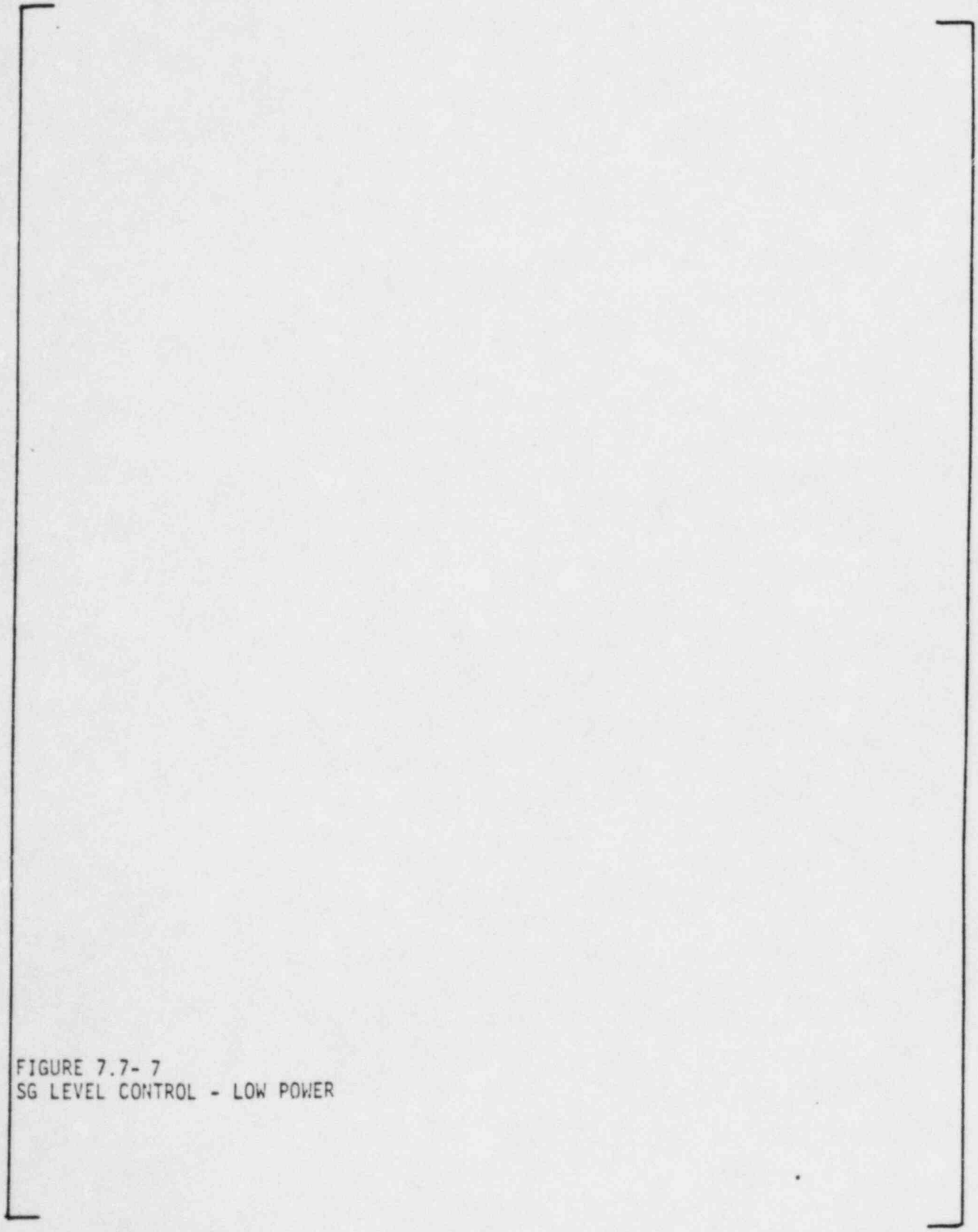


FIGURE 7.7- 7
SG LEVEL CONTROL - LOW POWER

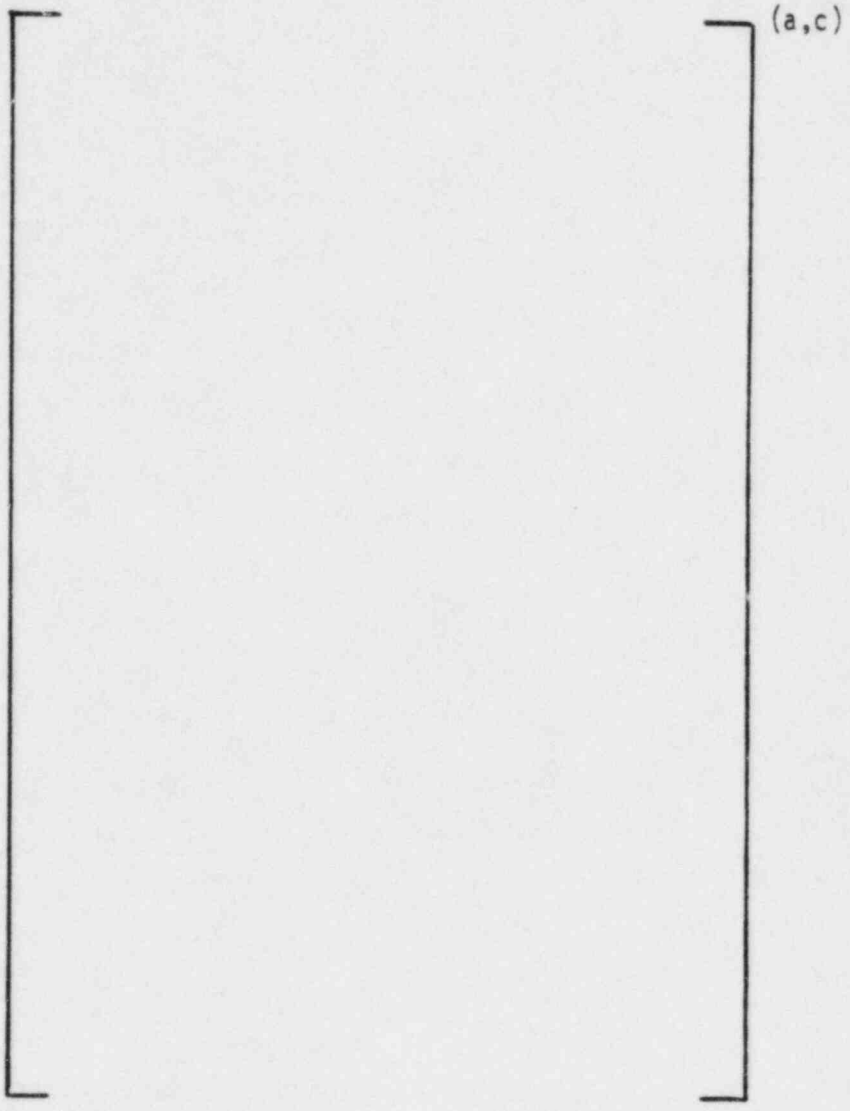


FIGURE 7.7-8 SG LEVEL CONTROL - STARTUP/SHUTDOWN

(a,c)

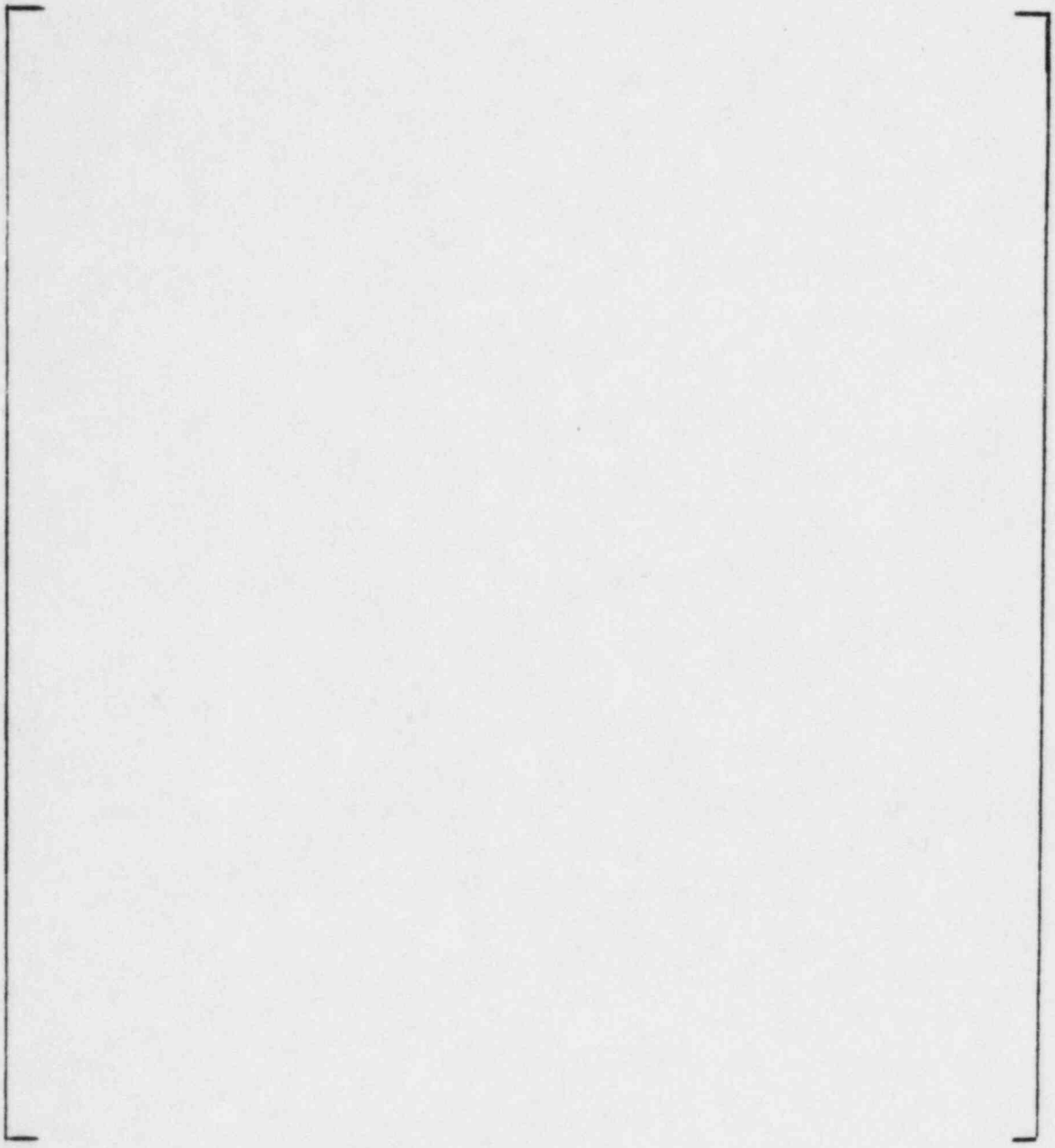


FIGURE 7.7-9 STEAM DUMP - POWER IMBALANCE CONTROL

(a,c)

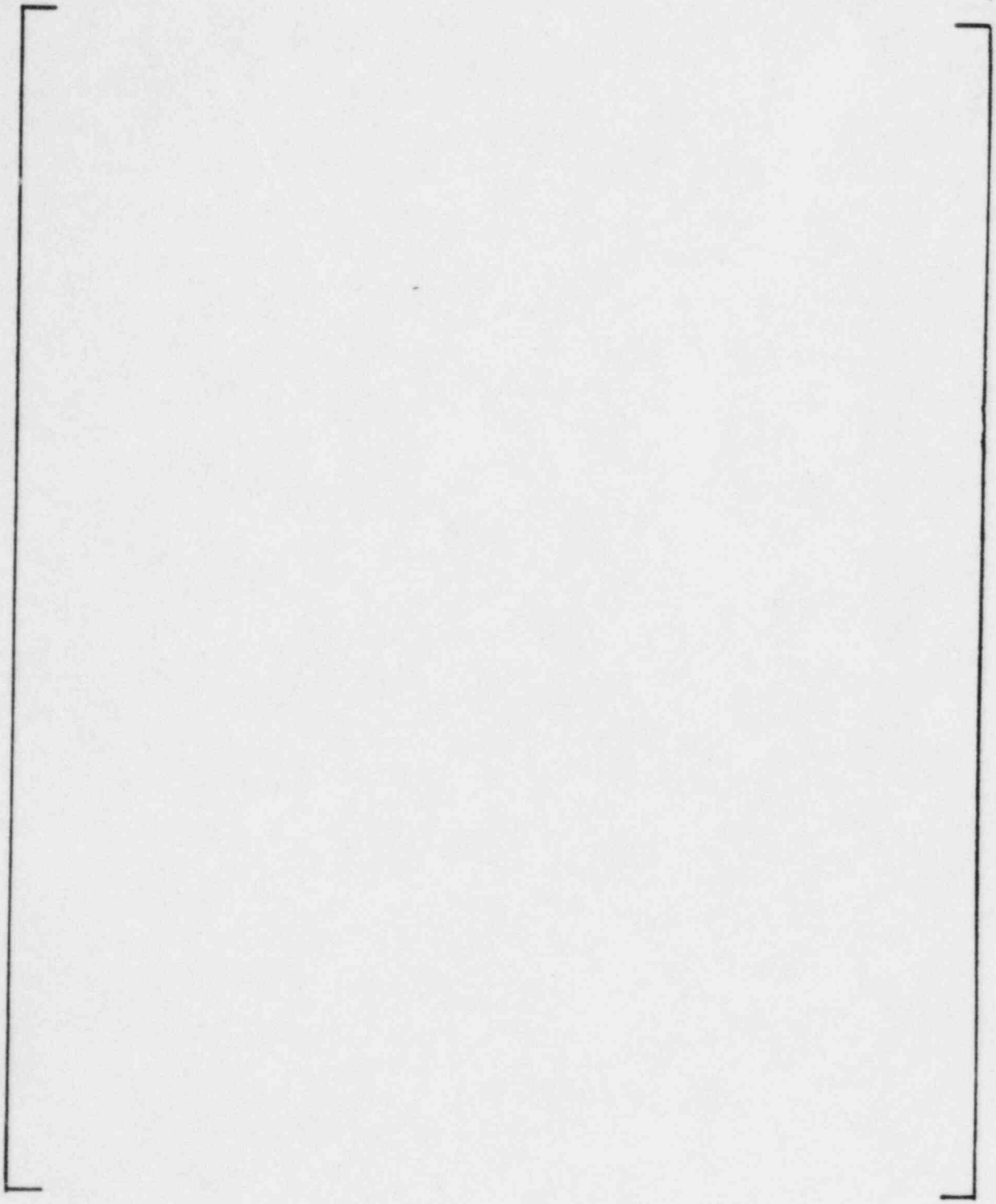


FIGURE 7.7-10 STEAM DUMP - PRESSURE CONTROL