CHAPTER 7

PLANT PROTECTION, INSTRUMENTATION, AND CONTROL

CONTENTS

CONTENTS
(Continued)

CONTENTS
(Continued)

CONTENTS
(Continued)

CONTENTS
(Continued)

CONTENTS
(Continued)

CONTENTS

(Continued)

LIST OF TABLES

LIST OF FIGURES
(Continued)

LIST OF EFFECTIVE PAGES

Page Number	Amendment
7-i through 7-vii	2
7-viii through xi	0
7-xii	6
7-xiii	4
7-xiv	6
7.1-1	2
7.1-2 through 7.1-5	0
Table 7.1-1	0
Figure 7.1-1	0
7.2-1	0
7.2-2 and 7.2-2a	4
7.2-3 through 7.2-6	2
7.2-7	0
7.2-8	2
7.2-9 and 7.2-10	0
7.2-11 through 7.2-12a	2
7.2-13 and 7.2-14	0
7.2-15	2
7.2-16 through 7.2-18	0
7.2-19 through 7.2-20a	2
7.2-21	2
7.2-22 through 7.2-30	0
7.2-31	2
7.2-32	0
7.2-33	3
7.2-34 through 7.2-38	0
7.2-39 and 7.2-40	2
7.2-41 and 7.2-42	0
Table 7.2-1	0
Table 7.2-1A (1 of 3/3 of 3)	2
Table 7.2-2	2
Table 7.2-3 (1 of 4)	2

LIST OF EFFECTIVE PAGES
(Continued)

Page Number	Amendment
Table 7.2-3 (2 of 4)	0
Table 7.2-3 (3 of 4)	0
Table 7.2-3 (4 of 4)	2
Table 7.2-4 (1 of 6/2 of 6)	0
Table 7.2-4 (3 of 6)	2
Table 7.2-4 (4 of 6)	0
Table 7.2-4 (5 of 6/6 of 6)	0
Table 7.2-5 (1 of 2)	0
Table 7.2-5 (2 of 2)	2
Table 7.2-6 (1 of 6/6 of 6)	0
Table 7.2-7 (1 of 6/6 of 6)	0
Table 7.2-8	0
Table 7.2-9 (1 of 6/6 of 6)	0
Figures 7.2-1 and 7.2-2	2
Figures 7.2-3 through 7.2-10	0
7.3-1	0
7.3-2 through 7.3-5	2
7.3-6 through 7.3-11	0
7.3-12 through 7.3-14	2
7.3-15 and 7.3-16	0
7.3-17 and 7.3-18	2
7.3-19 through 7.3-34	0
Tables 7.3-1 through 7.3-3	0
Table 7.3-4 (1 of 6)	2
Table 7.3-4 (2 of 6/6 of 6)	0
Table 7.3-4A	2
Table 7.3-5 (1 of 2)	0
Table 7.3-5 (2 of 2)	3
Table 7.3-6 (1 of 5/5 of 5)	0
Table 7.3-7 (1 of 3/2 of 3)	0
Table 7.3-7 (3 of 3)	2

LIST OF EFFECTIVE PAGES
(Continued)

Page Number	Amendment
Figures 7.3-1 through 7.3-3	2
Figures 7.3-4 through 7.3-7	0
Figure 7.3-8	2
Figure 7.3-9	0
Figures 7.3-10 and 7.3-11	2
7.4-1	0
7.4-2	2
7.4-3 through 7.4-5	0
7.4-6	2
7.4-7	0
7.4-8	2
7.4-9 through 7.4-15	0
7.4-16 and 7.4-17	2
7.4-18 through 7.4-22	0
7.4-23	2
7.4-24 and 7.4-25	0
7.4-26	2
7.4-27 and 7.4-28	6
7.4-29	2
7.4-30	0
Table 7.4-1 (1 of 2)	0
Table 7.4-1 (2 of 2)	2
Table 7.4-2 (1 of 2/2 of 2)	5
Tables 7.4-3 and 7.4-4	2
Table 7.4-5	0
Tables 7.4-6 and 7.4-7	2
Figures 7.4-1 through 7.4-3	0

CHAPTER 7
PLANT PROTECTION, INSTRUMENTATION, AND CONTROL

7.1 INTRODUCTION

The Standard MHTGR plant provides automatic control for the four reactor modules and two turbine generator systems for power generation. The automatic control is used during normal operational control and abnormal events to maintain power generation while averting challenges to safety and investment protection. The multimodule plant is controlled from a single main control room with one primary operator and an assistant.

The three Standard MHTGR plant systems that provide plant protection, instrumentation, and control are as follows:

1. Plant Protection and Instrumentation System (PPIS)

2. Plant Control, Data and Instrumentation System (PCDIS)

3. Miscellaneous Control and Instrumentation Group (MCIG)

These systems and subsystems for Standard MHTGR plant protection, instrumentation, and control are shown on Figure 7.1-1. Power generation and radionuclide control functions, 10CFR100 Design Criteria, classifications, design descriptions, design evaluations, and system interfaces are discussed in Sections 7.2, 7.3, and 7.4 for each system respectively.

The PPIS is an independent system of hardware and software provided to protect the public health and safety and to protect the plant investment. The PPIS monitors and initiates actions to protect plant systems and features to assure the maintenance of fission product barriers. The system monitors selected process variables, compares the sensed values to preselected levels and, as required, commands and initiates predetermined corrective actions. The PPIS provides "safety-related" actions to trip the reactor with the outer control rods or reserve shutdown material and to shut down the main loop.

Investment protection actions of the PPIS include reactor trips, steam generator isolation and dump, and Shutdown Cooling System initiation. The PPIS Subsystems included to perform and support these functions are as follows:

1. Safety Protection Subsystem

2. Special Nuclear Area Instrumentation Subsystem

3. Investment Protection Subsystem

The PCDIS is a functionally hierarchical set of hardware and software that automatically controls the Standard MHTGR plant from startup to full power and return to shutdown. The subsystems of the PCDIS are:

1. Plant Supervisory Control Subsystem (PSCS)

2. Nuclear Steam Supply System (NSSS) Control Subsystem

3. Energy Conversion Area Control Subsystem

4. Data Management Subsystem (DMS)

The PSCS automatically supervises and coordinates balancing of load (power) levels among the energy production (NSSS) and energy conversion (BOP) areas. There are individual NSSS control subsystems for each reactor that control reactor conditions and the supply of steam to the main steam header in response to PSCS direction load demands. The BOP provides monitoring and control for those systems that directly impact the continuity of power generation. The DMS provides plant-wide communication and centralized data processing. The DMS supports the PCDIS subsystems by transmitting control and monitoring communications between subsystems.

The Miscellaneous Control and Instrumentation Group senses, acquires, and processes data from the plant. The data are processed for display to the plant operator and/or retention for historical purposes. The subsystems that

support these functions are as follows:

1. NSSS Analytical Instrumentation System

2. Radiation Monitoring System

3. Seismic Monitoring System

4. Meteorological Monitoring System

5. Fire Detection and Alarm System

7.1.1 Identification of "Safety-Related" Systems

The Standard MHTGR "safety-related" control and instrumentation important to assure 10CFR100 limits are not exceeded is located in the PPIS. Within the PPIS, only the Safety Protection Subsystem is "safety related". Table 7.1-1 identifies the "safety-related" equipment of the Safety Protection Subsystem. Each reactor has an independent Safety Protection Subsystem. Section 3.2 describes the method used to establish safety classification.

"Safety-related" equipment within the PPIS is necessary to assure the retention of radionuclides within the fuel particles under "safety-related" design conditions (SRDC). The SRDCs envelope all design basis events of Chapter 15. Retention of radionuclides within the fuel particles requires accomplishing the following functions:

1. Control heat generation

2. Remove core heat

3. Control chemical attack

The Safety Protection Subsystem provides active control or initiation of systems to control heat generation (reactivity control). "Safety-related"

core decay heat removal is accomplished passively with the Reactor Cavity Cooling System (RCCS) without initiation or control from the PPIS. Safety Protection Subsystem actions are required for SRDCs to control chemical attack caused by water ingress to the primary system. In addition to a reactor trip, the steam generator is isolated to limit water ingress.

7.1.2 Identification of Special Nuclear Area Instrumentation

INTERFACING SYS?

The Special Nuclear Area Instrumentation is a subsystem of the PPIS that provides the monitoring and interlocks to assure that "safety-related" systems are operable or have performed their safety function. Included in this subsystem are the:

1. Vessel System pressure relief block valve closure interlock

2. Safety System information displays

3. Investment protection information displays

4. Post-accident monitoring instrumentation

The Vessel System pressure relief block valve closure interlock prevents the simultaneous closure of both Vessel System relief block valves to ensure that at least one vessel relief valve is always available to protect the reactor vessel and primary coolant boundary.

The Safety System information displays sense those plant variables necessary to determine that the Plant Safety Systems and preventive features are operable during normal operation, and that they have performed their function. Information is provided at local displays and also to the control room via the DMS to inform the operators that the plant is safely shut down, and that core cooling and fission product barrier integrity are maintained during normal shutdown and following the occurrence of a design basis event (DBE).

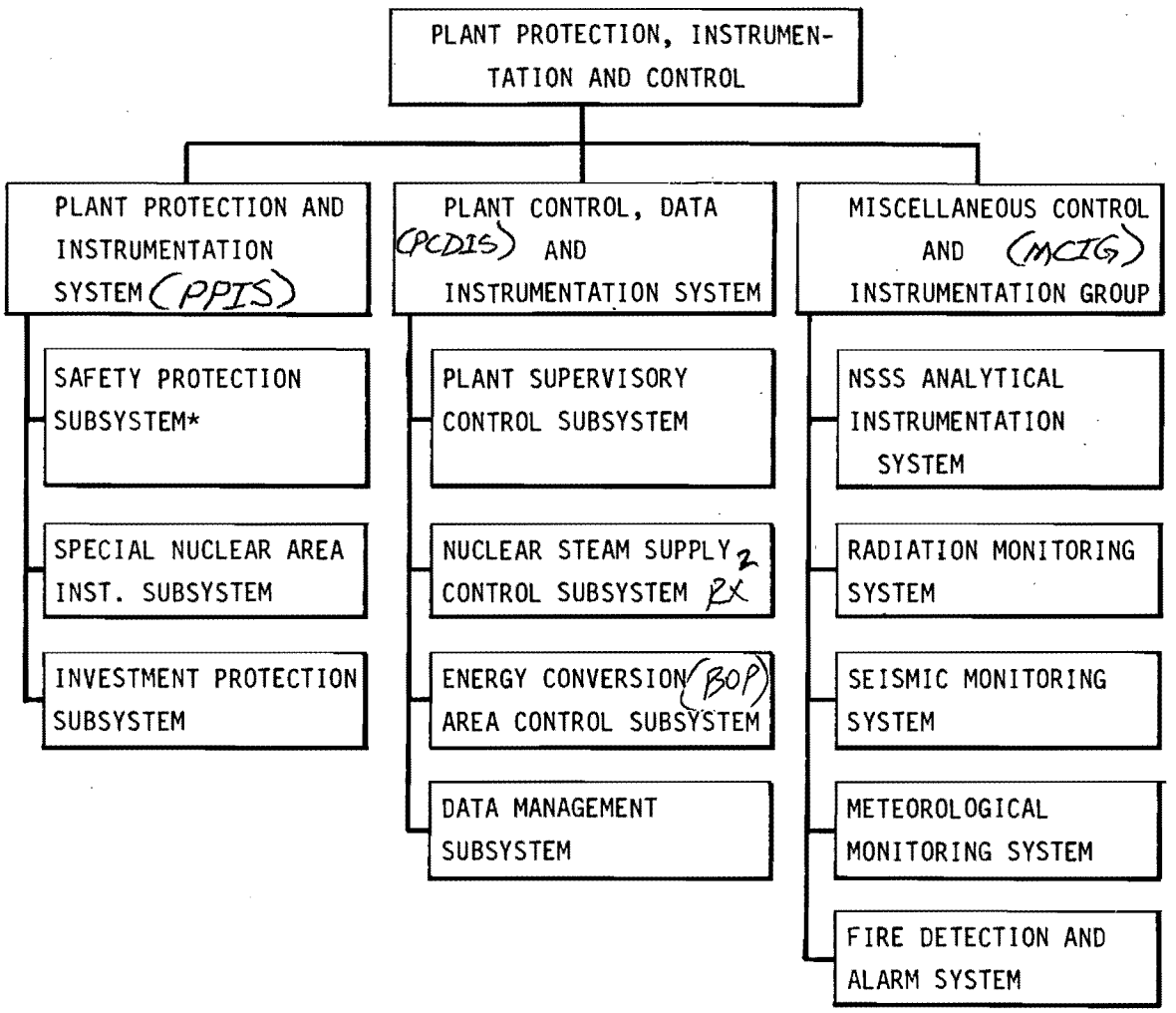
The post-accident monitoring instrumentation senses a subset of safety system parameters plus additional parameters such as site radiological and site meteorological parameters. The post-accident monitoring instrumentation uses field-mounted electronic multiplexer modules to acquire plant signals and convert the signals to a digital format. These signals are transmitted over redundant Data Management Subsystem data highways to microprocessor driven displays located in the control room. This information is also available at other plant locations.

TABLE 7.1-1

"SAFETY-RELATED" INSTRUMENTATION

AND CONTROL EQUIPMENT

Principal Component	"Safety-Related" Function
Safety Protection Subsystem:	
Safety protection cabinets	Control reactivity
Safety protection remote instrumentation	Control reactivity
Instruments, hardware, and software	Control reactivity



*SAFETY-RELATED

FIGURE 7.1-1
PLANT PROTECTION, INSTRUMENTATION AND CONTROL SYSTEMS
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

7.2 PLANT PROTECTION AND INSTRUMENTATION SYSTEM

The Plant Protection and Instrumentation System (PPIS) is composed of three major subsystems: Safety Protection, Special Nuclear Area Instrumentation, and Investment Protection. The PPIS is designed to meet top-level investment protection goals. It has reactor trip, main loop shutdown, steam generator isolation and dump, primary coolant pumpdown, and initiation of the Shutdown Cooling System (SCS) functions. Some of these functions are also required to meet 10CFR100 requirements, and the hardware portions of the PPIS that accomplish these functions have been grouped and labeled as the Safety Protection Subsystem. The PPIS hardware that provides the other active functions have been grouped and labeled Investment Protection Subsystem. The scope of these subsystems and the division into their subordinate subsystems or major components are shown in Table 7.2-1.

The Safety Protection Subsystem provides the sense and command features necessary to initiate reactor trip using the outer control rods and the reserve shutdown control equipment (RSCE) and to initiate main loop shutdown. The Safety Protection Subsystem contains the PPIS "safety-related" equipment.

The Special Nuclear Area Instrumentation Subsystem provides plant protection interlock and monitoring features. This includes the Vessel System pressure relief block valve closure interlock, equipment that monitors plant protection systems status, and equipment that monitors the plant safety and investment under normal operating and accident conditions. The Special Nuclear Area Instrumentation Subsystem contains only equipment that is not "safety related".

The Investment Protection Subsystem provides the sense and command features necessary to initiate protective actions to limit plant investment risk. The Investment Protection Subsystem contains only equipment that is not "safety related".

A functional overview of the PPIS protective trip actions is shown in Figure 7.2-1.

7.2.1 Safety Protection Subsystem

7.2.1.1 Summary Description

The Safety Protection Subsystem provides the safety system sense and command features necessary to sense process variables, detect abnormal plant conditions, and initiate reactor trip and/or main loop shutdown to mitigate the consequences of design basis events (DBEs). Each reactor module has a separate and independent Safety Protection Subsystem.

7.2.1.2 Functions and 10CFR100 Design Criteria

7.2.1.2.1 Power Generation Functions

The power generation function of the Safety Protection Subsystem is to protect the capability to maintain energy production, shutdown, refueling, and startup/shutdown by sensing process variables to detect abnormal plant conditions and actuating a reactor trip to maintain plant parameters within acceptable limits.

7.2.1.2.2 Radionuclide Control Functions

The functions of the Safety Protection Subsystem for maintaining control of radionuclide release are to limit heat generation, within acceptable limits, to limit radiation transport from the primary coolant, and to control chemical attack on the fuel particles by sensing process variables to detect abnormal plant conditions and actuating a reactor trip and/or main loop shutdown.

7.2.1.2.3 Classification

The Safety Protection Subsystem is classified as "safety related". The features of the Safety Protection Subsystem that are not required for meeting 10CFR100-related radionuclide control functions are not "safety related". However, these "nonsafety-related" features will have the appropriate

reliability to meet other Top-Level Regulatory Criteria and user requirements.

For additional information related to this section, see the response to NRC Comment 5-29.

7.2.1.2.4 10CFR100 Design Criteria for Radionuclide Control

The following 10CFR100 Design Criteria apply to this subsystem:

10CFR100 Design Criterion II: The vessels and other components that limit or prevent the ingress of air or water shall be designed, fabricated, and operated such that the amount of air or water reacting with the core will not exceed acceptable values.

10CFR100 Design Criterion III: The reactor shall be designed, fabricated, and operated such that the inherent nuclear feedback characteristics ensure that the reactor thermal power will not exceed acceptable values. Additionally, the reactivity control system(s) shall be designed, fabricated, and operated such that during insertion of reactivity the reactor thermal power will not exceed acceptable values.

7.2.1.3 Radionuclide Control Design Requirements

1. The Safety Protection Subsystem shall sense plant process variables to detect abnormal plant conditions and actuate reactor trip to limit heat generation to assure that 10CFR100 radionuclide release limits are not exceeded.

2. The Safety Protection Subsystem shall sense plant process variables to detect large steam generator leaks and actuate main loop shutdown to isolate the steam generator to limit chemical attack of the fuel to assure that 10CFR100 radionuclide release limits are not exceeded.

3. The Safety Protection Subsystem shall meet the requirements of ANSI/IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", with the exception of the location of manual initiation capability in the main control room and the format for documenting safety system design bases.

4. The Safety Protection Subsystem shall be designed, fabricated, and erected to performance standards that will enable it to withstand the

forces that might be imposed by an earthquake with ground acceleration levels corresponding to an operating basis earthquake (OBE) and a safe shutdown earthquake (SSE) and operate as required without undue risk to the reactor plant and ultimately to the health and safety of the public. The Safety Protection Subsystem shall be seismically qualified in accordance with IEEE Standard 344, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

5. The Safety Protection Subsystem shall be capable of performing its safety functions before, during, and for an adequate time after being subjected to environmental conditions associated with normal plant operation, abnormal plant operation, anticipated operational occurrences (AOOs), design basis events, and "safety-related" design conditions (SRDCs). The Safety Protection Subsystem shall be environmentally qualified in accordance with IEEE Standard 323, "Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

7.2.1.4 Design Description

The safety protection functions of the PPIS are implemented on a per reactor basis with a fully automatic, remote multiplexed, microprocessor based protection system. The protection system architecture consists of multiple separate and redundant optical digital data highways from the local multiplex units that communicate with four separate, redundant computers to implement the four channel protection systems for each reactor module.

Separate and independent Safety Protection Subsystem operator interfaces for each reactor module are located in the PPIS equipment room and the remote shutdown area. The operator interfaces include color video displays, function input devices, and keyboards. Since no operator action is required for safety, these interfaces are not classified as "safety-related". However, these operator interfaces are provided as part of the PPIS, and they are separate and independent of all other plant instrumentation and controls. In addition, data on the Safety Protection Subsystem are transmitted through a unidirectional isolator to the Data Management Subsystem for display by the

Plant Supervisory Control Subsystem in the main control room. The PPIS operator interfaces in the remote shutdown area provide an operator the capability of initiating reactor trip or main loop shutdown from a position remote from the main control room. No manual inputs to the Safety Protection Subsystem are provided in the main control room.

Each reactor module has a separate and independent Safety Protection Subsystem which consists of four separate (redundant) safety channels with two-out-of-four coincidence solid-state logic to command initiation of reactor trip or main loop shutdown. Each safety channel includes the field-mounted process variable sensors (e.g., resistance thermometers, flow transducers, pressure transducers, neutron detectors, etc.), electronic signal conditioning equipment, and electronic trip setpoint comparators to provide a trip signal when the process variable value reaches the trip setpoint. The two-out-of-four coincidence logic circuitry provides a reactor trip or main loop shutdown initiation signal when any two or more separate safety system channels reach the trip setpoint. The reactor trip and main loop shutdown initiation signals are sent to separate and redundant actuation devices. The boundaries of the Safety Protection Subsystem include the safety system sensors to the input of the actuation devices. A summary of the logic used in the sense, command and execute features of the Safety Protection Subsystem is shown in Table 7.2-1A.

7.2.1.4.1 Subsystem Configuration

The Safety Protection Subsystem is composed of the following subsystems for each reactor module:

1. Reactor Trip Using Outer Control Rods

   This "safety-related" subsystem initiates a reactor trip upon detection of reactivity excursions, loss of core cooling, water ingress events that cause positive reactivity insertion, or breach of the primary coolant barrier by initiating the automatic insertion of all outer control rods including any that may be in the process of being withdrawn. Since this subsystem provides the primary reactor

trip capability, it is also used to provide a reactor trip for "nonsafety-related" purposes. To protect the plant investment, this subsystem initiates a rapid reduction in reactor power upon detection of water ingress events which cause graphite oxidation, loss of main loop cooling, overheating of NSSS components, and also upon receipt of a manual initiation command from the PPIS operator interface located in the remote shutdown area. A simplified one-channel block diagram of the outer control rod reactor trip subsystem is shown in Figure 7.2-2.

The outer control rod reactor trip subsystem inputs, each derived from four separate and redundant sensor channels are:

a. Neutron flux to helium mass flow ratio high. ("Safety related". To detect reactivity excursions and loss of core cooling.)

b. Primary coolant pressure low. ("Safety related". To detect breach of primary coolant barrier.) Automatic bypass for startup when neutron flux is low.

c. Primary coolant pressure high. ("Safety related". To detect large water ingress events.)

d. Primary coolant moisture concentration high. (Not "saftey related". To detect water ingress events which cause graphite oxidation.)

e. Main loop trip signal. (Not "safety related". To provide signal on investment protection trip of main cooling loop.)

f. Steam generator inlet helium temperature high. (Not "safety related". To detect potential overheating of NSSS components.)

g. Manual initiation. (Not "safety related". To provide independent backup to the automatic trip systems.)

The outer control rod reactor trip subsystem actuated equipment are the outer control rods and their release mechanisms. Upon initiation of the reactor trip signal, all outer control rods are released and inserted into the core.

2. Reactor Trip Using Reserve Shutdown Control Equipment

This "safety-related" subsystem actuates the Reserve Shutdown Control Equipment (RSCE) to perform reactor trip whenever the outer control rod reactor trip subsystem fails to trip when commanded [anticipated transient without scram (ATWS)] or when the positive reactivity of water ingress in the reactor core exceeds the negative reactivity of the outer control rods. For investment protection purposes, a manual initiation capability is provided at the PPIS operator interface located in the remote shutdown area. A simplified one channel block diagram of the reserve shutdown reactor trip subsystem is shown in Figure 7.2-3.

The RSCE reactor trip inputs, each derived from four separate and redundant sensor channels, are:

a. Reactor neutron flux to main helium circulator speed ratio high after appropriate delay time to allow the outer control rod reactor trip system to correct the transient. ("Safety related". To detect ATWS.)

b. Primary coolant pressure high. ("Safety related". To detect large water ingress events.)

c. Manual initiation. (Not required for safety. To provide independent backup to the automatic trip systems.)

The actuated equipment for this reactor trip subsystem are the RSCE fusible links. Upon actuation the fusible links are energized, they open, causing the reserve shutdown hoppers to release the reserve

shutdown material into the reactor core inner graphite reflector. The protective action is completed when the reserve shutdown hoppers empty and the resulting negative reactivity in the reactor core shuts down the reactor.

The reactor neutron flux to circulator speed ratio trip input is inhibited by an automatic operating bypass when both neutron flux and circulator speed are low. This operating bypass prevents unnecessary actuation of reserve shutdown when both the reactor and circulator are shut down.

3. Main Loop Shutdown

This "safety-related" subsystem initiates a main loop shutdown to isolate the steam generator upon detection of a large steam generator leak as indicated by high primary coolant pressure. This limits chemical attack of the fuel by limiting water ingress. The main loop shutdown subsystem also limits the temperature of the steam generator tubes and tubesheets and limits the temperature and speed of helium circulator to limit investment risk by protecting the steam generator, circulator, and the primary coolant boundary. Main loop shutdown is executed by automatically initiating the opening of the main helium circulator motor trip contactors and the closure of the valves necessary to shut off the secondary side of the coolant loop.

The main loop shutdown subsystem trip inputs, each derived from four separate and redundant sensor channels, are:

a. Primary coolant pressure high. ("Safety related". To detect large water ingress events.)

b. Circulator speed high or low compared to a nominal circulator speed setpoint programmed by feedwater flow. (Not "safety related". To detect primary and secondary coolant mismatches.)

c. Primary coolant pressure low and main steam temperature <u>not</u> low. (Not "safety related". This is to prevent a steam generator quench on primary coolant depressurization where the feedwater reduction does not match the decrease in primary coolant mass flow.)

d. Steam generator dump and isolation signal. (Not "safety related". To command main loop shutdown before steam generator dump.)

e. Manual initiation (Not "safety related". To provide independent backup to automatic trip systems.)

The actuated equipment includes the feedwater block valves, superheater outlet valves, and circulator motor trip contactors.

A simplified one-channel block diagram of the main loop shutdown subsystem is shown in Figure 7.2-4.

7.2.1.4.2 Subsystem Arrangement

The Safety Protection Subsystem is arranged into modular electronic components with four separate "safety-related" channels. Each of the four Standard MHTGR reactor modules has a separate four-channel "safety-related" protection system. The "safety-related" components for each reactor module are associated with that reactor module. The Safety Protection Subsystem operator interface equipment is located in the PPIS equipment room in the Reactor Building and remote shutdown area in the Reactor Service Building. These functional components of the PPIS and their locations are shown in Figure 7.2-5.

7.2.1.4.3 Subsystem Operating Modes

The Safety Protection Subsystem is operable during all plant modes. The status of the plant is monitored at all times and trip actions are initiated as required. Continual surveillance of the Safety Protection Subsystem is performed automatically through self-diagnostics routines and abnormal conditions are indicated. Portions of the system may be bypassed for

surveillance, testing, and maintenance; however, because of the system's redundancy this does not cause loss of the protective function. The sense and command two-out-of-four coincidence logic automatically reverts to two-out-of-three coincidence logic when one channel is bypassed for maintenance. Operation of the plant with portions of the Safety Protection Subsystem out of service is governed by the plant procedures.

Shutdown of the entire Safety Protection Subsystem is generally not required to perform maintenance because of the redundancy within the system. Inadvertent shutdowns of redundant portions of the Safety Protection Subsystem result in a reactor trip using the outer control rods due to the fail-safe characteristics of the design.

Abnormal operation of the Safety Protection Subsystem is limited to plant operation with the subsystems operating in a degraded mode (failed or inoperable equipment). Operation in a degraded mode is governed by plant procedures.

The Safety Protection Subsystem is designed not to adversely affect plant safety or plant availability in the event of a single failure. Therefore, a single failed component or input channel will not cause an unwanted (spurious) reactor trip nor prevent a required reactor trip.

The cause for spurious channel trips will be determined, corrected, and the channel reset in a timely fashion. Continued plant operation with an input channel in a tripped condition is undesirable because a second channel trip will result in an unwanted subsystem trip. The two-out-of-four coincidence logic allows the maintenance bypass of one spuriously tripped channel. In this case the logic reverts to two-out-of-three coincidence logic and a degree of redundancy of one is maintained. The Safety Protection Subsystem may be operated in a degraded condition as long as a degree of redundancy of one is maintained.

7.2.1.4.4 Subsystem Limitations

Trip setpoints are conservatively established to assure that component damage

limits are not reached. Figure 7.2-6 illustrates the relationship between trip setpoints, damage limits, and analysis trip levels used in DBE and SRDC analysis. The limiting protection system settings (allowable values) conservatively bound component damage thresholds so that if the limiting system setting is reached, automatic protective action corrects the abnormal situation before the damage threshold is exceeded. The limiting protection system setting takes into consideration sensor calibration errors, instrument accuracy, and transient overshoot. The actual protection system settings (trip setpoints), are conservatively bounded by the limiting protection system settings with allowance for instrument and setpoint drift. The lower setpoint limit is specified to prevent unnecessary system trips during normal operation transients.

The analysis trip levels and setpoints (actual system settings) for the Safety Protection Subsystem are shown in Table 7.2-2.

Dynamic transient analysis has been performed at an analysis trip level. The actual system setting (nominal trip setpoint) is below this analysis trip level, as shown in Figure 7.2-6, and reflects allowances for calibration errors, instrument accuracy, transient overshoot, instrument and setpoint drift, etc., in accordance with IEEE Standard 603 and ISA Standard S67.04.

7.2.1.5 Design Evaluation

7.2.1.5.1 Failure Modes and Effects

The Safety Protection Subsystem is redundant and single failure proof. Therefore, failure of one component does not prevent the system from responding correctly when required. Failures within the subsystem are either immediately alarmed through the Special Nuclear Area Instrumentation Subsystem or become apparent during the routine surveillance and testing of the system.

Equipment classified not "safety-related" will not prevent the "safety-related" portions of the Safety Protection Subsystem from performing their safety functions. This will be ensured by satisfying the independence requirements of IEEE-603, Section 5.6, or the use of associated circuits as

defined in IEEE-384, Section 5.5, and will be demonstrated by a failure modes and effects analysis at the final design stage.

Design features are included to assist the operator in verifying that Safety Protection Subsystem degree of redundancy of at least one is always maintained. For example, whenever any essential safety system component is bypassed such that a safety channel is inoperable, a continuous bypass indication/alarm is displayed in the remote shutdown area and also indicated in the main control room. Whenever one channel of the two-out-of-four logic is disconnected or bypassed, the remainder of the subsystem maintains a degree of redundancy of one. Whenever a one-out-of-two actuation device is disconnected or bypassed, the time of inoperability will be kept to a minimum and will be within acceptable subsystem reliability analysis constraints. Whenever the two-out-of-four logic is operated with one channel tripped, the remaining channels are in a one-out-of-three operating mode. The Safety Protection Subsystem is designed to fail into a safe state or into a state demonstrated to be acceptable on conditions such as disconnection of the system and loss of electric power. A reactor trip occurs using outer control rods on loss of all electrical power. Reactor trip using the RSCE and main loop shutdown requires electric power to trip and is powered by a "safety-related" uninterruptible power supply with adequate capacity to perform the safety function. This design is adequate to meet the safety function and also meet plant availability requirements by avoiding spurious RSCE insertions or main loop shutdowns.

7.2.1.5.2 Steady-State Performance

The required steady-state performance of the Safety Protection Subsystem is to remain operable during all plant operating modes and monitor various plant process parameters to detect abnormal plant conditions and initiate reactor trip as necessary to limit heat generation rate and initiate main loop shutdown to limit chemical attack of the fuel and to limit investment risk to NSSS components.

7.2.1.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. In this section only the response of the Safety Protection Subsystem to AOOs is described. A summary of the AOO trip functions of the Safety Protection Subsystem is shown in Table 7.2-3.

limits are not reached. Figure 7.2-6 illustrates the relationship between trip setpoints, damage limits, and analysis trip levels used in DBE and SRDC analysis. The limiting protection system settings (allowable values) conservatively bound component damage thresholds so that if the limiting system setting is reached, automatic protective action corrects the abnormal situation before the damage threshold is exceeded. The limiting protection system setting takes into consideration sensor calibration errors, instrument accuracy, and transient overshoot. The actual protection system settings (trip setpoints), are conservatively bounded by the limiting protection system settings with allowance for instrument and setpoint drift. The lower setpoint limit is specified to prevent unnecessary system trips during normal operation transients.

The analysis trip levels and setpoints (actual system settings) for the Safety Protection Subsystem are shown in Table 7.2-2.

Dynamic transient analysis has been performed at an analysis trip level. The actual system setting (nominal trip setpoint) is below this analysis trip level, as shown in Figure 7.2-6, and reflects allowances for calibration errors, instrument accuracy, transient overshoot, instrument and setpoint drift, etc., in accordance with IEEE Standard 603 and ISA Standard S67.04.

7.2.1.5 Design Evaluation

7.2.1.5.1 Failure Modes and Effects

The Safety Protection Subsystem is redundant and single failure proof. Therefore, failure of one component does not prevent the system from responding correctly when required. Failures within the subsystem are either immediately alarmed through the Special Nuclear Area Instrumentation Subsystem or become apparent during the routine surveillance and testing of the system.

Design features are included to assist the operator in verifying that Safety Protection Subsystem degree of redundancy of at least one is always maintained. For example, whenever any essential safety system component is

bypassed such that a safety channel is inoperable, a continuous bypass indication/alarm is displayed in the remote shutdown area and also indicated in the main control room. Whenever one channel of the two-out-of-four logic is disconnected or bypassed, the remainder of the subsystem maintains a degree of redundancy of one. Whenever a one-out-of-two actuation device is disconnected or bypassed, the time of inoperability will be kept to a minimum and will be within acceptable subsystem reliability analysis constraints. Whenever the two-out-of-four logic is operated with one channel tripped, the remaining channels are in a one-out-of-three operating mode. The Safety Protection Subsystem is designed to fail into a safe state or into a state demonstrated to be acceptable on conditions such as disconnection of the system, loss of electric power, and loss of HVAC. A reactor trip occurs using outer control rods on loss of all electrical power. Reactor trip using the RSCE and main loop shutdown requires electric power to trip and is powered by a "safety-related" uninterruptible power supply with adequate capacity to perform the safety function. This design is adequate to meet the safety function and also meet plant availability requirements by avoiding spurious RSCE insertions or main loop shutdowns.

7.2.1.5.2 Steady-State Performance

The required steady-state performance of the Safety Protection Subsystem is to remain operable during all plant operating modes and monitor various plant process parameters to detect abnormal plant conditions and initiate reactor trip as necessary to limit heat generation rate and initiate main loop shutdown to limit chemical attack of the fuel and to limit investment risk to NSSS components.

7.2.1.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. In this section only the response of the Safety Protection Subsystem to AOOs is described. A summary of the AOO trip functions of the Safety Protection Subsystem is shown in Table 7.2-3.

AOO-1(A) Loss of Main Loop Cooling. Upon loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high which initiates a reactor trip using the outer control rods. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch which initiates a main loop shutdown as defined in Section 7.2.1.4.1. Main loop shutdown in turn signals for a reactor trip using the outer control rods and for Shutdown Cooling System initiation.

AOO-1(B) Loss of Offsite Power and Turbine Trip. Loss of offsite power and turbine trip causes the main loop helium circulator to lose electrical power and coast down. The neutron flux to helium mass flow measurement is detected as high which initiates a reactor trip using the outer control rods. Coastdown of the main loop is detected as a circulator speed to feedwater flow mismatch which initiates a main loop shutdown. Main loop shutdown in turn signals for a reactor trip using the outer control rods and for Shutdown Cooling System initiation.

AOO-1(C) Spurious Reactor Trip with Cooling on HTS. The Safety Protection Subsystem has no response to AOO-1(C) other than to continue to be operable.

AOO-1(D) Main Loop Transient Without Reactor Trip. The Safety Protection Subsystem has no response to AOO-1(D) other than to continue to be operable.

AOO-2 Loss of Main Loop Cooling and Shutdown Cooling. This response is identical to AOO-1(A).

AOO-3 Rod Withdrawal with Reactor Trip and Cooling on HTS. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint which initiates a reactor trip using the outer control rods.

AOO-4 Small Steam Generator Leak. A small steam generator leak causes a slow moisture ingress. The high primary coolant moisture concentration is detected by the "nonsafety-related" moisture monitors which initiates a reactor trip using the outer control rods. A main loop shutdown is initiated by the steam

generator isolation and dump trip signal and signals for Shutdown Cooling System initiation.

AOO-5 Small Primary Coolant Leak. A small primary coolant leak causes a slow depressurization of the primary coolant. The primary coolant pressure reaches the low pressure setpoint which initiates a reactor trip using the outer control rods. When the primary coolant pressure reaches a lower setpoint and the main steam temperature has not reached saturation temperature, a main loop shutdown is commanded. Main loop shutdown also signals for reactor trip using the outer control rods and for Shutdown Cooling System initiation.

7.2.1.5.4 Design Basis Event Performance

DBEs are described in Chapter 15. In this section only the response of the Safety Protection Subsystem to DBEs is described.

The Safety Protection Subsystem is designed and qualified to perform its safety function under environmental conditions or other plant service conditions experienced during all DBEs.

A summary of the DBE trip functions of the Safety Protection Subsystem is shown in Table 7.2-4.

DBE-1 Loss of HTS and SCS Cooling. The initiating event for DBE-1 is loss of offsite power and turbine trip. A loss of offsite power and turbine trip causes a loss of all normal ac power supplies. This causes the main loop helium circulator to coast down due to loss of power. Loss of primary coolant flow is detected as a high neutron flux to helium mass flow measurement which initiates a reactor trip using the outer control rods. Coastdown of the main loop is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown, as defined in Section 7.2.1.4.1, is commanded. Main loop shutdown in turn signals a reactor trip using the outer control rods and for Shutdown Cooling System initiation but the SCS fails to start due to unavailability of standby ac power. The Safety Protection Subsystem takes no further action for this DBE. If primary ac power is not restored and standby

ac power is not available, the Safety Protection Subsystem loses battery backup power after approximately one hour. At this time the Safety Protection Subsystem fails "as is" with the outer control rods inserted into the reactor core.

DBE-2 HTS Transient Without Control Rod Trip. The initiating event for DBE-2 is main loop cooling rampdown with a failure of reactor trip using the outer control rods to take place. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch which causes a main loop shutdown. Main loop shutdown signals a reactor trip using the outer control rods. For this DBE, the outer control rods fail to trip. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation. This event is an anticipated transient without scram (ATWS). This ATWS event is detected as a high neutron flux to circulator speed ratio measurement. If after a time delay, the reactor trip using the outer control rods has not executed protective action, reactor trip using the RSCE is automatically initiated.

DBE-3 Rod Withdrawal Without HTS Cooling. The initiating event for DBE-3 is an inadvertent control rod bank withdrawal. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint which initiates a reactor trip using the outer control rods. DBE-3 also includes a main loop upset. This is detected as a circulator speed to feedwater flow mismatch which causes a main loop shutdown. Main loop shutdown signals a reactor trip using the outer control rods and for Shutdown Cooling System initiation.

DBE-4 Rod Withdrawal Without HTS and SCS Cooling. The initiating event for DBE-4 is an inadvertent control rod bank withdrawal. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint which initiates a reactor trip using the outer control rods. DBE-4 also includes a main loop upset. This is detected as a circulator speed to feedwater flow mismatch which causes a main loop shutdown. Main loop shutdown signals a reactor trip using the outer control rods and for Shutdown Cooling System initiation but the SCS fails to start. Core cooling on the Reactor Cavity Cooling System (RCCS) may cause the primary coolant pressure to exceed the high pressure setpoint that is designed to

detect moisture ingress events and a reactor trip using the RSCE may be initiated.

DBE-5 Earthquake. The initiating event for DBE-5 is a 0.3 g earthquake. It is assumed that main loop cooling is lost. Upon loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high which initiates a reactor trip using the outer control rods. Trouble with the main cooling loop is also detected as a circulator speed to feedwater flow mismatch and a main loop shutdown is commanded. Main loop shutdown also signals a reactor trip using the outer control rods and for Shutdown Cooling System initiation.

The Safety Protection Subsystem and its "safety-related" auxiliary supporting features are qualified to withstand an SSE and perform their safety functions.

DBE-6 Moisture Inleakage. The initiating event for DBE-6 is a steam generator offset tube rupture and subsequent moderate moisture ingress rate. This event is detected as high primary coolant moisture measured by the "nonsafety-related" moisture monitors. When the "nonsafety-related" high moisture setpoint is reached a reactor trip using the outer control rods is initiated and steam generator isolation is performed as a main loop shutdown. The main loop shutdown is initiated by the steam generator isolation and dump. Main loop shutdown signals for SCS to start.

DBE-7 Moisture Inleakage Without SCS Cooling. The initiating event for DBE-7 is a moderate steam generator leak and subsequent moderate moisture ingress rate. The response of the Safety Protection Subsystem to this event is identical to DBE-6 except as follows: The SCS fails to start on demand and core cooling by the RCCS may cause the primary coolant pressure to exceed the high pressure setpoint that is designed to detect moisture ingress events and a reactor trip using the RSCE may be initiated.

DBE-8 Moisture Inleakage with Moisture Monitor Failure. The initiating event for DBE-8 is a small steam generator leak and subsequent small moisture

ingress rate. DBE-8 also includes a failure of the "nonsafety-related" moisture monitors. The moisture ingress causes the primary coolant pressure to increase slowly. The primary coolant pressure reaches the high pressure setpoint which initiates a reactor trip using both the outer control rods and the RSCE. High primary coolant pressure also initiates main loop shutdown. Main loop shutdown also signals for SCS to start.

DBE-9 Moisture Inleakage with Steam Generator Dump Failure. The initiating event for DBE-9 is a small steam generator leak and subsequent small moisture ingress rate. In this DBE the "nonsafety-related" Investment Protection Subsystem moisture monitors detect the moisture inleakage and initiate steam generator isolation and dump and reactor trip using the outer control rods. Steam generator isolation is performed as a main loop shutdown. The main loop shutdown also signals for SCS to start. The steam generator dump valves fail to reclose but the primary coolant is contained by the dump tank.

DBE-10 Primary Coolant Leak. The initiating event for DBE-10 is a moderate primary coolant leak. A moderate primary coolant leak causes a rapid depressurization of the primary coolant. The primary coolant pressure reaches the low pressure setpoint which initiates a reactor trip using the outer control rods. When the primary coolant pressure decreases to a lower setpoint and main steam temperature is still above saturation, a main loop shutdown is commanded to prevent steam generator quench. Main loop shutdown also signals for SCS to start.

DBE-11 Primary Coolant Leak Without HTS and SCS Cooling. The initiating event for DBE-11 is a small primary coolant leak. A small primary coolant leak causes a slow depressurization of the primary coolant. This DBE assumes that the main cooling loop is upset 15 hours into the DBE. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch which causes a main loop shutdown. Main loop shutdown signals a reactor trip using the outer control rods. Main loop shutdown also signals for Shutdown Cooling System initiation.

7.2.1.5.5 "Safety-Related" Design Condition Performance

"Safety-related" design conditions (SRDCs) are described in Chapter 15. In this section only the performance of the Safety Protection Subsystem under SRDCs is described. The Safety Protection Subsystem is designed and qualified to perform its safety function under environmental conditions or other plant service conditions experienced during all SRDCs.

A summary of the performance of the Safety Protection Subsystem under SRDCs is provided in Table 7.2-5.

SRDC-1 Pressurized Conduction Cooldown. SRDC-1 is loss of offsite power and turbine trip. A loss of offsite power and turbine trip causes a loss of all normal ac power supplies. This causes the main loop helium circulator to coast down due to loss of power. Loss of primary coolant flow is detected as a high neutron flux to helium mass flow measurement which initiates a reactor trip using the outer control rods. The Safety Protection Subsystem takes no further action. If primary ac power is not restored and standby ac power is not available, the Safety Protection Subsystem loses battery backup power after approximately one hour. At this time the Safety Protection Subsystem fails "as is" since it has no further safety function to perform.

SRDC-2 Pressurized Conduction Cooldown Without Control Rod Trip. SRDC-2 is main loop cooling rampdown with a failure of reactor trip using the outer control rods to take place. This condition is an anticipated transient without scram (ATWS). This ATWS is detected as a high neutron flux to circulator speed ratio measurement. If after a time delay, the reactor trip using the outer control rods has not executed protective action, reactor trip using the RSCE is initiated.

SRDC-3 Pressurized Conduction Cooldown with Control Rod Withdrawal. SRDC-3 is an inadvertent control rod bank withdrawal. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint which initiates a reactor trip using the outer control rods. Core cooling by the RCCS may cause the primary coolant pressure to

exceed the high pressure setpoint designed to detect moisture ingress and a main loop shutdown and reactor trip using the RSCE may be initiated.

SRDC-4 Pressurized Conduction Cooldown with Control Rod Withdrawal. The performance of the Safety Protection Subsystem under SRDC-4 is identical to its performance under SRDC-3.

SRDC-5 Pressurized Conduction Cooldown with Earthquake. SRDC-5 is a 0.3 g earthquake. It is assumed that main loop cooling is lost. Upon loss of main loop cooling, the neutron flux to helium mass flow measurement is detected as high which initiates a reactor trip using the outer control rods.

The Safety Protection Subsystem and its "safety-related" auxiliary supporting features are qualified to withstand an SSE and perform their safety functions.

SRDC-6 Depressurized Conduction Cooldown with Moderate Moisture Ingress. SRDC-6 is a steam generator leak and subsequent moisture ingress. The water ingress rate causes a positive reactivity insertion and neutron flux to helium mass flow measurement to exceed the high setpoint. This initiates a reactor trip using the outer control rods. The primary coolant pressure also increases, and the high pressure setpoint is reached which causes a reactor trip using the RSCE and a main loop shutdown. A main loop shutdown isolates the steam generator to limit the water ingress.

SRDC-7 Depressurized Conduction Cooldown with Moderate Moisture Ingress. The performance of the Safety Protection Subsystem under SRDC-7 is identical to its performance under SRDC-6.

SRDC-8 Depressurized Conduction Cooldown with Small Moisture Ingress. The initiating event for SRDC-8 is a small steam generator leak and subsequent small moisture ingress rate. The moisture ingress causes the primary coolant pressure to increase slowly. The primary coolant pressure reaches the high pressure setpoint which initiates a reactor trip using both the outer control rods and the RSCE. High primary coolant pressure also initiates main loop shutdown which isolates the steam generator to limit the water ingress.

SRDC-9 Depressurized Conduction Cooldown with Small Moisture Ingress. The Safety Protection Subsystem has no function for SRDC-9 other than to continue to be operable.

SRDC-10 Depressurized Conduction Cooldown with Moderate Primary Coolant Leak. SRDC-10 is a moderate primary coolant leak. A moderate primary coolant leak causes a rapid depressurization of the primary coolant. The primary coolant pressure reaches the low pressure setpoint which initiates a reactor trip using the outer control rods.

SRDC-11 Depressurized Conduction Cooldown with Small Primary Coolant Leak. The performance of the Safety Protection Subsystem under SRDC-11 is identical to the response to SRDC-10.

7.2.1.6 Interfaces

Interface requirements imposed on other systems or subsystems within other systems by the Safety Protection Subsystem are identified in Table 7.2-6, which also includes a description of the interface and a quantitative expression for the interface.

7.2.2 Special Nuclear Area Instrumentation Subsystem

7.2.2.1 Summary Description

The Special Nuclear Area Instrumentation Subsystem provides interlocks and instrumentation that monitors the protection systems' status and the plant under normal operating and accident conditions.

7.2.2.2 Functions and 10CFR100 Design Criteria

7.2.2.2.1 Power Generation Functions

The power generation function of the Special Nuclear Area Instrumentation Subsystem is to protect the capability to maintain energy production, shutdown, refueling, and startup/shutdown by monitoring PPIS status and plant variables to verify that protection equipment is operable.

7.2.2.2.2 Radionuclide Control Functions

The functions of the Special Nuclear Area Instrumentation Subsystem for maintaining control of radionuclide release are to limit heat generation to limit radiation transport from the primary coolant and to control chemical attack on the fuel particles by providing PPIS status and plant variables data to verify that the protection system is operable and by actuating the interlocks on the Pressure Relief Subsystem.

7.2.2.2.3 Classification

This subsystem is not "safety related". Since the special nuclear area instrumentation does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, the subsystem will have appropriate reliability to meet other Top-Level Regulatory Criteria and user requirements.

7.2.2.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to this subsystem.

7.2.2.3 Radionuclide Control Design Requirements

1. The special nuclear area instrumentation shall monitor plant process variables, "safety-related" equipment status, and investment protection equipment status to verify that radionuclide control is maintained.

2. The special nuclear area instrumentation shall be designed, fabricated, and erected to performance standards that will enable it to withstand the forces that might be imposed by an earthquake with ground acceleration levels corresponding to an operating basis earthquake and a safe shutdown earthquake and operate as required.

3. The special nuclear area instrumentation required for accident monitoring shall be capable of performing its functions before,

during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions.

7.2.2.4 Design Description

The interlock feature of the special nuclear area instrumentation is the Vessel System pressure relief block valve closure interlock. The vessel pressure relief block valve closure interlock consists of redundant electrical sensors, and electrical interlocks to prevent the simultaneous closure of both Vessel System relief valve trains. This prevents the complete bypass of the vessel overpressure protection.

The safety protection information equipment consists of field mounted electronic multiplexer modules, redundant digital data highways, redundant microprocessor equipment, and instrumentation displays in the remote shutdown area and PPIS equipment room to provide the integration of safety protection sensor channel readouts, safety protection status (e.g., trip, alarm, normal, etc.) indication, and safety protection bypass indication. These displays assist the operator in verifying that the plant "safety-related" systems are operable, that the proper degree of redundancy is maintained, and that protective action has been completed after a design basis event. The displays also are used in performing safety protection calibration, testing, and maintenance.

This display equipment also provides a continuous, dedicated display of a minimum set of plant parameters or derived variables used by the operator during all plant conditions to assess the plant safety status. These displays are also accessible in the main control room and other locations in the plant through the Data Management Subsystem.

The post-accident monitoring (PAM) instrumentation indicates plant variables which are required by the operating personnel during accident situations to 1) provide information required to permit the operator to assess that the reactor is safely shut down and is being cooled; 2) determine whether reactor

trip and other "safety-related" systems are performing their intended functions; and 3) provide information to the operators that will enable them to determine status of radioactivity barriers. In addition to the above, the post accident monitoring instrumentation indicates plant variables that provide information on the operation of plant safety systems and other systems that are required by the operating personnel during an accident to 1) furnish data regarding the operation of plant systems so the operator can make appropriate decisions as to their use and to 2) provide information regarding the release of radioactive materials.

7.2.2.4.1 Subsystem Configuration

The Special Nuclear Area Instrumentation Subsystems are as follows:

1. Vessel System Pressure Relief Block Valve Closure Interlock

   This subsystem prevents the simultaneous closure of both Vessel System relief block valves to ensure that at least one vessel relief valve is always available to protect the reactor vessel and primary coolant boundary.

   The Vessel System pressure relief block valve closure interlock is actuated whenever either vessel pressure relief block valve is not fully open, and prevents the simultaneous closure of both reactor vessel pressure relief block valves. The interlock function is accomplished when the power necessary to drive the block valves closed is interrupted. The interlock does not interfere with opening the block valves individually or simultaneously. Actuation of the interlock is alarmed in the remote shutdown area and the main control room.

   The Vessel System pressure relief block valve interlock consists of a redundant train (two sensors and logic) for each block valve. Two limit switches (one in each train) for each block valve sense when the

block valve is not fully open. Actuation of either redundant logic train interrupts the block valve power for closing the valve. At no time does the Vessel System pressure relief block valve interlock prevent power from being used to open the block valve.

2. Safety Protection Information Displays

Safety protection information displays consist of an integrated system using digital data highways and computer-based displays to provide:

a. Safety protection channel readouts.

b. Safety protection status indications including status indications for safety protection actuation devices, actuated equipment, and safety protection auxiliary supporting features.

c. Safety protection bypass indications including bypass indications for safety protection actuation devices, actuated equipment, and safety protection auxiliary supporting features.

In general, the subsystem provides those displays in the remote shutdown area which enable the reactor operator to perform the equipment surveillance and plant condition monitoring necessary to determine that the plant "safety-related" systems are operable during normal operation, and that they have performed their function, that the plant is safely shut down, and that core cooling and fission product barrier integrity are maintained during normal shutdown and following the occurrence of a design basis event. These displays are provided by the Plant Protection and Instrumentation System to the Data Management Subsystem for display in the main control room by the Plant Supervisory Control Subsystem.

3. Investment Protection Information Displays

Investment protection information displays function like the safety protection information displays. They include monitoring to facilitate plant restarts for the purpose of verifying that plant equipment has not been damaged in AOOs and DBEs. An integrated system using digital data highways and computer-based displays provides:

a. Investment protection channel readouts.

b. Investment protection status indications including status indications for investment protection actuation devices, actuated equipment, and investment protection auxiliary supporting features.

c. Bypass indications for Investment Protection Subsystem actuation devices, actuated equipment, and auxiliary supporting features.

In general, the Special Nuclear Area Instrumentation Subsystem provides those displays in the remote shutdown area which enable the reactor operator to perform the equipment surveillance and plant condition monitoring necessary to determine that the plant investment protection subsystems are operable during normal operation, and that they have performed their function, that the plant investment is protected during transient events. The investment protection information displays provide information which may allow the reactor operator to take manual actions from the PPIS equipment in the remote shutdown area which are important to protecting plant investment. These displays are provided by the PPIS to the Data Management Subsystem for display in the main control room by the Plant Supervisory Control Subsystem.

4. Post Accident Monitoring Instrumentation

The post-accident monitoring instrumentation includes a subset of safety protection parameters plus additional parameters such as site

radiological and site meteorological parameters. The post accident monitoring instrumentation uses field-mounted electronic multiplexer modules to acquire plant signals and convert the signals to a digital format. These signals and other "safety-related" signals are transmitted over redundant digital data highways to microprocessor driven PPIS displays located in the remote shutdown area. Post accident monitoring data is also recorded for future analysis. These displays are also accessible at the main control room and other locations throughout the plant through the Data Management Subsystem.

7.2.2.4.2 Subsystem Arrangement

The Special Nuclear Area Instrumentation Subsystem is arranged into modular electronic components with two separate channels. Each of the four Standard MHTGR reactor modules has separate special nuclear area instrumentation associated with that reactor module. The special nuclear area instrumentation equipment includes its own operator interface equipment, operator interface equipment for the Safety Protection Subsystem, and operator interface equipment for the Investment Protection Subsystem. This operator interface equipment is located in the PPIS equipment room in the Reactor Building, and remote shutdown area in the Reactor Service Building. These functional components of the Plant Protection and Instrumentation System and their locations are shown in Figure 7.2-5.

The Vessel System pressure relief block valve interlock utilizes interlock limit switches located on the valve actuator. The actuator relays are located in the motor control centers associated with the block valves.

7.2.2.4.3 Subsystem Operating Modes

The special nuclear area instrumentation is operable during all plant modes.

The status of the plant is monitored at all times and interlock actions are initiated as required. Portions of the system may be bypassed for

surveillance, testing, and maintenance; however, due to the subsystem's redundancy this does not necessitate loss of the function. Operation of the plant with portions of the special nuclear area instrumentation out of service is governed by the plant procedures.

Shutdown of the entire special nuclear area instrumentation to perform maintenance is generally not required because of the redundancy of the subsystem. To the extent possible, maintenance and partial shutdown of the special nuclear area instrumentation will be performed during scheduled plant shutdowns.

Abnormal operation of the special nuclear area instrumentation is limited to operation with the subsystem operating in a degraded mode (failed or inoperable equipment).

The Special Nuclear Area Instrumentation Subsystem is designed not to adversely affect plant availability with a single failure.

The cause of failed equipment or input channel measurements will be determined, corrected, and the equipment repaired in a timely fashion.

7.2.2.4.4 Subsystem Limitations

The Special Nuclear Area Instrumentation Subsystem is a two channel subsystem. Since it has a degree of redundancy of one, it is limited to being able to perform its function with one of the redundant channels failed.

7.2.2.5 Design Evaluation

7.2.2.5.1 Failure Modes and Effects

<u>Vessel System Relief Valve Block Valve Closure Interlock</u>. The interlock function is accomplished when the power necessary to drive the block valves closed is interrupted. The interlock does not interfere with opening the block valves individually (or simultaneously). The system is a one-out-of-two

logic arrangement where actuation of either logic train interrupts the block valve power for closing the other block valve. Loss of power or single circuit failures could prevent block valve closure which is the fail safe mode.

Information Displays. The safety protection, investment protection, and accident monitoring information displays located in the remote shutdown area are designed using a redundant computer based acquisition processing and display subsystem. Therefore, failure of any single component will not result in failure of the subsystem. Portions of the subsystem required for accident monitoring will be qualified for the accident conditions during which it is expected to perform.

7.2.2.5.2 Steady-State Performance

The steady-state performance is with the subsystem operating and continuously monitoring inputs. Output signals and display as required are generated for use on demand. The general use of this subsystem is for determining the status of protection systems, performance of protection systems, status of bypasses, and accident monitoring.

7.2.2.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. In this section only the response of the Special Nuclear Area Instrumentation Subsystem is described. The response of the Special Nuclear Area Instrumentation Subsystem to all AOOs is as follows:

1. Monitors and displays in the remote shutdown area all Safety Protection and Investment Protection Subsystem sensor channels before, during, and after all AOOs.

2. Monitors and displays in the remote shutdown area Safety Protection and Investment Protection Subsystem actuated device states before, during, and after all AOOs.

3. Monitors and displays in the remote shutdown area Safety Protection and Investment Protection Subsystem operability and status before, during, and after all AOOs.

4. Monitors and displays in the remote shutdown area the minimum set of parameters necessary to determine that plant radionuclide control is maintained before, during, and after all AOOs.

7.2.2.5.4 Design Basis Event Performance

Design basis events (DBEs) are described in Chapter 15. In this section only the response of the Special Nuclear Area Instrumentation Subsystem is described. The response of the Special Nuclear Area Instrumentation Subsystem to all DBEs is identical, except where noted, and is as follows:

1. Monitors and displays in the remote shutdown area all Safety Protection and Investment Protection Subsystems' sensor channels before, during, and after all DBEs.

2. Monitors and displays in the remote shutdown area all Safety Protection and Investment Protection subsystems' actuated device states before, during, and after all DBEs.

3. Monitors and displays in the remote shutdown area all Safety Protection and Investment Protection Subsystems' operability and status before, during, and after all DBEs.

4. Monitors and displays in the remote shutdown area the minimum set of parameters necessary to determine that plant radionuclide control is maintained before, during, and after all DBEs.

In DBE-1, loss of Heat Transport System and Shutdown Cooling System cooling, the Special Nuclear Area Instrumentation Subsystem continues to operate from the uninterruptible power system.

For DBE-5, 0.3 g earthquake, the Special Nuclear Area Instrumentation Subsystem is seismically qualified to be operable following a 0.3 g seismic event.

Except as noted above, environmental conditions or plant performance parameters experienced during DBEs have no effect on the ability of the Special Nuclear Area Instrumentation Subsystem to perform its function.

7.2.2.6 Interfaces

Interface requirements imposed on other systems or subsystems by the Special Nuclear Area Instrumentation Subsystem are identified in Table 7.2-7, which also includes a description of the interface and a quantitative expression for the interface.

7.2.3 Investment Protection Subsystem

7.2.3.1 Summary Description

The Investment Protection Subsystem provides the sense and command features necessary to sense plant variables, detect abnormal conditions, and initiate protective actions required to protect the plant investment. The Investment Protection Subsystem protects major plant equipment and is, therefore, investment risk oriented. It is not required to prevent DBEs from exceeding 10CFR100 limits; therefore, it is not "safety related". The investment protection provides an integrated response to various plant upsets and events to ensure that major equipment damage limits are not exceeded. The subsystem uses redundancy and other system characteristics to meet the plant investment and availability goals. Each reactor module has a separate and independent Investment Protection Subsystem. The Investment Protection Subsystem is part of the PPIS and is separate and independent of all other plant instrumentation and controls.

7.2.3.2 Functions and 10CFR100 Design Criteria

7.2.3.2.1 Power Generation Functions

The power generation function of the Investment Protection Subsystem is to protect the capability to maintain energy production, shutdown, refueling, and startup/shutdown by sensing process variables to detect abnormal plant conditions and actuating a reactor trip to maintain plant parameters within acceptable limits.

7.2.3.2.2 Radionuclide Control Functions

The functions of the Investment Protection Subsystem for maintaining control of radionuclide release are to limit heat generation, within acceptable limits, to limit radiation transport from the primary coolant, and to control chemical attack on the fuel particles by sensing process variables to detect plant conditions and actuating various equipment.

7.2.3.2.3 Classification

This subsystem is not "safety related". Since the Investment Protection Subsystem does not perform any 10CFR100 related radionuclide control functions, no special classification is applied to it. However, the subsystems will have appropriate reliability to meet other Top-Level Regulatory Criteria and user requirements.

7.2.3.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to this subsystem.

7.2.3.3 Radionuclide Control Design Requirements

1. The Investment Protection Subsystem shall sense plant process variables to detect abnormal plant conditions and actuate equipment to maintain plant parameters within limits that assure that 10CFR50

Appendix I, 10CFR20, and user requirement radionuclide release limits are not exceeded.

2. The Investment Protection Subsystem shall be designed, fabricated, and erected to performance standards that will enable it to withstand the forces that might be imposed by an earthquake with ground acceleration levels corresponding to a 0.3 g earthquake.

3. The Investment Protection Subsystem shall be capable of performing its functions before, during, and for an adequate time after being subjected to the environmental conditions associated with normal plant operation, abnormal plant operation, and design basis events.

7.2.3.4 Design Description

Each reactor module has a separate and independent Investment Protection Subsystem.

The investment protection function is implemented on a per reactor basis with a remote multiplexed, microprocessor-based modular protection system. The protection system architecture consists of multiple optical digital data highways from the local multiplex units communicating with four centrally located, separate, redundant computers to implement the four-channel protection subsystem for each reactor module.

Each Investment Protection Subsystem consists of five supporting trip subsystems. Each trip subsystem consists of four separate (redundant) instrument channels and redundant two-out-of-four coincidence solid-state logic to initiate a protective action. Each instrument channel includes the field-mounted sensors, electronic signal conditioning equipment, and electronic trip setpoint comparator to provide a trip signal when the process variable value reaches the trip setpoint. The two-out-of-four coincidence logic circuitry provides a protective action initiation signal when any two or more separate instrument channels reach the trip setpoint. The protective action initiation signal is sent to separate and redundant actuation devices.

The boundaries of the Investment Protection Subsystem are generally from, and including, the sensors to the input of the actuation devices.

The Investment Protection Subsystem operator interfaces are located in the PPIS equipment room in the Reactor Building and the remote shutdown area in the Reactor Service Building. The operator interfaces include color video displays, function input devices, and keyboards. In addition, data on the Investment Protection Subsystem are transmitted through a unidirectional isolator to the Data Management Subsystem for display by the Plant Supervisory Control Subsystem in the main control room. The remote shutdown area operator interfaces provide the reactor operators with the capability of initiating investment protection trip actions and taking the necessary actions to shut down the plant from a position remote from the main control room. No manual inputs to the Investment Protection Subsystem are provided in the main control room.

7.2.3.4.1 Subsystem Configuration

The Investment Protection Subsystem is composed of the following subsystems for each reactor module:

1. Reactor Trip Using Inner Control Rods

   The reactor trip using the inner control rods acts as a "nonsafety-related" reactor trip for use during reactor startup and rise to power maneuvering. This subsystem initiates a rapid reduction in reactor power following the receipt of a reactor trip signal from the "safety-related" outer control rod reactor trip subsystem. The inner control rod reactor trip is inhibited by an automatic operating bypass once all six inner control rods are full out and one bank of three outer control rods are full out. This operating bypass reduces the investment risk to the inner control rods of possible exposure to elevated conduction cooldown temperatures. The manual reactor trip initiation is located in the circuitry downstream of the bypass and as such it overrides the bypass. A simplified one-channel block diagram of the Inner Control Rod Reactor Trip Subsystem is shown in Figure 7.2-7.

2. Shutdown Cooling System Initiation

The Shutdown Cooling System Initiation Subsystem starts the Shutdown Cooling System upon loss of main loop cooling.

The Shutdown Cooling System Initiation Subsystem trip inputs, each derived from four separate and redundant channels, are:

a. Main loop shutdown (to start the Shutdown Cooling System)

b. Manual initiation (to provide independent backup to automatic trip systems)

A simplified one-channel block diagram of the Shutdown Cooling System Initiation Subsystem is shown in Figure 7.2-8.

3. Steam Generator Isolation and Dump

This subsystem limits the quantity of water that can leak into the reactor vessel because of a steam generator tube leak, limiting damage to the reactor core and protecting the vessel pressure boundary.

Upon detection of high moisture concentration in the primary coolant, the steam generator isolation and dump subsystem automatically initiates a main loop shutdown and automatically opens the steam generator dump valves to allow its secondary coolant inventory to be rapidly dumped. The protection is completed when all isolation valves are closed, and the dump valves have cycled open sufficiently to reduce steam generator pressure to slightly above primary coolant pressure, and then the dump valves are closed.

The trip inputs to the steam generator isolation and dump subsystem are high primary coolant moisture concentration and manual initiation. Four separate and redundant primary coolant loop moisture measurement signals are provided by the investment protection moisture monitors.

The steam generator isolation and dump actuated equipment includes the steam generator dump valves and the main loop shutdown actuated equipment.

A simplified one-channel block diagram of the steam generator isolation and dump subsystem is shown in Figure 7.2-9.

4. Primary Coolant Pressure Pumpdown

The primary coolant pressure pumpdown subsystem starts a controlled pressure pumpdown of the primary helium coolant through the Helium Purification Subsystem following detection of a primary coolant leak and subsequent reactor trip. This primary coolant pumpdown reduces investment risk by limiting the release of radioactive helium into the Reactor Building. The trip inputs to this subsystem are primary coolant pressure low <u>and</u> Reactor Building radiation high, and manual initiation.

A simplified one-channel block diagram of the primary coolant pressure pumpdown subsystem is shown in Figure 7.2-10.

7.2.3.4.2 Subsystem Arrangement

The Investment Protection Subsystem is arranged into modular electronic components with four separate channels. Each of the four Standard MHTGR reactor modules has a separate four channel Investment Protection Subsystem. The components for each reactor module are associated with that reactor module. The Investment Protection Subsystem operator interface equipment is provided by the Special Nuclear Area Instrumentation Subsystem and is located in the PPIS equipment room, and remote shutdown area. These functional components of the Plant Protection and Instrumentation System and their locations are shown in Figure 7.2-5.

7.2.3.4.3 Subsystem Operating Modes

The Investment Protection Subsystem is operable during all plant modes. The status of the plant is monitored at all times and trip actions are initiated as required. Continual surveillance of the Investment Protection Subsystem is performed automatically through self-diagnostic routines and abnormal conditions are indicated. Portions of the subsystem may be bypassed for surveillance, testing, and maintenance; however, because of the subsystem's redundancy this does not necessitate loss of the protective function. The sense and command two-out-of-four coincidence logic automatically reverts to two-out-of-three coincidence logic when one channel is bypassed for maintenance.

Shutdown of the entire Investment Protection Subsystem is generally not required to perform maintenance because of the redundancy of the channels. Inadvertent shutdowns of redundant portions of the Investment Protection Subsystem can result in unprotected plant operation due to the characteristics of the design.

The Investment Protection Subsystem is designed not to adversely affect plant availability in the event of a single failure. Therefore, a single failed component of input channel will not cause an unwanted (spurious) subsystem trip nor prevent a required one.

The cause for spurious channel trips will be determined, corrected, and the channel reset in a timely fashion. Continued plant operation with an input channel in a tripped condition is undesirable because a second channel trip will result in an unwanted subsystem trip. The two-out-of-four coincidence logic allows the maintenance bypass of one spuriously tripped channel. In this case the logic reverts to two-out-of-three coincidence logic and a degree of redundancy of one is maintained. The Investment Protection Subsystem may be operated in a degraded condition as long as a degree of redundancy of one is maintained.

7.2.3.4.4 Subsystem Limitations

Trip setpoints are established conservatively to assure that component damage limits are not reached. Figure 7.2-6 illustrates the relationship between trip setpoints and damage limits, and analysis trip levels used in DBE and SRDC analysis. The limiting system settings conservatively bound component damage thresholds so that if the limiting system setting is reached, automatic protective action corrects the abnormal situation before the damage threshold is exceeded. The limiting system setting considers sensor calibration errors, instrument accuracy, and transient overshoot. The actual system settings (trip setpoints), are bounded conservatively by the limiting system settings considering allowance for instrument and setpoint drift. The lower setpoint limit is specified to prevent unneccessary system trips during normal operating transients. The actual system setting is the trip setpoint specified in the system operation and maintenance procedures.

The analysis trip levels and trip setpoints (actual system settings) for the Investment Protection Subsystem are shown in Table 7.2-8.

Dynamic transient analysis has been performed at an analysis trip level. The actual protection system setting (nominal trip setpoint) is below this analysis trip level, as shown in Figure 7.2-6, and reflects allowances for calibration errors, instrument accuracy, transient overshoot, instrument and setpoint drift, etc.

7.2.3.5 Design Evaluation

7.2.3.5.1 Failure Modes and Effects

The Investment Protection Subsystem is redundant and single failure proof. Therefore, failure of one component does not prevent the ability of the system to respond correctly when required. Failures within the subsystem are either alarmed immediately or become apparent during the routine surveillance and testing of the subsystem.

Design features are included to help the operator verify that Investment Protection Subsystem degree of redundancy of at least one is always maintained. For example, whenever any essential protection system component is bypassed, such that a protection channel is inoperable, a continuous protection system bypass indication/alarm is displayed in the remote shutdown area and in the main control room. Whenever one protection channel of the two-out-of-four logic is disconnected or bypassed, a degree of redundancy of one is maintained. Whenever a one-out-of-two actuation device is disconnected or bypassed, the time of inoperability will be kept to a minimum and will be within acceptable protection system reliability analysis constraints.

Whenever the two-out-of-four logic protection system is operated with one channel tripped (i.e., the remaining channels in a one-out-of-three operating mode) extreme care will be exercised to avoid the introduction of spurious signals which could cause a spurious trip signal and subsequent impact on plant availability.

The Investment Protection Subsystem is designed to fail into a safe state (or into a state demonstrated to be acceptable) on conditions such as disconnection of the system, loss of energy, and loss of HVAC.

Portions of the subsystem, where power is required to perform an action and it is potentially detrimental to the plant availability to spuriously initiate such actions (i.e., isolate main cooling loop), utilize transmission logic (energize to initiate action). This means the subsystem requires power to initiate protective action and no action occurs on loss of power or loss of signal.

7.2.3.5.2 Steady-State Performance

The required steady-state performance of the Investment Protection Subsystem is to remain operable during all plant operating modes and to monitor various plant parameters to detect abnormal plant conditions and perform protective action to limit investment risk.

7.2.3.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. In this section only the response of the Investment Protection Subsystem to AOOs is described. A summary of the AOO trip functions of the Investment Protection Subsystem is shown in Table 7.2-3.

AOO-1(A) Loss of Main Loop Cooling. After receiving a main loop shutdown signal, the Investment Protection Subsystem initiates shutdown cooling.

AOO-1(B) Loss of Offsite Power and Turbine Trip. The Investment Protection Subsystem response to AOO-1(B) is identical to AOO-1(A).

AOO-1(C) Spurious Reactor Trip With Cooling on HTS. The Investment Protection Subsystem has no response to AOO-1(C) other than to continue to be operable.

AOO-1(D) Main Loop Transient Without Reactor Trip. The Investment Protection Subsystem has no response to AOO-1(D) other than to continue to be operable.

AOO-2 Loss of Main Loop Cooling and Shutdown Cooling. The Investment Protection Subsystem has no response to AOO-2 other than continue to be operable.

AOO-3 Rod Withdrawal with Reactor Trip and Cooling on HTS. The Investment Protection Subsystem has no response to AOO-3 other than to continue to be operable.

AOO-4 Small Steam Generator Leak. The moisture monitor detects high primary coolant moisture concentration which causes reactor trip using the outer control rods and steam generator isolation and dump. The reactor trip signal is commanded by the Safety Protection Subsystem. Steam generator isolation is performed by a main loop shutdown command. The steam generator dump valves open, the steam generator inventory is emptied into a dump tank, and the dump valves close. After receiving the main loop shutdown signal, the Investment Protection Subsystem initiates shutdown cooling.

AOO-5 Small Primary Coolant Leak. When the primary coolant pressure decreases to the low setpoint and high Reactor Building radiation is detected the Helium Purification System is commanded to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. Upon receipt of a main loop shutdown signal, the Investment Protection Subsystem initates shutdown cooling.

7.2.3.5.4 Design Basis Event Performance

Design basis events (DBEs) are described in Chapter 15. In this section only the response of the Investment Protection Subsystem to DBEs is described. A summary of DBE trip functions of the Investment Protection Subsystem is shown in Table 7.2-4.

DBE-1 Loss of HTS and SCS Cooling. The initiating event for DBE-1 is loss of offsite power and turbine trip. A loss of offsite power and turbine trip causes a loss of all primary ac power supplies. This causes the main loop helium circulator to coast down because of loss of power. Main loop shutdown signals for Shutdown Cooling System initiation but the SCS fails to start due to failure of standby ac power.

DBE-2 HTS Transient Without Control Rod Trip. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch which causes a main loop shutdown. Main loop shutdown signals for Shutdown Cooling System (SCS) initiation.

DBE-3 Rod Withdrawal Without HTS Cooling. The initiating event for DBE-3 is an inadvertent control rod bank withdrawal. DBE-3 also includes a main loop upset. Main loop shutdown signals for Shutdown Cooling System initiation.

DBE-4 Rod Withdrawal Without HTS and SCS Cooling. The response of the Investment Protection Subsystem to DBE-4 is identical to DBE-3 but DBE-4 also includes SCS failure to start.

DBE-5 Earthquake. The initiating event for DBE-5 is a 0.3 g earthquake. It is assumed that the main cooling loop is upset. Main loop shutdown signals for Shutdown Cooling System initiation.

The Investment Protection Subsystem and its auxiliary supporting features are designed to withstand a 0.3 g earthquake and perform their functions.

DBE-6 Moisture Inleakage. The initiating event for DBE-6 is a steam generator offset tube rupture and subsequent large moisture ingress rate.

The moisture monitor detects high primary coolant moisture concentration which causes reactor trip using the outer control rods and steam generator isolation and dump. The reactor trip signal is commanded by the Safety Protection Subsystem. Steam generator isolation is performed as a main loop shutdown. The steam generator dump valves open, the steam generator inventory is emptied into a dump tank, and the dump valves close. Main loop shutdown also signals for Shutdown Cooling System initiation.

DBE-7 Moisture Inleakage Without SCS Cooling. The response of the Investment Protection Subsystem to DBE-7 is identical to DBE-6 but DBE-7 also includes SCS failure to start.

DBE-8 Moisture Inleakage With Moisture Monitor Failure. The initiating event for DBE-8 is a small steam generator leak and subsequent small moisture ingress rate. The moisture monitor is assumed to fail to detect the moisture ingress. The reactor operator performs a manual initiation of steam generator isolation and dump from the PPIS operator interface located in the remote shutdown area.

Steam generator isolation is performed as a main loop shutdown. The steam generator dump valves open, the steam generator inventory is emptied into a dump tank, and the dump valves close. Main loop shutdown also signals for Shutdown Cooling System initiation.

DBE-9 Moisture Inleakage With Steam Generator Dump Failure. The initiating event for DBE-9 is a small steam generator leak and subsequent small moisture ingress rate. The moisture monitor detects high primary coolant moisture concentration which causes a reactor trip using the outer control rods and steam generator isolation and dump. The reactor trip is commanded by the

Safety Protection Subsystem. Steam generator isolation is performed as a main loop shutdown. The steam generator dump valves open and the steam generator inventory is emptied into a dump tank. DBE-9 assumes the steam generator dump valves fail to reclose. Main loop shutdown also signals for Shutdown Cooling System initiation.

DBE-10 Primary Coolant Leak. The initiating event for DBE-10 is a moderate primary coolant leak which causes a rapid depressurization of the primary coolant. When the primary coolant pressure decreases to the low setpoint and high Reactor Building radiation is detected the Helium Purification System is commanded to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. This pumpdown is assumed to be ineffective because of the size of the primary coolant leak. When a main loop shutdown is initiated, the SCS is commanded to start.

DBE-11 Primary Coolant Leak Without HTS and SCS Cooling. The initiating event for DBE-11 is a small primary coolant leak and subsequent slow primary coolant depressurization. This DBE assumes that the main cooling loop is upset 15 hours into the DBE.

Main loop shutdown signals for SCS initiation.

When the primary coolant pressure decreases to the low setpoint and high Reactor Building radiation is detected the Helium Purification Subsystem is commanded to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant.

7.2.3.6 Interfaces

Interface requirements imposed on other systems or subsystems by the Investment Protection Subsystem are identified in Table 7.2-9, which also includes a description of the interface and a quantitative expression for the interface.

TABLE 7.2-1

SCOPE OF THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM

Safety Protection Subsystem	Special Nucler Area Instrumentation	Investment Protection Subsystem
Reactor trip using outer control rods	Vessel System pressure relief block valve closure interlock	Reactor trip using inner control rods
Reactor trip using reserve shutdown control equipment	Safety protection information displays	Steam generator isolation and dump
Main loop shutdown	Investment protection information displays	Shutdown cooling system initiation
	Post-accident monitoring instrumentation and displays	Primary coolant pressure pumpdown

TABLE 7.2-1A
SAFETY PROTECTION SUBSYSTEM SENSE, COMMAND AND EXECUTE FEATURES

PROTECTIVE ACTION	SENSORS	COMMAND LOGIC	EXECUTE LOGIC	ACTUATED EQUIPMENT
Reactor Trip Using Outer Control Rods	4 independent Neutron Flux Channels ("safety-related") 4 independent Helium Mass Flow Channels ("safety-related") 4 independent Primary Coolant Pressure Channels ("safety-related") 4 independent Primary Coolant Moisture Concentration Channels (not "safety-related") 4 independent Main Loop Trip Signals (not "safety-related") 4 independent Steam Generator Inlet Helium Temperature Channels (not "safety-related") 4 independent Manual Initiation Inputs (not "safety-related")	2-out-of-4 coincidence logic	Dual 2-out-of-4 (one 2-out-of-4 matrix of electrical contactors in outer control rod holding power line and another 2-out-of-4 matrix of electrical contactors in return line)	Independent control rods located in outer reflector

TABLE 7.2-1A (Cont)

PROTECTIVE ACTION	SENSORS	COMMAND LOGIC	EXECUTE LOGIC	ACTUATED EQUIPMENT
Reactor Trip Using Reserve Shutdown Control Equipment	4 independent Neutron Flux Channels (these are the same "safety-related" Neutron Flux Channels used for the reactor trip using the outer control rods) 4 independent Circulator Speed Channels ("safety-related") 4 independent Primary Coolant Pressure Channels (these are the same "safety-related" Primary Coolant Pressure Channels used for the reactor trip using the outer control rods) 4 independent Manual Initiation Inputs (not "safety-related")	2-out-of-4 coincidence logic	1-out-of-2 coincidence logic (2 fusible links for each RSCE mechanism, each powered by a separate and independent Essential DC Electrical system channel	2 independent hoppers of reserve shutdown material located in each of the 6 inner neutron control assemblies

TABLE 7.2-1A (Cont)

PROTECTIVE ACTION	SENSORS	COMMAND LOGIC	EXECUTE LOGIC	ACTUATED EQUIPMENT
Main Loop Shutdown	4 independent Primary Coolant Pressure Channels (these are the same "safety-related" Primary Coolant Pressure Channels used for the reactor trip using the outer control rods) 4 independent Circulator Speed Channels (these are the same "safety-related" channels used for the reactor trip using the RSCE) 4 independent Feedwater Flow Channels (not "safety-related") 4 independent Main Steam Temperature Channels (not "safety-related") 4 independent Steam Generator Isolation and Dump Signals (not "safety-related") 4 independent Manual Initiation Inputs (not "safety-related")	2-out-of-4 coincidence logic	1-out-of-2 coincidence logic	2 independent circulator motor electrical contactors 2 independent super-heater outlet block valves 2 independent feed-water block valves

TABLE 7.2-2

SAFETY PROTECTION SUBSYSTEM ANALYSIS TRIP LEVELS AND SETPOINTS

	Analysis Trip Level	Nominal Setpoint (Actual Protection System Setting)
Reactor Trip Using Outer Control Rods		
Neutron flux (%) to helium mass flow (%) ratio	1.50	1.40
Primary coolant pressure - high	7.07 MPa (1025 psia)	7.00 MPa (1015 psia)
Primary coolant pressure - low	5.69 MPa (825 psia)	5.76 MPa (835 psia)
and		
Neutron Flux - greater than	12%	10%
Steam generator helium inlet temperature	760°C (1400°F)	746°C (1375°F)
Primary coolant moisture concentration	1200 ppmv	1000 ppmv
Reactor Trip Using Reserve Shutdown System		
Neutron flux (%) to circulator speed (%) ratio	1.90 and 50 sec time delay	1.80 and 30 sec time delay
Primary coolant pressure	7.07 MPa (1025 psia)	7.00 MPa (1015 psia)
Main Loop (HTS) Shutdown		
Primary coolant pressure - high	7.07 MPa (1025 psia)	7.00 MPa (1015 psia)
Circulator speed (high or low compared to nominal circulator speed programmed by feedwater flow)	±1487 rpm	±1144 rpm
Primary coolant pressure	4.31 MPa (625 psia)	4.41 MPa (640 psia)
and		
Main steam temperature	385°C (725°F)	393°C (740°F)

TABLE 7.2-3

PLANT PROTECTION AND INSTRUMENTATION SYSTEM AOO PERFORMANCE

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
AOO-1(A) Loss of Main Loop Cooling	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals for outer control rod reactor trip and Shutdown Cooling System initiation)		
AOO-1(B) Loss of Offsite Power and Turbine Trip	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation

TABLE 7.2-3 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
AOO-1(B) (Cont.)	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals for outer control rod reactor trip and Shutdown Cooling System initiation)		
AOO-1(C) Spurious Reactor Trip with Cooling on HTS	None	None	None	None
AOO-1(D) Main Loop Transient Without Reactor Trip	None	None	None	None

TABLE 7.2-3 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
AOO-2 Loss of Main Loop Cooling and Shutdown Cooling	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	None	None
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals for outer control rod reactor trip and Shutdown Cooling System initiation)		
AOO-3 Rod Withdrawal With Reactor Trip and Cooling on HTS	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	None	None
AOO-4 Small Steam Generator	Primary coolant moisture - high	Reactor trip (outer control rods)	Primary coolant moisture - high	Steam generator isolation and dump leak

TABLE 7.2-3 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
A00-4 (Cont.)	Steam generator isolation and dump	Main loop shutdown (which in turn signals for outer control rod reactor trip and Shutdown Cooling System initiation)	Main loop shutdown	Shutdown Cooling System initiation
A00-5 Small Primary Coolant Leak	Primary coolant pressure-low	Reactor trip (outer control rods)	Primary coolant pressure - low and Reactor building radiation - high	Primary coolant pumpdown
	Primary coolant pressure - low and Main steam temperature - not low	Main loop shutdown (which in turn signals for outer control rod reactor trip and Shutdown Cooling System initiation	Main loop shutdown	Shutdown Cooling System initiation

TABLE 7.2-4

PLANT PROTECTION AND INSTRUMENTATION SYSTEM DBE PERFORMANCE

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-1 Loss of HTS and SCS Cooling	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		
DBE-2 HTS Transient Without Control Rod Trip	Neutron flux to circulator speed ratio - high	Reactor trip (Reserve Shutdown Control Equipment)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		

TABLE 7.2-4 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-3 Rod Withdrawal Without HTS Cooling	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		
DBE-4 Rod Withdrawal Without HTS and SCS Cooling	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		

TABLE 7.2-4 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-5 Earthquake	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		
DBE-6 Moisture Inleakage	Primary coolant moisture - high	Reactor trip (outer control rods)	Primary coolant moisture - high	Steam generator isolation and dump
	Steam generator isolation and dump	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)	Main loop shutdown	Shutdown Cooling System initiation

TABLE 7.2-4 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-7 Moisture Inleakage Without SCS Cooling	Primary coolant moisture - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
	Steam generator isolation and dump	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)	Primary coolant moisture - high	Steam generator isolation and dump
DBE-8 Moisture Inleakage with Moisture Monitor Failure	Primary coolant pressure - high	Reactor trip (outer control rods)	Main loop shutdown	Shutdown Cooling System initiation
		Reactor trip (Reserve Shutdown Control Equipment)	Manual input	Steam generator isolation and dump
		Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)		

TABLE 7.2-4 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-9 Moisture Inleakage With Steam Generator Dump Failure	Primary coolant moisture-high	Reactor trip (outer control rods)	Primary coolant moisture-high	Steam generator isolation and dump
	Steam generator isolation and dump	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)	Main loop shutdown	Shutdown Cooling System initiation
DBE-10 Primary Coolant Leak	Primary coolant pressure-low	Reactor trip (outer control rods)	Primary coolant pressure-low and Reactor building radiation-high	Primary coolant pumpdown
	Primary coolant pressure-low and Main steam temperature - not low	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)	Main loop shutdown	Shutdown Cooling System initiation

TABLE 7.2-4 (Cont)

	Safety Protection Subsystem		Investment Protection Subsystem	
	Trip Parameter	Protective Action	Trip Parameter	Protective Action
DBE-11 Primary Coolant Leak Without HTS and SCS Cooling	Primary coolant pressure - low	Reactor trip (outer control rods	Main loop shutdown	Shutdown Cooling System initiation
	Circulator speed to feedwater flow mismatch	Main loop shutdown (which in turn signals an outer control rod reactor trip and Shutdown Cooling System initiation)	Primary coolant pressure - low and Reactor building radiation - high	Primary coolant pumpdown

TABLE 7.2-5
SAFETY PROTECTION SUBSYSTEM SRDC PERFORMANCE

	Trip Parameter	Protective Action
SRDC-1 Pressurized conduction cooldown	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-2 Pressurized conduction cooldown without control rod trip	Neutron flux to circulator speed ratio - high	Reactor trip (Reserve Shutdown Control Equipment)
SRDC-3 Pressurized conduction cooldown with control rod withdrawal	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-4 Pressurized conduction cooldown with control rod withdrawal	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-5 Pressurized conduction cooldown with earthquake	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-6 Depressurized conduction cooldown with moderate moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown
SRDC-7 Depressurized conduction cooldown with moderate moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown

TABLE 7.2-5 (Cont)

	Trip Parameter	Protective Action
SRDC-8 Depressurized conduction cooldown with small moisture ingress	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown
SRDC-9 Depressurized conduction cooldown with small moisture ingress	No "safety-related" trip required	
SRDC-10 Depressurized conduction cooldown with moderate primary coolant leak	Primary coolant pressure - low	Reactor trip (outer control rods)
SRDC-11 Depressurized conduction cooldown with small primary coolant leak	Primary coolant pressure - low	Reactor trip (outer control rods)

TABLE 7.2-5
SAFETY PROTECTION SUBSYSTEM SRDC PERFORMANCE

	Trip Parameter	Protective Action
SRDC-1 Pressurized conduction cooldown	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-2 Pressurized conduction cooldown without control rod trip	Neutron flux to circulator speed ratio - high	Reactor trip (Reserve Shutdown Control Equipment)
SRDC-3 Pressurized conduction cooldown with control rod withdrawal	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-4 Pressurized conduction cooldown with control rod withdrawal	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-5 Pressurized conduction cooldown with earthquake	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
SRDC-6 Depressurized conduction cooldown with moderate moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown
SRDC-7 Depressurized conduction cooldown with moderate moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown

TABLE 7.2-5 (Cont)

	Trip Parameter	Protective Action
SRDC-8 Depressurized conduction cooldown with small moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown
SRDC-9 Depressurized conduction cooldown with small moisture ingress	Neutron flux to helium mass flow ratio - high	Reactor trip (outer control rods)
	Primary coolant pressure - high	Reactor trip (outer control rods) Reactor trip (Reserve Shutdown Control Equipment) Main loop shutdown
SRDC-10 Depressurized conduction cooldown with moderate primary coolant leak	Primary coolant pressure - low	Reactor trip (outer control rods)
SRDC-11 Depressurized conduction cooldown with small primary coolant leak	Primary coolant pressure - low	Reactor trip (outer control rods)

TABLE 7.2-6

IDENTIFICATION OF INTERFACES FOR SAFETY PROTECTION SUBSYSTEM

Interfacing Systems	Nature of Interface	Interface Requirements
Reactor System (Neutron Control Subsystem)	Provide control rod drive mechanism to act as the safety system actuated equipment for the reactor trip subsystem.	Quantity: One control rod mechanism for each outer control rod. One redundant actuated reserve shutdown mechanism in each inner rod drive mechanism assembly. Physical Interface: Function only.
	Provide for installation of control rod holding coil current relay/contactors in both sides of the current loop to act as the actuation devices for the reactor trip subsystem.	Quantity: Two two-out-of-four logic matrices. Physical Interface: Electrical signals.
	Provide neutron detector safety system sensor channel input to the reactor trip subsystem.	Quantity: Twelve neutron flux detectors required, arranged in four independent channels to measure reactor power. Physical Interface: Electrical signals.

TABLE 7.2-6 (Continued)

Interfacing Systems	Nature of Interface	Interface Requirements
Reactor System (Cont.)		Location: Twelve sensors required (three sensors/channel), located in six equally spaced wells in the reactor vessel cavity. The two sensors in each well will be located in the top half and the bottom half of the well.
	Provide for automatic control of reactor trip using reserve shutdown control equipment	Quantity: Two fuse link release signals. Physical Interface: Electrical signals.
Heat Transport System (Main Circulator Subsystem)	Provide for installation of separate safety system circulator speed sensors in the circulator.	Quantity: Four circulator speed sensors. Physical Interface: Electrical signals.
	Provide for PPIS circulator trip contactors as output actuation for main loop shutdown.	Quantity: Two (redundant) per main circulator. Physical Interface: Electrical signals.

TABLE 7.2-6 (Continued)

Interfacing Systems	Nature of Interface	Interface Requirements
(Steam Generator Subsystem)	Provide for installation of protection system sensors to measure primary coolant parameters.	Quantity: Four pressure transmitters to measure primary coolant pressure. Four core differential pressure transmitters. (The measurement is used in calculating main loop helium mass flow.) Physical Interface: Pipe connection.
	Provide steam generator penetrations to accommodate Safety Protection Subsystem sensors.	Quantity: Four thermowell access penetrations in the circulator outlet duct. Physical Interface: Steam generator penetrations.
Plant Control, Data, and Instrumentation System (NSSS Control Subsystem)	Adjust control system settings following trips.	Quantity: Two (reactor trip outer rods and reactor trip reserve shutdown). Physical Interface: Electrical signals.

TABLE 7.2-6 (Continued)

Interfacing Systems	Nature of Interface	Interface Requirements
Plant Control, Data, and Instrumentation System (Data Management Subsystem)	Transmit Safety Protection Subsystem status data to Plant Supervisory Control Subsystem.	Quantity: Four independent digital data channels per reactor module. Physical Interface: Electrical signals
(Plant Supervisory Control Subsystem)	Display Safety Protection Subsystem status data in main control room.	Quantity: Redundant displays in main control room. One display continuously displays Safety Protection Subsystem status data. Physical Interface: Data signals received from Data Management Subsystem.
Power Conversion Group (Feedwater and Condensate Subsystem)	Provide for installation of feedwater flow transmitters monitoring the steam generator feedwater inlet line to act as an input sensor channel to the Safety Protection Subsystem.	Quantity: Four feedwater flow transmitters monitoring the steam generator feedwater inlet pipe. Physical Interface: Electrical signals.

TABLE 7.2-6 (Continued)

Interfacing Systems	Nature of Interface	Interface Requirements
(Main and Bypass Steam Subsystem)	Provide for installation of thermowell assemblies in the superheater outlet lines to act as an input sensor channel to the Safety Protection Subsystem.	Quantity: Four resistance thermometers in the superheater outlet pipe. Physical Interface: In pipe thermowell.
Vessel System	Provide two feedwater block valves in the steam generator inlet pipe to act as actuated equipment for the main loop shutdown subsystem.	Quantity: The two feedwater block valves per steam generator. Physical Interface: Electrical signals.
	Provide superheater outlet valves in the steam generator outlet pipe to act as actuated equipment for the main loop shutdown subsystem.	Quantity: Two superheater outlet valves for the steam generator. Physical Interface: Electrical signals.

TABLE 7.2-6 (Continued)

Interfacing Systems	Nature of Interface	Interface Requirements
Buildings, Structures, and Building Service Group (Reactor Building)	Provide building space and structural support to accommodate Safety Protection Subsystem equipment.	Quantity: Eight cabinets. Physical Interface: Floor mounting.
Mechanical Service Group (HVAC)	Provide HVAC to support the normal operation of the Safety Protection Subsystem.	Quantity: Two. Physical Interface: None.
Electrical Group (Class 1E Uninterruptible Power Supply)	Provide separate Class 1E uninterruptible power distribution channels to power the Safety Protection Subsystem.	Quantity: Four separate Class 1E sources. Physical Interface: Electric feeders.

TABLE 7.2-7

IDENTIFICATION OF INTERFACES FOR THE SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM

(Given on a per reactor module basis)

Interfacing Systems	Nature of Interface	Interface Requirements
Reactor System (Neutron Control Subsystem)	Provide signals to indicate when the control rod is fully inserted into the reactor core to act as a sensor input to the Special Nuclear Area Instrumentation.	Quantity: One per control rod drive. Physical Interface: Electrical signals.
	Provide signals to indicate when the reserve shutdown hopper gate is opened to act as a sensor input to the Special Nuclear Area Instrumentation.	Quantity: One per reserve shutdown mechanism. Physical Interface: Electrical signals.
Vessel System (Pressure Relief Subsystem)	Provide signals from pressure relief block valves to indicate when either valve is not in the full	Quantity: Two (redundant) and electrically separate limit switches from each pressure relief valve.

TABLE 7.2-7 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Vessel System (Cont.)	open position. This signal acts as an input to the pressure relief block valve closure interlock.	Physical Interface: Electrical signals.
	Provide the capability of accepting a signal from the pressure relief block valve closure interlock to the block valve motor current relay/contactor to prevent the closure of one block valve if the other block valve is not fully open.	Quantity: Redundant relay contacts for each relief block valve control circuit. Physical Interface: Electrical signals.
	Provide signals from each pressure relief valve to the Special Nuclear Area Instrumentation to indicate if the relief valve is not fully closed.	Quantity: Two (redundant) per valve. Physical Interface: Electrical signals.

TABLE 7.2-7 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
(Vessel and Duct Subsystem)	Provide status and bypass signals to the Special Nuclear Area Instrumentation Subsystem Information displays.	Quantity: Eight Physical Interface: Electrical signals.
Reactor Service System (Essential Cooling Water, Gaseous Radioactive Waste, and Helium Purification)	Provide for status signals of those essential systems which support the moisture monitors to act as input to the Special Nuclear Area Instrumentation Subsystem information displayed.	Quantity: Six. Physical Interface: Electrical signals.
Heat Transport System (Main Circulator Subsystem)	Provide sensor signals to indicate the status of the main loop shutoff valve to act as an input to the Special Nuclear Area Instrumentation Subsystem information displays.	Quantity: Two (redundant) main loop shutoff valves. Physical Interface: Electrical signals.

TABLE 7.2-7 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Shutdown Cooling System (Shutdown Heat Removal Control Subsystem)	Provide information, trip status, and bypass status to the Special Nuclear Area Instrumentation Subsystem information displays.	Quantity: Four. Physical Interface: Electrical signals.
Miscellaneous Control and Instrumentation Group (Radiation Monitoring and and Meteorological Monitoring Subsystems)	Provide information, trip status, and bypass status to the Special Nuclear Area Instrumentation Subsystem information displays.	Quantity: Twelve. Physical Interface: Electrical signals.
Power Conversion Group (Steam and Water Dump Subsystem)	Provide status and bypass signals to the Special Nuclear Area Instrumentation Subsystem information displays.	Quantity: Eight Physical Interface: Electrical signals.

TABLE 7.2-7 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Buildings, Structures, and Building Service Group (70) (Reactor Building)	Provide building space and structural support to accommodate Special Nuclear Area Instrumentation Subsystem equipment.	Quantity: Eight cabinets. Physical Interface: Floor mounting.
Mechanical Service Group (HVAC)	Provide HVAC to support the normal operation of the Special Nuclear Area Instrumentation Subsystem	Quantity: Two. Physical Interface: None.
Electrical Group (Class 1E Uninterruptible Power Supply)	Provide separate Class 1E uninterruptible power distribution channels to power the Special Nuclear Area Instrumentation Subsystem as a 1E associated circuit.	Quantity: Two separate Class 1E sources. Physical Interface: Electric Feeders.
	Provide status and bypass sensors for all Class 1E	Quantity: Sixteen.

TABLE 7.2-7 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Electrical Group (Cont.)	power buses to act as an input signals to the Special Nuclear Area Instrumentation Subsystem information displays.	Physical Interface: Electrical signals.

TABLE 7.2-8
INVESTMENT PROTECTION SUBSYSTEM ANALYSIS TRIP LEVELS AND SETPOINTS

	Analysis Trip Level	Nominal Setpoint (Actual Protection System Setting
Steam Generator Isolation And Dump		
Primary coolant moisture concentration	1200 ppmv	1000 ppmv
Superheater steam pressure to primary coolant pressure (for steam generator dump termination)	344 kPa (50 psid)	517 kPa (75 psid)
Primary Coolant Pressure Pumpdown (with Helium Purification System)		
Primary coolant pressure	5.5 MPa (800 psia)	5.5 MPa (810 psia)
Reactor Building radiation	[TBD] mr/hr	[TBD] mr/hr

TABLE 7.2-9

IDENTIFICATION OF INTERFACES FOR THE INVESTMENT PROTECTION SUBSYSTEM

(Given on a per reactor module basis)

Interfacing Systems	Nature of Interface	Interface Requirements
Plant Control, Data, and Instrumentation System (Data Management Subsytem)	Transmit Safety System Information display data, Investment Protection Information display data, and post-accident monitoring display data to Plant Supervisory Control Subsystem.	Quantity: Two independent digital data channels per reactor module. Physical Interface: Electrical signals
(Plant Supervisory Control Subsystem)	Display Safety System Information, Investment Protection Information, and post-accident monitoring data in main control room.	Quantity: Redundant displays in main control room. At least one continuously displayed. Physical Interface: Data signals received from Data Management Subsystem.
Reactor System (Neutron Control Subsystem)	Provide control rod drive mechanisms to act as the actuated equipment for the reactor trip subsystem.	Quantity: One control rod mechanism for each inner control rod. Physical Interface: Function only.

TABLE 7.2-9 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Reactor Service System (Helium Purification Subsystem)	Provide reprocessing of primary helium coolant extracted by the moisture monitors.	Quantity: One sample line per module. Physical Interface: Piping.
	Provide primary coolant system pumpdown upon receipt of initiation signal.	Quantity: Redundant initiation signals. Physical Interface: Electrical signals.
(Reactor Plant Cooling Water Subsystem)	Provide cooling water to the moisture monitors.	Quantity: Two coolers per module. Physical Interface: Piping.
(Gaseous Radioactive Waste Subsystem)	Provide gaseous radioactive waste management for the moisture monitors.	Quantity: One waste line per module. Physical Interface: Piping.
Heat Transport System (Main Circulator Subsystem)	Provide for installation of moisture sample rake at the outlet of main circulator.	Quantity: Four independent sample rakes. Physical Interface: Piping.

TABLE 7.2-9 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
(Steam Generator Subsystem)	Provide for installation of protection system sensors to measure primary coolant parameters.	Quantity: Four low range pressure transmitters to measure primary coolant pressure for use in steam generator dump termination. Physical Interface: Piping.
	Provide steam generator penetrations to accommodate Investment Protection Subsystem sensors.	Quantity: Four steam generator inlet duct thermowell access penetrations. Physical Interface: Steam generator penetrations.
Plant Control, Data, and Instrumentation System (NSSS Control Subsystem)	Adjust control system settings following investment protection trips.	Quantity: Five (reactor trip-inner rods, main loop shutdown, SG isolation and dump, SCS initiation, and primary pressure pumpdown). Physical Interface: Electrical signals.

TABLE 7.2-9 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
(Data Management Subsystem)	Transmit Investment Protection Subsystem data to Plant Supervisory Control Subsystem.	Quantity: Four independent digital data channels per reactor module. Physical Interface: Electrical signals
(Plant Supervisory Control Subsystem)	Display Investment Protection Subsystem status data in main control room.	Quantity: Redundant displays in main control room. At least one continuously displayed. Physical Interface: Data signals received from Data Management Subsystem.
Miscellaneous Control and Instrumentation Group (Radiation Monitoring Subsystem)	Provide signals for monitoring reactor building radiation to act as an input to the primary coolant pumpdown system.	Quantity: Four separate signals. Physical Interface: Electrical signals.
(Main and Bypass Steam Subsystem)	Provide for installation of pressure transmitters in superheater outlet pipe to measure superheat steam pressure for use in steam generator dump termination.	Quantity: Four pressure transmitters in the superheater outlet pipe. Physical Interface: Valved pressure tap in piping.

TABLE 7.2-9 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
(Steam and Water Dump)	Provide feedwater dump system valving in the steam generator inlet line for use in the steam generator isolation and dump subsystem.	Quantity: Four valve matrix. Physical Interface: Electrical signals.
Shutdown Cooling System (Shutdown Heat Removal Control Subsystem)	Provide capability to accept signals to initiate the SCS on automatic command from the Investment Protection Subsystem.	Quantity: Two separate signals. Physical Interface: Electrical signals.
Building, Structures, and Building Service Group (Reactor Building)	Provide building space and structural support to accommodate Investment Protection Subsystem.	Quantity: Nine cabinets, one hygrometer module, one compressor assembly, and one accumulator tank assembly. Physical Interface: Floor mounting, piping, and electrical.
Mechanical Service Group (HVAC)	Provide HVAC to support the proper operation of the Investment Protection Subsystem.	Quantity: Two. Physical Interface: None.

TABLE 7.2-9 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Electrical Group (Non-Class 1E AC Distribution)	Provide low-voltage AC distribution for the moisture monitor compressors.	Quantity: Two. Physical Interface: Electric feeders.
(Class 1E Uninterruptible Power Supply)	Provide separate Class 1E uninterruptible power distribution channels to power the Investment Protection Subsystem as a 1E associated circuit.	Quantity: Four separate Class 1E sources. Physical Interface: Electric feeders.

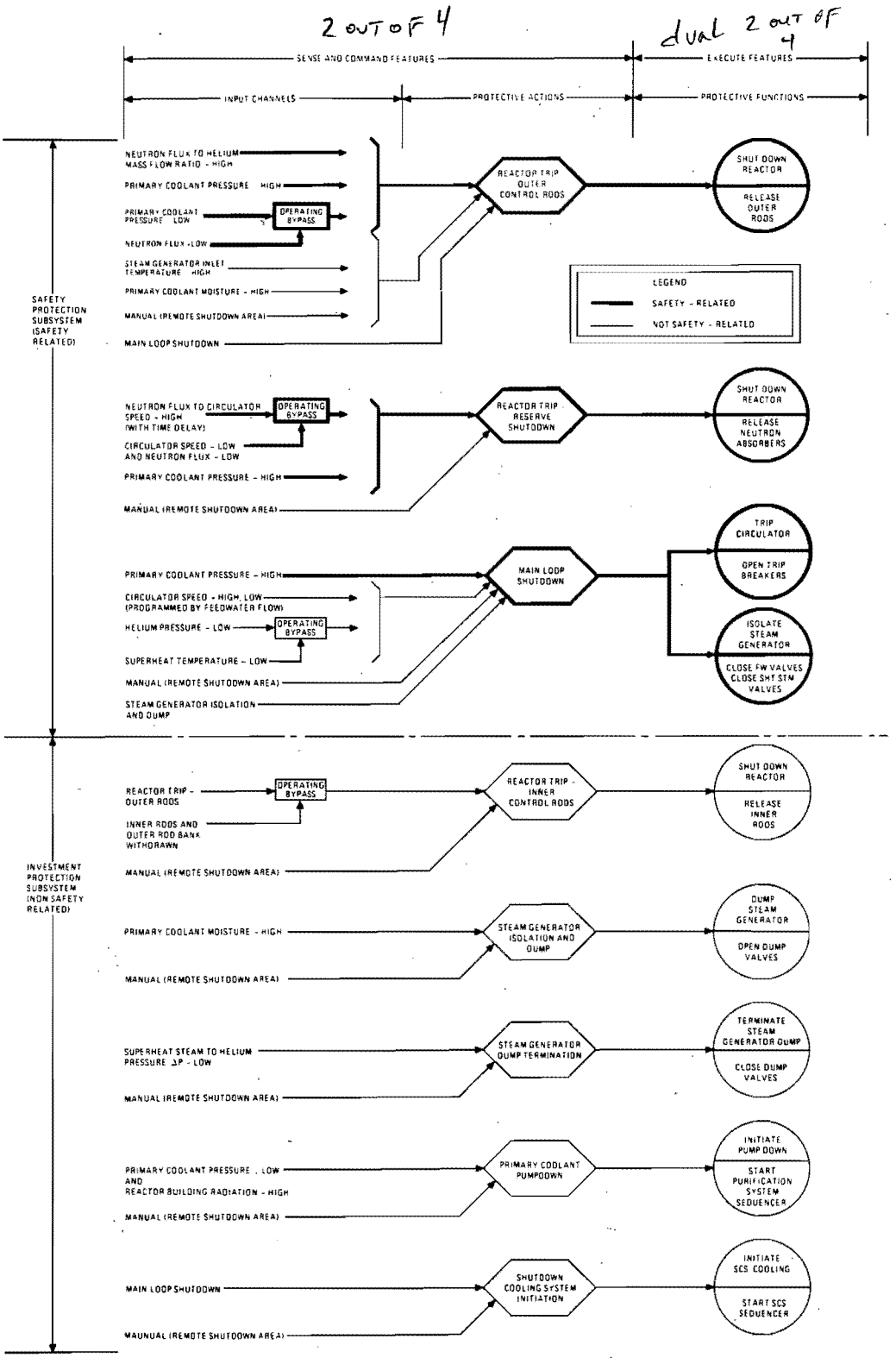


FIGURE 7.2-1

FUNCTIONAL OVERVIEW PPIS TRIP SUBSYSTEMS

HIGH TEMPERATURE GAS-COOLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024

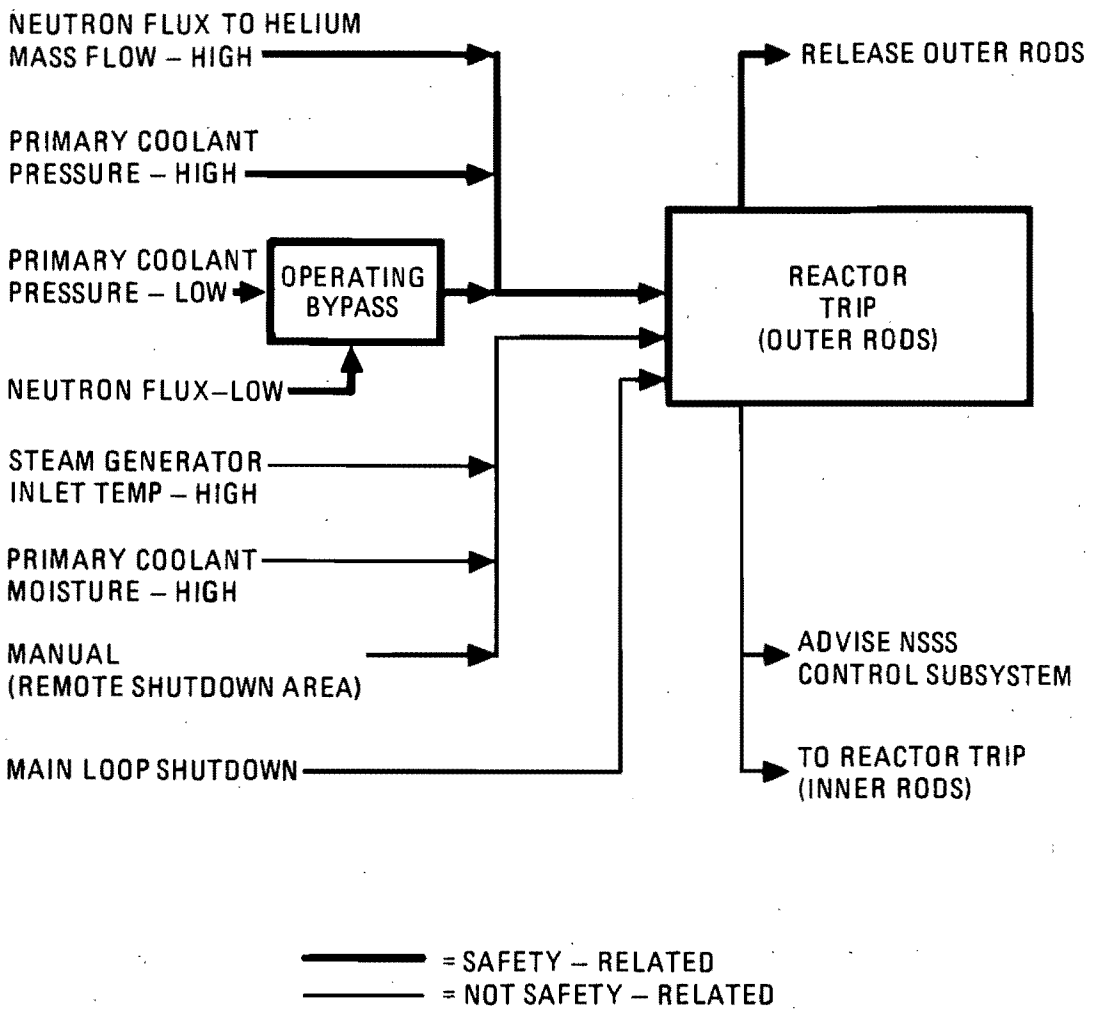


FIGURE 7.2-2

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF SAFETY PROTECTION SUB-SYSTEM REACTOR TRIP USING THE OUTER CONTROL RODS

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

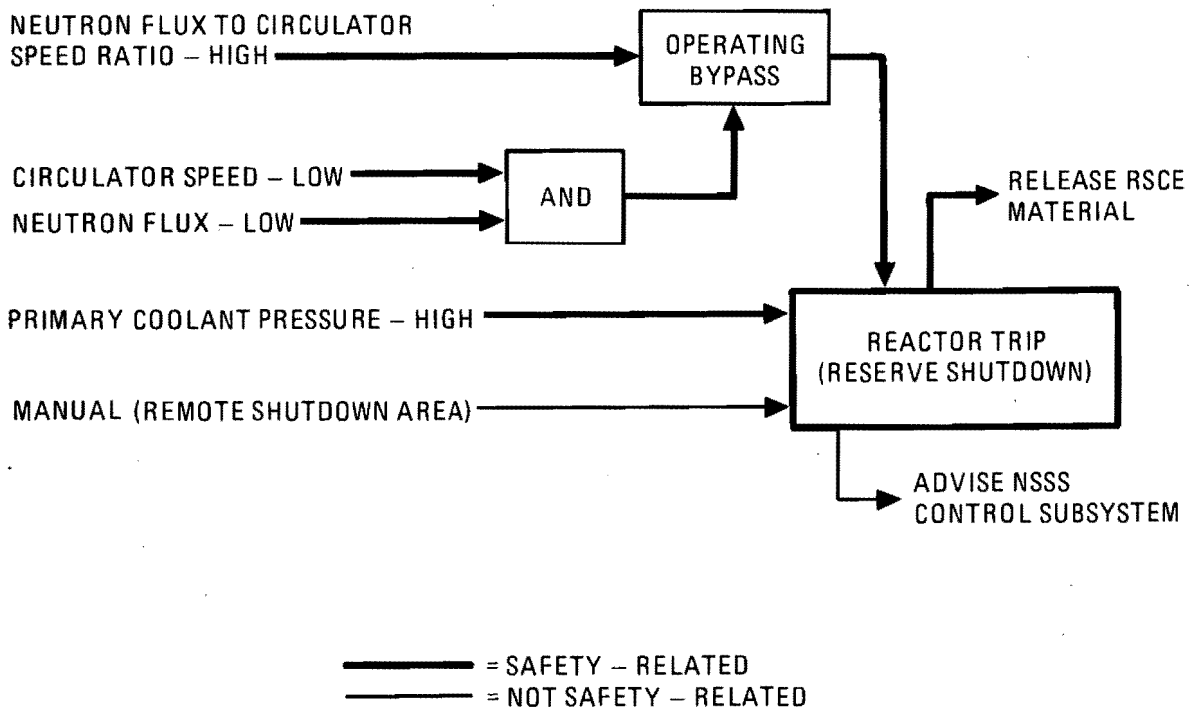


FIGURE 7.2-3

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF SAFETY PROTECTION SUB-SYSTEM REACTOR TRIP USING THE RESERVE SHUTDOWN CONTROL EQUIP-MENT

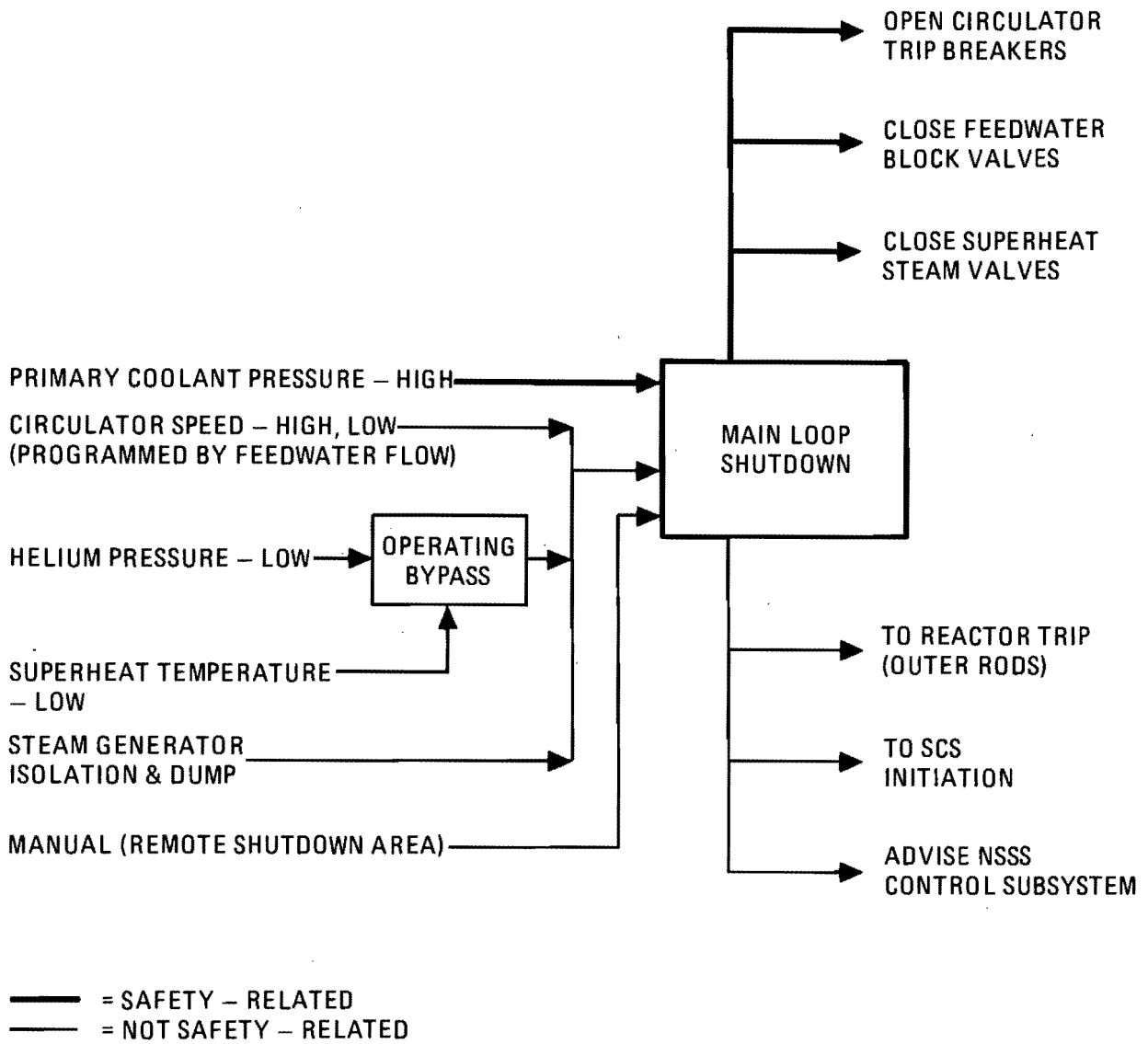


FIGURE 7.2-4

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF SAFETY PROTECTION SUB-SYSTEM MAIN LOOP SHUTDOWN

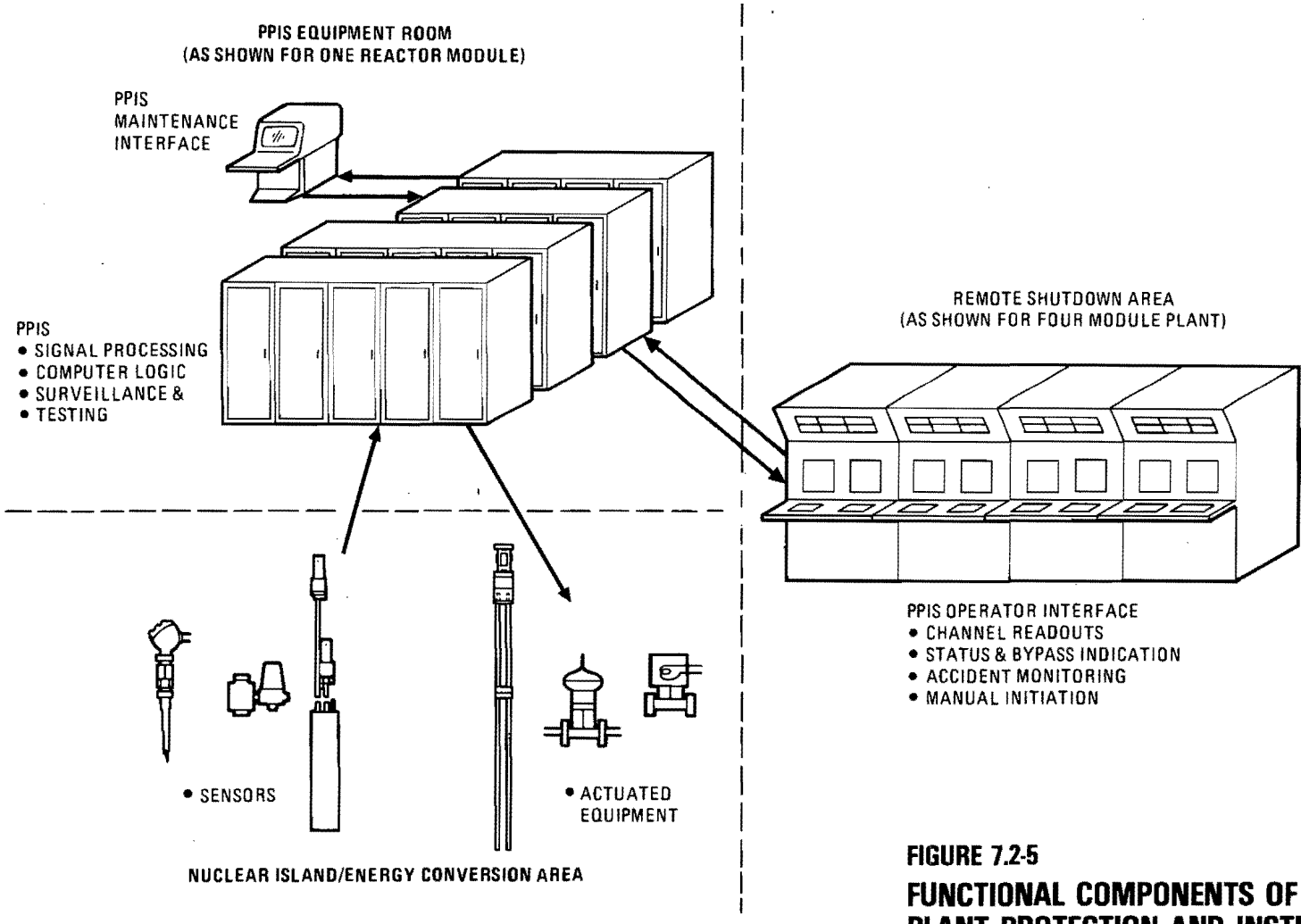


FIGURE 7.2-5

FUNCTIONAL COMPONENTS OF THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

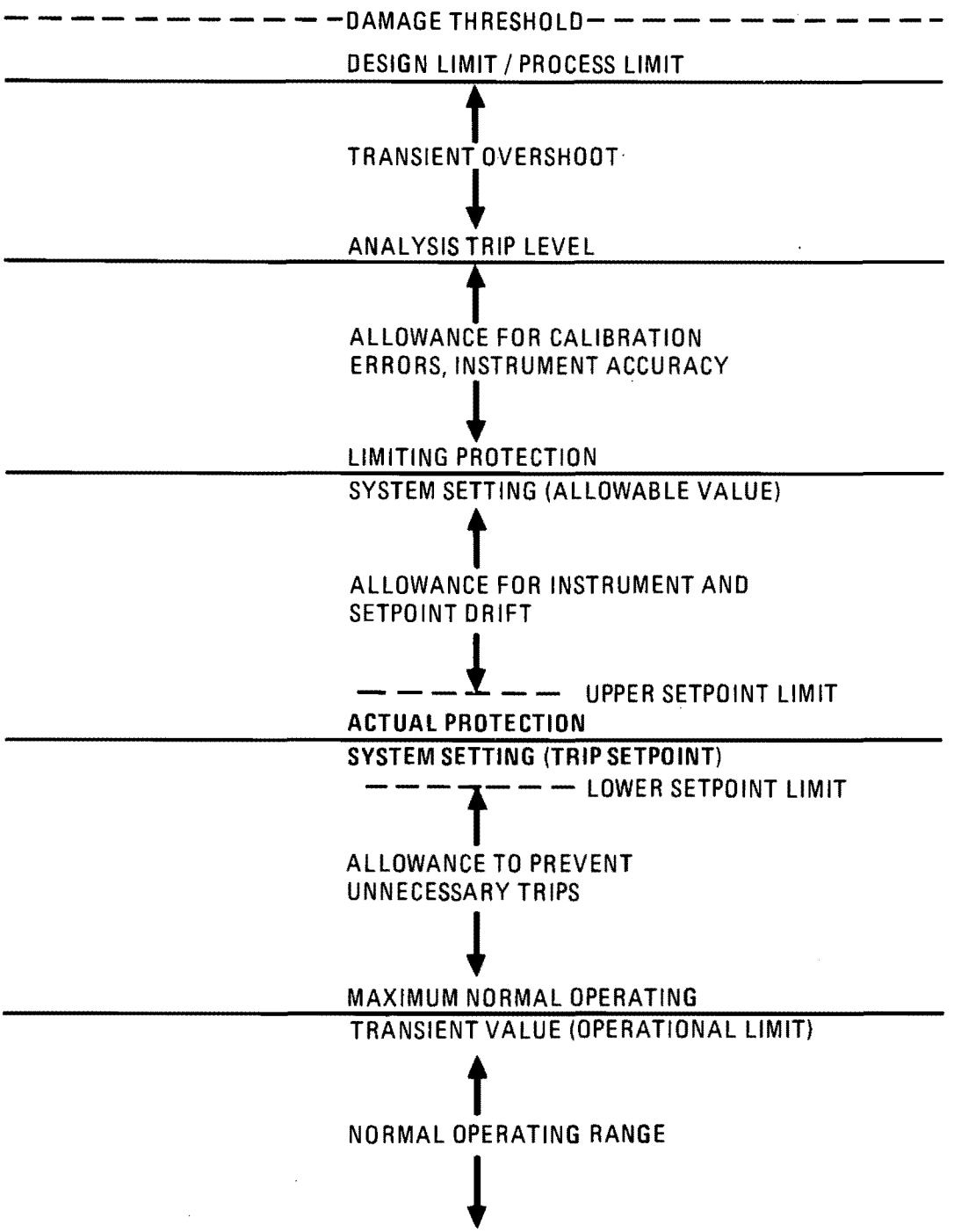


FIGURE 7.2-6

RELATIONSHIP BETWEEN PROTECTION SETPOINTS AND COMPONENT DAMAGE LIMITS

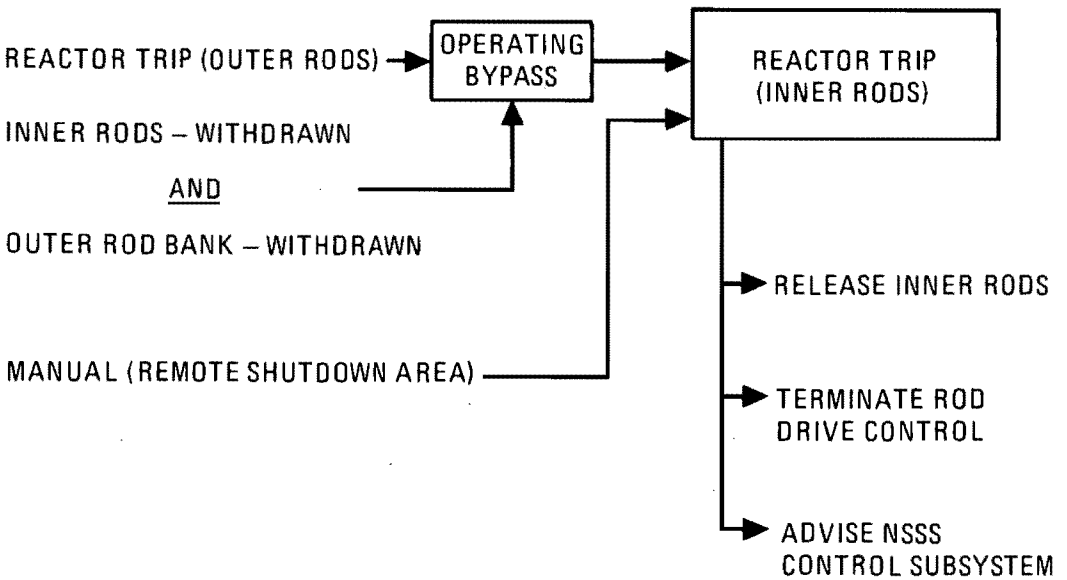


FIGURE 7.2-7

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF INVESTMENT PROTECTION SUBSYSTEM REACTOR TRIP USING THE INNER CONTROL RODS

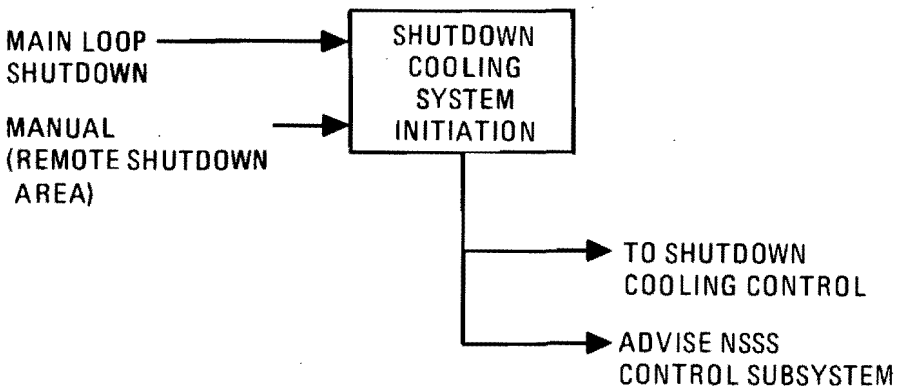


FIGURE 7.2-8

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF INVESTMENT PROTECTION SUBSYSTEM SHUTDOWN COOLING SYSTEM INITIATION

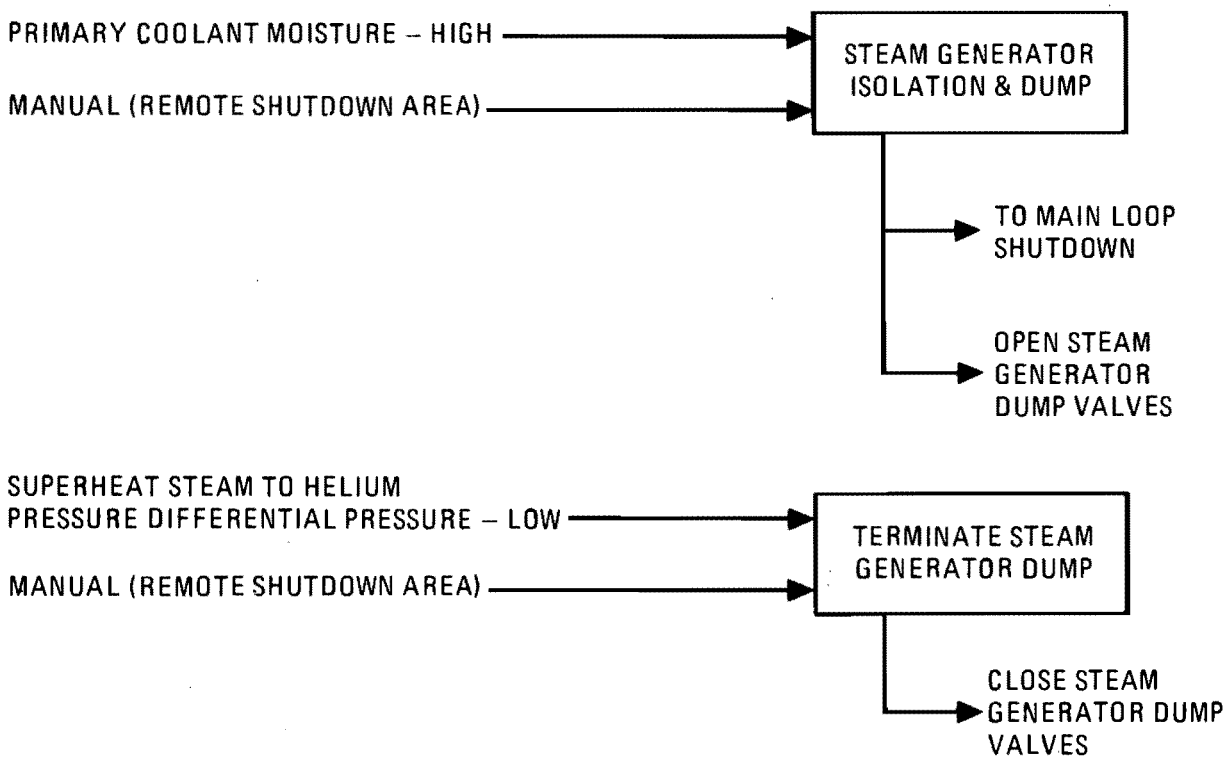


FIGURE 7.2-9

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF INVESTMENT PROTECTION SUBSYSTEM STEAM GENERATOR ISOLATION AND DUMP

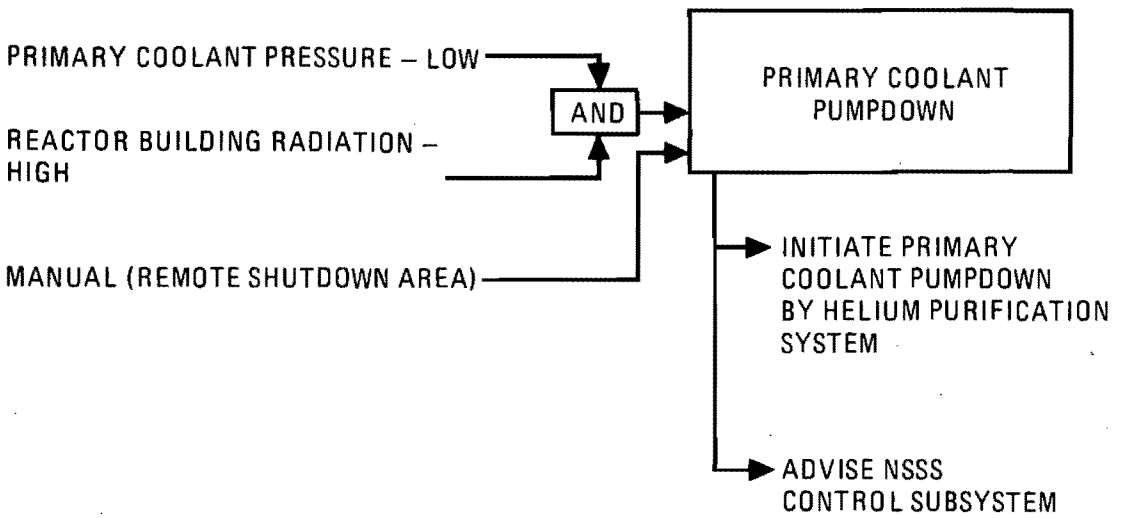


FIGURE 7.2-10

SIMPLIFIED ONE CHANNEL BLOCK DIAGRAM OF INVESTMENT PROTECTION SUBSYSTEM PRIMARY COOLANT PRESSURE PUMPDOWN

7.3 PLANT CONTROL, DATA, AND INSTRUMENTATION SYSTEM

7.3.1 Plant Supervisory Control Subsystem

The Plant Control, Data and Instrumentation System (PCDIS) provides the subsystems to control the Standard MHTGR operation. The subsystems of the PCDIS include the:

1. Plant Supervisory Control Subsystem (PSCS)

2. NSSS Control Subsystem

3. Energy Conversion Area (ECA) Control Subsystem

4. Data Management Subsystem (DMS)

Figure 7.3-1 shows the relationship between the PCDIS subsystems. The PSCS provides supervisory control (load allocations) to the NSSS Control Subsystem and the ECA Control Subsystem. PSCS also provides work stations for operator monitoring and interaction. The NSSS Control Subsystem provides individual control for each Nuclear Steam Supply System. The ECA Control Subsystem provides for control of equipment associated with each of two individual turbine plants. The Data Management Subsystem provides the communication link to transmit control systems and data between systems and to the main control room. These subsystems provide an integrated control of the four reactor modules and two turbine plants.

7.3.1.1 Summary Description

Plant-level control functions are performed by the Plant Supervisory Control Subsystem (PSCS). The PSCS automatically supervises and coordinates balancing of load (power) levels among the energy production Nuclear Steam Supply System (NSSS) and energy conversion (ECA) areas. The PSCS automatically determines what contribution each NSSS (or energy production

area) will make to the ultimate delivery of steam for the energy conversion process. Likewise, the PSCS automatically determines what contribution each turbine-generator in the Energy Conversion Area (or Turbine Plant) will make to the overall plant electrical output. The PSCS also monitors the performance, response, and limitations of each NSSS and the ECA.

The PSCS consists of three major elements, the supervisory control hardware, supervisory control software, and control room operator workstations. Plant-level control strategies and algorithms are implemented in software embedded in the computer hardware.

Included in the main control room (MCR) of the plant is a seated-operator arrangement of plant control initiators and monitors required by the operator to operate the plant. The control initiators and monitors collectively form the operator workstation; the workstation is referred to as the control room operator workstation (CROW). The CROW generates displays, interprets and executes operator instructions, and communicates with the PSCS computers and the Data Management System.

7.3.1.2 Functions and 10CFR100 Design Criteria

7.3.1.2.1 Power Generation Functions

The power generation function of the PSCS is to coordinate plant control during energy production, shutdown, refueling, and startup/shutdown. The PSCS accomplishes this function by accepting direction, observing status, making decisions, effecting control, and reporting information. The PSCS computers accept and process power generation directions from the MCR operator, plant load requests from the grid dispatcher, and communications from the operator workstation to provide data for display. The PSCS computers observe key plant variables such as reactor module feedwater and steam conditions, turbine-generator performance, and reactivity levels and primary coolant temperatures. These data are used to determine load allocations and present information required by the operator. The PSCS determines how to partition and allocate the overall plant load demand to

individual reactor modules and turbine-generators. The PSCS determines the rate of main steam production and feedwater flow changes necessary to achieve optimum plant response to simultaneous or unbalanced load maneuvers. The PSCS effects control at the plant level by communicating operator instructions received from the CROW and communicating its own automatic control instructions for changing load. The PSCS computers report plant and self-status information required by the operators and maintenance personnel.

7.3.1.2.2 Radionuclide Control Functions

The PSCS does not perform any radionuclide control functions.

7.3.1.2.3 Classification

This system is not "safety related". Since the subsystem does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, the subsystem will have the appropriate reliability to meet user requirements.

7.3.1.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to this subsystem.

7.3.1.3 Radionuclide Control Design Requirements

The PSCS does not have any radionuclide control requirements.

7.3.1.4 Design Description

7.3.1.4.1 Subsystem Configuration

The PSCS is configured with multiple, computer-based control and display equipment interconnected for high reliability and availability.

The configuration of the PSCS computer elements is diagrammed in Figure 7.3-2. The PSCS computers coordinate overall operational control of

the plant during normal and off-normal power generation, startup, refueling, and shutdown.

PSCS Computers

The PSCS computers accept plant control and operating directions through the following:

1. An automatic plant load limiter which provides physical interface with grid dispatcher communications in order to accept, with concurrence by the operator, baseload and load following net electrical output load demands

2. A communication link with the operator workstations

3. An operator instruction interpreter

The PSCS computers observe plant status through a communication link with the DMS and plant status analyzer.

The PSCS computers make plant-level control decisions through the following:

1. A plant control strategy selector selects the necessary mode of plant operation and the control strategy that best facilitate operation of reactor modules and turbine-generators independently and at different power levels.

2. Control and operator instruction validator automatically analyzes, diagnoses, verifies, and validates control actions, analytic results and observations

The PSCS computers effect control at the plant level through the automatic control instruction generator, which is for load allocation, startup, data requests, etc.

The PSCS computers report plant information through the following:

1. A communication link with the DMS, which is for communicating control commands, directions, and instructions to other systems

2. A communication link with the operator workstation which is for display or printing

Control Room Operator Workstation

The CROW contains the control initiators and monitors required in the MCR for a single operator to control four reactor modules and two turbine-generators in the plant. The operator manages (supervises and monitors) automatic process control within the energy production (NSSS) and energy conversion (ECA) areas in conjunction with the PSCS computers.

The CROW accepts plant operating directions through touch-activated control devices (e.g., push-button switches).

The CROW observes plant operating status through a communication link with the PSCS computers and a communication link with the DMS.

The CROW makes operator workstation decisions through an operator instruction decoder and a PSCS computer instruction interpreter.

The CROW effects (generates) plant operating instructions through the operator instruction digitizer.

The CROW reports real-time plant status information through video-display generators.

The configuration of these workstation elements is indicated in Figure 7.3-3.

Control Room Assistant Workstation

The control room assistant workstation (CRAW) is a workstation for a licensed assistant operator. The CRAW contains display generation and printing equipment that can generate any display or print any information normally

available to the operator at the CROW. It provides the capability to access plant data bases maintained by the Data Management Subsystem. Plant systems, equipment, and components cannot be controlled or operated from the CRAW.

During normal plant operations, the role of the assistant operator at the CRAW is to monitor startup, shutdown, and refueling activities and auxiliary systems whose operations are not a direct function of the main energy production and energy conversion process. During abnormal plant conditions, the assistant operator monitors the remainder of the plant while the operator at the CROW tends to the controls for the affected portion of the plant. The assistant operator monitors the affected portion of the plant once it is restored to normal operating conditions or removed from service while the operator at the CROW resumes normal operating tasks.

Communication and Display Generation Equipment

Cabinets located behind the CROW contain communication and display generation equipment associated with the touch control devices and video monitors, respectively, in the CROW. This equipment is a part of the PSCS. The cabinets also house data communication interface equipment. This equipment is part of the DMS and it provides the capability to communicate operator instructions and plant data in and out of the MCR, respectively. Communication, test and maintenance instrumentation is also housed within these cabinets. Peripheral equipment is located in the control room to meet operator and shift supervisor information requirements (e.g., low-noise printers, display copiers, etc.). A workstation is provided for the shift supervisor as part of the DMS.

7.3.1.4.2 Subsystem Arrangement

The PSCS is functionally independent from Safety Protection Subsystems, structures, and components. The PSCS does not have any direct, physical interfaces with "safety-related" systems. The PSCS is physically separated from "safety-related" systems with data transmission between the systems provided by the DMS. Safety systems provide the electrical isolation devices

at the interface with the DMS. Thus, as shown in Figure 7.3-1, the DMS has physical interfaces with safety systems but these interfaces are not used to perform safety functions.

The PSCS computers are located in a secured area of the computer facility near the MCR in the operations center.

The CROW and the CRAW are located in the MCR within the operations center. Figure 7.3-4 depicts the workstation arrangements within the MCR.

7.3.1.4.3 Subsystem Operating Modes

Startup/Shutdown

Table 7.3-1 summarizes the control strategy implemented by the PSCS during startup and shutdown. Reactor module startups from depressurized shutdown conditions are accomplished by sequentially bringing each module up to minimum stable operating conditions under a series of operational check points requiring operator acknowledgment. Operator acknowledgment (i.e., removal of the operational check points) is required before the PSCS requests proceeding to the next stage of the startup process. The operator acknowledgments are required at the following stages of reactor module startup:

1. Subcriticality testing and initial rod withdrawal

2. Reactor criticality (including criticality tests when required)

3. Approximately 205°C (400°F) steam generator secondary outlet temperature (for feedwater chemistry/cleanup as necessary)

4. Module steam pressurization to 12.41×10^6 Pa (1800 psia) and feedwater temperature heatup to 190°C (374°F)

5. Steam generator boilout [approximately 16 percent reactor power and 425°C (797°F) main steam temperature]

6. Achievement of rated steam conditions and connection of reactor module to main steam header (approximately 25 percent reactor module load)

7. Turbine-generator turning gear operation, rolling and loading (at least one reactor module at or above 25 percent load, grid dispatcher notified)

Module load levels are adjusted in parallel to a common average load level at normal load ramp rates of +0.5 percent per minute. From a control standpoint, the logistics of bringing reactor modules to shutdown conditions are essentially the reverse of those used for startup control. The reactor modules are maneuvered sequentially in order to keep the turbines on-line as long as possible; otherwise the reactor modules are shut down in parallel manner at incremental stages.

Reactor modules are disconnected from the main steam header one at a time. For example, with one feedwater train operating at full capacity (i.e., two modules and one turbine operating at 100 percent load) a reactor module to be disconnected is maneuvered down to a 25 percent load level. At 25 percent load, closure of the reactor module steam isolation valve is initiated. Reactor module steam is bypassed by opening the reactor module startup bypass valve. The other reactor module in operation remains at 100 percent load and the turbine load is reduced from 62.5 percent capacity. The main steam header pressure is stabilized to its setpoint established by the NSSS Control Subsystem. Main steam flow to the turbine is gradually reduced from the initial 62.5 percent level to a final level of 50 percent as the reactor module at 25 percent power (corresponding to 12.5 percent turbine load) is disconnected from the main steam header.

Modules are normally connected to the main steam line one at a time. The procedure is described in Section 7.3.2.4.3.

Normal Operation

Table 7.3-2 summarizes the control strategy implemented by the PSCS computers during normal power generation. Within the normal power generation range of 25 percent to 100 percent load, the primary plant-level control function of the PSCS is to determine and allocate turbine-generator load indices (main steam flow demands) and reactor module load indices (feedwater flow demands) to the ECA and NSSS Control Subsystems, respectively. The principle plant-level control function in this operating mode is referred to as load apportioning.

The PSCS derives a plant electrical power demand from the electrical load demand of the grid dispatcher, the current plant total electrical power output, and prior turbine-generator load allocations. The plant electrical power demand is compared against the electrical power generating capacity available from the generators to limit generator electrical power demands. The generator electrical power demands are derived using comparisons with the maximum steam supplies available from the reactor modules.

The PSCS computers calculate the main steam demand equivalent of the generator electrical power demand. An algorithm operating on this calculation and the current generator electrical load results in a total plant feedwater demand. The main steam and feedwater demands are apportioned into the respective load indices (turbine-generator main steam demands and reactor module feedwater flow demands).

Prior to communicating the load indices over the DMS data highways, the load indices are compared against the maximum steam supply and feedwater flow available to each turbine-generator and reactor module, respectively. This comparison is made in order to limit the demands should any reactor modules or turbine-generators be operationally constrained. The NSSS load index is used by the NSSS Control Subsystem to determine the reactor thermal power levels, helium flow rates and module feedwater flow setpoint. The ECA main steam load index is used to determine the turbine throttle valve positions, feedwater pump speeds, and the condensate return conditions.

Provided investment protection is not challenged or compromised, the PSCS coordinates continuous plant operation in response to step changes of ±15 percent in plant load caused, for example, by utility electrical transmission grid upsets. To meet 15 percent step load changes, the PSCS normally allocates load demands equally among the available reactor modules and turbines. It also sets the rate of step change in reactor module and turbine loads based upon component performance histories and component limits.

The rate of step load change is normally set at 500 percent per second. Using the turbine load index and rate specification, the ECA Control Subsystem opens the turbine throttle valve to meet the step load increase demand. At a rate of 500 percent per second, the main steam header pressure remains virtually constant without experiencing unacceptable perturbations. However, reactor module steam temperatures decrease significantly during the rapid changes in reactor power.

Refueling

The control room operators and the PSCS do not perform any refueling control functions. With respect to the reactor module being refueled, control room operator-initiated functions which could add positive reactivity during operation or startup/shutdown (e.g., control rod movement), are deactivated.

Refueling control is performed by the refueling operations crew using the Core Refueling Subsystem of the Fuel Handling and Storage System (refer to Section 9.1.1). Status information on refueling operations is presented in the MCR. The DMS provides the data communication interconnection between the fuel handling control stations and the CROW for monitoring. The control room and refueling operators are provided with voice communication equipment at their respective workstations.

Shutdown

The PSCS and the operators primarily perform monitoring functions with respect to that portion of the plant in a shutdown mode. The status of

reactor and vessel systems, components, and equipment are monitored to ensure the reactor is being properly maintained in a shutdown condition [for cold shutdown, neutron multiplication factor k less than 0.99 at fuel temperatures of 23°C (73°F)], the necessary core geometry is established, neutron source range measurements are within specification, and normal decay heat and residual heat transfer is provided. Also, various checks are made to ascertain that startup and shutdown instrumentation is operating, reactivity shutdown margins are verified, and that the necessary auxiliary and bypass systems and process loops are operating (e.g., for shutdown with condenser or deaerator unavailable).

The PSCS computers and workstations normally remain in an operational mode irrespective of the mode of operation of the plant or portions thereof. With respect to system shutown, only redundant portions of the PSCS computers are placed in a shutdown mode. Only one computer may be placed in a shutdown mode at any time.

Abnormal Operating Modes

Table 7.3-3 summarizes the control strategy implemented by the PSCS computers during abnormal power generation. Provided investment protection is not challenged or compromised, the PSCS coordinates continuous plant operation through and following transients associated with the unavailability of major components or systems including reactor modules and turbine-generators. The PSCS computers contain control strategies for reloading the plant at a maximum rate of 5 percent per minute once the abnormal operating conditions have been diagnosed and corrected. The reloading is performed in response to load rejection from full generator output to house electrical load without reactor trips occurring. A similar strategy is used in response to turbine trips (except on low condenser vacuum) from any load level without reactor trips occurring.

Under abnormal conditions (e.g., reactor power greater than heat sink capability) a set of actions referred to as automatic load runback are performed. Runback commands are given automatically to the NSSS Control

Subsystem and the ECA Control Subsystem which minimize temperature transients to the steam generator, reactor, and turbine components. The control objective is to mitigate transient conditions which would otherwise lead to a turbine trip and loss of power generation. If certain modules become constrained during these transients, then the maximum load change rate limits are lowered for constrained modules to avoid challenges to equipment and component protection.

When plant load demand is sufficiently less than plant power generating capability, load levels of constrained modules are maintained (approximately 10 percent) below their respective load limits provided stable module operation can be maintained (e.g., above 25 percent rated load). This control strategy permits a higher rate of plant load increase than the rate allowable (i.e., 1.25 percent per minute times the number of nonlimited modules in operation) if limited modules were at their upper load limits.

Controls and instrumentation of other plant systems located outside the MCR can be used, if necessary, to complete reactor shutdown, initiate and maintain cooling, and maintain the plant in a stable shutdown condition. Their use is required under any combination of the following when conditions require a plant shutdown:

1. The MCR becomes uninhabitable

2. The PSCS computers become unavailable

3. The CROW becomes unavailable

For Item 1 above, the MCR operator initiates orderly reactor shutdowns prior to evacuation of the MCR. Completion and verification of an orderly plant shutdown is performed at the Remote Shutdown Area. For Item 2 above, a controlled plant shutdown is performed at the Remote Shutdown Area upon a loss, or long-term anomalous status indication, of PSCS computers. For Item 3 above, the PSCS computers are designed to coordinate an orderly plant shutdown upon unavailability of the CROW. Reliable operator response is

ensured by the response time requirements (on the order of hours), and environmental, access, and security control measures.

7.3.1.5 Design Evaluation

7.3.1.5.1 Failure Modes and Effects

The PSCS is functionally and physically independent from Safety Protection Subsystems, structures, and components. The PSCS does not have any direct, physical interfaces with safety equipment and the PSCS equipment is physically separated from safety protection equipment. The PSCS indirectly interfaces with safety systems via the DMS to monitor safety system status. The DMS has physical interfaces with safety systems but these interfaces are not required for performing safety protection functions. All failure modes of the PSCS leave the safety protection features of the plant intact without compromising their reliability or their capability to meet safety requirements.

PSCS Computers

The PSCS computers do not perform any functions that the failure or unavailability of could lead to an unacceptable release of radioactivity to the public or environment. In addition, the computers cannot prevent or inhibit any safety protection function from being performed.

All MCR operator instructions are processed by the PSCS computers. The computers acknowledge, verify, and validate the operator instructions. However, the control logic does not prohibit execution of an operator instruction if it appears invalid to the PSCS computers and the operator requests an override. Deliberate operator interaction is normally not required for operational control unless the automatic control portion of the computer software fails and the computer system is still available. This scheme allows overriding the automatic PSCS controls if necessary for operator response to abnormal operations.

Operator instruction validation is complemented by automated operator aids such as symptom-oriented diagnostics, visual feedback and procedural directives. The operator aids are designed to reduce the probability of operator error ensuring reliable operator performance.

Control Room Operator Workstation

The CROW contains no devices nor performs any functions that the failure or unavailability of could lead to an unacceptable release of radioactivity to the pubic or environment. The plant is normally operated from the CROW in the MCR except under conditions that render the MCR uninhabitable and/or the PSCS unavailable. Should these conditions occur, control and monitoring of safety and selected nonsafety systems can be performed at the Remote Shutdown Area in the Reactor Service Building.

Failure or unavailability of the CROW does not cause loss of the PSCS computers. However, the PSCS computers initiate an automatic plant shutdown upon long-term anomalous indication or loss of a CROW status monitoring signal. There are sufficient time, environmental control, and security measures for the plant operating staff to access the PSCS computers in the computer equipment room near the control room if the CROW becomes unavailable and/or the MCR becomes uninhabitable.

7.3.1.5.2 Steady-State Performance

The steady-state control objective of the PSCS is to coordinate the operation of the reactor modules and the turbine plant to achieve the expected overall plant steady-state performance. The principal, active PSCS control function during steady-state operation is to allocate loads on the basis of observed performance and refueling and maintenance schedules. The PSCS apportions loads and schedules operational transitions (startup, shutdown) in a manner that optimizes overall plant time operating efficiency and limits component operational duty cycling.

The majority of plant steady-state operating time is characterized by loads apportioned such that the overall plant load demand is equally shared among available reactor modules and turbine-generators. However, if some of the available reactor modules or turbine-generator sets are operationally load constrained or scheduled for maintenance, the loads are proportionately allocated for efficient transitioning between startup, shutdown, and refueling modes. Once the loads have been allocated, the PSCS primarily monitors NSSS and ECA (turbine plant) performance. The types of performance monitored include heat balancing, thermodynamic efficiency, stability and regulation, approaches and margins to setpoints, and core fuel management.

7.3.1.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. In this section only the response of the Plant Supervisory Control Subsystem is described. The PSCS is supplied with uninterruptible electrical power that allows continued operation with loss of offsite power. The response of the PSCS to all AOOs is as follows:

1. The PSCS monitors the affected portion of the plant. The PSCS acquires and makes available for presentation to the MCR operators, status information on safety protection response, investment protection response, automatic control responses and plant conditions.

2. The PSCS reallocates loads to the unaffected reactor modules and turbines in the power generation mode. Load reallocation is discussed under normal operation in Section 7.3.1.4.3.

7.3.1.5.4 Design Basis Event Performance

Design basis events (DBEs) are described in Chapter 15. In this section only the response of the Plant Supervisory Control Subsystem is described. The response of the PSCS to all DBEs is as follows:

1. The PSCS monitors the affected portion of the plant. The PSCS acquires and makes available for presentation to the MCR operators, status information on safety protection response, investment protection response, automatic control responses and plant conditions.

2. The PSCS reallocates loads to the unaffected reactor modules and turbines in the power generation mode. Load reallocation is discussed under normal operation in Section 7.3.1.4.3.

3. For DBEs with associated environments that exceed the PSCS qualification, the PSCS is assumed to be unavailable. The "safety-related" PPIS will take necessary protective actions as discussed in Section 7.2.1.5.4. DBE-5, Earthquake, is an identified event for which the PSCS is not environmentally qualified.

7.3.1.6 Interfaces

The PSCS has numerous functional interfaces with nearly every plant system. The nature of these functional interfaces is the capability to exchange control and monitoring signals for the plant to be automatically controlled and operated from a single control room. Table 7.3-4 provides a descriptive list of these key functional interfaces.

7.3.2 Nuclear Steam Supply System Control Subsystem

7.3.2.1 Summary Description

There are individual NSSS Control Subsystems, one for each reactor module, that control reactor conditions and the supply of steam to the main steam header. The systems utilize a distributed computer control architecture. For power generation, the individual NSSS Control Subystems respond to individual load demands allocated to them by the Plant Supervisory Control Subsystem. Each NSSS Control System controls its feedwater flow demand to meet its allocated load and the delivery of steam at the rated conditions of 16.7 MPa (2400 psig) and 538°C (1000°F).

7.3.2.2 Functions and 10CFR100 Design Criteria

7.3.2.2.1 Power Generation Functions

The power generation function of the NSSS Control Subsystem is to coordinate NSSS control during energy production, shutdown, refueling, and startup/shutdown.

During power generation the NSSS Control Subsystem performs its function by accomplishing five operations.

1. To follow the mission prescribed by the PSCS, the NSSS Control Subsystem automatically accepts, with operating staff concurrence, load apportionment and sequence hold signals. This includes startup and shutdown sequences such as shown in Table 7.3-1.

2. The system also senses, processes, and analyzes those variables, states, modes, limits, and conditions required for the NSSS processes and subsystems to be observable.

3. Subsequently, the NSSS Control Subsystem decides what strategy, based on the sensed data, shall be used within the NSSS module to produce steam.

4. On the basis of the decision made, NSSS Control Subsystem effects final control element action to bring steam conditions to desired levels.

5. Finally, NSSS Control Subsystem generates display information regarding NSSS status and conditions, and provides it to the PSCS and the operator stations.

7.3.2.2.2 Radionuclide Control Functions

The NSSS Control Subsystem has no radionuclide control functions.

7.3.2.2.3 Classification

The NSSS Control Subsystem is not "safety-related". Since this system does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, this system will have the appropriate reliability to meet user requirements.

7.3.2.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria for radionuclide control apply to the NSSS Control Subsystem.

7.3.2.3 Radionuclide Control Design Requirements

The NSSS Control Subsystem does not have any radionuclide control requirements.

7.3.2.4 Design Description

The NSSS Control Subsystem accepts energy production direction through a communications link between module data highways and the DMS data highway, and local operator interfaces.

The NSSS Control Subsystem observes energy production status through the NSSS process sensors connected to module data highways and ECA sensors connected to DMS and module data highways.

The NSSS Control Subsystem makes energy production control decisions through the decision logic resident in NSSS control software and hardware, and interaction with ECA and PSCS decision logic.

The NSSS Control Subsystem effects energy production control through the programmable control algorithms and final control elements interfaced with NSSS data highways. Table 7.3-4A shows measurements which are used to control the NSSS module. None of the sensors used for thses measurements are shared with the PPIS.

The NSSS Control Subsystem reports energy production information through the module data highways that pass on information to the DMS data highway, and display, annunciator, and alarm drivers resident in the NSSS Control Subsystem.

7.3.2.4.1 Subsystem Configuration

Figure 7.3-5 shows the relative location of the NSSS Control Subsystem in the modular hierarchy of the PCDIS architecture (see also Figure 7.3-1). Figure 7.3-6 shows the main loops of the NSSS controls. As shown in the figure, the major functions of the NSSS controls are:

1. Module feedwater flow control demand.

2. Reactor module circulator speed characterization.

3. Reactor module power characterization.

4. Module main steam temperature control.

5. Module main steam pressure control during startup. Pressure in the main steam header is controlled by the turbine throttle valve and the indexed feedwater flow in the individual NSSS modules.

NSSS controls are designed to automatically follow the load apportioned to each module by the PSCS over the range between 25 and 100 percent of full module output. In addition, the NSSS automatic control loops are configured to accommodate feedwater, reactor module, and turbine trips. Special compensation and limiting are used after these events to minimize transient extremes, thereby protecting major equipment and increasing NSSS availability.

NSSS feedback control algorithms are proportional plus integral plus derivative expressions (commonly known as P+I+D). The result of this feedback algorithm normally is summed with a feedforward signal (if used for

the specific control algorithm). The sum of the compensation output and the feedforward signal are then passed through limiter logic which may provide high, low, and/or rate limits. The control algorithm output from the limiter is then sent to the manipulated variable (dependent variable). When and if the limiter is on one of the limits, a signal is sent to the P+I+D function to force it to "track" such that the sum of the compensation output and the feedforward indeed satisfy the limit condition.

Distributed digital control electronics are used for data acquisition display, control logic, status assessment, and calculations. The NSSS Control Subsystem is part of a hierarchical data highway system which provides the communication paths between active NSSS components. The subsystem is both redundant and functionally partitioned so that a single failure in any attached electronics module can at most eliminate only the functions associated with that module.

Each reactor module has its own dedicated data highway system. These data highways communicate with the DMS highway system.

The conceptual architecture of the NSSS Control Subsystem is shown in Figure 7.3-7.

The multiplexers and controllers are connected to the redundant module data highways. The highways receive supervisory control commands via the DMS data highway system, and transmit NSSS data through it. The basic functions of each multiplexer are controlled by instructions contained in firmware.

The NSSS Control Subsystem is designed to supply information and control capabilities to personnel with responsibilities for operations, test and calibration, engineering, maintenance (hardware and software), and management. Typical locations where the NSSS control systems have man machine interfaces are the control room, the computer room, the test and calibration stations, local control stations, and engineering offices.

Information handling equipment consists of a variety of computers which are distributed on the various data highways to satisfy NSSS Control Subsystem functional and reliability needs. Processing and storage functions are provided for alarm handling, core performance monitoring, status assessment, operator guides, historical data base and logs, and other information needs.

Redundant capacity for both NSSS data processing and storage is utilized so that no single failure can eliminate information handling functions. All detectable failures are alarmed.

Since the NSSS Control Subsystem has a data highway network for each reactor module which is linked to the DMS highway network, all NSSS data users are supported by a common and consistent set of information which includes current values as well as historical data.

7.3.2.4.2 Subsystem Arrangement

Controls and displays required to monitor and operate the NSSS equipment are located in the main control room and at local control stations installed near major components. Sensors and sampling systems are located near the point of measurement. Additional display terminals, keyboards, printers, and removable storage devices are located in the primary work areas of others who need access to the NSSS data base.

Other devices such as NSSS data processing computers (heat balances, etc.), computer peripherals, maintenance stations, data highway, and communication controllers, etc., are installed in computer and relay rooms.

7.3.2.4.3 Subsystem Operating Modes

The NSSS Control Subsystem provides the means to perform the following general groups of operations:

1. Startup and shutdown

2. Normal operation

3. Refueling

4. Shutdown

5. Abnormal operation

Startup and Shutdown

Startup and shutdown covers the range of operating conditions encountered in the 0 to 25 percent module feedwater flow and reactor power range.

Special equipment and provisions are utilized to start up and shut down a module. Specifically, special reactor core instrumentation is utilized for reactor startup in order to monitor core power from the source range up to the design power range. The total range spans several orders of magnitude.

One of the most important systems required to start up and shut down a reactor module is the module Steam Bypass System. This system allows hot water and steam produced during the startup and shutdown sequences to bypass the main turbines. To route the hot water and steam into this bypass, there is a module isolation valve and a module main steam bypass valve. In order to allow independent operation of reactor modules, each module is equipped with its own bypass.

During startup or shutdown, the module main steam isolation and check valve is closed. This allows other reactor modules that may be on line to continue supplying steam to the turbine for power generation. Steam from the isolated module is passed via the module main steam bypass valve to a flash tank. The bypass valve is modulated to control steam pressure at the steam generator outlet through a wide range of steam generator outlet pressure setpoints, 48.3 to 179.3 bars abs (700 to 2600 psia). This pressure varies during the startup sequence from depressurized conditions as shown in Table 7.3-5. The pressure setpoint is generated by the NSSS Control Subsystem to control steam generator boiling.

The hot water and steam temperatures during startup (and shutdown) range from 27°C (80°F) subcooled liquid to rated 541°C (1010°F) superheated steam. This temperature is controlled by the NSSS Control Subsystem by varying reactor power and circulator speed.

When a module reaches rated steam conditions in the startup sequence and it is requested by the PSCS to transfer its flow of steam into the main steam header for use by the turbines, the NSSS Control Subsystem slowly raises the module steam pressure above the main steam header pressure. This results in a slow closure of the module main steam bypass valve and a slow opening of the isolation check valve.

During startup and shutdown, an individual reactor module requires feedwater at a temperature within the range of 27°C (80°F) to 193°C (380°F) while other modules continue in operation with feedwater at the design temperature of 193°C (380°F). A startup feedwater system (part of the ECA) generates the appropriate feedwater temperature as demanded by the NSSS Control Subsystem.

Some special handling of NSSS control loop gains is made during startup and shutdown. Special control gains, selected to allow automatic control with outlet steam conditions below rated values and feedwater flow less than 25 percent, are used. This allows automatic NSSS control during the final stages of steam generator and turbine warmup (startup) and during the initial stage of steam generator cooldown (shutdown).

Reactor module startup and shutdown are highly automated. The reactor module startup sequence is fully automated, except for required safety checks. Operator control is exercised through the use of holds at various points in the startup sequence. Operator input is required to allow continuation of the automatic sequence. The shutdown procedure is similarly automated. Of course, manual startup and shutdown capabilities are also available to handle unusual situations.

Normal Operation

During normal operation, main steam header pressure response is fast relative to module thermal response and, for most events, little pressure excursion occurs. Even at low loads where the main steam header pressure control frequency is less than at full load, 1.0 percent pressure setpoint increases are achieved within 2.0 seconds. Because of the main steam header pressure control loop speed, pressure response is largely decoupled from steam temperature response during load ramps, load steps, reactor trips, and turbine trips.

Control of module main steam temperature is accomplished by the NSSS Control Subsystem by manipulating reactor power and circulator speed. Steam temperature is kept between 532°C (990°F) and 543°C (1010°F) during a 100 percent to 25 percent load ramping maneuver. One hour after initiation of this maneuver, main steam temperature deviations are negligible, and reactor power deviations are within control algorithm deadband. During a 15 percent step load change from full load, module main steam temperature control maintains temperature between 536°C (997°F) and 552°C (1030°F). Special steam temperature controls, used following a module reactor trip, significantly limit thermal transients in the steam generator by ramping down main steam temperature setpoint at 0.2°C/sec (0.35°F/sec) from 541.6°C (1010°F) to saturation, then returning circulator speed to feedforward demand through a 30-second time constant. The NSSS Control Subsystem tightly controls the time over which stored heat is removed from the core and placed into the secondary fluid. Runback and steam bypass functions allow individual operation of the remaining, untripped Standard MHTGR reactor modules by the NSSS Control Subsystems. The turbine bypass and startup bypass setpoints for load range operation are set for 172.4 bars abs (2500 psia) and 175.9 bars abs (2550 psia), respectively. The turbine bypass acts for turbine side upsets such as turbine trip, while the startup bypass is used for events where the modules are (or may be) separated from the main steam header in their operation, such as starting up, shutting down, reactor trip, etc. An isolation check valve is closed to separate the module(s) on startup bypass from the main steam header.

In load range operation, if one or more reactor trips occur, the feedwater flow to each tripped module is ramped back by its NSSS Control Subsystem at 0.50 percent/sec to 15 percent. Simultaneously, the PSCS is notified, and it causes the ECA Control System to ramp back turbine load at the rate of 0.09 percent/sec per tripped module. This makes the turbine load compatible with the loss of flow from the tripped modules.

Figures 7.3-8 through 7.3-11 show Reactor and Steam System parameters for a load ramp, a load step, module reactor trip, and turbine trip.

Refueling

During refueling the NSSS Control Subsystem is configured to allow core decay heat removal at subatmospheric reactor pressure. Helium is circulated through the module main loop in a balance with feedwater flow so that no boiling occurs in the steam generator and core outlet helium temperature remains less than 116°C (240°F). This is accomplished automatically by the NSSS Control Subsystem after reactor depressurization and upon receipt of a refueling mode enable.

Shutdown

At module shutdown, the NSSS Control Subsystem can enter one of two operating modes - pressurized decay heat removal or depressurized decay heat removal. In the pressurized shutdown mode, the NSSS Control Subsystem automatically holds circulator speed at 20 percent of design and feedwater flow at 15 percent of design. These conditions are sufficient to avoid core recirculation and to maintain subcooled conditions at the steam generator outlet.

In the depressurized shutdown mode, the NSSS Control Subsystem automatically holds circulator speed at 100 percent of design and supplies enough feedwater flow so boiling does not occur in the steam generator.

Abnormal Operation

Abnormal operation of an NSSS module occurs when a component that directly affects module operation fails and the module continues to operate. Section 7.3.2.5.1 examines several possibilities for module operation on failure of an NSSS Control Subsystem major loop. In general, if the PPIS action does not shut down the affected module, the NSSS Control Subsystem continues to operate the module at reduced output automatically. Some of the features built into the NSSS Control Subsystem, i.e., fault tolerance, feedforward, etc., promote operation during abnormal conditions. One of the key feedforward circuits, for example, is the characterization of circulator speed setpoint with feedwater flow. This feature keeps module primary and secondary coolant flow balanced even during feedwater flow excursions due to module feedwater valve failure. A similar action programmed into the algorithm for module reactor power setpoint causes power to follow module feedwater flow excursions. If module protective limits are challenged, the NSSS Control Subsystem automatically assists in bringing the module to a shutdown condition. The latter action, though not required during protective system action, reduces the severity of transients that module components must endure during abnormal operation.

7.3.2.5 Design Evaluation

The NSSS Control Subsystem is designed to operate in the modes described in Section 7.3.2.4.3.

7.3.2.5.1 Failure Modes and Effects

Parts of the NSSS Control Subsystem are redundant and single-failure proof. Therefore, a failure in one of these subsystem parts allows the system to respond correctly. A failure within the system is alarmed or identified during the routine surveillance testing of the system.

The NSSS Control Subsystem is designed to fail into a state demonstrated to be acceptable on disconnection of any failed parts or loss of power.

Failure of any electronic component has a high probability of being detected by the subsystem itself via frequent periodic self-test diagnostic routines.

Table 7.3-6 presents the failure modes and effects analysis for the major NSSS Control Subsystem loops.

7.3.2.5.2 Steady-State Performance

NSSS information monitors in the NSSS Control Subsystem provide information on NSSS module steady-state performance to the DMS. The reactor operators have access to this information, as well as other plant steady-state conditions in the control room. Module steady-state information is also available from the module data highway at local operator interfaces. The acquisition, processing, and presentation of NSSS steady-state data is accomplished efficiently and simply by the use of state-of-the-art, computer-based monitoring equipment. NSSS control loops provide essentially zero deviation steady-state operation by using the algorithms described in Section 7.3.2.4.1.

7.3.2.5.3 Anticipated Operational Occurrence Performance

Anticipated operational occurrences (AOOs) are described in Section 11.6. The NSSS Control Subsystem performance during these events is given below. AOO-1 is a family of events involving main loop transients but with forced core cooling.

<u>AOO-1 Main Loop Transient with Forced Cooling</u>. The loss of forced core cooling is enveloped by the responses discussed for reactor trip and turbine trip in Section 7.3.2.4.3.

<u>AOO-2 Loss of Main Loop Cooling and Shutdown Cooling</u>. The NSSS Control Subsystem performance during AOO-2 is enveloped by the responses discussed for reactor trip and turbine trip in Section 7.3.2.4.3.

AOO-3 Rod Withdrawal with Reactor Trip and HTS Cooling. The NSSS Control Subsystem performance during AOO-3 is reflected in Figure 11.6-4. All operating parameters automatically modulated by the NSSS Control Subsystem move in a direction to mitigate the consequences of the accidental rod withdrawal. Before the reactor module trips at 106 seconds after accident initiation, the main steam temperature control algorithm reacts to increasing negative main steam temperature error by decreasing helium flow. The algorithm also signals the flux setpoint to decrease, but because the flux control algorithm output has failed high, the control rods move out. When the reactor module trips on high power to flow ratio, the transient is enveloped by the reactor trip described in Section 7.3.2.4.3.

AOO-4 Small Steam Generator Leak. The NSSS Control Subsystem performance during AOO-4 is shown in Figure 11.6-5. Until the reactor module trips on high primary coolant moisture 390 seconds after steam generator leakage starts, the NSSS Control Subsystem automatically holds all controlled variables at setpoint. After module trip, NSSS Control Subsystem performance is enveloped by the reactor trip response discussed in Section 7.3.2.4.3.

AOO-5 Small Primary Coolant Leak. The NSSS Control Subsystem performance during AOO-5 is shown in Figure 11.6-6. The main steam temperature control algorithm responds to increasing positive error by increasing reactor power and circulator speed. Main steam temperature decreases in spite of this action because of decreased primary coolant mass flow. In fact, the effect of the primary coolant leak shows clearly when key system and main control parameters are compared. Reactor power rises to the 110 percent control limit, helium flow decreases to 93 percent of design, primary coolant pressure drops to 56.9 bars abs (825 psia), and the module trips 112 seconds after leak initiation. During the same time interval, modified main steam temperature control algorithm outputs to reactor power and circulator speed setpoints have risen to 110 and 103 percent. Concurrently, because of decreased heat transport to the steam generator, module main steam temperature drops from 538°C (1000°F) to 531°C (987°F). After module trip, NSSS Control Subsystem performance is enveloped by the reactor trip response discussed in Section 7.3.2.4.3.

7.3.2.5.4 Design Basis Event Performance

NSSS Control Subsystem performance during design basis events (DBEs) is assessed by considering each of the events described in Chapter 15 and determining what control actions are accomplished.

DBE-1 Loss of HTS and SCS Cooling. Transient conditions for DBE-1 and NSSS Control Subsystem functions during this event are enveloped by the responses discussed for reactor and turbine trip in Section 7.3.2.4.3.

DBE-2 HTS Transient Without Control Rod Trip. Transient conditions for DBE-2 and NSSS Control Subsystem functions during this event are enveloped by responses discussed for reactor trip in Section 7.3.2.4.3.

DBE-3 Accidental Rod Withdrawal Without HTS Cooling. Transient conditions for DBE-3 and NSSS Control Subsystem functions during this event are enveloped by the responses discussed for AOO-3 in Section 7.3.2.5.3.

DBE-4 Accidental Rod Withdrawal Without HTS and SCS Cooling. Transient conditions for DBE-4 and NSSS Control Subsystem functions during this event are enveloped by the responses discussed for AOO-3 in Section 7.3.2.5.3.

DBE-5 Earthquake. Transient conditions for DBE-5, a large earthquake, and NSSS Control Subsystem functions during this event are enveloped by the responses discussed for a reactor trip in Section 7.3.2.4.3.

DBE-6 Moisture Inleakage. Transient conditions for DBE-6, a 12.51 lbm/sec water ingress, and NSSS Control Subsystem functions during this event are enveloped by responses discussed for AOO-4 in Section 7.3.2.5.3.

DBE-7, DBE-8, DBE-9 Moisture Inleakage. Transient conditions for DBE-7, DBE-8, and DBE-9, water ingresses at lower rates than DBE-6, and NSSS Control Subsystem functions during the events are enveloped by responses discussed for AOO-4 in Section 7.3.2.5.3.

DBE-10 Primary Coolant Leak. Transient conditions for DBE-10 and NSSS Control Subsystem functions during this event are enveloped by responses discussed for AOO-5 in Section 7.3.2.5.3.

DBE-11 Primary Coolant Leak Without HTS and SCS Cooling. Transient conditions for DBE-11, a slow primary coolant leak, and NSSS Control Subsystem functions during this event are enveloped by responses discussed for AOO-5 in Section 7.3.2.5.3.

7.3.2.6 Interfaces

Interface requirements imposed on other systems or subsystems by the Nuclear Steam Supply Control Subsystem are identified in Table 7.3-7, which also includes a description of the interface and a quantitative expression for the interface.

7.3.3 Energy Conversion Area Control Subsystem

7.3.3.1 Functional Description

The Energy Conversion Area portion of the Plant Control and Data Instrumentation System provides monitoring and control from the main control room for those systems which directly impact continuity of power generation. For auxiliary and support systems which do not have an immediate impact on power generation, primary control will be from local control panels with selected controls and displays provided in the MCR.

For the following ECA systems, primary monitoring and control will normally be from the MCR with provision for secondary monitoring and control from local panels to facilitate maintenance activities.

1. Power Conversion Group

   Turbine-Generator and Auxiliaries
   Feedwater and Condensate

Demineralized Water Makeup
Main and Bypass Steam
Extraction and Auxiliary Steam
Heater Drains and Condensate Returns
Condensate Polishing
Steam Vents and Drains
Turbine Plant Sampling
Chemical Feed
Turbine Building Closed Cooling Water
Startup and Shutdown
Steam and Water Dump

2. Heat Rejection Group

Circulating Water
Circulating Water Makeup and Blowdown
Plant Service Water
Shutdown Service Water
Shutdown Cooling Water

3. Electrical Group - all Systems and Subsystems

4. Reactor Services Group

Helium Storage and Transfer
Liquid Nitrogen
Reactor Plant Cooling Water

The following ECA systems and facilities will normally be monitored and controlled from the local control panels or console. Key parameters and alarms will be displayed in the MCR to indicate proper operation/readiness or malfunctions.

1. Reactor Services Group

   Reactor Equipment Service Facility
   Decontamination Service Facility
   Radwaste Systems

2. Fuel Handling Storage and Shipping System

   Site Fuel Handling
   Spent Fuel Storage Cooling

3. Mechanical Service Group

   Potable Water
   Plant Fire Protection
   Waste Water Treatment
   Auxiliary Boiler
   Raw Water Treatment
   Instrument and Service Air
   Central Hot Water Heating
   Plant Drains
   Backup Power Generator Fuel Oil
   HVAC Systems, including Chilled Water Subsystem

7.3.3.2 Interface with Nuclear Island

The ECA Control Subsystem has no direct interface with the Nuclear Island. It does interface with the Nuclear Island indirectly, however, by means of the PCDIS, to which it is responsive.

7.3.3.3 Safety Evaluation of the Interface

The interface with the PCDIS has no adverse effect on safety because none of the controls for the above systems and subsystems are "safety related".

7.3.4 Data Management Subsystem

7.3.4.1 Functional Description

The Data Management Subsystem (DMS) serves two plant-level PCDIS functions; plant-wide data communication and centralized data processing. The DMS acquires, transmits, processes, records, stores, diagnoses, and distributes data/information for both onsite and offsite, and immediate and future use. Distributed data communication controllers and high-speed digital computers perform the two plant-level DMS functions, respectively. A distributed communication network (illustrated in Figure 7.3-1) interconnects the data communication controllers. The network consists of multiple sets of optical communication cables referred to as data highways. The DMS interfaces directly with the systems listed in The PSCS interface Table 7.3-4. The DMS is required to be available and operable during every operating mode of the plant.

The DMS does not initiate any plant control or protection functions. The DMS is not a "safety-related" subsystem; it does not perform any 10CFR100-related radionuclide control functions. The DMS does not directly perform any power generation functions. However, it indirectly supports the power generation control functions of the other PCDIS subsystems by transmitting the control and monitoring communications between them.

The DMS communication network accepts directions from the PSCS on where to send and receive communications and the purpose of the communications (e.g., control command, request, monitor, print, display, file, annunciate, etc.).

The DMS network observes communications by detecting acknowledgment of readiness status for communication and monitoring digital signal transmission integrity. The network controllers schedule transmissions, select available communication routes, and determine and report if any communication errors occur.

The DMS data processors accept system user instructions to execute software

programs (routines) and retrieve or store data. The data processors acquire data from the DMS communication network, store plant process variable and status data, and record sequence of events. The data processors schedule execution of processing tasks and identify unauthorized interactions or data security violations. The data processors communicate data to peripheral devices (e.g., printers, video display generators, etc.) and report processing errors and corrective measures.

7.3.4.2 Interface with the Nuclear Island

The DMS has electronic signal communication interfaces with the instrumentation and control portions of those Nuclear Island Systems listed in the PSCS interface Table 7.3-4. The interfaces consist of digital, analog, and discrete electrical signal wiring/cabling connections. For those interfaces with "safety-related" systems (e.g., the Safety Protection Subsystem of the PPIS), the interface consists of DMS optical signal conditioning electronics mounted within a DMS cabinet and an optical signal cable/coupler. The cable/coupler carries unidirectional signals transmitted from an optoisolator device that is a part of the "safety-related" equipment. The cable/coupler is supplied as part of the "safety-related" system. These interfaces, like all other interfaces with the DMS, are used for "nonsafety-related" functions.

7.3.4.3 Safety Evaluation of Interfaces

Since the DMS does not perform any "safety-related" functions, unavailability of those portions of the DMS that interface with "safety-related" systems does not challenge plant safety protection. The DMS equipment is physically separated and electrically isolated from "safety-related" equipment.

TABLE 7.3-1

PLANT SUPERVISORY CONTROL SUBSYSTEM
NORMAL STARTUP/SHUTDOWN STRATEGY

OBJECTIVE: SEQUENTIALLY MANEUVER REACTOR MODULES (incrementally if in parallel) TO STABLE OPERATING CONDITIONS.

(underlined items below are operator permissives required to continue automatically.)

- CONFIRM AUXILIARY SYSTEMS IN SERVICE AND INITIAL CONDITIONS MET (pressurization, etc.)
- REQUEST MODULE STARTUP
- MONITOR SUBCRITICALITY TESTS AND CONDITIONS
- INDICATE ACHIEVEMENT OF CRITICALITY TO OPERATOR
- ASCERTAIN PROPER FEEDWATER CHEMISTRY
- REQUEST MODULE STEAM PRODUCTION
- CONFIRM ESTABLISHMENT OF REQUIRED MODULE STEAM AND MAIN STEAM HEADER CONDITIONS (e.g., pressure, temperature, etc.) FOR MODULE HEADERING
- REQUEST CONNECTION TO MAIN STEAM HEADER AND INCREASE MAIN STEAM LOAD INDEX
- REQUEST ESTABLISHMENT OF TURBINE SEALS, CONDENSER VACUUM AND TURNING GEAR OPERATION

TABLE 7.3-2

PLANT SUPERVISORY CONTROL SUBSYSTEM
NORMAL POWER GENERATION STRATEGY

OBJECTIVE: MANEUVER ALL MODULES IN PARALLEL FROM 25 PERCENT TO 100 PERCENT RATED LOAD AFTER OPERATOR PERMISSIVES ARE ACKNOWLEDGED.

STRATEGY:

- o CONVERT PLANT OUTPUT DEMAND (MWe or percent capacity) INTO TOTAL FEEDWATER AND MAIN STEAM DEMANDS

- o DETERMINE LOAD DEMANDS AND RATES OF LOAD CHANGE RELATIVE TO

  <u>design rated</u> plant capacity if all modules are unconstrained

  <u>available</u> plant capacity if any modules are constrained

- o EQUALLY ALLOCATE INDIVIDUAL REACTOR MODULE FEEDWATER AND MAIN STEAM ADMISSION DEMANDS (FOR AVAILABLE REACTOR MODULES AND T-G's)

- o IF - ANY MODULES ARE CONSTRAINED and

  IF - THE PLANT LOAD CHANGE RATE REQUIRES MODULE LOAD CHANGES AT RATES EXCEEDING THOSE USED TO MEET 15 PERCENT STEP LOAD INCREASES

  THEN - DECREASE THE PLANT LOAD CHANGE RATE TO THAT RATE ACHIEVABLE BY THE UNCONSTRAINED MODULES

TABLE 7.3-3

PLANT SUPERVISORY CONTROL SUBSYSTEM
ABNORMAL POWER GENERATION STRATEGY

OBJECTIVE: MAINTAIN POWER GENERATION UNLESS INVESTMENT PROTECTION IS CHALLENGED OR COMPROMISED.

STRATEGY:

o	IF	- REACTOR POWER IS GREATER THAN HEAT SINK CAPABILITY (e.g., turbine trip, feedwater reduction, etc.)
	THEN	- INITIALLY DECREASE REACTOR MODULE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK
	AND	- FOR A TURBINE TRIP, EVENTUALLY INCREASE ALL LOAD INDICES IF AT LEAST ONE TURBINE IS AVAILABLE
o	IF	- REACTOR POWER IS LESS THAN HEAT SINK CAPABILITY (e.g., module trip, etc.)
	THEN	- ASCERTAIN PLANT ABILITY TO MAINTAIN THE ORIGINAL PLANT OUTPUT
	AND	- EVENTUALLY INCREASE REACTOR MODULE LOAD INDICES TO COMPENSATE FOR REDUCED PLANT OUTPUT
	OTHERWISE	- REDUCE TURBINE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK

TABLE 7.3-4

IDENTIFICATION OF INTERFACES FOR THE PLANT SUPERVISORY CONTROL SYSTEM

Interfacing Systems	Nature of the Interface	Interface Requirements
Reactor System	Provide the capability for data, information, or signal inputs to be acquired for the following:	Ascertain shutdown margins and reactor power levels
		Ascertain control rod position and rate of vertical movement
		Monitor neutron flux levels
		Ascertain block valve operational status
		Ascertain pressure relief valve operational status
		Ascertain rupture disc operational status
		Monitor He gas storage, transfer, and delivery

TABLE 7.3-4 (Cont.)

Interfacing Systems	Nature of the Interface	Interface Requirements
Reactor System (Cont)	Provide the capability to accept "nonsafety-related" signal inputs representing the following:	Request for movement of inner control rods
		Request for movement of outer control rods
		Trip (release) of inner rods
		Trip (release) of outer rods
Vessel System	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of pressure relief processes
Reactor Services Group	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of reactor service equipment and storage wells
		Conditions and operational status of helium purification processes
		Operational status of helium storage and transfer
		Conditions and status of liquid nitrogen systems

TABLE 7.3-4 (Cont.)

Interfacing Systems	Nature of the Interface	Interface Requirements
Reactor Services Group (Cont.)		Conditions and operational status of reactor plant cooling water
		Status of liquid, gaseous and solid radioactive waste handling
Heat Transport System	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of main circulators and steam generators
Miscellaneous Control Instrumentation Group	Provide the capability for data, information or signal inputs to be acquired for the following:	Monitor radiation, seismic, meteorological, fire and security conditions
Plant Protection and Instrumentation System	Provide the capability for data, information or signal inputs to be acquired for the following:	Ascertain whether or not plant parameters are within the limits used to avoid exceeding 10CFR100 radionuclide release limits.
		Being informed of the occurrence of reactor trips

TABLE 7.3-4 (Cont.)

Interfacing Systems	Nature of the Interface	Interface Requirements
Plant Protection and Instrumentation System (Cont.)		Being informed of PPIS equipment operating status
		Accident conditions
		Completion of protective actions
		Assess whether or not a reactor is shut down and maintained as such when required
		Assess the type and extent of release of radioactive materials
		Assess site meteorological conditions
Power Conversion Group	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of feedwater and condensate processes Turbine-generators and their auxiliaries Main and bypass steam processes Extraction auxiliary steam processes Drains and condensate returns Condensate polishing processes

TABLE 7.3-4 (Cont.)

Interfacing Systems	Nature of the Interface	Interface Requirements
Power Conversion Group (Cont.)		Steam venting and draining processes Turbine plant sampling processes Chemical feed processes Turbine Building closed cooling water processes Startup and shutdown system and processes Steam and water dump processes
Heat Rejection Group	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of circulating water processes Circulating water makeup and blowdown processes Service water processes
Fuel Handling, Storage and Shipping	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of core refueling Site fuel handling Spent fuel storage cooling

TABLE 7.3-4 (Cont.)

Interfacing Systems	Nature of the Interface	Interface Requirements
Fuel Handling, Storage and Shipping (Cont)		Ensure that provisions are made in the FHSSS for communication between refueling operators and control room operators.
Shutdown Cooling System	Provide the capability for data, information or signal inputs to be acquired for the following:	Conditions and operational status of shutdown circulators and heat exchangers
		Monitor shutdown cooling circulator speed and helium flows and temperatures

TABLE 7.3-4A

NSSS MODULE CONTROL MEASUREMENTS

Primary Measurements

- Module feedwater flow
- Helium flow
- Circulator speed
- Reactor power
- Control rod positions
- Module main steam temperatures
- Module steam pressure
- Helium pressure
- Circulator motor cooling water temperature

Other measurements:

- Isolation and shutoff valve positions
- Isolation and startup control breaker positions
- Analog valve positions
- Status of SCS and HPS systems

TABLE 7.3-5

NSSS MODULE STARTUP SEQUENCE FROM DEPRESSURIZED CONDITIONS

Time	Action
STARTING POINT	
0-0.5	Increase secondary pressure (startup bypass setpoint) to 82.8 bars abs (1200 psia) at 1.17 bars/min (17 psi/min).
0-5	Pressurize primary coolant vessels to full helium inventory, perform precritical checks, and bring reactor to critical (0.5% power).
5-5.8	Increase feedwater flow to 15% (0.21%/min). Increase reactor power to 3% (0.053%/min). Increase circulator speed from 5% (minimum value) to 12.5% (0.16%/min).
6-11	[Hold at about 204°C (400°F) steam generator secondary outlet temperature for feedwater cleanup as necessary].
HOLD	
10-10.5	Increase secondary pressure to 124.14 bars abs (1800 psia) at 1.38 bars/min (20 psi/min).
11.1-13.8	Increase feedwater temperature from 104°C (220°F) to 194°C (380°F) at 0.56°C/min (1.0°F/min).
11.1-12.8	Increase power to 7% (0.039%/min).
HOLD	
12.8-13.3	Increase power to 16% (0.30%/min). Increase circulator speed to 30% (0.58%/min).
13.0-13.6	(Transition to boiling.)
14.3-16.3	Decrease reactor power to 14.7% (0.011%/min).
14.5-18.6	[Hold at about 427°C (800°F) main steam temperature for secondary component warmup as necessary.]
HOLD	
18.1	Place reactor power and circulator speed in automatic main steam temperature control [setpoint at 442°C (826°F)].

TABLE 7.3-5 (Cont)

Time	Action
18.6-20.1	Ramp main steam temperature setpoint to 542°C (1010°F) at 1.11°C/min (2.0°F/min).
19.1-20.1	Increase secondary pressure setpoint to 268.96 bars abs (2450 psia) at 0.76 bars/min (11 psi/min).
HOLD	
20.1-20.8	Stabilize module parameters and transfer steam flow from startup bypass to main steam header. Place feedwater flow in automatic control.

TABLE 7.3-6

FAILURE MODES AND EFFECTS ANALYSIS FOR THE NSSS CONTROL SUBSYSTEM

No of Affected Modules	Function	Failure Mode	Failure Effect	Detection Method	Remarks
1	Module Main Steam Temperature	Control Algorithm Output fails:			
		High:	Reactor power or circulator speed increases. Possible PPIS reactor module trip on high power to flow ratio.	Measured neutron flux, circulator speed and primary coolant flow. High main steam temperature alarm in NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
		Low:	Reactor power or circulator speed decreases. Possible circulator speed to feedwater flow mismatch trip or main turbine trip on low steam temperature.	Measured neutron flux, circulator speed and main steam temperature. Low main steam temperature alarm in NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

TABLE 7.3-6 (Cont.)

No of Affected Modules	Function	Failure Mode	Failure Effect	Detection Method	Remarks
1	Module Feed-water Flow	Control Algorithm Output Fails:			
		High	Reactor module output increases beyond load allocated by the Supervisory Control System. Possible PPIS action on exceeding module load output limits.	High module load alarm in the Supervisory Control System. High feedwater flow alarm in NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
		Low	Reactor module output decreases to less than load allocated by the Supervisory Control System. Possible PPIS action on-module parameters decreasing to less than investment or safety limits.	Low module load alarm in the Supervisory Control System. Feedwater flow error high alarm in the NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

TABLE 7.3-6 (Cont.)

No of Affected Modules	Function	Mode	Failure Effect	Failure Method	Detection Remarks
All	Main Steam Pressure in the main steam header in the 25% to 100% power range. This pressure is controlled in part by the BOP throttle valve. However, a failure of this function is discussed in this NSSS section to cover its effects on the NSSS module and its control system.	Control Algorithm Output fails:			
		High	Main turbine admission valves begin to open. Main steam pressure decreases in all modules. Turbine speedload controls stabilize load at lower pressure or initial pressure limiter acts to protect turbines. Possible turbine trip and load runback.	High plant load alarm in the supervisory control system. Low main steam pressure alarm in the NSSS Control Subsystem.	Possible loss of plant load. Control hardware and software fault tolerance may allow minimum decrease in plant output.
		Low	Main turbine admission valves begin to close. Main steam pressure increases in all modules. Turbine speedload controls stabilize load at higher pressure or main steam bypass and/or relief valves open. Possible PPIS action on module parameters increasing to investment or safety limits.	Low plant load alarm in the supervisory control system. Main steam pressure error low alarm in the NSSS NSSS Control Subsystem.	Possible loss of plant load. Control hardware and software fault tolerance may allow minimum decrease in plant output.

TABLE 7.3-6 (Cont.)

No of Affected Modules	Function	Mode	Failure Effect	Failure Method	Detection Remarks
1	Circulator Speed	Control Algorithm Output Fails:			
		High	Module circulator speed increases. PPIS speed-to-primary coolant flow mismatch trip.	Measured circulator speed high alarm in the NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
		Low	Module circulator speed decreases. PPIS speed-to primary coolant flow mismatch trip.	Measured circulator speed low alarm in the NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

TABLE 7.3-6 (Cont.)

No of Affected Modules	Function	Mode	Failure Effect	Failure Method	Detection Remarks
1	Reactor Power	Control Algorithm Output fails:			
		High	Module reactor power increases. Group rod insertion occurs on high neutron flux. Possible PPIS action to trip module when parameters increase to investment or safety limits.	High measured neutron flux and main steam temperature alarm in the NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
		Low	Module reactor power decreases. Module primary and secondary coolant temperatures decrease. Possible PPIS action to trip module when parameters decrease to investment or safety limits.	Low measured neutron flux and main steam temperature alarm in the NSSS Control Subsystem.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

TABLE 7.3-7

IDENTIFICATION OF INTERFACES FOR THE NSSS CONTROL SUBSYSTEM

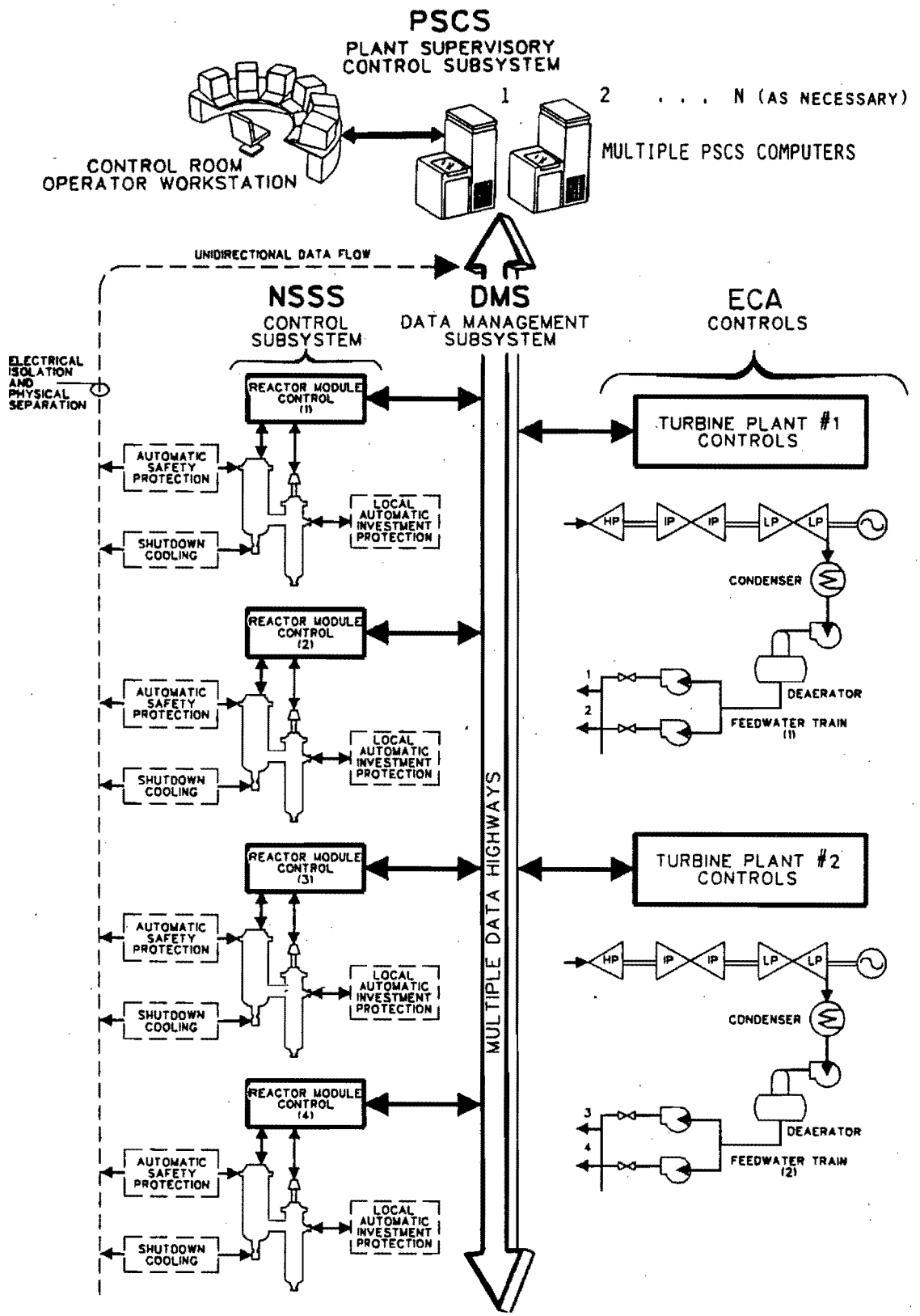
Interfacing Systems	Nature of Interface	Interface Requirements
PSC Subsystem	Transmission of module load index signals and sequence hold points from PSCS to NSSS Control Subsystem. Transmission of acknowledgement signals from NSSS Control Subsystem to PSCS. Transmission of module load limitations to PSC Subsystem.	Compatible data highway protocol HDLC-based.
Feedwater and Condensate System	Transmission of module feedwater flow signals to NSSS Control Subsystem.	4-20 mA transmitter output or compatible data highway protocol.
	Feedpump trip signal.	1-5 V dc or suitable relay contact closure.
	Transmission of module flow control algorithm output to plant feedwater flow controls.	4-20 mA transmitter output or compatible data highway protocol.
	Transmission of NSSS component trip signals to T/G controls	4-20 mA transmitter output or compatible data highway protocol.
	Transmission of T/G runback signals to NSSS Control Subsystem.	4-20 mA transmitter output or compatible data highway protocol.
Main and Bypass Steam System	Transmission of main steam pressure measurement to NSSS main steam pressure control. algorithm.	4-20 mA transmitter output or compatible data highway protocol.

TABLE 7.3-7 (Cont.)

Interfacing Systems	Nature of Interface	Interface Requirements
Main and Bypass Steam System (Cont.)	Thermocouple wells for main steam temperature sensors.	Compatibility of temperature sensor with thermocouple well (location, size, time, response, etc.)
	Transmission of main steam pressure control algorithm output signal to main steam bypass valve servo amplifiers.	4-20 mA transmitter output or compatible data highway protocol.
Neutron Control Subsystem	Transmission of reactor module power characterization output signal to the neutron flux control algorithm setpoint receiver.	4-20 mA transmitter put or compatible data highway protocol.
	Transmission of NSSS startup, shutdown, etc. sequence hold points to neutron flux control sequencing logic.	1-5 V dc or suitable relay contact closure.
Heat Transport System	Transmission of reactor module circulator speed characterization output signal to the circulator speed control algorithm setpoint receiver.	4-20 mA transmitter output or compatible data highway protocol.
	Transmission of HTS parameters to module data highway.	4-20 mA transmitter output or compatible data highway protocol.
PPIS	Transmission of PPIS actions to NSSS Control Subsystem logic.	Compatible data highway protocol.

TABLE 7.3-7 (Cont.)

Interfacing Systems	Nature of Interface	Interface Requirements
Reactor System	Transmission of reactor parameters to NSSS Control Subsystem data highways.	4-20 mA transmitter output or compatible data highway protocol.
Data Management Subsystem (DMS)	Data link between PSCS and NSSS module data highways.	Compatible data highway protocol.
Control Building and HVAC System	Space to house NSSS Control Subsystem equipment. HVAC capacity.	TBD sq m (sq ft). 75°F 55% max relative humidity MIL-STD-1472C.
Uninterruptible Power Supply System	Power supply to critical NSSS Control Subsystem components.	120 V ac 2 divisions. TBD kW per division.
AC Distribution System	Power supply to NSSS Control Subsystem components.	120 V ac 2 divisions. 26 kW per division.
Reactor Building and HVAC System	Space to house NSSS Control Subsystem equipment. HVAC capacity.	TBD sq m (sq ft). [TBD°C]. ([TBD°F]) [TBD% r.h.].



---- DASHED PORTIONS ARE NOT A PART OF THE PCDIS (INCLUDED FOR COMPLETENESS OF ILLUSTRATING KEY FUNCTIONAL PARTITIONS)

FIGURE 7.3-1
PCDIS INTEGRATED CONTROL OVERVIEW
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

LEGEND

1. For limiting plant baseload & load following demands
2. For receiving operator instructions
3. For decoding operator instructions
4. For acquiring plant data
5. For monitoring the status of plant systems, processes, maintenance refueling, etc.
6. For automatic control decision-making
7. For preventing improper automatic actions & assisting operator decisions
8. For issuing commands to subordinate control systems
9. For communicating commands and reporting data/status
10. For providing data to be presented to the operator

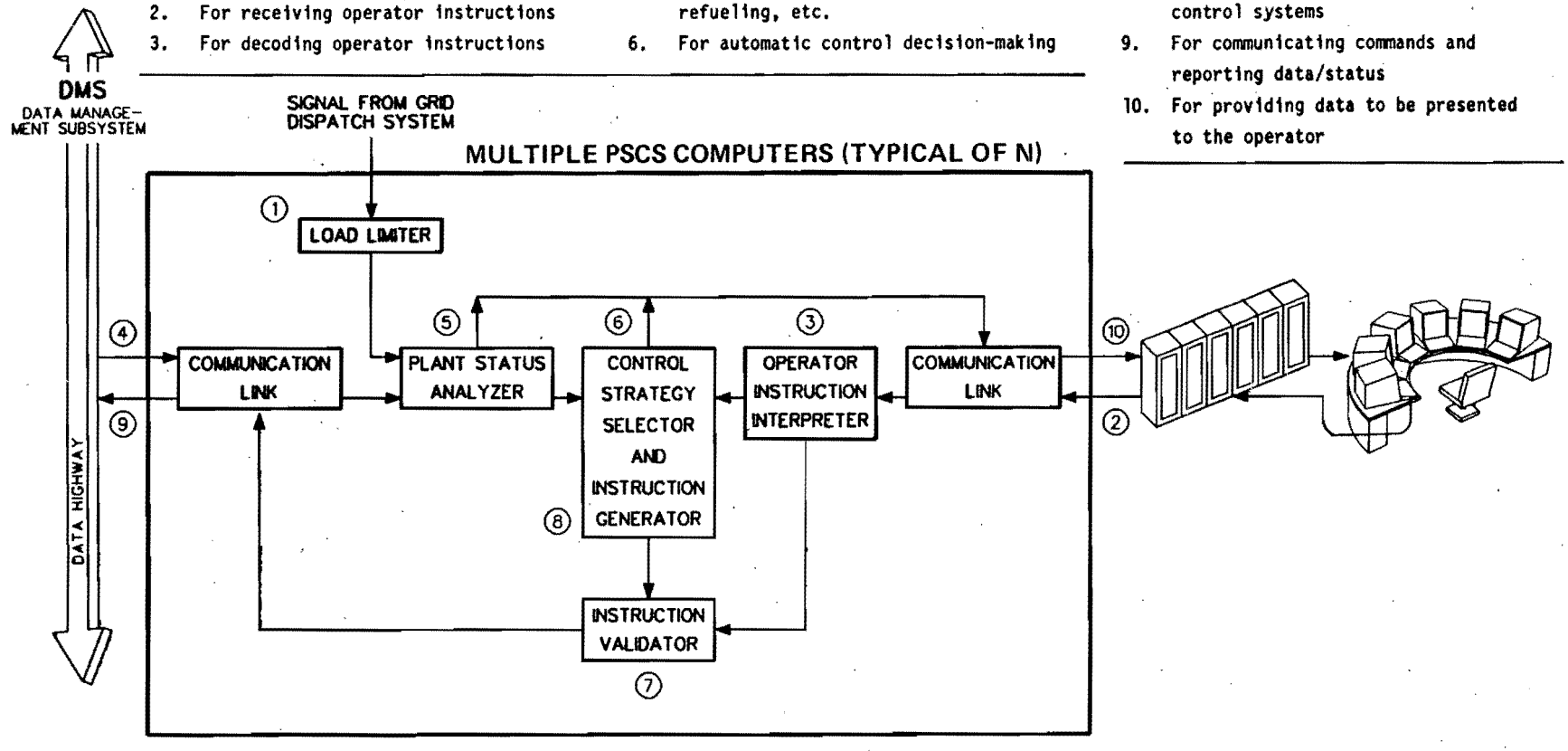
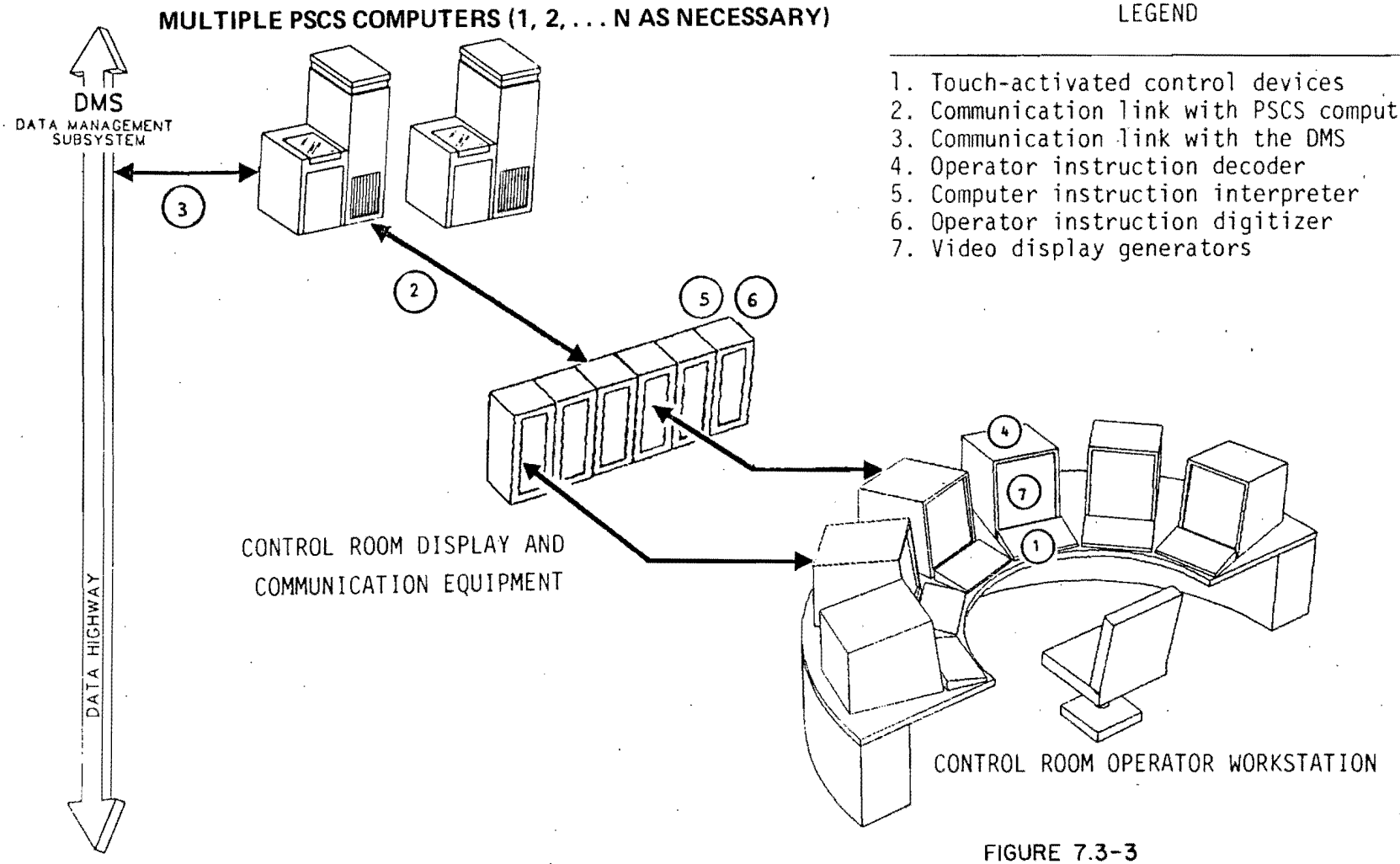


FIGURE 7.3-2
FUNCTIONAL CONFIGURATION OF PSCS COMPUTERS
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024



LEGEND

1. Touch-activated control devices
2. Communication link with PSCS computers
3. Communication link with the DMS
4. Operator instruction decoder
5. Computer instruction interpreter
6. Operator instruction digitizer
7. Video display generators

FIGURE 7.3-3
FUNCTIONAL CONFIGURATION OF OPERATOR WORKSTATION
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

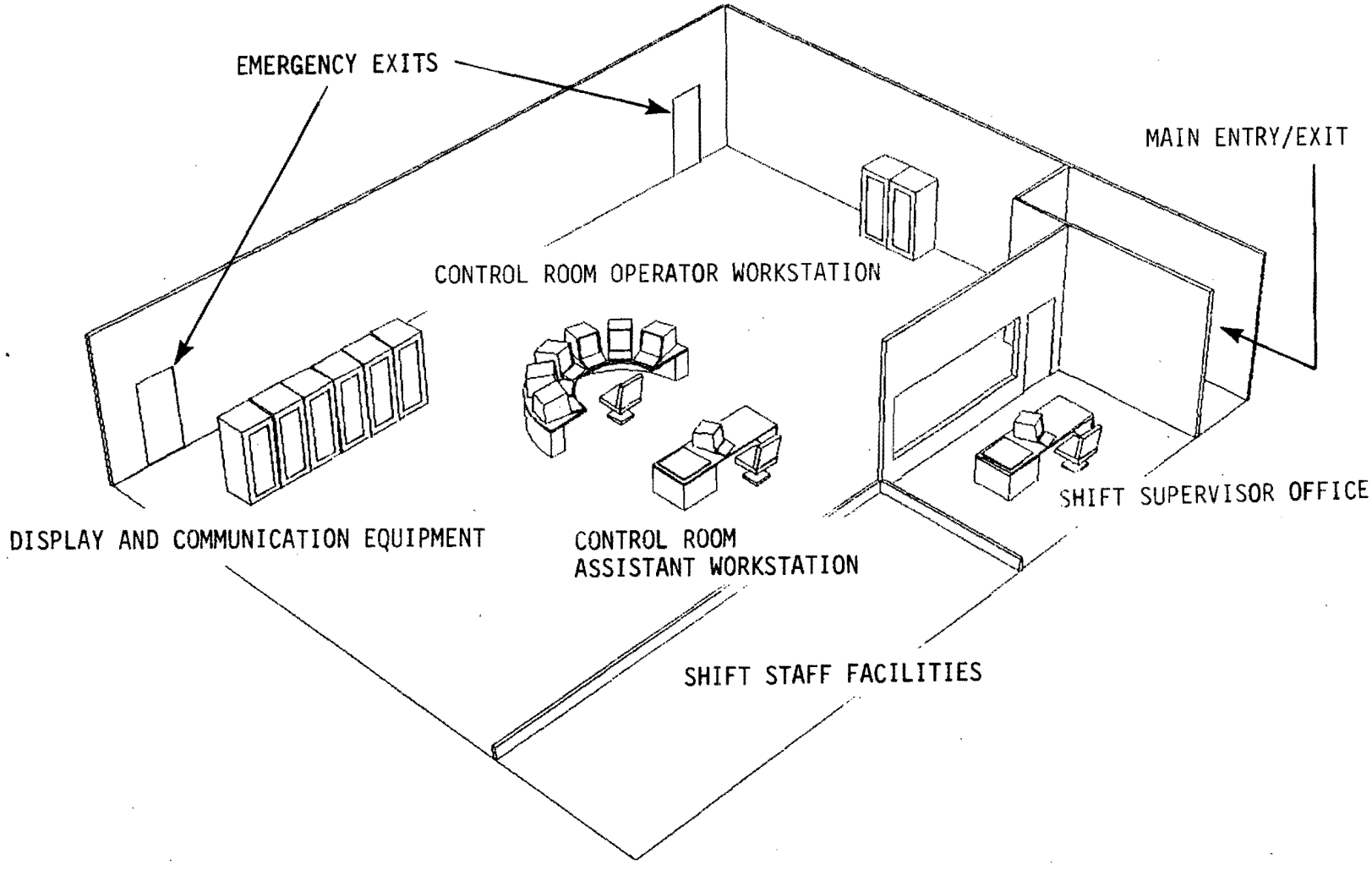


FIGURE 7.3-4
SINGLE CONTROL ROOM ARRANGEMENT
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

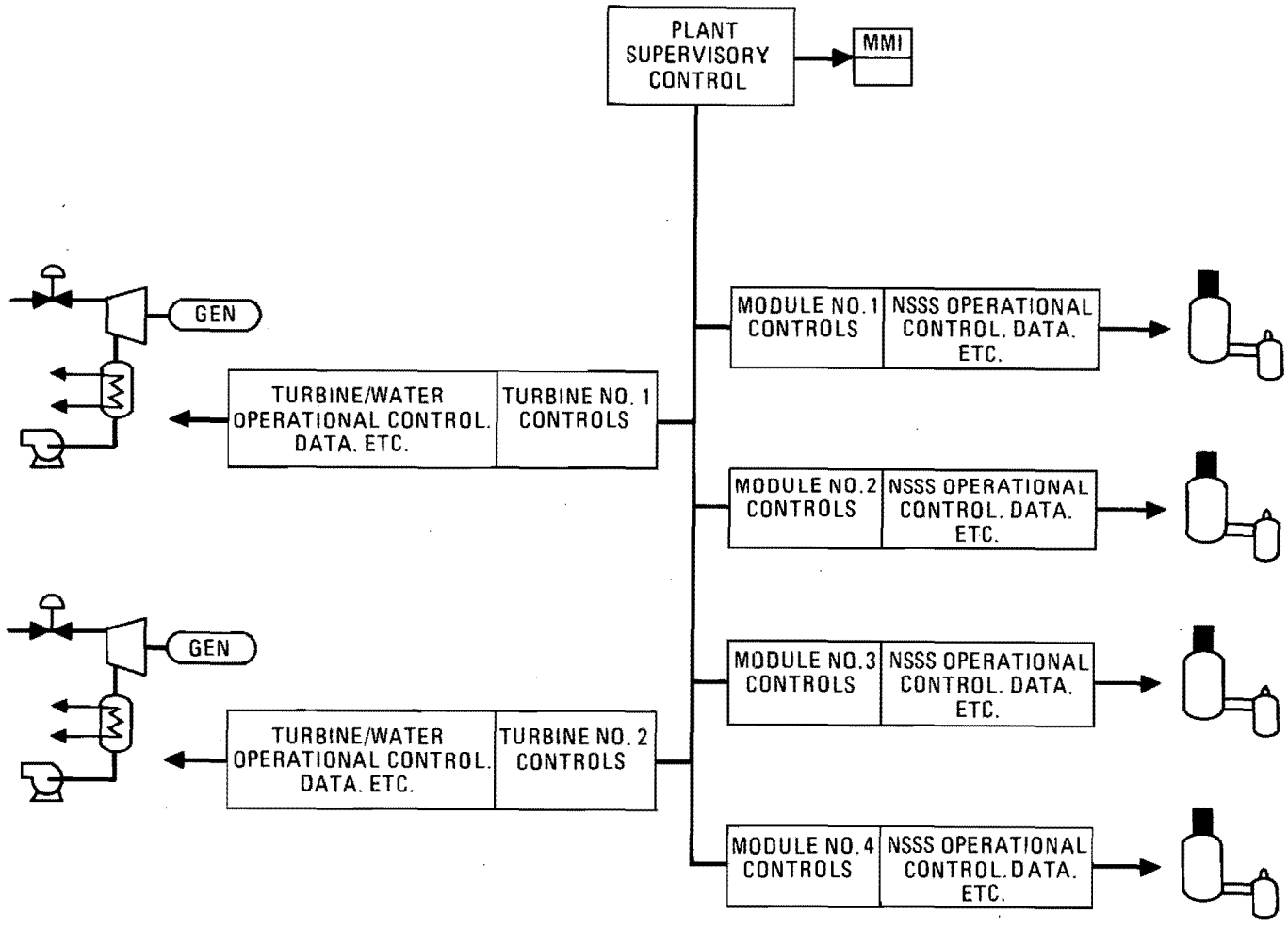


FIGURE 7.3-5

SUMMARY DESCRIPTION: DISTRIBUTED, MODULAR ARCHITECTURE

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

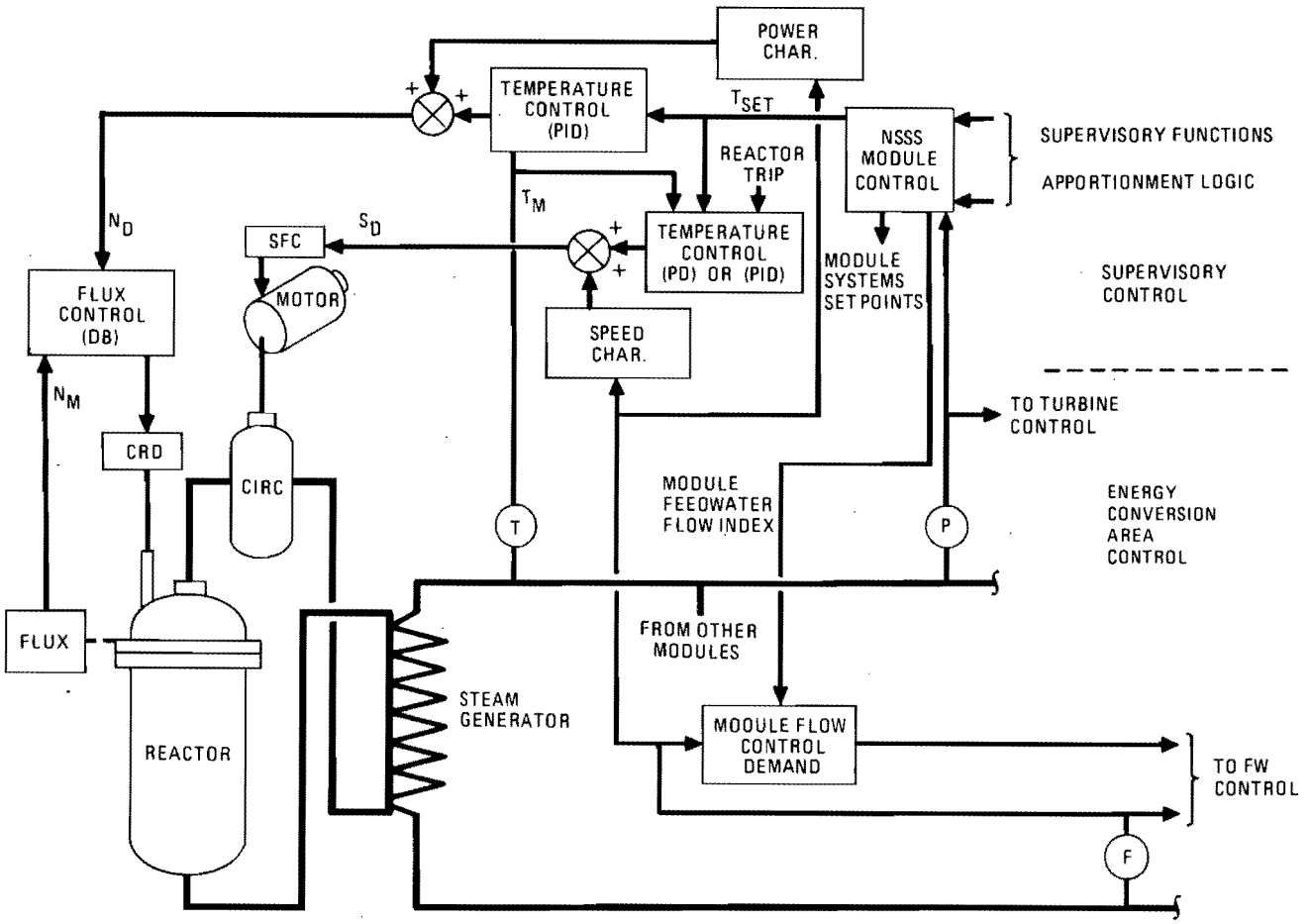


FIGURE 7.3-6

NSSS CONTROL FUNCTIONS AND INTERFACES

HIGH TEMPERATURE GAS-COOLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024

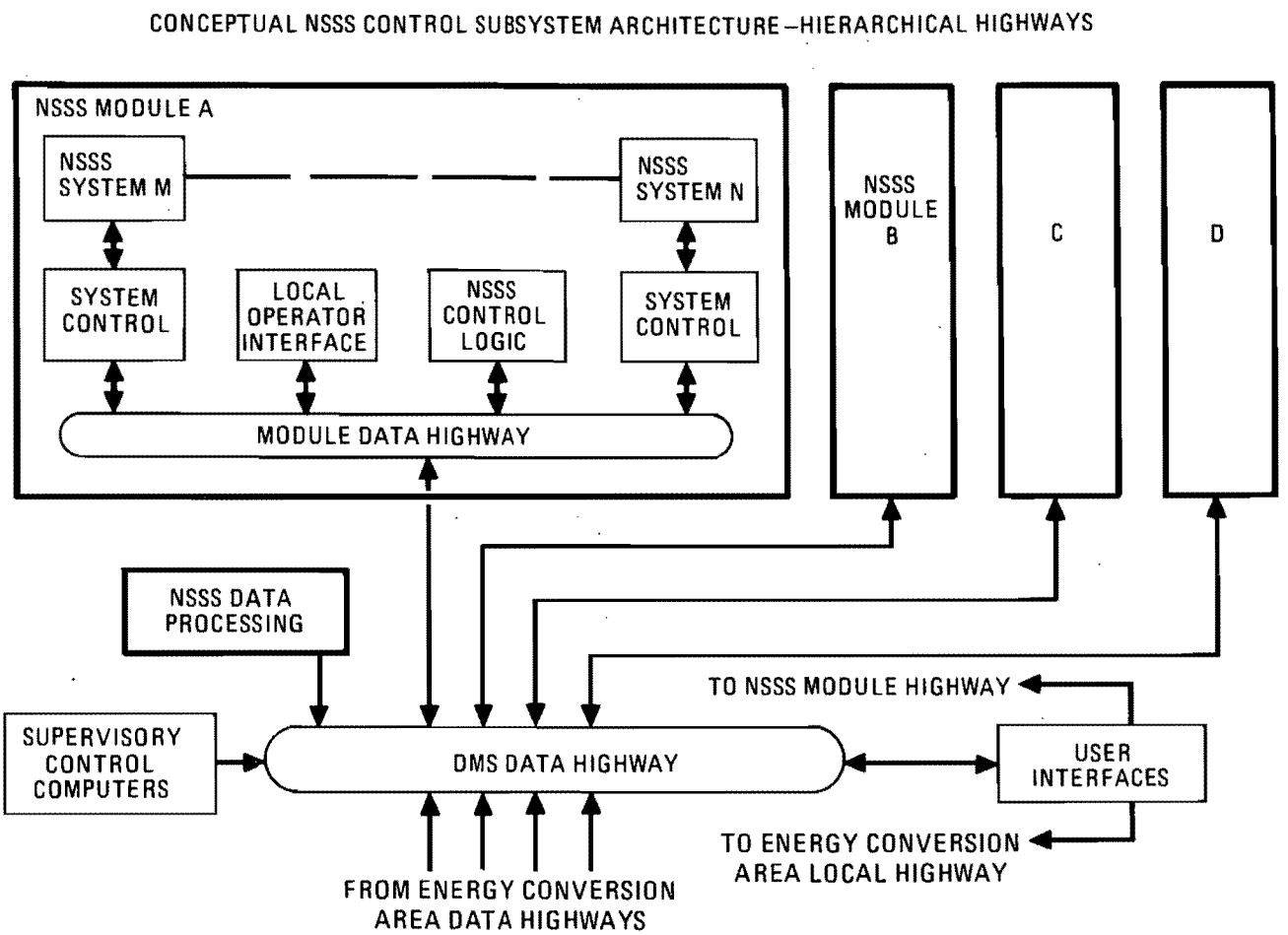


FIGURE 7.3-7

CONCEPTUAL NSSS SUBSYSTEM ARCHITECTURE

HIGH TEMPERATURE GAS-COOLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024

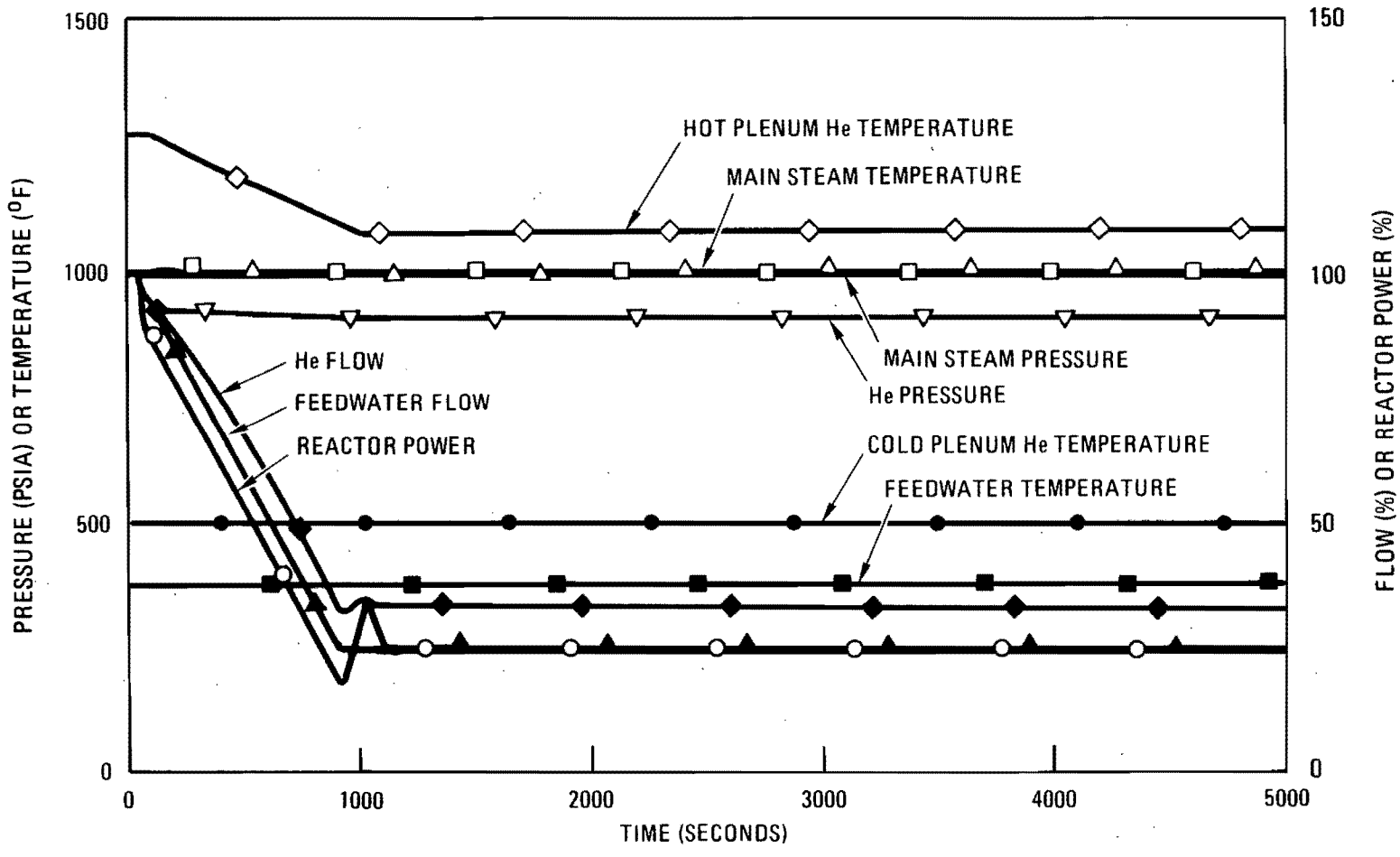


FIGURE 7.3-8

MHTGR MODULE RESPONSE TO LOAD RAMP

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

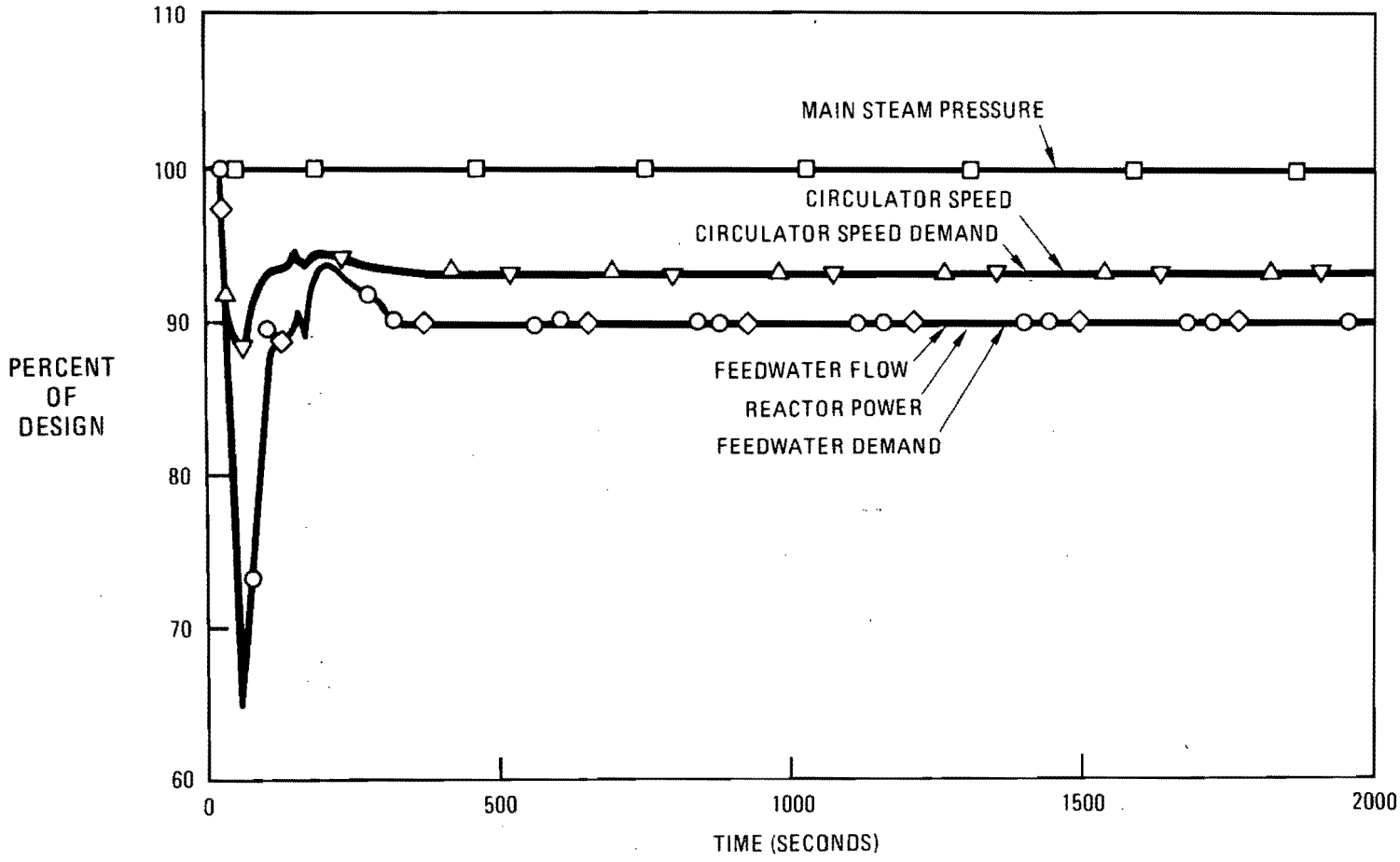


FIGURE 7.3-9

MHTGR MODULE RESPONSE TO LOAD STEP

HIGH TEMPERATURE GAS-COOLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024

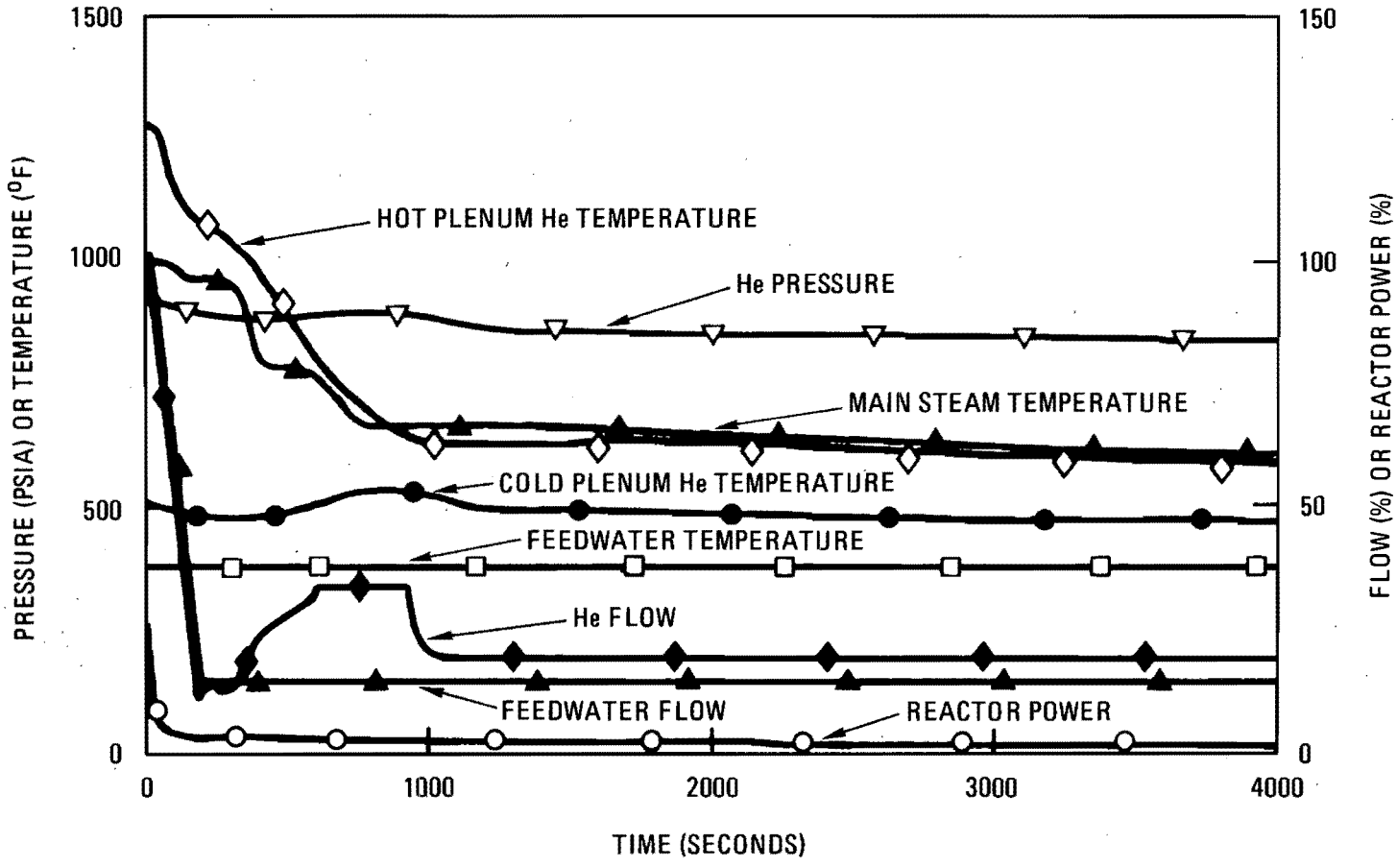


FIGURE 7.3-10

MHTGR MODULE RESPONSE TO REACTOR TRIP

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024

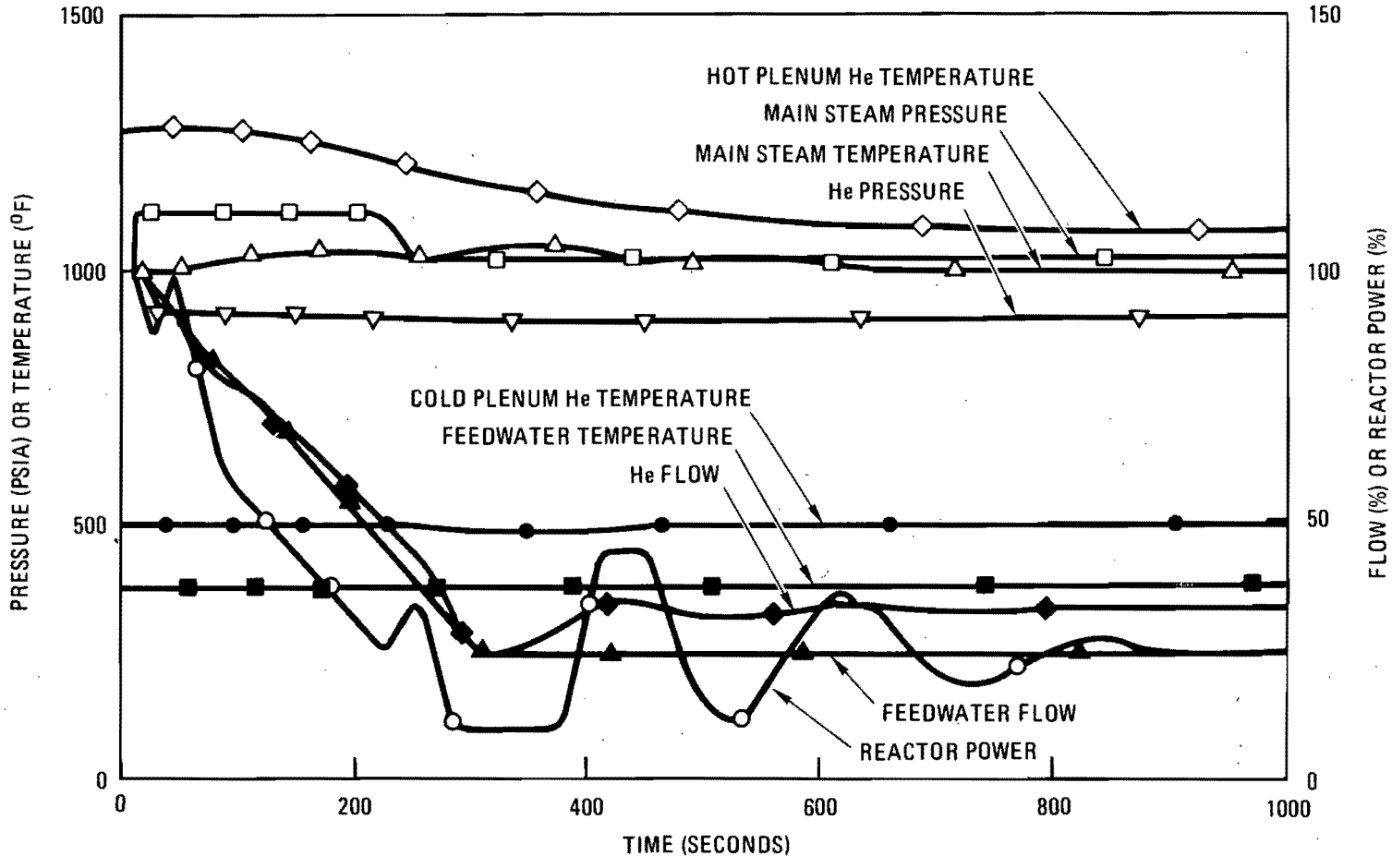


FIGURE 7.3-11

MHTGR MODULE RESPONSE TO TURBINE TRIP

HIGH TEMPERATURE GAS-CODLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024

7.4 MISCELLANEOUS CONTROL AND INSTRUMENTATION GROUP

The Miscellaneous Control and Instrumentation Group includes the following systems:

1. NSSS Analytical Instrumentation
2. Radiation Monitoring
3. Seismic Monitoring
4. Meteorological Monitoring
5. Fire Detection and Alarm

7.4.1 NSSS Analytical Instrumentation System

7.4.1.1 Summary Description

The Analytical Instrumentation System (AIS) provides analytical instrumentation piping and controls needed for gas sampling and sample conditioning, as well as primary coolant impurity detection, identification, and measurement.

The monitored primary coolant impurities include noncondensible gases (gases which do not condense under reactor conditions) and condensible vapors. The noncondensible gases consist of the chemical impurities carbon monoxide (CO), carbon dioxide (CO_2), methane (CH_4), nitrogen (N_2), hydrogen (H_2), oxygen (O_2), water (H_2O); the noble gas radionuclides argon (Ar), krypton (Kr) and xenon (Xe); and the radionuclide tritium. Also water may be present in the primary coolant as a vapor or liquid. The important condensible vapors are the radionuclides iodine (I), cesium (Cs), strontium (Sr), and silver (Ag).

7.4.1.2 Functions and 10CFR100 Design Criteria

7.4.1.2.1 Power Generation Functions

The power generation function of the AIS is to maintain energy production, shutdown, refueling, and startup/shutdown by monitoring the primary coolant for impurities.

7.4.1.2.2 Radionuclide Control Functions

The functions of the AIS for maintaining control of radionuclide release are to limit radiation transport from the primary coolant by monitoring circulating primary coolant and plateout activities, and to control radiation exposure by monitoring radionuclides within the system.

7.4.1.2.3 Classification

The AIS is not "safety related". Since this system does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, this system will have the appropriate reliability to meet user requirements.

7.4.1.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to this system.

7.4.1.3 Radionuclide Control Design Requirements

1. The AIS shall provide the means to monitor circulating primary coolant activity.

2. The AIS shall provide the means to monitor primary coolant plateout activity.

3. The AIS shall provide the means to protect the operator from radionuclide activity within the subsystem.

7.4.1.4 Design Description

7.4.1.4.1 System Configuration

The AIS automatically extracts samples of circulating primary coolant from the Vessel System, Helium Purification Subsystem, and Gaseous Radioactive Waste Subsystem as illustrated in Figure 7.4-1. It detects, identifies, and measures the presence and quantity of primary coolant noncondensible gases as well as iodine and provides this data to plant personnel to confirm primary coolant quality and satisfactory operation of the Helium Purification Subsystem.

The capability for gas sampling and radiological monitoring is provided while the source systems and subsystems are either pressurized or depressurized. Each primary coolant impurity is detected automatically by on-line analytical instruments such as chromatographs. The sequence in which this is done is established by programmable controllers.

The presence and quantity of noncondensible gases and iodine can also be determined by extracting grab samples in a sample container of primary coolant from the Vessel System, Helium Purification Subsystem, or the Gaseous Radioactive Waste Subsystems for further diagnostic analysis in a radiological laboratory.

The AIS consists of two major components. The first is the depressurization rack. Its purpose is to reduce the pressure of the incoming gas samples to the required operating pressure of the analytical instruments. The second component is the analytical instrument module. It contains the analytical instruments, signal conditioning, and interfacing electronics. Both modules contain activity monitors to ensure personnel protection from radiological exposure while servicing the components.

A "block and bleed" piping arrangement is provided for multiple sample streams which are routed to a common manifold. This approach prevents measurement error caused by contamination of an incoming sample stream by leakage past a shutoff valve.

The sample piping and valves are sized to minimize flow rates without excessively long sample transport delays. Means are included for measuring sample pressures, flow rates, and for detecting low flows.

Eleven types of measurements are needed for process radiation and primary coolant impurity monitoring. Each type monitors a process activity or primary coolant impurity and includes all of the needed instrumentation and sampling equipment. The first six types employ sampling detectors wherein a gas sample is drawn into a shielded container for activity analysis. The seventh uses airborne activity and gamma monitors which provide for operator protection from radiological exposure. Types 8 through 10 perform primary coolant impurity monitoring which is accomplished with a process chromatograph or dedicated analysis instrument. The eleventh type provides the capability of measuring condensible vapors by the use of a plateout probe.

The following tabulation lists each measurement type and its description. Note that primary coolant is assumed to be present in the Vessel System, Helium Purification Subsystem, and Gaseous Radioactive Waste Subsystem.

Measurement Type Number	Description
1	Continuous monitoring of gross gaseous activity to detect changes in primary coolant noble gas concentration to provide process control checks.
2	Provision for sampling of primary coolant for tritium analysis.
3	Detection of noble gas breakthrough from the first low temperature adsorber in the Helium Purification Subsystem. Types 3 and 4 use the same radiation monitor.

4 Measurement of noble gas activity in outlet of filter downstream of Helium Purification Subsystem second low temperature adsorber to provide process control. Types 3 and 4 use the same radiation monitor.

5 Measurement of noble gas activities in the Radioactive Gaseous Waste Subsystem surge tanks.

6 Provision for manual grab sampling of primary coolant for tritium analysis or other radionuclides.

7 Measurement of gamma and airborne activity changes in the enclosed area of analytical instrument module. Two monitors are used.

8 Primary coolant impurity monitoring.

9 On-line monitoring for carbon monoxide in the Vessel System.

10 On-line monitoring of primary coolant for water in the Vessel System and Helium Purification Subsystem.

11 Manually removable probe to detect primary coolant condensible vapor plateout.

7.4.1.4.2 System Arrangement

The depressurization rack is located as close as practical to the Vessel System to minimize the length of the high-pressure sample lines. The analytical instrument module is located adjacent to the depressurization rack to minimize sample line length but in a location where manned access is easily attainable.

7.4.1.4.3 System Operating Modes

The system is normally operated in an automatic mode wherein a data base of information is maintained and alarms are actuated when primary coolant impurities are excessive. An operator programs a controller to take samples of primary coolant automatically and insert them into either a process chromatograph for impurity analysis or radiation monitors for analysis of tritium and noble gases. A separate monitor continuously monitors carbon monoxide in the Vessel System.

Parts of the system also can be operated manually. Special grab samples of primary coolant can be taken from the Vessel, Helium Purification, or Gaseous Radioactive Waste Systems and analyzed manually. The plateout probe must be handled manually.

Sampling operations can be performed at all levels of reactor power and vessel pressure. When the reactor is fully depressurized, gas samples are pumped to provide a positive pressure at the inlet of the analytical instruments.

7.4.1.5 Design Evaluation

7.4.1.5.1 Failure Modes and Effects

The AIS has two failure modes. The first is if the analytical instruments fail or provide an incorrect analysis of impurities. If this happens, the failure would not affect short-term reactor operation and the system will provide diagnostic data in the control room to help determine the cause of the failure and perform corrective maintenance. The second failure is a radioactive gas leak in the sample piping and valves from the Vessel System, Gaseous Radioactive Waste System, Helium Purification System, or internal to the AIS. If this happens, airborne activity monitors in the AIS or Radiation Monitoring Subsystem would alarm this condition and automatically isolate the system.

7.4.1.5.2 Steady-State Performance

The AIS continuously monitors primary coolant impurities and activity levels during all phases of plant operation. If preset alarm levels are exceeded, the control room operator is alerted. If a sample line leaks, it is automatically isolated, the control room operator is alerted, and the Plant Control Data and Instrumentation System (PCDIS) is alerted.

7.4.1.5.3 Anticipated Operational Occurrence Performance

Except for the loss of electrical power in AOO-1, the AIS operates the same as described in Section 7.4.1.5.2. A loss of electrical power will not result in any failures or release of radioactive gases. When power is restored, the AIS will return to normal operation.

7.4.1.5.4 Design Basis Event Performance

The AIS is not required to function during any design basis event (DBE), but it will be available unless electric power is lost.

7.4.1.6 Interfaces

Interface requirements imposed on other systems by the Analytical Instrumentation System are identified in Table 7.4-1, which also includes a description of the interface and a quantitative expression for the interface.

7.4.2 Radiation Monitoring System

7.4.2.1 Summary Description

The Radiation Monitoring System (RMS) consists of area monitors, airborne monitors, and process monitors located throughout the plant and at the site boundary. Certain monitors located at specific areas in the plant, in plant effluents, and at the site boundary are capable of monitoring post-accident conditions. A central radiation processor (CRP) includes RMS control and

monitoring consoles and instrumentation cabinets located in the Reactor Service Building. All RMS displays and alarms are provided to the PCDIS for presentation (see Section 7.3) in the main control room (MCR) and in the health physics/access control area in the Personnel Service Building.

7.4.2.2 Functions and 10CFR100 Design Criteria

7.4.2.2.1 Power Generation Functions

The RMS has no power generation functions.

7.4.2.2.2 Radionuclide Control Functions

The functions of the RMS for maintaining control of radionuclide release are to control radiation from various sources and to control onsite and public radiation exposure by monitoring and displaying the dose levels and effluent radionuclide concentrations at various locations in the plant and at the site boundary.

7.4.2.2.3 Classification

The RMS is not "safety related". Since the RMS does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, the system will have the appropriate reliability to meet other Top-Level Regulatory Criteria and user requirements.

7.4.2.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to the RMS.

7.4.2.3 Radionuclide Control Design Requirements

The limiting dose levels and effluent radionuclide concentrations are given in the discussion of the Top-Level Regulatory Criteria in Section 3.1. The RMS shall be capable of detecting, indicating, and reporting radionuclide

concentrations and radiation levels that are 1/10 of the top level criteria to permit timely action to be taken for problems which may cause these Top-Level Regulatory Criteria to be exceeded.

7.4.2.4 Design Description

7.4.2.4.1 System Configuration

The RMS is intended to detect, indicate, and report radionuclide concentrations and radiation levels at various locations in the plant buildings, structures and systems and at the site boundary. The monitors are controlled by local radiation processors (LRP) which transmit data on a data bus (or loop) to a central radiation processor (CRP). The CRP provides display and alarm functions and, optionally, can prepare release reports for normal and abnormal conditions. The RMS also provides input to the PPIS, with post-accident monitors providing input to the Special Nuclear Area Instrumentation Subsystem (see Section 7.2.2), and the airborne radioactivity monitors in the blowdown vent path for each Reactor Building provide input to the primary coolant pressure pumpdown portion of the Investment Protection Subsystem (see Section 7.2.3).

To minimize failures, the RMS is a microprocessor-based system employing the following features:

1. Local processor with fault diagnostics and automatic testing to detect failures.

2. Modular design for ease of replacement of components to minimize the mean time to repair.

3. Dual redundant central processors for high data processing reliability.

4. Regular periodic detector and instrument calibration and operational checks.

Also, the sampling system and portable monitors are independent of the continuous 'on-line' monitors and provide a backup means of monitoring radioactivity should a failure occur.

The Radiation Monitoring System is composed of the following equipment:

Area radiation monitors

Airborne radioactivity monitors

Portable monitors

Process radioactivity monitors

Site boundary monitors

Area Radiation Monitoring

The area radiation monitors complement the personnel and area radiation survey provisions of the plant radiation protection program (see Section 12.1) by serving to:

1. Immediately alert plant personnel entering or working in normally nonradiation or low-radiation areas (1.0 mR/hr, see Section 12.3) of abnormally high radiation levels which could result in inadvertent overexposures.

2. Inform the main control room (MCR) operators of the occurrence and approximate location of an abnormal radiation level in nonradiation or low-radiation areas.

The Area Radiation Monitors perform no function related to the quantitative monitoring of releases of radioactive material to the environment.

Airborne Radioactivity Monitoring

Airborne radioactivity monitors are used to monitor the air within an enclosure by either direct measurement of the enclosure atmosphere or of the exhaust air from the enclosure. Also, potential release paths to the environment are monitored for radionuclides. The system indicates and records the concentrations of airborne radioactivity, and, if abnormal levels occur, actuates alarms. Local alarms are provided to alert personnel in the area where airborne radioactivity concentration is at or above the setpoint value selected to ensure that top-level criteria are met. The system provides a continuous record of airborne radioactivity concentrations which will aid operating personnel in maintaining airborne radioactivity at the lowest practicable concentrations.

The type of airborne radioactivity monitors are based upon the nature and type of radioactivity expected and the location being monitored. In the case of airborne radioactivity monitors which are used to detect leakage from the reactor coolant pressure boundary, the monitors shall be seismically qualified per the guidance of Regulatory Guide 1.45 to meet specific Standard MHTGR requirements. (Ref. 1)

Where inhalation of radioactive airborne materials by plant personnel is a possibility, combination particulate halogen gaseous monitors are used to analyze, record, and alarm should the radioactivity approach the limits established by 10CFR20. The sampling system for the particulate halogen gaseous monitors is designed and installed in accordance with the ANSI-N13.1-1969 guide to sampling of airborne radioactive materials. (Ref. 2)

Portable Monitoring

Portable air activity samplers are provided to allow periodic localized monitoring of specific air volumes of interest independent of the fixed monitor systems. The samplers are used to verify that airborne activity concentrations within the plant operating spaces are within allowable limits and also to verify the proper operation of fixed monitor systems.

Process Radioactivity Monitoring

Process radioactivity monitoring is designed to keep the operators informed about the condition of routine or potential sources of radiation or radionuclide releases. For example, heat exchangers that are used between processes that may contain radioactive materials and those that do not may develop leaks from primary to the secondary side. The secondary (nonradioactive) side of the heat exchanger is monitored for radionuclides and alarms actuated in the main control room so that corrective maintenance or other appropriate action can be taken. The RMS provides a continuous record of such conditions.

Site Boundary Monitoring

Site boundary monitoring is designed to keep operators informed concerning the concentration of airborne radionuclide releases at the site boundary.

In conjunction with meteorological data, radionuclide levels at the site boundary will be assessed routinely to verify that the dose due to airborne effluents does not exceed that permitted by the Top-Level Regulatory Criteria (see Section 3.1).

7.4.2.4.2 System Arrangement

Potential locations for radiation monitors are shown in Table 7.4-2. Specific locations and numbers of monitors will be determined based on plant system layouts and the results of the shielding assessments. The location of the principal radiation monitors will be shown on the radiation zoning drawings.

The subsystem control and monitoring console is located in the Reactor Service Building in a location with convenient and continuous personnel access. Monitoring and interpretation of the radiation monitoring displays and reports will be performed by personnel other than main control room operating personnel. Selected output data are transmitted to the MCR and health physics/access control area.

Area radiation monitoring is provided in areas where personnel have routine access and for which there is a potential for personnel unknowingly to receive radiation doses in excess of defined limits in a short period of time because of system failure or improper personnel action. Any plant area which meets one or more of the following criteria is monitored:

1. Zone I areas which, during normal plant operation, including refueling, could exceed the radiation limit of 0.25 mR/hr upon system failure or personnel error or which will be continuously occupied following an accident requiring plant shutdown.

2. Zone II areas where personnel could otherwise unknowingly receive high levels of radiation exposure due to system failure or personnel error.

3. Areas in which the new and spent fuel is received and stored.

The location of fixed airborne radioactivity monitors are dependent upon the point of leakage, the ability to identify the source of radioactivity so that corrective action may be performed, and whether personnel may be exposed to the airborne radioactivity.

1. Airborne radioactivity monitors sample normally accessible personnel operating areas in which there is a potential for airborne radioactivity.

2. Exhaust ducts will be monitored which serve an area containing processes which, in the event of major leakage, could result in concentrations within the plant approaching the limits established by 10CFR20 for plant workers.

3. Dilution from other exhaust ducts is considered when locating monitors in exhaust systems to ensure maximum coverage and still be able to detect 10CFR20 airborne radioactivity limits in the area with the lowest ventilation flow.

4. Outside air intake ducts for the Operations Center will be monitored to measure possible introduction of radioactive materials into the Operations Center.

5. Exhaust to the environment will be monitored to determine that concentrations exceeding those of the Top-Level Regulatory Criteria are not released.

The location of process radioactivity monitors is dependent on the types of processes, the process fluids, the location of the potential leaks, the capability of available radioactivity detectors, the type of corrective action possible, and potential hazards to personnel.

The site boundary monitors are located on the meteorological tower and other selected locations depending upon an assessment of prevailing meteorological conditions (TBD).

Areas not normally accessible are monitored prior to personnel entry with portable monitors or samplers (see Section 7.4.2.4.1.3) depending upon the potential for airborne radioactivity and work to be performed in the area.

7.4.2.4.3 System Operating Mode

During normal RMS operation, "on-line" monitors provide continuous information about the condition of routine or potential sources of radionuclide release.

Portable continuous air monitors will be used to monitor local areas where there is a possibility of airborne radioactivity during maintenance on radioactive systems. Abnormal operation involving the spread of airborne radioactivity will also be monitored locally using portable monitors. Periodic grab samples for particulates, iodine, and noble gases will be taken throughout the plant and analyzed in the radioactive chemistry laboratory in the Personnel Service Building to ensure that the fixed monitors are operating properly. In addition, all monitors will be calibrated on a

quarterly schedule using radioactive transfer sources. The periodic recalibration will be based on primary calibration traceable to National Bureau of Standards standard sources.

7.4.2.5 Design Evaluation

7.4.2.5.1 Failure Modes and Effects

The RMS has built-in diagnostics to detect malfunction of a monitor or processor.

The main control room operator is alerted of any RMS malfunction to aid in initiating corrective actions. If the RMS monitors fail, portable monitors and/or sampling systems (TBD) provide a backup means of monitoring.

7.4.2.5.2 Steady-State Performance

The RMS is designed to provide continuous monitoring through all modes of plant operation.

7.4.2.5.3 Anticipated Operational Occurrence Performance

The RMS is not required to mitigate the effect of any of these occurrences. However, the RMS is expected to function normally during AOOs, providing information and alarms as appropriate.

7.4.2.5.4 Design Basis Event Performance

The RMS is not required to respond to mitigate the effect of any of these events. These transients have no effect on operation of the Radiation Monitoring System. However, the RMS is expected to function normally during DBEs providing information and alarms as appropriate with the possible exception of a DBE-5 Earthquake.

7.4.2.6 Interfaces

Interface requirements imposed on other systems or subsystems by the Radiation Monitoring System are identified in Table 7.4-3, which also includes a description of the interface and a quantitive expression for the interface.

7.4.3 Seismic Monitoring System

7.4.3.1 Summary Description

The Seismic Monitoring System (SMS) consists of an array of sensors and a system control and monitoring console housing data handling and recording equipment.

7.4.3.2 Functions and 10CFR100 Design Criteria

7.4.3.2.1 Power Generation Functions

The power generation function of the SMS is to maintain energy production, shutdown, refueling, and startup/shutdown by permitting offline assessment of the continued functionality of systems, subsystems, and components to allow plant restart following a seismic event.

7.4.3.2.2 Radionuclide Control Functions

The SMS has no radionuclide control function.

7.4.3.2.3 Classification

The SMS is not "safety related". Since the SMS does not perform any 10CFR100 related radionuclide control functions, no special classification is applied to it. However, the system will have the appropriate reliability to meet the user requirements. The SMS will be seismically qualified.

7.4.3.2.4 10CFR100 Design Criteria for Radionuclide Control

No 10CFR100 Design Criteria apply to this system.

7.4.3.3 Radionuclide Control Design Requirements

The SMS has no radionuclide control design requirements.

7.4.3.4 Design Description

7.4.3.4.1 System Configuration

The SMS is intended to detect, indicate, and record the seismic accelerations experienced by structures and equipment required to fulfill, with a high degree of confidence, 10CFR100-related radionuclide control functions during an earthquake. The basic set of SMS sensors is provided for two of the four identical Reactor Buildings (one of the sets is a backup). Because the Reactor Buildings are identical, the data from the instrumented ones will be applicable to all. The seismic instruments are designed to respond to the Reactor Building design acceleration levels. The redundant set of Reactor Building seismic sensors permits major maintenance on any reactor module, including removing a set of sensors from service, without jeopardizing seismic surveillance of the plant.

The SMS is designed using the following sensing and monitoring instrumentation:

1. Peak accelerographs (PA)

   Each sensor contains three accelerographs mounted in a mutually orthogonal array. PAs, which are mounted directly on equipment, have one axis coincident with the principal equipment axis. All other PAs have their principal axes oriented identically, with one horizontal axis parallel to the major horizontal axis assumed in the seismic analysis. Specific sensor locations are chosen which exhibit

significant responses to seismic motion. These sensors do not require a power source but have the capability of permanently recording peak acceleration. Data from PAs must be retrieved manually following an earthquake and are used in the detailed investigations for particular systems, structures, and equipment.

2. Peak strain gauges

Peak strain gauges (PSG) are used as necessary to verify the continued availability of systems and equipment required to fulfill, with a high degree of confidence, 10CFR100-related radionuclide control functions. They are mounted directly on the equipment, equipment supports, or piping at a point chosen to display the maximum earthquake-induced strain. Data from PSGs must be retrieved manually following an earthquake and are used in the detailed investigation of particular systems and equipment.

3. Seismic switches (SS)

These devices actuate alarms in the SMS when seismic accelerations exceed selected setpoints. Information on the exceeded setpoints is presented in the main control room. The seismic switches have independently adjustable setpoints for the vertical and horizontal axes. These switches are installed adjacent to each of the time history accelerometers (THA).

4. Response spectrum analyzer

The response spectrum analyzer (RSA) determines the response spectra attained in three mutually orthogonal directions at any THA location, and displays this information at the monitoring console. The display unit is either an X-Y or stripchart recorder that plots response acceleration versus frequency or a hard-copy printer that prints the response acceleration values and their respective frequencies.

5. Time history accelerometers

Time history accelerometers produce a record of the time varying acceleration at the sensor location. These data are used directly for analysis and comparison with reference information, and may be converted to response-spectra form for spectral comparisons with design parameters.

Each sensor unit contains three accelerometers mounted in a mutually orthogonal array. All accelerometers have their principal axes oriented identically, with one horizontal axis parallel to the major horizontal axis assumed in the seismic analysis.

A magnetic tape recording and playback unit is provided for multiple channel recording and playback of the signals from time history accelerometers. The data recordings include an additional recording channel which contains a timing signal. The recording and playback system has a special cabinet furnished for these instruments and devices necessary for system testing, annunciating, calibration, and control. This cabinet is located adjacent to the monitoring console.

6. System control and monitoring console

A console located in the Reactor Service Building houses the recording, playback, and calibration units which are used in conjunction with the THA sensors to produce a time/history record of the earthquake. It also contains signal conditioning and display equipment associated with the remote indicating response spectrum recorder, audible and visual annunciators associated with the seismic switches, audible and visual annunciators wired to display initiation of the THA recorder, and the power supply components for all equipment contained within the console.

7.4.3.4.2 System Arrangement

The seismic sensors are located in the Reactor Building, Reactor Service Building and on selected equipment. The system control and monitoring console is located in the Reactor Service Building in a location with convenient personnel access. Monitoring and interpretation of the seismic monitoring displays and recordings will be performed by personnel other than main control room operating personnel.

7.4.3.4.3 System Operating Mode

During normal SMS operation, monitors provide continuous information about seismic accelerations experienced by structures and equipment during an earthquake.

During normal SMS operation, equipment-mounted peak recording accelerographs and peak strain gauges are used to determine if the design limitation of the specific equipment to which they are fastened has been exceeded. If the measured responses are less than the values used in the design and qualification of structures, systems, and equipment required to fulfill, with a high degree of confidence, 10CFR100-related radionuclide control function, the structure, system, or equipment is considered adequate for future operations. Otherwise, further analysis is made to check the adequacy of these items for future use. Initial determination of the earthquake severity is performed immediately after the earthquake by comparing the measured response spectra with the OBE and SSE response spectra for the corresponding location. If the measured spectra exceed the OBE response spectra by a significant amount, the plant will be shut down and a detailed analysis of the earthquake motion will be undertaken. The system performance characteristics are as specified in ANSI/ANS 2.2 Section 5 which defines the requirements for the acceleration sensors, recorders, seismic switches, time history accelerographs, peak accelerographs and the response spectrum recorder. (Ref. 3)

7.4.3.5 Design Evaluation

7.4.3.5.1 Failure Modes and Effects

During normal operation, the SMS provides continuous monitoring to determine if the design limitations of certain structures, systems, or equipment have been exceeded. If the SMS sensors fail to provide continuous information about seismic accelerations, the operator is alerted and will initiate proper actions. Continued outage of the SMS fails to provide the operator with the necessary data to carry out a detailed analysis should an earthquake occur.

7.4.3.5.2 Steady-State Performance

Prior to startup, the SMS is completely operational and provides continuous monitoring through all modes of plant operation and post-earthquake conditions.

7.4.3.5.3 Anticipated Operational Occurence Performance

These transients have no effect on operation of the SMS. The SMS is designed to function normally during AOOs providing information and alarms as appropriate.

7.4.3.5.4 Design Basis Event Performance

The SMS is designed to ensure operation following a DBE-5 as defined in licensing basis events for the Standard MHTGR.

7.4.3.6 Interfaces

Interface requirements imposed on other systems or subsystems within other systems by the Seismic Monitoring System are identified in Table 7.4-4, which also includes a description of the interface and a quantitive expression of the interface.

7.4.4 Meteorological Monitoring System

7.4.4.1 Summary Description

The Meteorological Monitoring System consists of a single meteorological tower with an array of meteorological sensors and an instrument building which houses data-handling, recording, and communication equipment as shown on Figure 7.4-2.

The Meteorological Monitoring System acquires and provides data to the Radiation Monitoring System (see Section 7.4.2) as required for making the following assessments:

1. A conservative assessment of the radiological consequences of airborne releases from design basis accidents, to aid in the evaluation of the acceptability of the site.

2. A realistic assessment of the potential radiation dose to the public resulting from the routine releases of radioactive materials in airborne effluents, to assist in demonstrating that the operation of the plant is being conducted safely and that the effluent control equipment meets its design objectives and is being operated properly.

3. A realistic assessment of the potential radioactive consequences of an actual or projective accidental release of radioactive material to the atmosphere.

4. A realistic assessment of the potential dispersion of radioactive materials from and the radiological consequences of a spectrum of accidents to aid in evaluating the environmental risk posed by a nuclear power plant.

5. A realistic assessment of potential nonradioactive environmental effects such as fogging, icing, and salt drift from cooling towers, to aid in evaluating the environmental impact of the plant.

7.4.4.2 Functions and 10CFR100 Design Criteria

7.4.4.2.1 Power Generation Functions

The power generation function of the Meteorological Monitoring System is to maintain energy production, shutdown, refueling, and startup/shutdown by acquiring and processing meteorological data for use in assessing potential environmental effects.

7.4.4.2.2 Radionuclide Control Functions

The Meteorological Monitoring System has no radionuclide control functions.

7.4.4.2.3 Classification

This system is not "safety related". Since this system does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, this system will have the appropriate reliability to meet user requirements.

7.4.4.2.4 10CFR100 Design Criteria for Radionuclide Control Functions

No 10CFR100 Design Criteria apply to the Meteorological Monitoring System.

7.4.4.3 Radionuclide Control Design Requirements

The Meteorological Monitoring System does not have any radionuclide control requirements.

7.4.4.4 Design Description

7.4.4.4.1 System Configuration

Meteorological Tower

The tower is a guyed-triangular 60-m (197-ft) tower, with an instrument elevator. A grounding system ties together the tower, the lightning rod, the guy anchors, the fence, the Instrument Building, the electronic equipment, the Power Distribution System, and the Communication System.

Meteorological Instruments

The meteorological instrument arrays are mounted on the tower or located near the base of the tower, as shown in Table 7.4-5.

Redundant sets of temperature sensors measure both reference air temperature at 10 m (33 ft) and the difference in temperature (Δ T) between the 60-m (197-ft) and 10-m (33-ft) tower elevations.

Instrument Building

The Instrument Building is climate controlled, located no less than ten Instrument Building heights from the tower. It is provided with a security system and a fire protection system.

Data Handling and Processing Equipment

The data handling and processing equipment provides for monitoring and recording the meteorological data. It provides the following functions:

1. Recording instantaneous data on analog recorders.

2. Computing and recording 15-minute and hourly averages of meteorological data, and standard deviations, on digital recorders.

3. Providing daily, weekly, monthly, quarterly, and yearly inputs.

4. Providing for calibration of system electronics, and reporting results.

5. Providing data to the Data Management Subsystem for display in the main control room.

6. Providing data to the Data Management Subsystem (see Section 7.3.4) as requested during a design basis event.

7. Providing data to the PPIS for post-accident monitoring.

8. Monitoring the local instrumentation and annunciating status and system operation to the control room via the Data Management Subsystem.

7.4.4.4.2 System Arrangement

The Meteorological Monitoring System is located at approximately the same elevation as finished plant grade, in an area where natural or man-made obstructions to windflow or the plant's Heat Dissipation System have little or no effect on the meteorological measurements. Natural or man-made obstructions to air movement are no higher than the measuring level, and with a horizontal separation of ten times the obstruction heights.

Instrumentation is located on booms oriented into the prevailing wind direction, a minimum distance of two tower widths from the tower. The aspirating temperature shields are pointed downward or laterally toward the north. The precipitation collector is located so that obstructions do not interfere with the collection of precipitation. The solar intensity instrument is located so that shadows from obstructions do not fall upon it.

7.4.4.4.3 System Operating Modes

The Meteorological Monitoring System is operational during all plant operating conditions, with a capability of measurements with a joint recovery of no less than 90 percent for an annual cycle of wind speed, wind direction, and indication of atmospheric stability for each sensor elevation, and for individual observations of the remaining parameters.

7.4.4.5 Design Evaluation

The Meteorological Monitoring System remains functional during all plant operating conditions. If ac power is lost, the uninterruptible power supply will provide the required electrical power.

7.4.4.6 Interfaces

Interface requirements imposed on other systems or subsystems by the Meteorological Monitoring System are identified in Table 7.4-6, which also includes a description of the interface and a quantitative expression for the interface.

7.4.5 Fire Detection and Alarm System

7.4.5.1 Summary Description

The Fire Detection and Alarm System (FDAS) is designed for reliable error-free operation achieved through a redundant design. The system will provide an alarm response when activated by a fire detector, a failure in the detector's power circuit, or any malfunction which affects the detector's ability to perform properly.

Redundancy will be provided by using independent transmission cables between remote zone panels and a central processing unit (CPU) located in the operations center.

7.4.5.2 Functions and 10CFR100 Design Criteria

7.4.5.2.1 Power Generation Functions

The power generation function of the Fire Dectection and Alarm System is to protect the capability to maintain energy production, shutdown, refueling, and startup/shutdown by protecting plant elements from fire, by detecting and annunciating the presence and location of combustion byproducts or presence of fire within the plant.

7.4.5.2.2 Radionuclide Control Functions

The FDAS has the function to protect the capability to control personnel radiation exposure by serving to control the release of radionuclides that may be caused by fire in components handling radioactive materials. The system also serves to protect the systems, structures, and components (SSCs) that do not contain radioactive materials but which otherwise perform functions necessary to control personnel radiation exposure.

7.4.5.2.3 Classification

The Fire Detection and Alarm System is not "safety related". Since this system does not perform any 10CFR100-related radionuclide control functions, no special classification is applied to it. However, this system will have the appropriate reliability to meet other top-level regulatory criteria and user requirements.

7.4.5.2.4 10CFR100 Design Criteria for Radionuclide Control Functions

No 10CFR100 Design Criteria apply to the Fire Detection and Alarm System.

7.4.5.3 Radionuclide Control Design Requirements

To acceptably limit the radiological risk from fire, the system shall provide the capability to detect and annunciate all types of fire in the areas around those NI SSCs that perform functions necessary to control the release of

radionuclides to meet top-level regulatory criteria drawn from 10CFR20 and 10CFR50, Appendix I.

7.4.5.4 Design Description

7.4.5.4.1 System Configuration

The Fire Detection and Alarm System consists of a central processing unit and remote interface zone panels. A multiplex system is used for communication between the CPU and the remote zone panels, as indicated on Figure 7.4-3. The remote zone panels receive inputs from various detectors and fire pull stations located in specific fire zone areas throughout the plant.

Various detectors, such as ionization, photoelectric, thermal, and ultraviolet type, sense the presence of combustion byproducts or the presence of fire and relay a change-of-state condition to the remote zone panel. Upon receipt of a fire signal from a detector, the zone panel sends a signal to the CPU via the multiplex system. The CPU annuciates the affected fire zone and relates it to the physical location within the plant.
Alarms are provided to alert personnel within the plant to the presence of fire. These alarms are both audible and visible.

Fire pull stations are also located within each fire zone for manual reporting of a fire.

7.4.5.4.2 System Arrangement

The Fire Detection and Alarm System is distributed throughout the plant and arranged so as not to interfere or be interfered with by other systems. Figure 7.4-3 shows the system arrangement. Detectors shall be located according to NFPA 72E. (Ref. 4) The cabling minimizes the effect of single failures to the balance of the system by providing Class A wiring as defined in NFPA 72D. (Ref. 5)

7.4.5.4.3 System Operating Modes

The Fire Detection and Alarm System is operational under all plant operating modes.

7.4.5.5 Design Evaluation

The Fire Detection and Alarm System is operational during all plant operating conditions. If ac power is lost, the uninterruptible power supply will provide the required electrical power.

7.4.5.6 Interfaces

Interface requirements imposed on other systems or subsystems within other systems by the Fire Detection and Alarm System are identified in Table 7.4-7, which also includes description of the interface and a quantitative expression for the interface.

REFERENCES-SECTION 7.4

1. Regulatory Guide 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems.

2. ANSI - N13.1 - 1969, Sampling Airborne Radioactive Materials in Nuclear Facilities, Guide 10.

3. ANSI/ANS 2.2, Earthquake Instrumentation Criteria for Nuclear Power Plants.

4. National Fire Protection Association. NFPA No. 72E, Automatic Fire Detectors. 1984

5. National Fire Protection Association. NFPA No. 72D, Proprietary Protective Signaling Systems. 1986

TABLE 7.4-1

IDENTIFICATION OF INTERFACES FOR THE ANALYTICAL INSTRUMENTATION SYSTEM

Interfacing Systems	Nature of Interface	Interface Requirements
Vessel System		
(Vessel and Ducts Subsystem)	Provides primary coolant sample.	Quantity: Flow of primary coolant.
	Provides access to primary coolant.	Expose plateout probe to primary coolant.
Reactor Services Group		
(Helium Purification Subsystem)	Provide helium samples.	Quantity: Flow of sample helium from [TBD] penetrations.
(Liquid Nitrogen Subsystem)	Provide liquid nitrogen for sample treatment.	Quantity: Flow of liquid nitrogen.
(Gaseous Radioactive Waste Subsystem)	Provides helium sample.	Quantity: Flow of sample helium.
	Receives gaseous waste from AIS.	Quantity: Receives flow of gaseous waste.
Misc. Control and Instrumentation Group		
(Radiation Monitoring Subsystem)	Receives AIS output signals.	Quantity: Digital signals.
Plant Protection and Instrumentation System		
(Special Nuclear Area Instrumentation Subsystem)	Receives AIS status signals.	Quantity: Digital signals.

TABLE 7.4-1 (Cont)

Interfacing Systems	Nature of Interface	Interface Requirements
Plant Control Data and Instrumentation System		
(NSSS Control Subsystem)	Receives AIS status signals.	Quantity: Digital signals.
Building Structures and Building Service Group		
(Reactor Building Subsystem)	Structural support.	Quantity: Floor space.
Mechanical Services Group		
(HVAC Subsystem)	Provide room cooling for equipment.	Quantity: Flow of cool air.
Electrical Group		
(AC Distribution Subsystem)	Power to equipment.	Quantity: Electrical power.

TABLE 7.4-2

RADIATION MONITORING SYSTEM

POTENTIAL LOCATIONS OF RADIATION MONITORS

Area Monitors

Main control room

PPIS cabinet rooms

Radwaste building corridors and processing areas

Reactor building rooms and corridors

Fuel storage and handling area

Local control panels in each reactor building and in the reactor service building

Radwaste pipeway

Helium Purification System (HPS) area

Reactor equipment service facility

Radwaste shipment area

Radwaste solidification area

Sampling rooms and radioactive chemistry laboratory

Airborne Radioactivity Monitors

Normal ventilation exhaust duct from each reactor building

Blowdown vent path from each reactor building

Reactor Cavity Cooling System (RCCS) exhaust ducts from each reactor silo

Ventilation exhaust duct from the fuel-handling area

Ventilation exhaust duct(s) from the radwaste building

Control room air supply intake (if necessary to protect operators)

Exhaust from each turbine plant air ejector

Two monitors located at grade between reactor modules 1 and 2 and 3 and 4.

TABLE 7.4-2 (Cont.)

Process Radioactive Monitors

Effluent from each Helium Purification System (HPS)

Sample flow from the primary coolant in each reactor module (to determine level of circulating activity)

Reactor Plant Cooling Water System (RPCWS) exit flow from each HPS, main helium circulators and moisture monitor instrumentation

Exit water stream from each spent fuel pool

Shutdown Cooling Water Subsystem (SCWS) exit flow from each Shutdown Cooling System (SCS) heat exchanger

Service Water System (SWS) exit flow from each SCWS heat exchanger

Condensate from each condenser

Site Boundary Monitors

Meteorological tower and other selected locations to be determined in the Meteorological Monitoring System

TABLE 7.4-3

IDENTIFICATION OF INTERFACES FOR THE RADIATION MONITORING SYSTEM

Interfacing System	Nature of Interface	Interface Requirements
Reactor Service Building	Provide space for, access to, support for the control and monitoring console.	Quantity: 1 Space for console, approximately 4 ft x 2 ft and 19-in. instrument racks (TBD) in an area with unlimited personnel access.
Data Management System	Transmits, processes and stores radioactive data.	Accept signals from RMS for transmission to MCR Post-accident monitoring data is transmitted to the Special Nuclear Area Instrumentation System.
UPS System	Provides power to RMS.	Quantity: 120 V ac, 60 Hz, 1 Ph, 8000 W Physical Interface: In the Reactor Service Building and at each monitor location.
Heating, Ventilating, and Air Conditioning	Provide environmental control.	Control temperature 50 to 104°F. Relative humidity maximum of 95 percent noncondensing.
Meteorological Monitoring	Provide space for access to, support for radiation monitors.	Space and support for monitors on tower, etc.

TABLE 7.4-4

IDENTIFICATION OF INTERFACE FOR THE SEISMIC MONITORING SYSTEM

Interfacing System	Nature of Interface	Interface Requirements
Reactor Service Building	Provide space for, access to, support for the control and monitoring console.	Space for console approximately 3 ft x 6 ft and one 19 in. instrument rack in an area with unlimited personnel access. Space to remain functional and, habitable during all seismic events including SSE.
Data Management System	Transmits, processes and stores seismic data.	Accept signals from SMS for transmission to MCR
UPS System	Provides power to SMS.	120 V ac, 60 Hz, 1 Ph, 1200 W. UPS to remain operable through SSE.
Heating, Ventilating, and Air Conditioning	Provide environmental control.	Control temperature 50°F to 80°F. Relative humidity maximum of 95 percent noncondensing

TABLE 7.4-5

METEOROLOGICAL MONITORING SENSORS

Parameter	Quantity	Location
Wind speed	4	2 each at 10 and 60 meters (33 and 197 ft)
Wind direction	4	2 each at 10 and 60 meters (33 and 197 ft)
Temperature	4	2 each at 10 and 60 meters (33 and 197 ft)
Dew point	2	1 each at 10 and 60 meters (33 and 197 ft)
Solar radiation	1	10 meters (33 ft)
Precipitation	1	Ground level

TABLE 7.4-6

IDENTIFICATION OF INTERFACES FOR THE METEOROLOGICAL MONITORING SYSTEM

Interfacing Systems	Nature of Interface	Interface Requirements
Plant Protection and Instrumentation System	Processes meteorological data for post accident monitoring	(TBD)
Plant Control Data and Instrumentation System		
Data Management System	Processes and stores meteorological data	(TBD)
Building Structures and Building Services	Provides nonseismic Category III structure	(TBD)
Plant Fire Protection System	Provides fire protection	(TBD)
AC Distribution System	Provides ac power	(TBD)
UPS System	Provides back-up power	(TBD)
Plant Security	Provides security	(TBD)
Grounding, Lightning, Heat Tracing, and Cathodic Protection	Provides grounding and lightning protection	(TBD)

TABLE 7.4-7

IDENTIFICATION OF INTERFACES FOR THE FIRE DETECTION AND ALARM SYSTEM

Interfacing System	Nature of Interface	Interface Requirements
Building Structures and Building Services	Provide nonseismic Category III structure	
AC Distribution System	Provides ac power	(TBD)
UPS System	Provides power to the Fire Detection and Alarm System	120 V, 60 Hz 1 phase UPS
Grounding, Lightning, Heat Tracing, and Cathodic Protection	Provides grounding for equipment	(TBD)

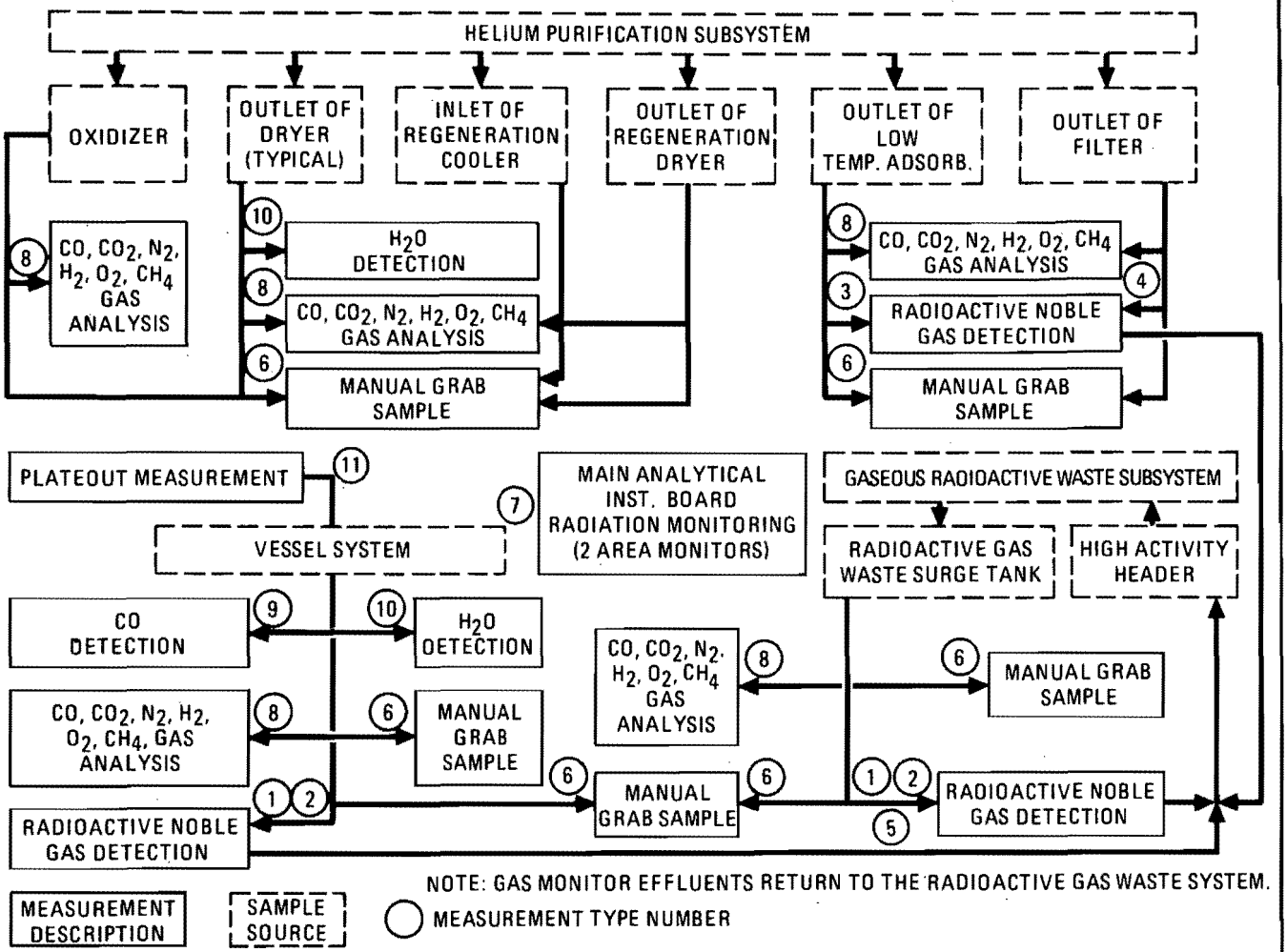
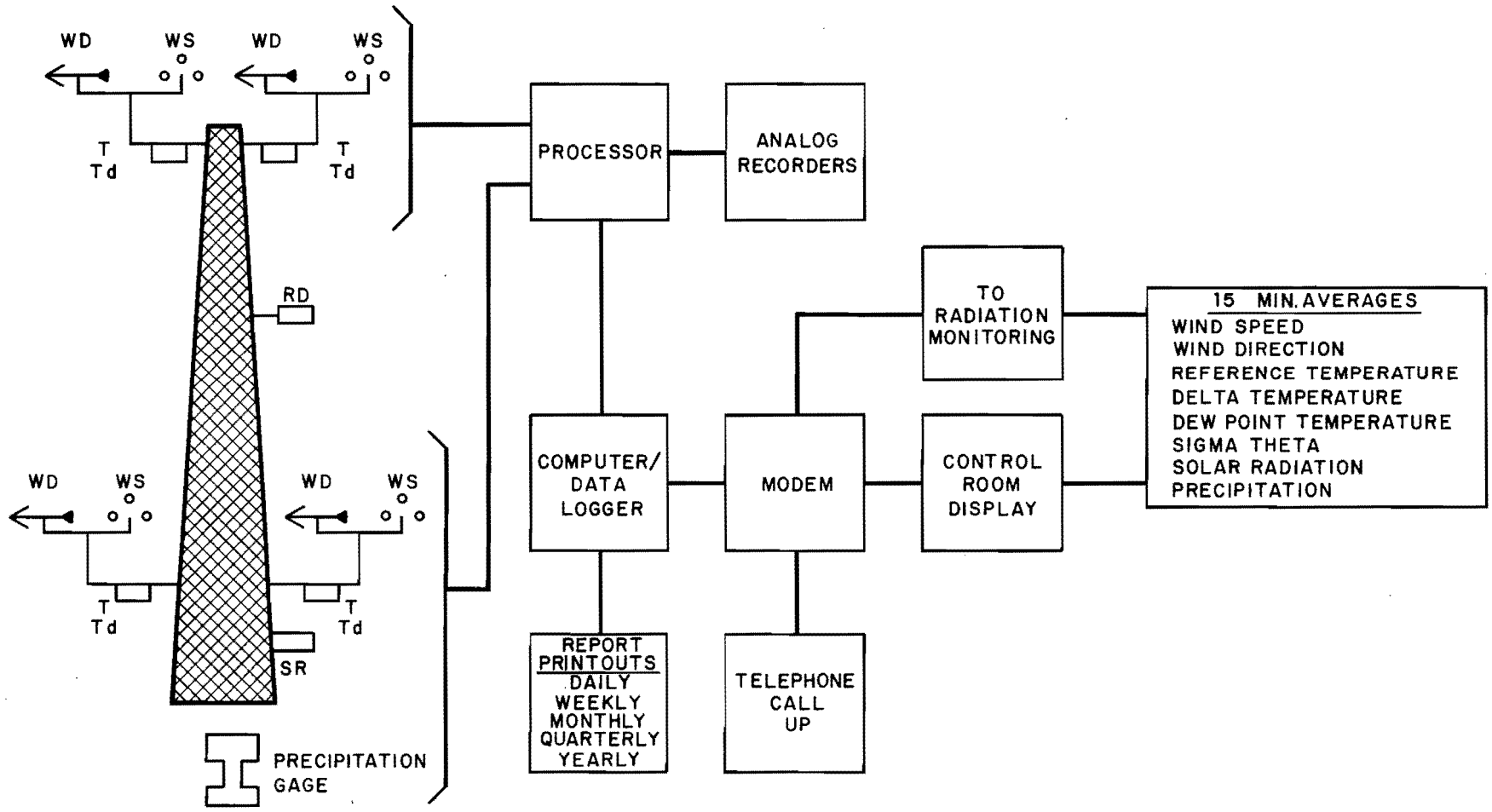


FIGURE 7.4-1

ANALYTICAL INSTRUMENTATION SUBSYSTEM

HIGH TEMPERATURE GAS-COOLED REACTOR PRELIMINARY SAFETY INFORMATION DOCUMENT HTGR-86-024



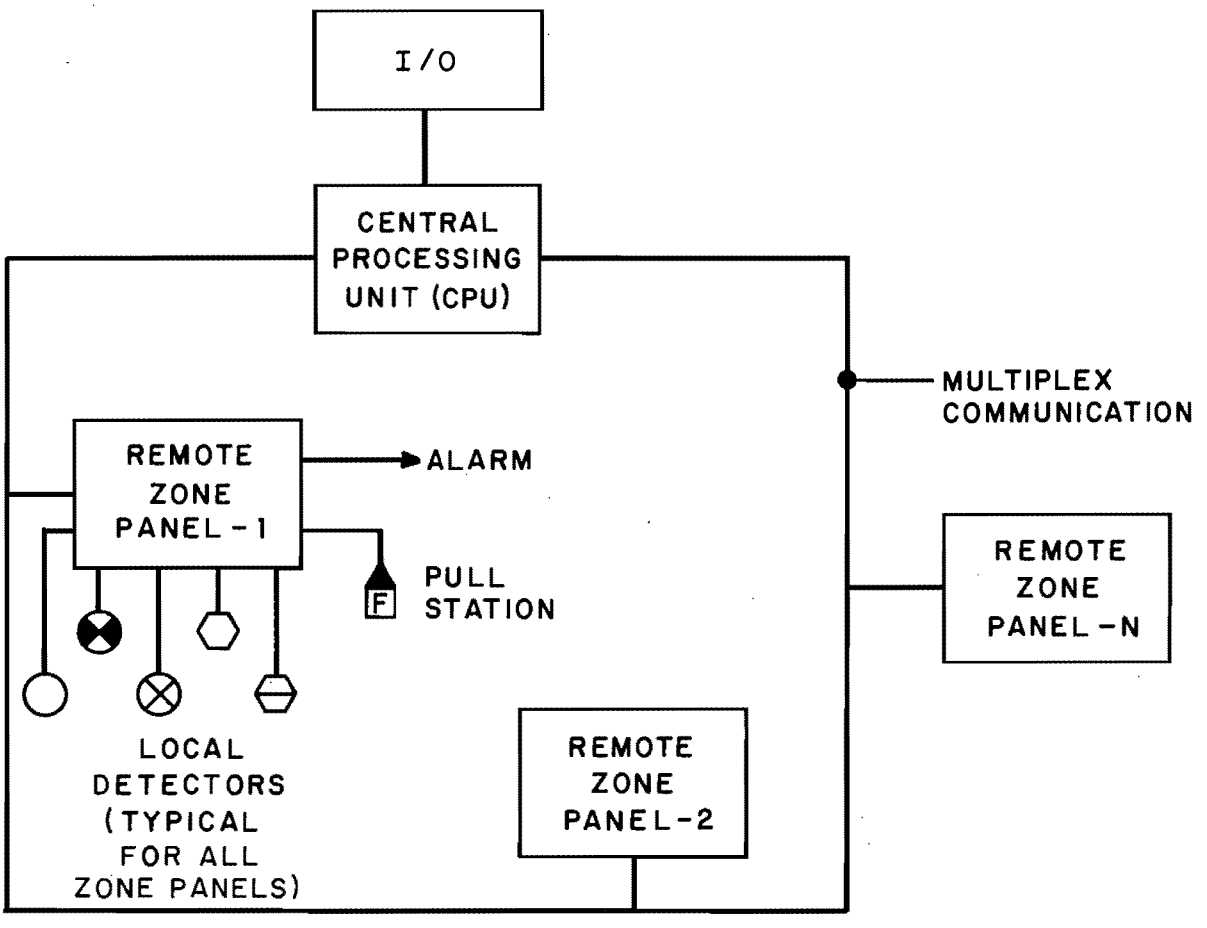
LEGEND

WS – WIND SPEED SENSOR
WD – WIND DIRECTION SENSOR
T – TEMPERATURE SENSOR
Td – DEW POINT TEMPERATURE SENSOR
SR – SOLAR RADIATION SENSOR
RD – RADIATION DETECTOR

FIGURE 7.4 - 2

METEOROLOGICAL MONITORING SYSTEM

HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024



LEGEND

- SMOKE - PHOTOELECTRIC
- SMOKE - IONIZATION
- HEAT - RATE OF RISE (THERMAL)
- HEAT - FIXED (THERMAL)
- FLAME - ULTRAVIOLET

FIGURE 7.4-3
FIRE DETECTION AND ALARM SYSTEM SCHEMATIC
HIGH TEMPERATURE GAS-COOLED REACTOR
PRELIMINARY SAFETY INFORMATION DOCUMENT
HTGR-86-024