DOE-HTGR-86-047
Revision 1

PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

**ISSUED BY GA TECHNOLOGIES INC.
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-84SF11963**

JULY 1987

DOE–HTGR–86–047
Revision 1
HFD–33200
Revision 2
908444/2

PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

Issued By:
GA Technologies Inc.
P.O. Box 85608
San Diego, California 92138–5608

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

JULY 1987

ROLL 2 ... 4-rev 0

GA 1485 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY

NUCLEAR SAFETY-RELATED

TITLE: PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

☐ R & D
☐ DV & S
☒ DESIGN

APPROVAL LEVEL 5

DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO.	ISSUE NO./LTR.
0	32 00	SDD	6300	908444	2

QUALITY ASSURANCE LEVEL	SAFETY CLASSIFICATION	SEISMIC CATEGORY	ELECTRICAL CLASSIFICATION
QAL I	SC 2	CAT I	1E

INFO ONLY

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: ~~FUNDING PROJECT~~	APPROVAL: ~~APPLICABLE PROJECT~~	~~ISSUE DESCRIPTION/ CWBS NO.~~
0	JUN 27 1986	J.Zgliczynski/ J.Bauer	C.Rodriguez	G.P.Connors	~~G.C.Bramblett~~		Initial issue (HFD-33200 Rev. 0) 6352320103

F.A.Silady

Interface Assurance

~~APPLIED TECHNOLOGY~~

~~Any Further Distribution by any Holder of this Document or of Other Data Therein to Third Parties Representing Foreign Interest, Foreign Governments, Foreign Companies and Foreign Subsidaries or Foreign Divisions of U.S. Companies Shall Be Approved by the Director, HTR Development Division, U.S. Department of Energy.~~

CONTINUE ON GA FORM 1485-1

*See List of Effective Pages

NEXT INDENTURED DOCUMENTS

908397
(~~HTGR~~-86-004)
(HFS-20100)

REV																										
SH																										
REV																										
SH	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
REV																										
SH	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

ROLL 2084/ rev. 1 & 2

GA 1485-1 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY
CONTINUATION SHEET

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION	908444	2

ISSUE	DATE	PREPARED BY	APPROVAL				ISSUE DESCRIPTION/ CWBS NO.
			ENGINEERING	QA	FUNDING PROJECT	APPLICABLE PROJECT	
INFO 1 1	SEP 09 1986	J.Zgliczynski for J. Zgliczynski J.Bauer	C.Rodriguez F.A.Silady Interface/ Assurance	G.P.Connors	G.L.Bramblett		HTGR cover added HTGR-86-047/0 (HFD-33200,Rev. 1) Class II Change 6301998201
INFO 2 1	JUN 30 1987	J. Bauer J.Zgliczynski	C.Rodriguez F.A. Silady for FAS Interface Assurance	G.P. Connors	G.L. Bramblett		Revision HTGR-86-047/Rev. 1 (HFD-33200, Rev. 2) Class II Change 6352320101

LIST OF EFFECTIVE PAGES

Page Number	Page Count	Revision
i through xxi	21	2
1-1 through 1-29	29	2
2-1 through 2-79	79	2
3-1 through 3-40	40	2
4-1 through 4-6	6	2
5-1 through 5-3	3	2
6-1 through 6-18	18	2
7-1 through 7-5	5	2
8-1	1	2
9-1	1	2
A-1 through A-16	16	2
B-1	1	2
C-1	1	2
D-1	1	2
E-1 through E-6	6	2
F-1	1	2
Total pages	229	

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF TABLES (Continued)

LIST OF ABBREVIATIONS AND ACRONYMS

ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BSDD	Building and Structures Design Description
CDS	Component Design Specification
CRT	Cathode Ray Tube
DBE	Design Basis Event
EFOH	Effective Forced Outage Hours
EMI	Electromagnetic Interference
HTS	Heat Transport System
HVAC	Heating Ventilating and Air Conditioning
IEEE	Institute of Electrical and Electronic Engineers
IB	Instrument Block
ICD	Interface Control Document
ISI	In-Service Inspection
LCO	Limiting Condition for Operation
MM	Moisture Monitor/Detection Equipment
NEMA	National Electrical Manufacturers Association
OBE	Operating Basis Earthquake
PAM	Post-Accident Monitoring
PCDIS	Plant Control, Data, and Instrumentation System
PPIS	Plant Protection and Instrumentation System
QA	Quality Assurance
RFI	Radio Frequency Interference
RSCE	Reserve Shutdown Control Equipment
SCS	Shutdown Cooling System
SDD	System Design Description
SHE	Shutdown Heat Exchanger
SRDI	Safety-Related Display Instrumentation
SSC	Structure, System, Component
SSDD	Subsystem Design Description
SSE	Safe Shutdown Earthquake

LIST OF ABBREVIATIONS AND ACRONYMS (Continued)

TBD	To Be Determined
USNRC	United States Nuclear Regulatory Commission

DEFINITIONS*

Actual Protection System Setting: Nominal protection system trip setpoint, including sufficient margin so that the maximum expected instrumentation drift will not cause the setpoint to exceed the limiting protection system setting. The maximum actual protection system setting is limited by maximum expected instrumentation drift and the limiting protection system setting. The minimum actual protection system setting is limited by the maximum value of the measured process variable during normal operations.

Actuated Equipment: The assembly of prime movers (such as turbines, motors, and solenoids) and driven equipment (such as control rods, pumps, and valves) used to accomplish a protective action.

Actuation Device: A component or assembly of components directly controlling the motive power (electricity, compressed air, hydraulic fluid, etc.) for actuated equipment. Examples of actuation devices are: circuit breakers, relays, and pilot valves.

Associated Circuits: Circuits not physically separated or electrically isolated from "safety-related" circuits by acceptable separation distance, "safety-related" structures, barriers, or isolation devices.

Auxiliary Supporting Features: Systems or components providing services (such as cooling, lubrication, and energy supply) that are required for the safety systems to accomplish their safety functions.

Channel: The designation applied to a given system or set of components enabling the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

---

*In general, definitions of terms used in this document (some of which are repeated herein) are defined in accordance with IEEE Standard 603-1980, and IEEE Standard 497-1981, unless otherwise specified herein.

DEFINITIONS (Continued)

Control Rod Bank: All of the groups of control rods of a specific type, i.e., the six inner rods constitute the inner bank and the 24 outer rods constitute the outer bank.

Control Rod Group: Three control rods, separated by 120 degrees, operated together.

Damage Threshold: The value of a component design variable at which component damage requiring replacement or repair is likely to occur.

Design Limit: For design basis events the design variables, whether measurable or not (e.g., steam generator tube temperature, bi-metallic weld temperature, reactor vessel pressure, etc.), that will be used to ensure a related damage threshold has not been exceeded.

Execute Features: The electrical and mechanical equipment and interconnections performing a function, associated directly or indirectly with a protection function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to, and including, the actuated equipment-to-process coupling. In some instances protective actions may be performed by execute features that respond directly to the process conditions (for example, check valves, self-actuating relief valves).

Isolation Device: A device in a circuit preventing malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit, or other circuits.

Limiting Conditions for Operation: The lowest functional capability or performance levels of equipment required for continued operation of the facility without undue risk to the health and safety of the public.

DEFINITIONS (Continued)

Limiting Protection System Setting: The setting for automatic protective devices related to those variables having significant protection functions. Where a limiting protection system setting is specified for a variable on which a damage limit has been placed, the setting shall be chosen so that automatic protective action will correct the abnormal situation before a damage limit is exceeded.

Load Group: An arrangement of buses, transformers, switching equipment, and loads fed from a common power supply.

Maintenance Bypass: The removal of the capability of a channel, component, or piece of equipment to perform a protective action due to a requirement for replacement, repair, test, or calibration. A maintenance bypass is not the same as an operating bypass. A maintenance bypass may reduce the degree of redundancy of equipment but it will not result in the loss of a protection function.

Operating Basis Earthquake (OBE): The earthquake which could reasonably be expectd to affect the plant site during the operating life of the plant.

Operating Bypass: Inhibition of the capability to accomplish a protection function that could otherwise occur in response to a particular set of generating conditions.

> NOTE: An operating bypass is not the same as a maintenance bypass. Different modes of plant operation may necessitate an automatic or manual bypass of a protection function. Operating bypasses are used to permit operating mode changes.

DEFINITIONS (Continued)

Process Limit: For expected events, the process variables or combinations of interrelated process variables (for example, flow, neutron flux, pressure) that are both measurable and indicative of or identical to the design limits.

Protection Function: One of the processes or conditions (for example, emergency negative reactivity insertion, postaccident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

Radiation Area: Any area, accessible to personnel, in which there exists radiation, originating in whole or in part within licensed material, at such levels that a major portion of the body could receive in any one hour a dose in excess of 5.0×10^{-5} Sv (5 millirems), or in any five consecutive days a dose in excess of 1.0×10^{-3} Sv (100 millirems).

Safe Shutdown Earthquake (SSE): That earthquake for which those structures, systems, and components required to meet 10CFR100 are designed to remain functional with a high degree of confidence.

"Safety-Related": Identifier on equipment necessary to perform the functions required to limit releases under accident conditions to those allowed by 10CFR100.

Sense and Command Features: The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the protection functions. The scope of the sense and command features extends from the measured process variables to the execute features input terminals.

PREFACE

The objective of the HTGR plant is to produce safe, economical power. Supporting this objective, four major goals and their associated plant states are identified as follows:

1. Maintain Safe Plant Operation
1.1 Maintain Safe Energy Production (State 1)
1.2 Maintain Safe Plant Shutdown (State 2)
1.3 Maintain Safe Plant Refueling (State 3)
1.4 Maintain Safe Plant Startup/Shutdown (State 4)

2. Maintain Plant Protection
2.1 Protect the capability to maintain safe energy production
2.2 Protect the capability to maintain safe plant shutdown
2.3 Protect the capability to maintain safe plant refueling
2.4 Protect the capability to maintain safe plant startup/shutdown

3. Maintain Control of Radionuclide Release
3.1 Control radiation
3.2 Control personnel access

4. Maintain Emergency Preparedness

The Overall Plant Design Specifications (OPDS) is the top-level technical document for the MHTGR plant. The OPDS (based on user/utility and regulatory requirements) establishes the overall performance, functional, institutional, operational, safety, maintenance, inspection and decommissioning requirements for design of the plant.

In response to the OPDS, a series of lower tier documents, System Design Description (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDDs), Component Design Specifications (CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability of requirement source from plant-level requirements to equipment-level requirements shall be maintained throughout this hierarchy of design documents.

SUMMARY

The Plant Protection and Instrumentation System is one of the systems comprising the MHTGR. The design of this system has been developed through the Integrated Approach (Ref. 1-1) toward safe and economical production of electrical power.

This document defines the functions of the Plant Protection and Instrumentation System, system design requirements derived from the functional analysis, and includes institutional requirements from the Overall Plant Design Specification (Ref. 1-1). A description of the system design which satisfies the requirements is then presented. Lower-tier requirements at the system level are next defined for the subsystem designs. This document also includes information on aspects of system construction, operation, and maintenance, and decommissioning.

The Plant Protection and Instrumentation System monitors and protects plant systems and equipment to protect plant investment and to protect public health and safety. The system monitors selected system process variables, compares the sensed values to preselected levels and, as required, commands and initiates predetermined plant corrective actions. The scope of the system starts with and includes the process sensors to the input of the actuated equipment. This function is accomplished by the Investment Protection Subsystem and the Safety Protection Subsystem.

Other functions of the Plant Protection and Instrumentation System are to provide plant interlock features, monitor protection systems status, monitor the plant safety and investment under normal operating and accident conditions and enable reactor shutdown from a remote shutdown area. These functions are accomplished by the Special Nuclear Area Instrumentation which include the vessel relief subsystem pressure relief block valve closure interlock, protection system information displays, post-accident monitoring instrumentation and investment protection information displays.

The major equipment of the Plant Protection and Instrumentation System is located in the Reactor Building and Reactor Service Building. Sensors and data transmission equipment are located throughout the plant near the measurement locations.

More detail design information at the subsystem level is presented with subordinate Subsystem Design Descriptions for the following Plant Protection and Instrumentation Subsystems as outlined in the Overall Plant Design Specification.

Subsystem	Subsystem No.	Document No.
Investment Protection	3201	HFD-43201
Safety Protection	3202	HFD-43202
Special Nuclear Area Instrumentation	3203	HFD-43203

SECTION 1
SYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SYSTEM FUNCTIONS

The function of the Plant Protection and Instrumentation System is to monitor and protect plant systems and equipment, to protect plant investment, and to protect public health and safety. This is accomplished by sensing process variables to detect abnormal plant conditions, and actuating equipment to maintain plant parameters within acceptable limits established for design basis events, thereby maintaining an acceptable level of public safety risk and plant investment risk.

Additional functions are to provide plant interlock features, monitor protection systems status, monitor plant safety and investment under normal operating and accident conditions, and enable control of reactor shutdown from a remote shutdown area.

1.2 SYSTEM DESIGN REQUIREMENTS

1.2.1 System Configuration and Essential Features Requirements

The Plant Protection and Instrumentation System shall be compatible with a plant that is configured to locate the reactor modules within a Nuclear Island (NI) that is physically separated from the Energy Conversion Area (ECA). (3200.0102.010)*

The design of the Plant Protection and Instrumentation System structures, systems, and components (SSCs) shall be standardized. (3200.0102.011)

*Requirements traceability number.

The level and extent of Plant Protection and Instrumentation System standardization to support design certification shall be determined in the MHTGR Design Certification Report (TBD). (3200.0102.012)

The NI shall include four (4) standard reactor modules. (3200.0102.013)

The ECA shall incorporate two (2) steam turbine-generators. (3200.0102.014)

The Plant, Protection and Instrumentation System shall be functionally independent from plant process control systems. (3200.0102.015)

Fixed audible alarm annunciator points shall be restricted to those critical parameters which can lead to initiation of protective action for major plant components or the loss of electrical production. (3200.0102.016)

Plant Protection and Instrumentation System trip actions shall be transmitted to the NSSS control subsystem. (3200.0102.020)

The Plant Protection and Instrumentation System shall include monitoring and diagnostics for the Reactor Cavity Cooling System. (3200.0102.021)

The Plant Protection and Instrumentation System shall provide the power control trip subsystems to cause the control rods to fall into the core and to cause reserve shutdown control equipment actuation when appropriate reactor trip(s) are needed. (3200.0102.022)

The Plant Protection and Instrumentation System shall provide source range neutron level and number of control rods withdrawn data for use by the refueling control operator. (3200.0102.023)

1.2.2 Operational Requirements

The Plant Protection and Instrumentation System shall be designed for an operating life of 40 calendar years. (3200.0102.030)

The Plant Protection and Instrumentation System shall accommodate the performance and transient characteristics of the following additional reactor/turbine-generator combinations: (3200.0102.031)

1. Two (2) reactor modules operating in parallel supplying steam to a single turbine-generator.

2. Four (4) reactor modules operating in parallel supplying steam to a single turbine-generator.

The plant structures, systems, and components shall provide sustained and controlled operation for the conditions listed below:

1. Load rejection from full generator electric output to house electrical load without receiving a reactor trip signal. Plant operating capability for up to 12 h under house electric load conditions shall be provided.

2. Turbine trip (except on low condenser vacuum) from any load level without receiving a reactor trip signal. Continuous reactor operation at reduced output shall be provided.

3. Step changes of ±15% in plant output caused by utility electrical transmission grid frequency upsets. (3200.0102.032)

The plant shall be designed to sustain continuous operation at reduced electrical output through the following transients associated with the loss

or failure of a major component, system, or train, including an individual reactor or turbine generator. (3200.0102.033)

Plant systems shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in Figures 1-1 through 1-5, Tables 1-1 and 1-2, and in the NSSS Thermal Performance Requirements Report (Ref. 1-2). (3200.0102.034)

Plant systems shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0102.035)

Provisions shall be made to remove a reactor from service, perform maintenance or refueling, and return it to service with the remaining reactors and the turbine plant in operation. (3200.0102.036)

Provisions shall be included to take a turbine-generator, its supporting auxiliaries, and associated regenerative feedwater heating train out of service, perform maintenance and return them to service with the reactors and remaining portions of the turbine plant in operation. (3200.0102.037)

The design of protective features shall provide for periodic functional testing that will not interfere with normal plant operation. (3200.0102.038)

The Plant Protection and Instrumentation System shall sense process variables and actuate equipment to detect abnormal plant conditions and maintain plant parameters within the plant damage thresholds established for the components listed in Table 1-4, preventing damage to components essential for the protection of the public health and safety and the plant investment. (3200.0102.039)

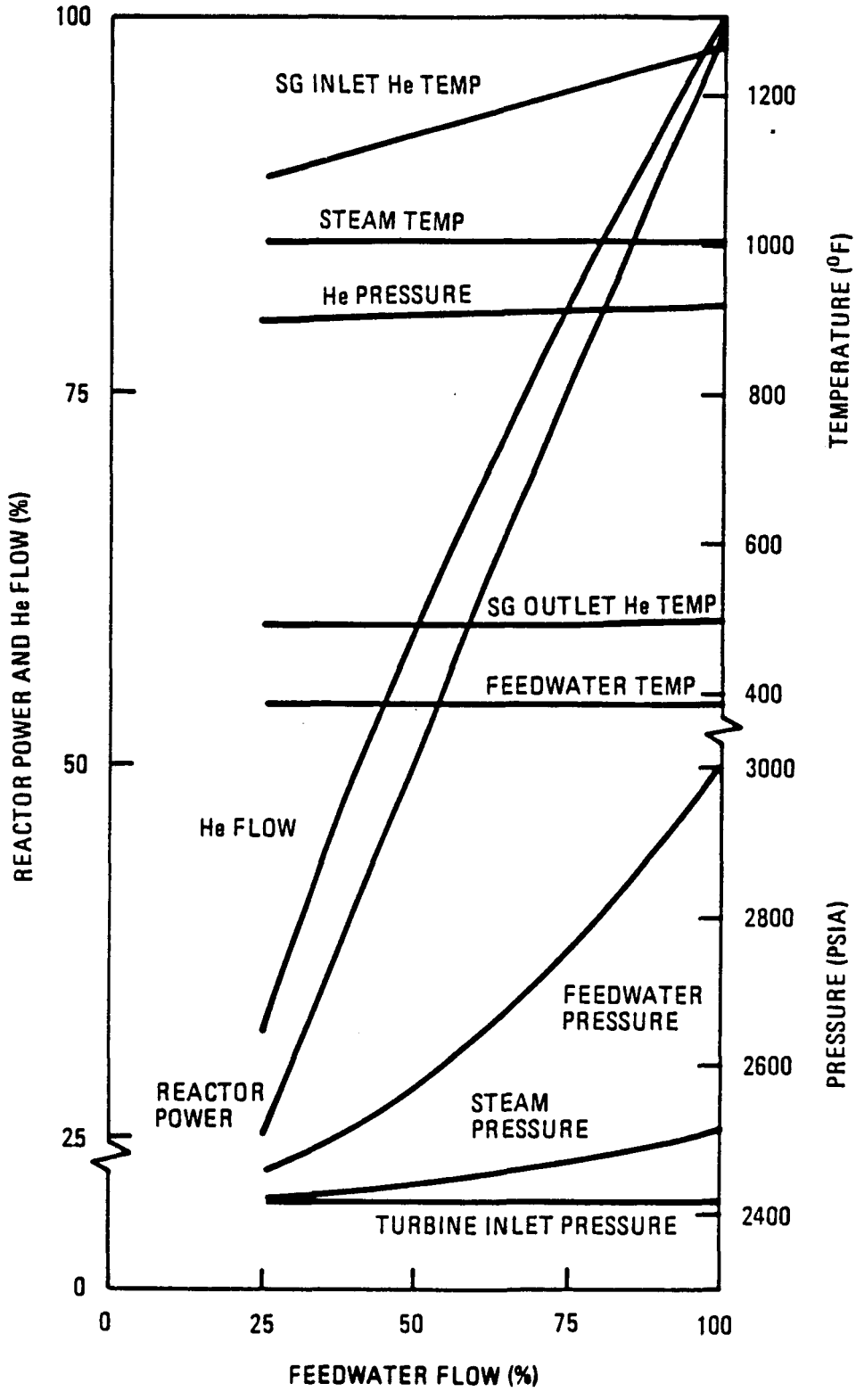
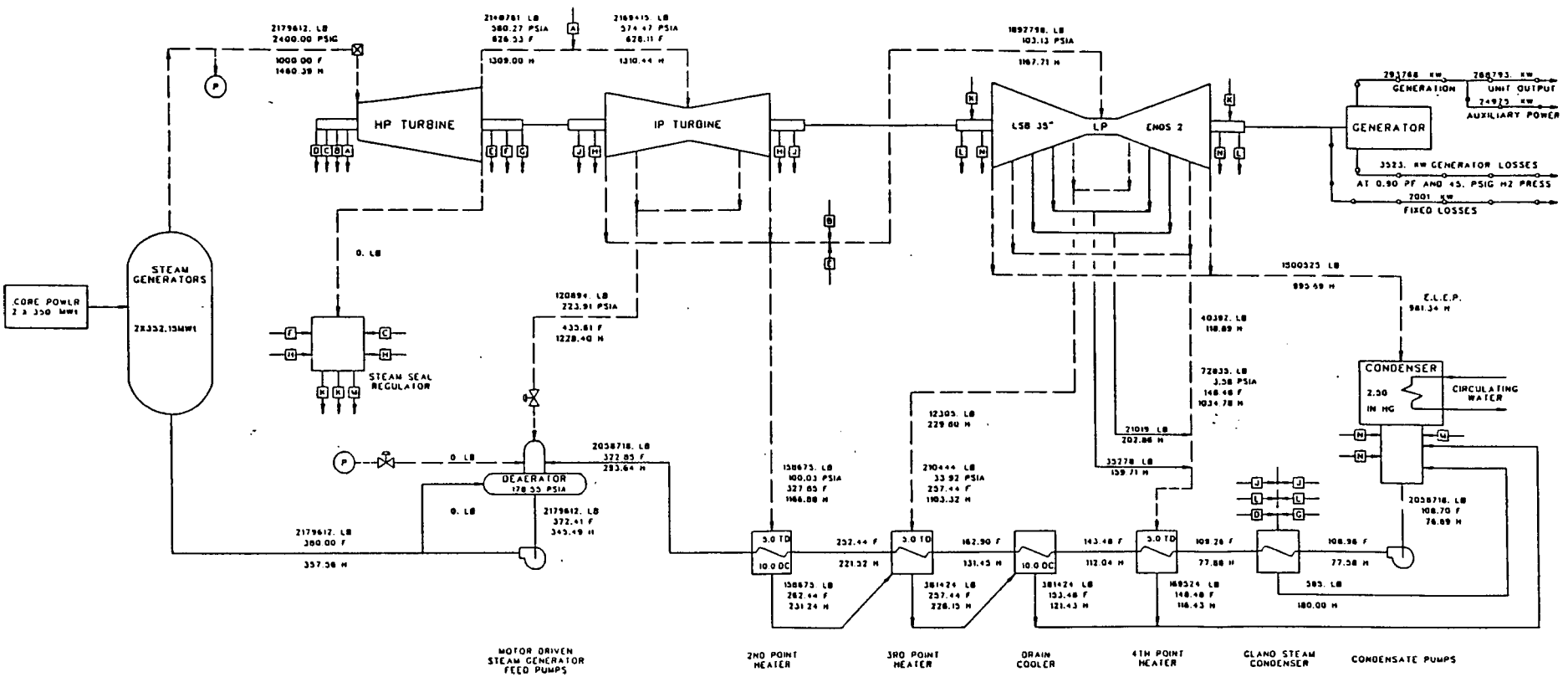


Figure 1-1
PART LOAD OPERATING CONDITIONS AT THE STEAM GENERATOR - FOUR MODULES OPERATING AT EQUAL LOADS



BASIS

THE TOTAL PLANT CONSISTS OF FOUR REACTORS AND TWO IDENTICAL 300 MWe TURBINE-GENERATOR UNITS. THIS DIAGRAM ILLUSTRATES ONE OF THE 300 MWe UNITS AND TWO STEAM GENERATORS.

STEAM GENERATOR FEED PUMP AND CONDENSATE PUMP EFFICIENCIES 83%

PRESSURE DROP IN EXTRACTION LINES 3%

	1X300 MWe UNIT	2X300 MWe UNIT TOTAL PLANT
CORE POWER, MWt	700.	1400.
HEAT INPUT, BTU/HR	2403746419.	4807492838.
SGFP POWER, KW	8371	16741.
AUXILIARY POWER, KW	24975	49950.
GENERATION, KW	293768	587536.
UNIT OUTPUT, KW	268793.	537586.

GROSS TURBINE HEAT RATE = HEAT INPUT / GENERATION = 8182. BTU/KW-HR

NET TURBINE HEAT RATE = HEAT INPUT / GENERATION − SGFP POWER = 8422. BTU/KW-HR

UNIT HEAT RATE = CORE POWER / UNIT OUTPUT = 8886. BTU/KW-HR

LEAKAGES

	FLOW	ENTHALPY
A	20634. LB	1460.39 H
B	3382. LB	1460.39 H
C	1405. LB	1460.39 H
D	38. LB	1460.39 H
E	4042. LB	1309.00 H
F	1295. LB	1309.00 H
G	35. LB	1309.00 H
H	2133. LB	1166.88 H
J	101 LB	1166.88 H
K	673. LB	1252.43 H
L	155. LB	1252.43 H
M	3824. LB	1252.43 H
N	318. LB	1252.43 H

LEGEND

STEAM
WATER
POWER

LB	FLOW, POUNDS PER HOUR
H	ENTHALPY, BTU PER POUND
F	TEMPERATURE, DEGREES F
TD	TERMINAL DIFFERENCE, DEGREES F
DC	DRAIN COOLER APPROACH, DEGREES F
KW	POWER, KILOWATTS
MWt	POWER, MEGAWATTS THERMAL
IN HG	PRESSURE, IN OF MERCURY, ABS.(AT 32 F)
PSIA	PRESSURE, LB PER SQUARE IN, ABS.

Figure 1-2 PLANT HEAT BALANCE DIAGRAM AT 100% (RATED) FEEDWATER FLOW

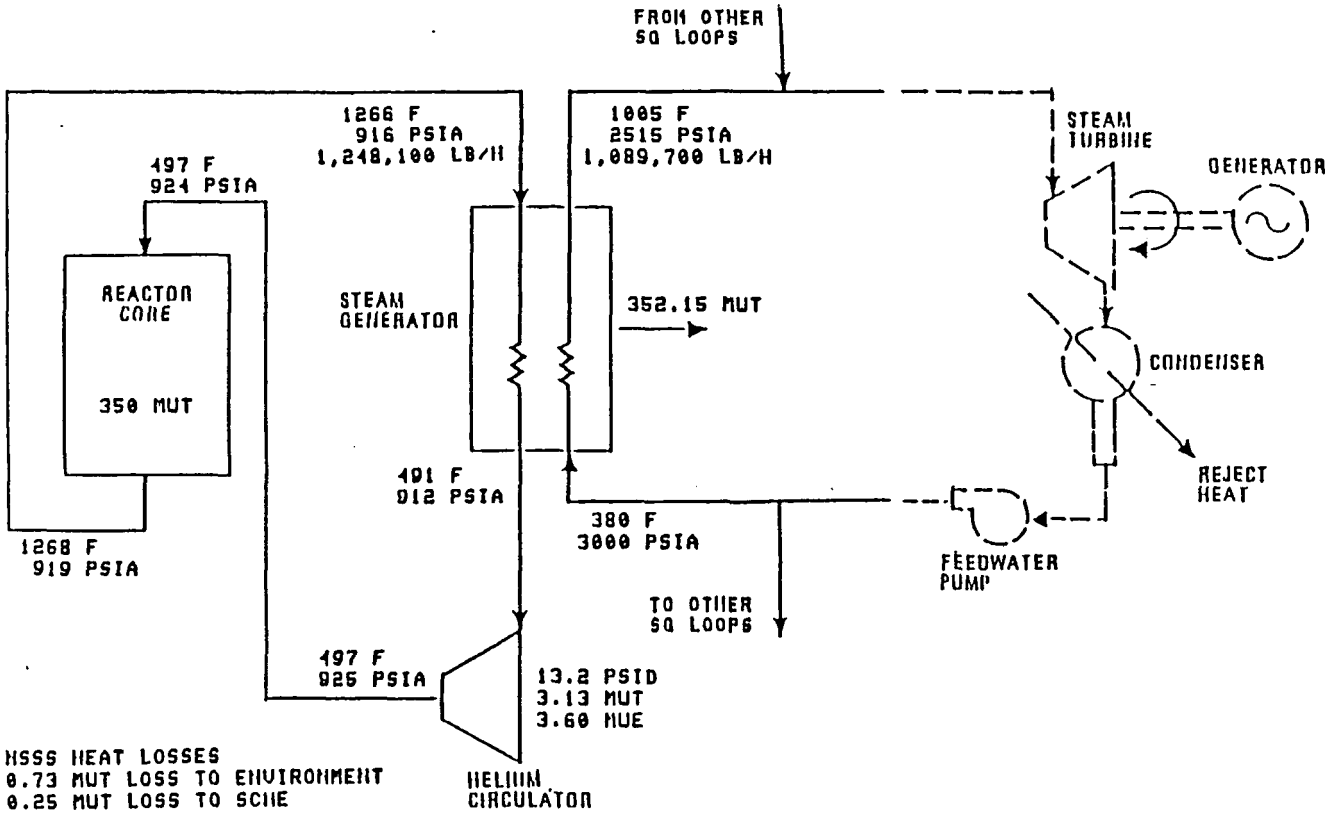
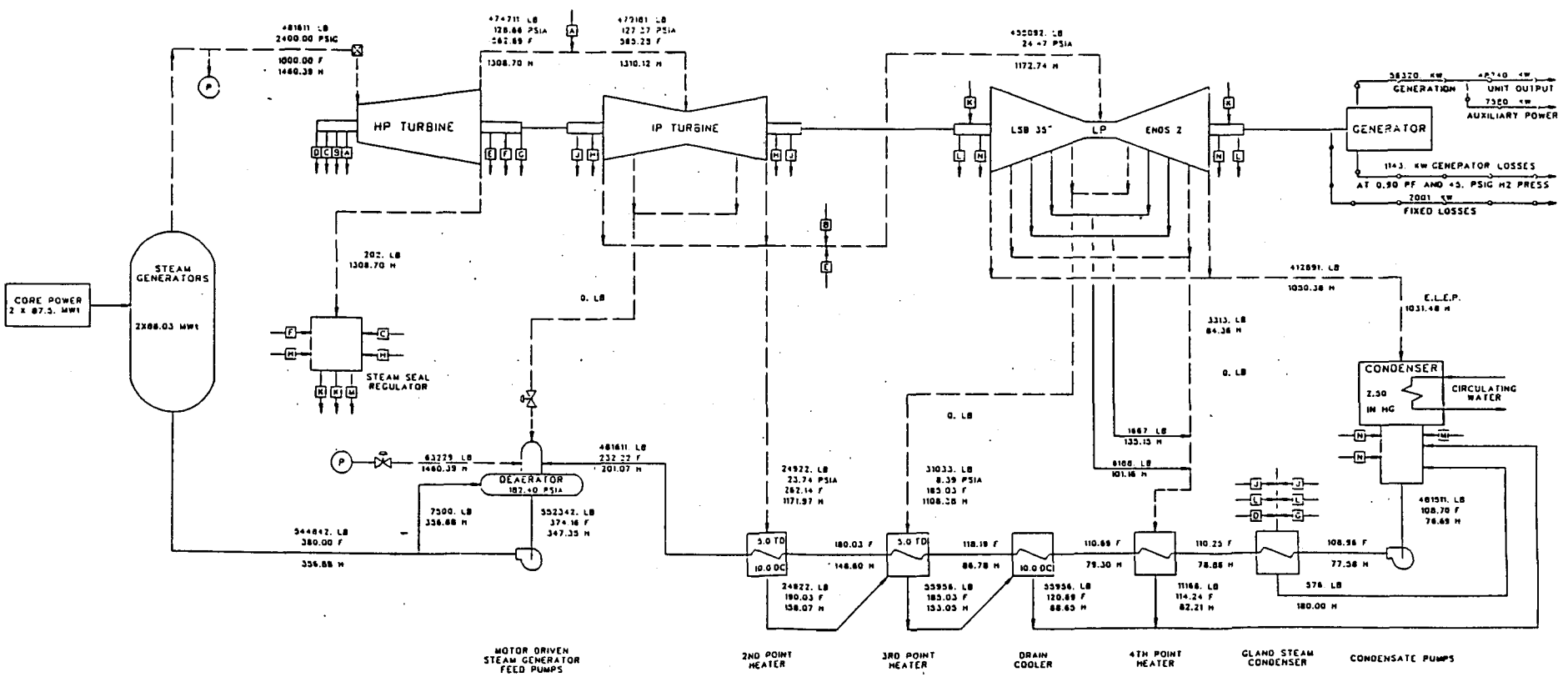


Figure 1-3 NSSS HEAT BALANCE DIAGRAM AT 100% (RATED) FEEDWATER FLOW



BASIS

THE TOTAL PLANT CONSISTS OF FOUR REACTORS AND TWO IDENTICAL 300 MWe TURBINE-GENERATOR UNITS. THIS DIAGRAM ILLUSTRATES ONE OF THE 300 MWe UNITS AND TWO STEAM GENERATORS.

STEAM GENERATOR FEED PUMP AND CONDENSATE PUMP EFFICIENCIES 83%

PRESSURE DROP IN EXTRACTION LINES 3%

	1X300 MWe UNIT	2X300 MWe UNIT TOTAL PLANT
CORE POWER, MWt	175.	350
HEAT INPUT, BTU/HR	601261727.	1202483453.
SGFP POWER, KW	1674	3348
AUXILIARY POWER, KW	7580.	15160.
GENERATION, KW	56320.	112640
UNIT OUTPUT, KW	48740.	97480.

GROSS TURBINE HEAT RATE = HEAT INPUT / GENERATION = 10675. BTU/KW-HR

NET TURBINE HEAT RATE = HEAT INPUT / GENERATION - SGFP POWER = 11002. BTU/KW-HR

UNIT HEAT RATE = CORE POWER / UNIT OUTPUT = 12351 BTU/KW-HR

LEAKAGES

	FLOW	ENTHALPY
A	4470. LB	1460.39 H
B	779. LB	1460.39 H
C	237. LB	1460.39 H
D	38. LB	1460.39 H
E	820 LB	1308.70 H
F	219 LB	1308.70 H
G	33. LB	1308.70 H
H	334. LB	1171.97 H
J	99. LB	1171.97 H
K	863. LB	1266.93 H
L	152. LB	1266.93 H
M	0. LB	1266.93 H
N	511. LB	1266.93 H

LEGEND

STEAM
WATER
POWER

LB	FLOW, POUNDS PER HOUR
H	ENTHALPY, BTU PER POUND
F	TEMPERATURE, DEGREES F
TD	TERMINAL DIFFERENCE, DEGREES F
DC	DRAIN COOLER APPROACH, DEGREES F
KW	POWER, KILOWATTS
MWt	POWER, MEGAWATTS THERMAL
IN HG	PRESSURE, IN OF MERCURY, ABS. AT 32 F
PSIA	PRESSURE, LB PER SQUARE IN. ABS.

Figure 1-4 PLANT HEAT BALANCE DIAGRAM AT 25% FEEDWATER FLOW

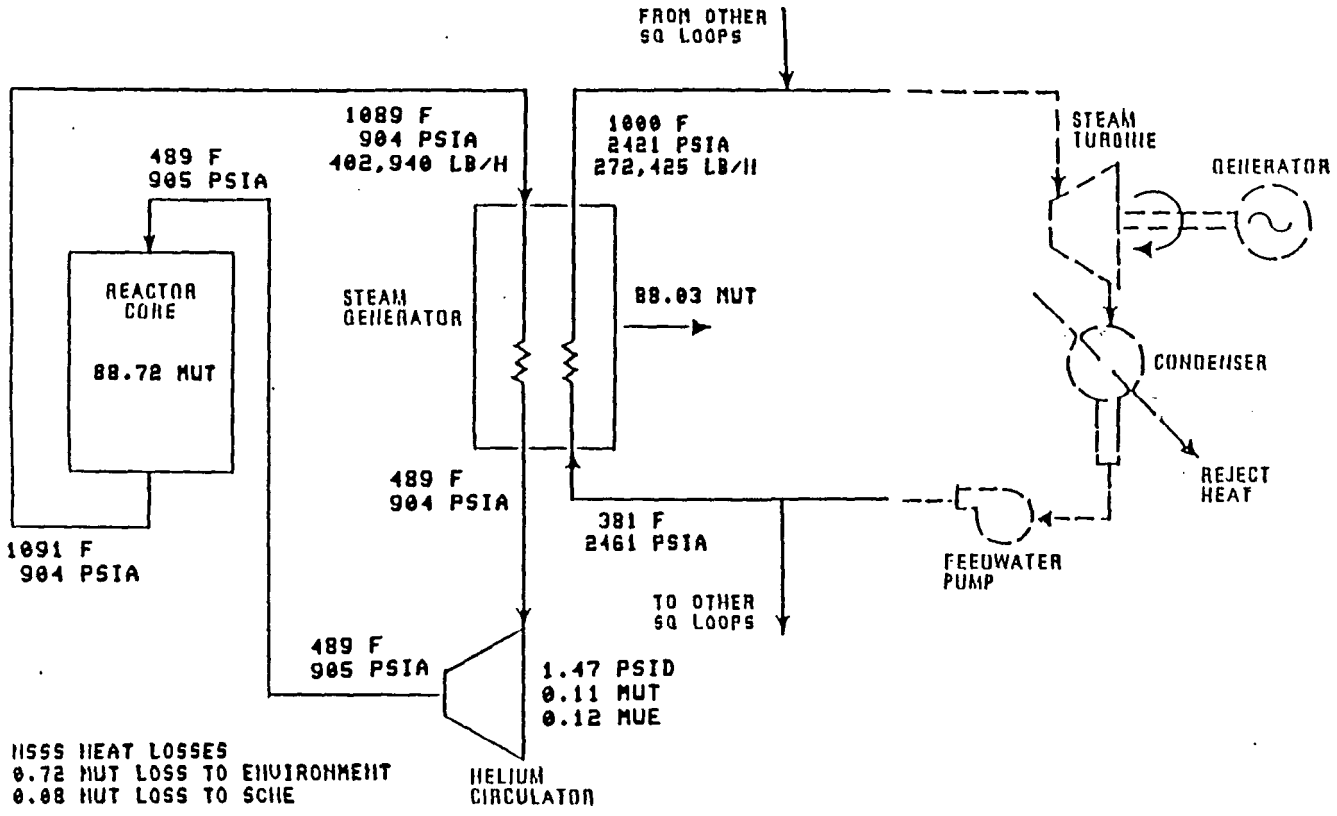


Figure 1-5 NSSS HEAT BALANCE DIAGRAM AT 25% FEEDWATER FLOW

Table 1-1
DESIGN POINT NSSS PERFORMANCE
AT RATED (100%) FEEDWATER FLOW

NSSS Heat Balance, MW(t)	
Heat generated by core	350.00
Heat added by circulators	3.13
Total heat to helium	353.13
Loss to environment from helium	0.73
Loss of SCHE from helium	0.25
Net steam generator power	352.15
Reactor	
Inlet helium flow rate, lb/h	1,246,397.0
Inlet helium temperature, °F	497.4
Inlet helium pressure, psia	924.5
Loss to vessel from core, MW(t)	0.62
Outlet helium temperature, °F	1,267.7
Helium pressure drop, psi	8.00
Steam Generator	
Inlet helium flow rate, lb/h	1,248100.0
Inlet helium temperature, °F	1,266.0
Inlet helium pressure, psia	915.8
Outlet helium temperature, °F	490.6
Helium pressure drop, psi	3.70
Inlet feedwater flow rate, lb/h	1,089,736.0
Inlet feedwater temperature, °F	380.0
Inlet feedwater pressure, psia	3,000.0
Inlet feedwater enthalpy, Btu/lb	357.60
Regenerative heat loss, MW(t)	0.33
Outlet steam temperature, °F	1,005.3
Outlet steam pressure, psia	2,515.0
Outlet steam enthalpy, Btu/lb	1,460.4
Steam pressure drop, psia	485.0
Main Circulator	
Circulator helium flow rate, lb/h	1,254,372.0
Bypass helium flow rate, lb/h	6,272.0
Inlet helium temperature, °F	490.7
Inlet helium pressure, psia	911.8
Helium temperature rise, °F	6.85
Helium pressure rise, psi	13.20
Circulator speed ratio	1.00

Table 1-2
NOMINAL NSSS PERFORMANCE AT 25% FEEDWATER FLOW

NSSS Heat Balance, MW(t)	
Heat generated by core	88.72
Heat added by circulators	0.11
Total heat to helium	88.83
Loss to environment from helium	0.72
Loss of SCHE from helium	0.08
Net steam generator power	88.03
Reactor	
Inlet helium flow rate, lb/h	402,390.0
Inlet helium temperature, °F	489.0
Inlet helium pressure, psia	905.2
Loss to vessel from core, MW(t)	0.61
Outlet helium temperature, °F	1,090.7
Helium pressure drop, psi	0.88
Steam Generator	
Inlet helium flow rate, lb/h	402,940.0
Inlet helium temperature, °F	1,089.2
Inlet helium pressure, psia	904.3
Outlet helium temperature, °F	488.5
Helium pressure drop, psi	0.42
Inlet feedwater flow rate, lb/h	272,425.0
Inlet feedwater temperature, °F	380.7
Inlet feedwater pressure, psia	2,460.6
Inlet feedwater enthalpy, Btu/lb	357.60
Regenerative heat loss, MW(t)	0.26
Outlet steam temperature, °F	1,000.3
Outlet steam pressure, psia	2,421.2
Outlet steam enthalpy, Btu/lb	1,460.4
Steam pressure drop, psia	39.4
Main Circulator	
Circulator helium flow rate, lb/h	404,965.0
Bypass helium flow rate, lb/h	2,025.0
Inlet helium temperature, °F	488.5
Inlet helium pressure, psia	903.8
Helium temperature rise, °F	0.77
Helium pressure rise, psi	1.47
Circulator speed ratio	0.33

Table 1-3 DESIGN DUTY CYCLE EVENTS

	Event	Design No. of Occurrences (per Reactor Module)	Level of Service Limits[a]
1.	Startup from refueling conditions	143	A
2.	Startup with full helium inventory	312	A
3.	Shutdown to refueling conditions	101	A
4.	Shutdown with full helium inventory	105	A
5.	Rapid load increase (5% per minute) (25% to 100%)	1,000	A
6.	Normal load increase (0.5% per minute) (25% to 100%)	20,800	A
7.	Rapid load decrease (5% per minute) (100% to 25%)	1,000	A
8.	Normal load decrease (0.5% per minute) (100% to 25%)	17,500	A
9.	Step load increase (+15%)	1,000	A
10.	Step load decrease (-15%)	1,000	A
11.	Depressurized decay heat removal, HTS to SCS transition	80	A
12.	Depressurized decay heat removal, SCS to HTS transition	122	A
13.	Pressurized decay heat removal, HTS to SCS transition	61	A
14.	Pressurized decay heat removal, SCS to HTS transition	86	A
15.	Circulator trip	30	B
16a. 16b.	Reactor trip from 100% Reactor trip from 25%	180[b]	B
17.	Turbine trip or load rejection	120	B
18.	Sudden reduction of feedwater flow	30	B

Table 1-3 (Continued)

	Event	Design No. of Occurrences (per Reactor Module)	Level of Service Limits[a]
19.	Steam generator tube leak (small)	9	B
20.	Control rod insertion	5	B
21.	Main loop overcooling	10	B
22.	Earthquake[c]	1	B
23.	Slow primary system depressurization	8	B
24a.	Rod withdrawal (normal rod speed) (power to flow ratio trip)	1	C
24b.	Rod withdrawal (slow) (steam generator helium inlet temperature trip)	1	C
25.	Failure of circulator speed control	1	C
26.	Circulator trip with helium shutoff valve failure	1	C
27.	Steam generator tube rupture	1	C
28.	SCS heat exchanger tube leak	1	C
29.	Total loss of feedwater flow	4	C
30a.	Total loss of SCS cooling water (HTS operating)	4	C
30b.	Total loss of SCS cooling water (SCS operating)	1	C
31.	Pressurized conduction cooldown	1	C
32.	Main steam pipe rupture	1	D

[a]Level of service limits per ASME Boiler and Pressure Vessel Code, 1986 addenda.

[b]For components where reactor trip from 100% load is worse, the breakdown should be 131 trips from 100% and 49 trips from 25%. For components where reactor trip from 25% load is worse, the breakdown should be 63 trips from 100% and 117 trips from 25%.

[c]OBE or ANSI A58.1 (see Section 1.2.3).

Table 1-4
PLANT EQUIPMENT DAMAGE LIMITS FOR USE IN DESIGNING THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM

Component	Requirements[a]
Graphite moderator, reflectors, core support, fuel compacts, lumped burnable poison compacts and reserve shutdown control pellets	Limit total oxidants in primary coolant to $\leq$10 ppm under steady state conditions and 600 ppm days per year during normal operation and to [TBD] during transients. (3200.0102.130)
Main circulator	Maintain helium circulator inlet temperature <{1100}°F. (3200.0102.200)
	Maintain helium circulator speed <{7440} rpm. (3200.0102.201)
Steel vessels	Maintain helium pressure at or below that indicated in pressure/temperature curve (Ref. 1-4). (3200.0102.310)
Steam generator	Maintain tubesheet and nozzle temperature (Alloy 800H, steam side) <1400°F. (3200.0102.350)
	Maintain tube bundle temperature (Alloy 800H, FSH) <1400°F. (3200.0102.351)
	Maintain support plates temperature (Alloy 800H, FSH) <1400°F. (3200.0102.352)
	Maintain bimetallic weld temperature <1150°F. (3200.0102.353)
	Maintain tube bundle temperature (2-1/4 CR-1Mo, EES) <1150°F. (3200.0102.354)
	Maintain tubesheet and nozzle temperature (SA-508, Class II, feedwater side) <700°F. (3200.0102.355)
	Maintain primary coolant flow rate <116% of nominal. (3200.0102.357)

Table 1-4 (Continued)

Component	Requirements[a]
Shutdown cooling water system	Limit helium ingress into SCWS {0.5 lb}. (3200.0102.370)
Main steam system	Maintain piping (between steam generator and isolation valve) temperatures to <[TBD]°F. (3200.0102.380)

[a]Numbers in { } are estimated and subject to change.

The Plant Protection and Instrumentation System shall be designed to contribute towards limiting the total (unrecovered) leakage of helium from the plant systems to less than 10% of plant inventory per year.
(3200.0102.040)

1.2.3 Structural Requirements

Plant structures, systems, and components (SSCs) shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3.
(3200.0102.400)

The Plant Protection and Instrumentation System shall be designed, fabricated, and erected to performance standards that will enable it to withstand the Operating Basis Earthquake (OBE) levels at appropriate locations as specified in Appendix D. (3200.0102.410)

The "safety-related" portions of the Plant Protection and Instrumentation System shall remain functional during and after for the Safe Shutdown Earthquake. (3200.0102.411)

Failures of Plant Protection and Instrumentation System SSCs which are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE. (3200.0102.412)

1.2.4 Environmental Requirements

The Plant Protection and Instrumentation System shall be capable of performing their functions before, during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions as specified in the Plant Environmental Specification [TBD].
(3200.0102.450)

The design shall provide for individual personnel access to normally accessible areas of the facility for 40 h per week to allow performance of operational, maintenance, and inspection duties while limiting the total average, long-term whole body radiation exposure from all sources to no more than 100 man-rem/year. (3200.0102.451)

The Plant Protection and Instrumentation System shall contribute to maintaining dose levels in the various areas of the plant as specified in Ref. 1-5. (3200.0102.452)

The Plant Protection and Instrumentation System shall be designed in conformance with the Occupational Safety and Health Administration Department of Labor, "Occupational Safety and Health Standards, (29CFR1910)." (3200.0102.453)

1.2.5 Instrumentation and Control Requirements

The plant shall be normally operated from a single control room except during postulated events that would render the control room uninhabitable or the controls inoperable. (3200.0102.502)

Instrumentation shall be provided to assure control of individual equipment items such that design conditions are not exceeded. (3200.0102.503)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within major plant control and electric systems. (3200.0102.504)

Human engineering techniques shall be employed in the design of the Plant Protection and Instrumentation System controls and instrumentation/operator interface to enhance the operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD]. (3200.0102.505)

Supporting controls and instrumentation for structures, systems, and components (SSCs) whose failure would not have an immediate impact on plant output shall be located outside the control room in the proximity of the SSCs with status indication provided to the control room. (3200.0102.506)

1.2.6 Surveillance and In-Service Inspection Requirements

Surveillance is required for the "safety-related" portions of the Plant Protection and Instrumentation Subsystem. This surveillance shall meet the criteria of IEEE Standard 603. The surveillance may be done in three parts: (1) every 10 s for pattern recognition, (2) monthly for logic channels function check, and (3) yearly for calibration check. (3200.0102.533)

1.2.7 Availability Assurance Requirements

The mean likelihood of exceeding the design limits associated with the Safety-Related Design Conditions, and which could therefore lead to the regulatory shutdown of other MHTGR plants, shall be less than 10^{-5} per plant year. (3200.0102.550)

To meet the plant forced outage requirement of less than 876 h/yr (10%), the EFOH values specified in Reliability Allocations for the Standard MHTGR (Table 1-5) shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. (3200.0102.551)

Outages of 6 months or greater shall not contribute more than 10% of the total equivalent unavailability from forced outages, including those not expected to occur in an individual plant's lifetime. (3200.0102.552)

The Plant Protection and Instrumentation System shall be designed to meet the reliability requirements specified in reliability allocations for the

Standard MHTGR (Table 1-5) and the investment protection performance requirements for the Standard MHTGR [TBD]. (3200.0102.553)

Design modifications and improvements that allow exceeding the availability in the above availability requirements shall be considered for incorporation in the design, if a one percentage increase in the total capital investment produces, at a minimum, a seven-tenths percentage improvement in the equivalent availability factor. (3200.0102.554)

1.2.8 Maintenance Requirements

The plant shall be configured to enable system and component/equipment maintenance within a plant total scheduled outage time of less than 876 h/yr (10% equivalent unavailability) averaged over the lifetime of the plant. The allocation to the Plant Protection and Instrumentation System is as defined in Table 1-6. (3200.0102.570)

Components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory. (3200.0102.571)

Special maintenance tools shall be provided by the equipment vendor. (3200.0102.572)

1.2.9 Safety Requirements

The Plant Protection and Instrumentation System shall be designed to meet the top-level regulatory criteria (Ref. 1-6). (3200.0102.600)

The Plant Protection and Instrumentation System shall be designed such that the mean probability of a release from the plant exceeding the Protective Action Guidelines for public shelter or evacuation beyond the plant Exclusion Area Boundary is less than 5×10^{-7} per year. (3200.0102.601)

Table 1-5 RELIABILITY ALLOCATIONS TO PLANT PROTECTION AND INSTRUMENTATION SYSTEM

System/Subsystem or Features	Mean Time to Failure (MTTF) of Operation	Probability of Failure to Start or Change	Mean Time to repair (MTTR)	Equivalent Forced Outage Hours (h/yr)	Other Description
Plant Protection and Instrumentation System					
Investment Protection	{33,000} h[a]		{65} h	{15.00}	
Moisture monitors		{1 x 10^{-3}}			Probability water ingress is not detected
Safety Protection	{10,000} h		{12} h	{9.00}	
Special Nuclear Area Instrumentation	{89,000} h		{12} h	{1.00}	

[a]Numbers in { } are estimated and subject to change.

Table 1-6
SCHEDULED OUTAGE ALLOCATIONS TO PLANT PROTECTION AND INSTRUMENTATION SYSTEM

	Scheduled Outage Summary (h/yr)			
	Planned	Maintenance	Planned Derating	Allocation
Plant protection and instrumentation system	[TBD]	[TBD]	[TBD]	[TBD]
Investment protection	[TBD]	[TBD]	[TBD]	[TBD]
Safety protection	[TBD]	[TBD]	[TBD]	[TBD]
Special nuclear area instrumentation	[TBD]	[TBD]	[TBD]	[TBD]

The Plant Protection and Instrumentation System shall be designed to retain radionuclides within the plant during short-term (0 to 2 h) and long-term (0 to 30 days) accidents according to the limits shown in Table 1-7. (3200.0102.602)

The Plant Protection and Instrumentation System safety classification shall be as specified in the equipment classification list in Table 1-8. (3200.0102.603)

SSCs designated "safety-related" shall be designed to perform their safety function(s) for the Safety-Related Design Conditions (SRDCs) listed in Table 1-9. The transient design conditions for the SRDCs are included in Ref. 1-3. (3200.0102.604)

"Safety-related" portions of SSCs shall be located in their entirety within the Nuclear Island. (3200.0102.605)

Compliance with the safety requirements shall be ensured by designing the plant SSCs to meet the reliability allocations for the Standard MHTGR (Table 1-5) and the safety performance requirements for the Standard MHTGR [TBD]. (3200.0102.606)

The plant shall be designed to meet 10CFR100 requirements without reliance on the control room, its contents, the automated plant control system, the operator, or his/her actions. (3200.0102.607)

The PPIS shall assure that 10CFR100 radionuclide release limits are not exceeded for the Safety-Related Design Conditions in Table 1-9 by:

1. Sensing plant process variables to detect abnormal plant conditions and actuate reactor trip to control heat generation.

Table 1-7 RADIONUCLIDE RELEASE LIMITS

Nuclide	Curies based on PAG (User) Limits		Curies based on 10CFR100 (Reg.) Limits	
	Short-Term	Long-Term	Short-Term	Long-Term
Kr-88	<[170]	<[TBD]	<[4,250]	<[TBD]
Xe-133	<[TBD]	<[2,300]	<[TBD]	<[57,500]
I-131	<[2.6]	<[29]	<[156]	<[1,740]
Sr-90	<[0.1]	<[1.2]	<[6]	<[72]
Ag-110m	<[TBD]	<[TBD]	<[TBD]	<[TBD]
Cs-137	<[TBD]	<[TBD]	<[TBD]	<[TBD]

Table 1-8 EQUIPMENT CLASSIFICATION

Principal Component	"Safety-Related"	Not "Safety-Related"	Safety Related Functions: Basic Function	Safety Related Functions: Subfunctions/ Operation	Applicable Codes and Standards
PLANT PROTECTION AND INSTRUMENTATION SYSTEM, HFD-33200					
Investment Protection, HFD-43201					
Investment protection modules and satellites		x			
Hygrometer module assemblies		x			ASME VII, Div. ANSI B31.1
Nonmodule equipment		x			
Instruments, hardware, and software		x			
Safety Protection, HFD-4302					
Safety protection cabinets	x				IEEE 603
Safety protection remote instrumentation	x		Control heat generation	Sense, command, execute actuate negative reactivity insertion	

Table 1-8 (Continued)

Principal Component	"Safety-Related"	Not "Safety-Related"	Safety Related Functions: Basic Function	Safety Related Functions: Subfunctions/ Operation	Applicable Codes and Standards
Special Nuclear Area Instrumentation, HFD-43202					
PPIS maintenance consoles		x			
PPIS operator interface panels		x			
Special nuclear area instrumentation		x			IEEE 603 (Section 5.8)
Special nuclear area monitors		x			
Instruments, hardware, and software		x			

Table 1-9
SAFETY-RELATED DESIGN CONDITIONS

Pressurized Conduction Cooldown
(SRDC No. 1)

Pressurized Conduction Cooldown Without Control Rod Trip
(SRDC No. 2)

Pressurized Conduction Cooldown With Control Rod Withdrawal
(SRDC Nos. 3, 4)

Pressurized Conduction Cooldown With Earthquakes (SSE)
(SRDC No. 5)

Depressurized Conduction Cooldown With Moderate Moisture Ingress
(SRDC No. 6, 7)

Depressurized Conduction Cooldown With Small Moisture Ingress
(SRDC No. 8, 9)

Depressurized Conduction Cooldown With Moderate Primary Coolant Leak
(SRDC No. 10)

Depressurized Conduction Cooldown With Small Primary Coolant Leak
(SRDC No. 11)

2. Sensing plant process variables to detect large steam generator leaks and actuate main loop shutdown to isolate the steam generator to control chemical attack of the fuel. (3200.0102.608)

1.2.10 Industry Codes and Standards

The plant design, analysis, fabrication, and construction shall comply with industry codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in component design specifications and other appropriate documentation during the design effort. Applicable state and local government regulations, codes, and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justified in appropriate lower level design documents. The specific industry codes and standards that have been selected to date as being applicable to the Plant Protection and Instrumentation System are as given in Table 1-10. (3200.0102.620)

The piping, valves, and mechanical components of the moisture monitor/detection equipment shall be designed in accordance with the ASME Boiler and Pressure Vessel Code, Section VIII, Division 1, and ANSI/ASME B31.1.* (3200.0102.621)

1.2.11 Quality Assurance Requirements

All structures, systems, and components designated "safety-related" shall come under a Quality Assurance Program which fully complies with the requirements of Title 10 Code of Federal Regulations Part 50 (10CFR50), Appendix B. The basic requirements and supplements of ANSI/ASME NQA-1 (as endorsed by Regulatory Guide 1.28, Revision 3) and the four additional supplements from DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0),

*The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

Table 1-10
INDUSTRY CODES AND STANDARDS APPLICABLE TO THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN[a]

ANSI/ASME NQA-1	Quality Assurance Program Requirements for Nuclear Facilities.
DOE NE F2-10	Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1).
ANSI/IEEE Std. 603	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations[b].
ASME B&PV Code Section VIII, Div. 1	ASME Boiler and Pressure Vessel Code.
ANSI/ASME B31.1	Power piping.

[a]The actual issue date, edition, addenda, etc., of applicable industrial codes and structures shall be specified at the time of plant site selection.

[b]IEEE-279 is required by 10CFR50.55a; however, it has been withdrawn by IEEE and IEEE-603 supersedes IEEE-279.

Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5) shall be implemented on activities that affect the quality of such items. Structures, systems, and components that are not "safety-related" shall come under a quality assurance program which complies with selected basic requirements and appropriate supplements of NQA-1 and the four additional supplements from F2-10 identified above. (3200.0102.680)

1.2.12 Construction Requirements

The design of Plant Protection and Instrumentation System shall be based upon parallel construction of the complete plant. Additionally, features shall be included to enable construction and startup in increments of two standard reactor modules and one turbine. (3200.0102.701)

Special installation equipment not commercially available shall be provided by the equipment vendor. (3200.0102.702)

1.2.13 Decommissioning Requirements

Until more specific criteria and/or rules are published, NUREG-0586, "Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities," January 1981, shall be used as guidance for anticipating NRC criteria concerning plant decommissioning. (3200.0102.720)

Features that enable decommissioning or refurbishment of one reactor while maintaining others in operation shall be included. (3200.0102.721)

SECTION 2
DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The Plant Protection and Instrumentation System to meet the requirements given in Section 1 is composed of three subsystems: Investment Protection, Safety Protection, Special Nuclear Area Instrumentation. The allocation of these subsystems within the Plant Protection and Instrumentation System is shown in Table 2-1.

The scope of the protection subsystems starts with and includes the process sensors to the inputs of the actuated equipment.

The Investment Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate protective actions required to protect the plant investment. The Investment Protection Subsystem's prime purpose is to protect major plant equipment and is, therefore, investment risk oriented. The investment protection provides an integrated response to various plant upsets and events to ensure 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 Safety Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate protective actions required to mitigate the consequences of design basis events, protecting the public health and safety. Each reactor module has a separate and independent Safety Protection Subsystem.

Table 2-1
ALLOCATION WITHIN THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM

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

The Special Nuclear Area Instrumentation Subsystem provides preventive features (interlocks) and instrumentation that monitors protection subsystems' status and the plant under normal operating and accident conditions. It is not "safety-related."

2.2 SYSTEM CONFIGURATION

The Plant Protection and Instrumentation System is designed to perform the function of detecting abnormal plant conditions and actuating equipment to maintain plant parameters within component damage thresholds, thereby protecting the public health and safety and protecting the plant investment. These functions are provided by the Safety Protection Subsystem and the Investment Protection Subsystem. Additional functions of providing preventive features and safety and investment protection plant monitors are included in the design of the Special Nuclear Area Instrumentation Subsystem.

The investment and safety protection functions are implemented on a per reactor basis with a remote multiplexed, central controlled, microprocessor based modular protection subsystems. The protection subsystem architecture consists of multiple digital data highways from the local instrumentation cabinets communicating with four centrally located, separate, redundant computers to implement the four channel protection subsystems for each reactor module as shown in Figure 2-1.

Separate and independent Plant Protection and Instrumentation System operator interfaces for each reactor module are located in the Reactor Building and in the Remote Shutdown Area (located in the Reactor Service Building). The operator interfaces include color video displays, function input devices, and keyboards. Since no operator action is required to meet 10CFR100 requirements, these interfaces are not classified as "safety-related." However, these operator interfaces are provided as part of the Plant Protection and Instrumentation System, and they are separate and independent of all other plant instrumentation and controls. In addition,

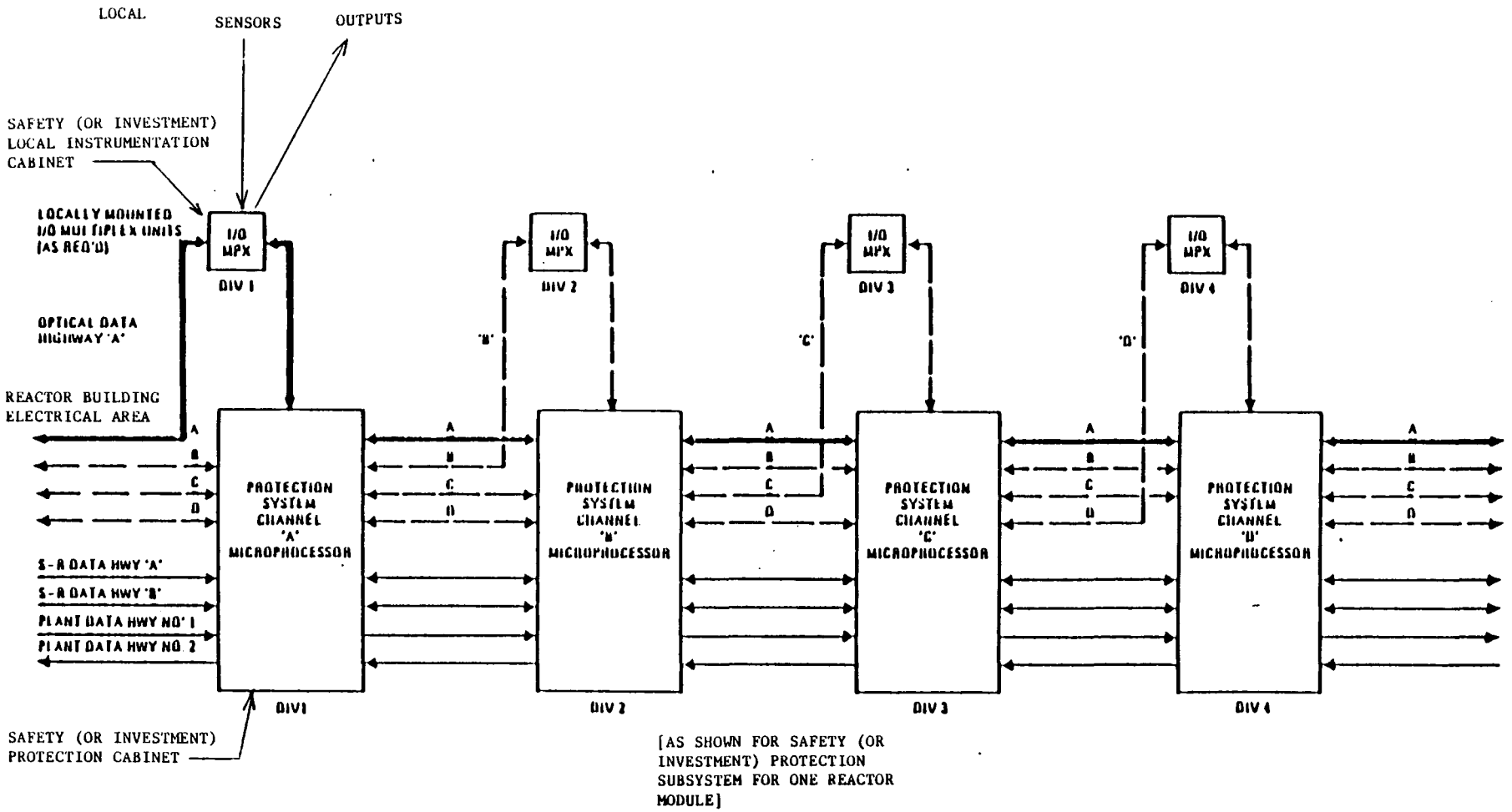


Figure 2-1 PROTECTION SYSTEM DATA BUSSES

data on the Plant Protection and Instrumentation System are transmitted through a unidirectional isolator to the Data Management Subsystem for display by the Plant Supervisory Control Subsystem in the main control room. Plant Protection and Instrumentation System operator interfaces in the remote shutdown area provide an operator the capability of initiating all Plant Protection and Instrumentation System productive actions from a position remote from the main control room. No manual inputs to the Plant Protection and Instrumentation System are provided in the main control room.

The design parameters of the Safety Protection and Investment Protection Subsystems are based on the results of transient analysis, and are discussed in greater detail in Section 2.3.

2.2.1 Investment Protection Subsystem

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

Each Investment Protection Subsystem consists of the supporting trip subsystems as shown in Figure 2-2. Each trip subsystem consists of four separate (redundant) instrument channels and redundant two-out-of-four coincidence solid-state logic to command initiation of a protective action. Each instrument channel includes the field mounted process variable 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 components may under some circumstances become associated circuits.

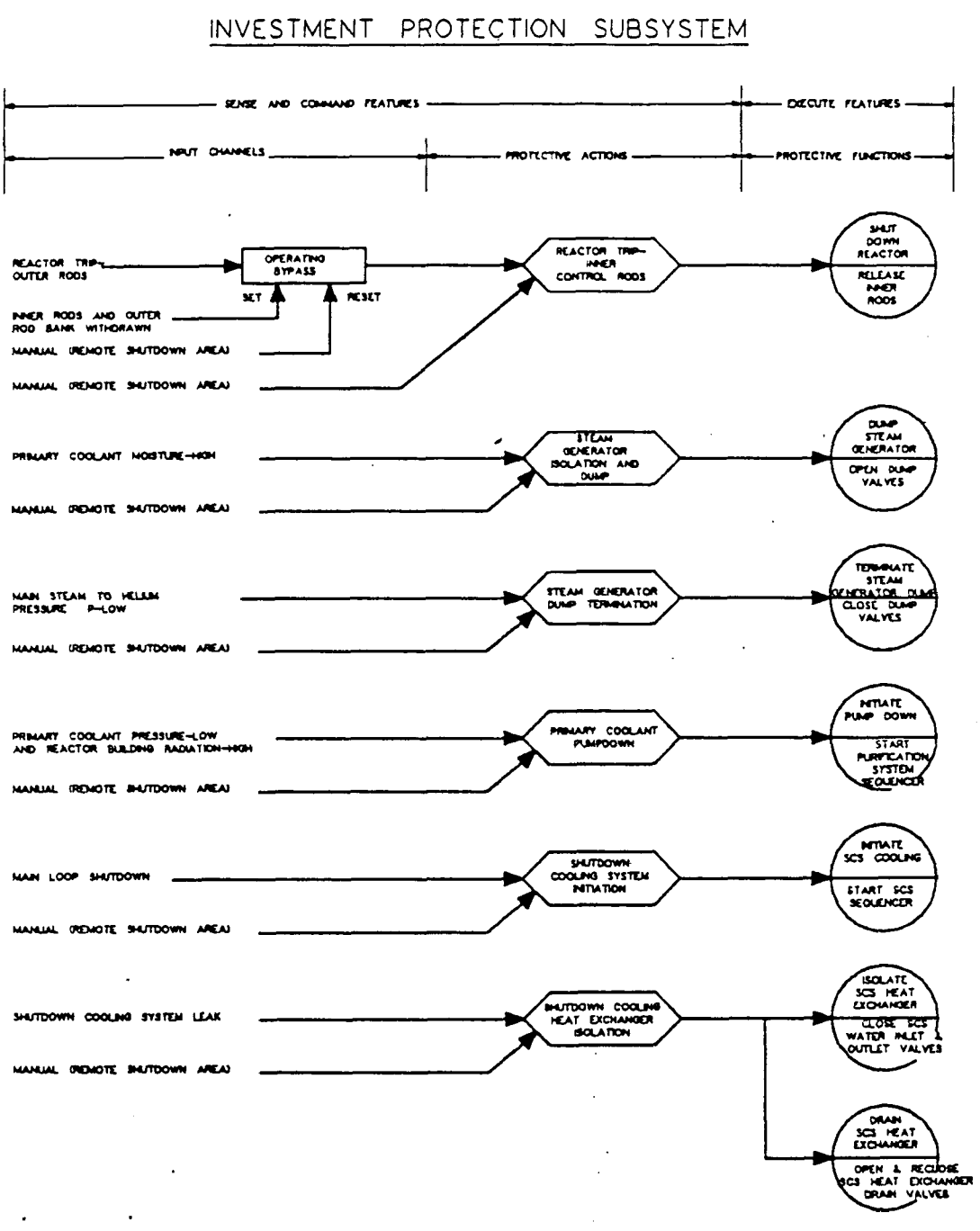


Figure 2-2 INVESTMENT PROTECTION SUBSYSTEM FUNCTIONAL OVERVIEW

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

2.2.1.1 Reactor Trip Using Inner Control Rods

The reactor trip using the inner control rods acts as a not "safety-related" reactor trip subsystem for use during reactor startup and rise to power maneuvering. A simplified one channel block diagram is shown in Figure 2-3. 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 or from a manual initiation input. The inner control rod reactor trip is automatically bypassed once all six inner control rods are full out and one bank of three outer control rods are full out. This automatic bypass reduces the investment risk to the inner control rods of possible exposure to elevated conduction cooldown temperatures. The manual inner control rod trip initiation input is not bypassed.

2.2.1.2 Steam Generator Isolation and Dump

This trip subsystem limits the quantity of water that can leak into the reactor vessel due to a steam generator tube leak, limiting damage to the reactor core and protecting the vessel pressure boundary. A simplified one channel block diagram is shown in Figure 2-4.

Upon detection of high moisture concentration in the primary coolant, the steam generator isolation and dump trip 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.

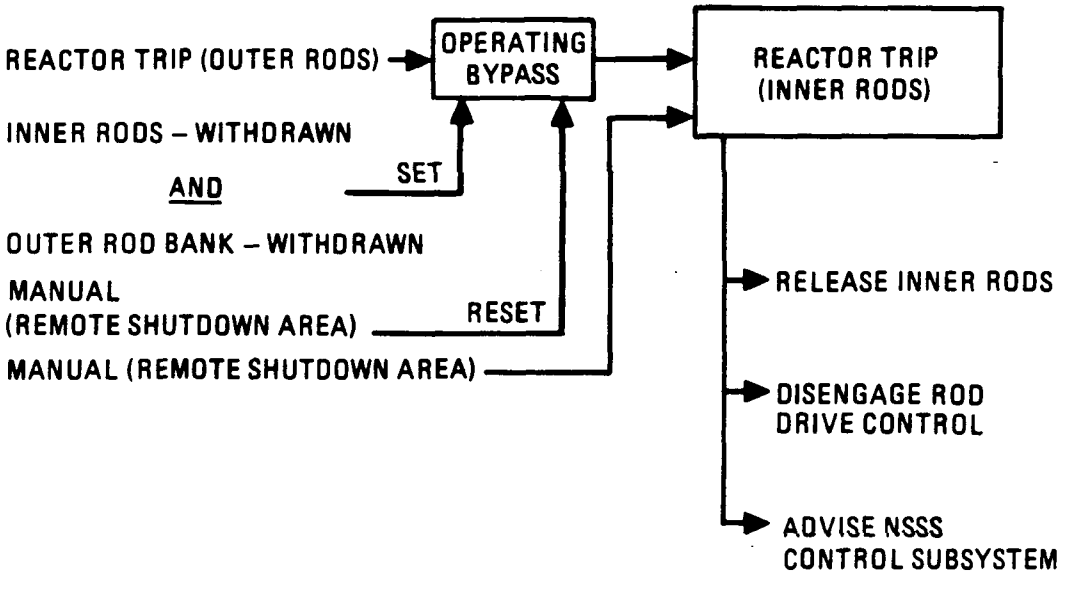


Figure 2-3 SIMPLIFIED BLOCK DIAGRAM REACTOR TRIP - INNER CONTROL RODS

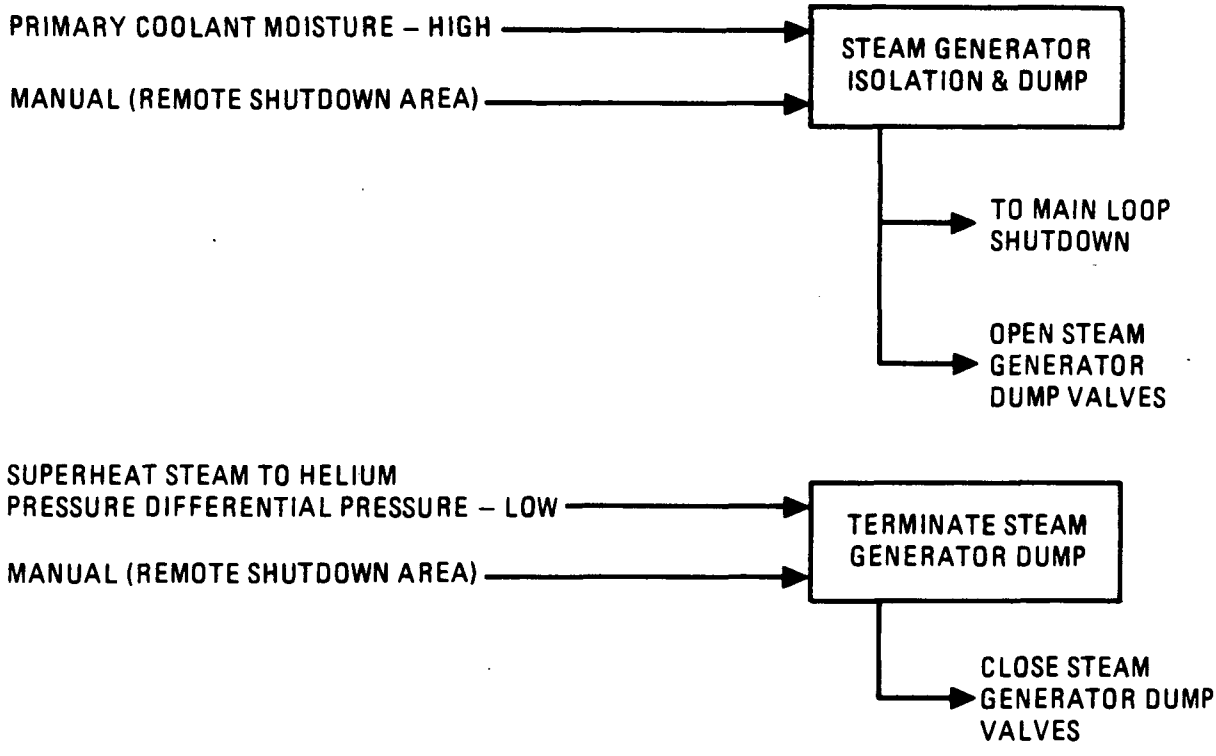


Figure 2-4
SIMPLIFIED BLOCK DIAGRAM, STEAM GENERATOR ISOLATION AND DUMP

The trip inputs to the steam generator isolation and dump trip subsystem are high primary coolant moisture concentration and manual initiation. Four separate and redundant primary coolant moisture measurement signals are provided by the investment protection moisture monitor. A main steam to helium differential pressure measurement and a manual dump termination signal are the inputs to the dump termination.

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

2.2.1.3 Primary Coolant Pumpdown

The Primary Coolant Pumpdown Trip Subsystem starts a controlled pressure pumpdown of the primary helium coolant through the helium purification system following detection of a primary coolant leak and subsequent reactor trip. This primary coolant pumpdown reduces investment risk by limiting the release of contaminated helium into the reactor building. The trip inputs to this trip subsystem are primary coolant pressure low and reactor building radiation high, or manual initiation. A simplified one channel block diagram is shown in Figure 2-5.

2.2.1.4 Shutdown Cooling System Initiation

The Shutdown Cooling System Initiation Trip Subsystem starts the shutdown cooling system upon loss of main loop cooling thus reducing thermal cycling of large module components. The trip subsystem inputs are the main loop shutdown signal and manual initiation. A simplified block diagram is shown in Figure 2-6.

2.2.1.5 Shutdown Cooling Heat Exchanger Isolation

The Shutdown Cooling Heat Exchanger Isolation Trip Subsystem isolates and drains the Shutdown Cooling Heat Exchanger following detection of helium in the cooling water. This limits the escape of primary coolant helium

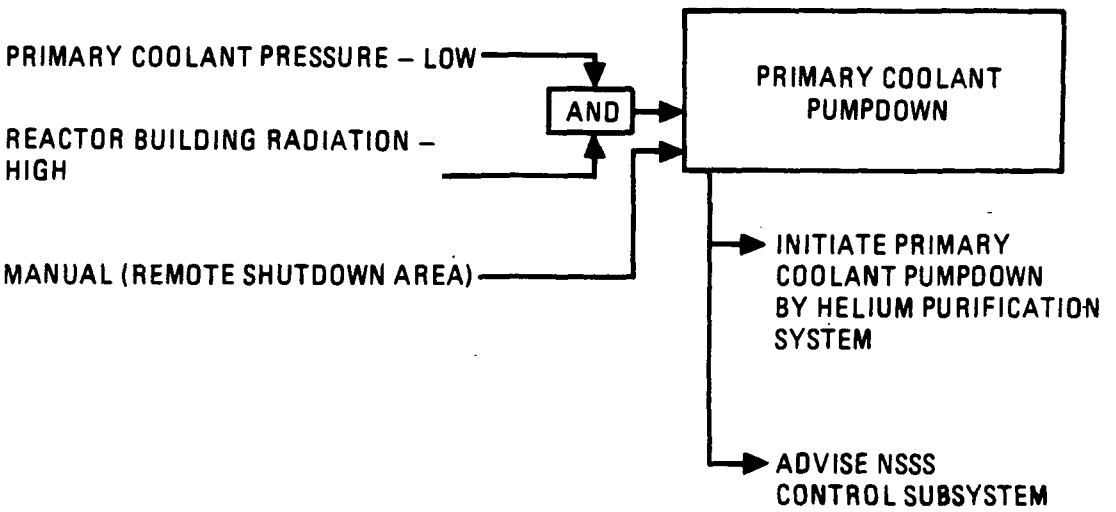


Figure 2-5 SIMPLIFIED BLOCK DIAGRAM, PRIMARY COOLANT PUMPDOWN

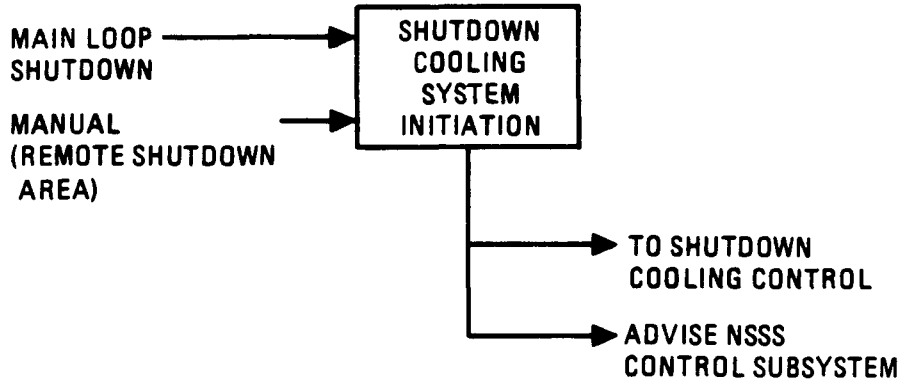


Figure 2-6
SIMPLIFIED BLOCK DIAGRAM, SHUTDOWN COOLING SYSTEM INITIATION

through a Shutdown Cooling Heat Exchanger leak. A simplified one channel block diagram is shown in Figure 2-7.

2.2.2 Safety Protection Subsystem

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

Each Safety Protection Subsystem consists of three supporting trip subsystems as shown in Figure 2-8. Each trip subsystem consists of four separate (redundant) safety channels and redundant two-out-of-four coincidence solid-state logic to command initiation of a protective action. Each channel includes the field mounted process variable sensors (e.g., thermocouples, flow transducers, pressure transducers, neutron detectors, etc.), electronic signal conditioning equipment, and trip setpoint computer 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 system channels reach the trip setpoint. The protective action initiation signal is sent to separate and redundant actuation devices. The boundaries of the Safety Protection Subsystem are generally from, and including, the system sensors to the input of the actuation devices.

The Safety Protection Subsystem meets the requirements of "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE-603, except the requirement for manual initiation capability to be located in the control room and the specific requirements for design basis document format. The Safety Protection Subsystem is composed of the following trip subsystems for each reactor module.

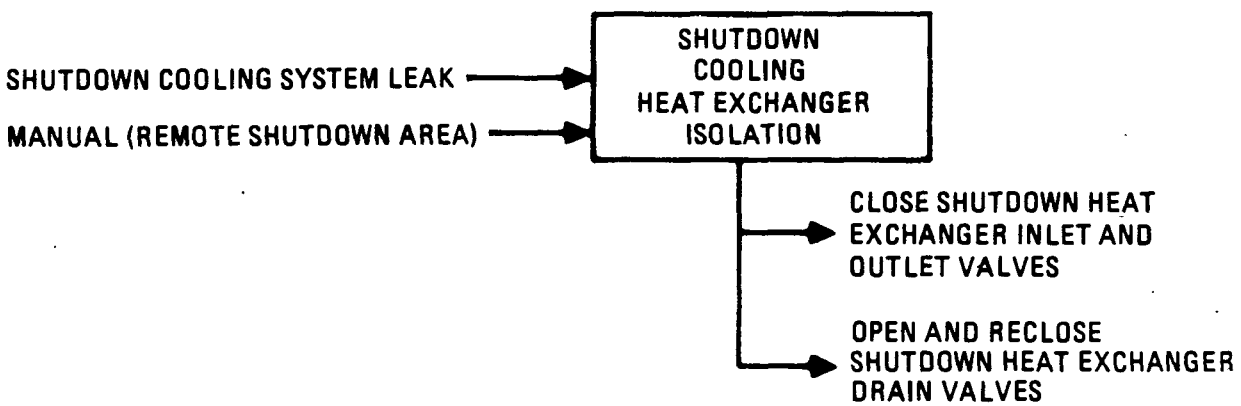


Figure 2-7
SIMPLIFIED BLOCK DIAGRAM, SHUTDOWN COOLING HEAT EXCHANGER ISOLATION

SAFETY PROTECTION SUBSYSTEM

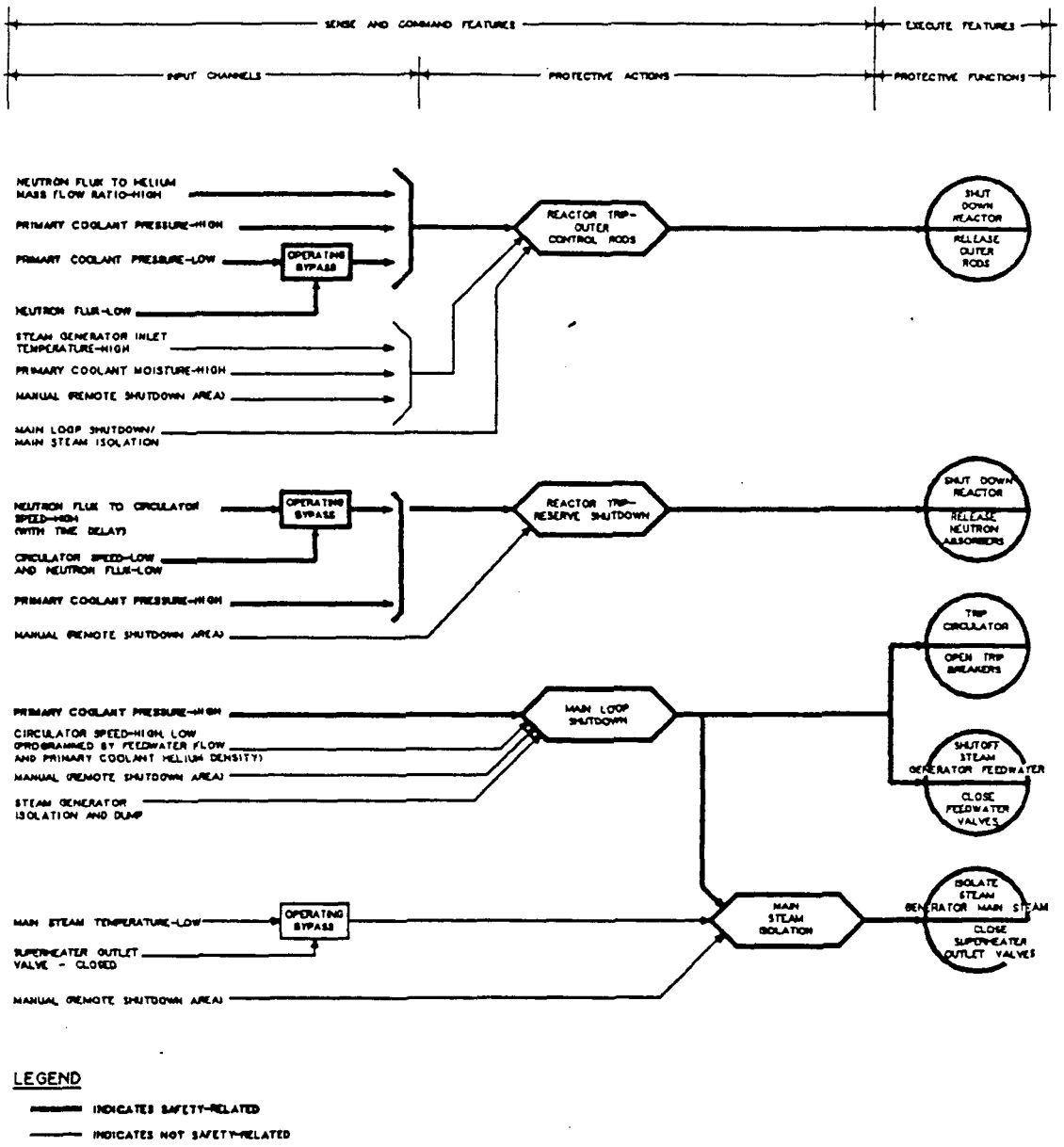


Figure 2-8 SAFETY PROTECTION SUBSYSTEM FUNCTIONAL OVERVIEW

2.2.2.1 Reactor Trip Using Outer Control Rods

This "safety-related" trip subsystem initiates a rapid reduction in reactor power following excessive reactivity increases, loss of adequate core cooling, water ingress events, 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. A simplified one channel block diagram is shown in Figure 2-9.

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

1. Neutron Flux to helium mass flow ratio high.

2. Primary coolant pressure low (automatically bypassed on low neutron flux).

3. Primary coolant pressure high.

4. Primary coolant moisture concentration high (not required for safety).

5. Main loop shutdown and main steam isolation trip signal (not required for safety).

6. Steam generator inlet helium temperature high (not required for safety).

7. Manual initiation (not required for safety).

The 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 fully inserted in the core. On occurrence of a reactor trip, the reactor trip subsystem sends signals to

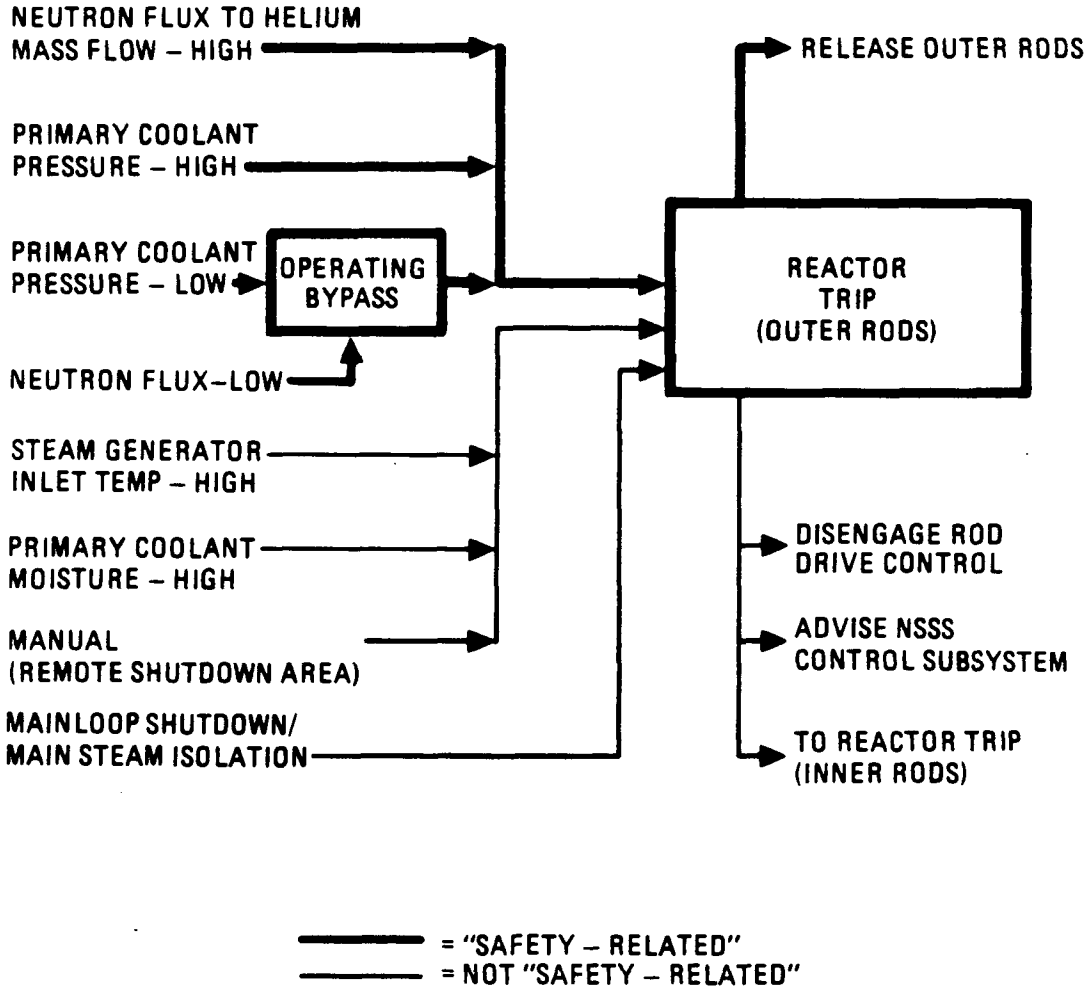


Figure 2-9
SIMPLIFIED BLOCK DIAGRAM REACTOR TRIP - OUTER CONTROL RODS

the NSSS Control Subsystem to initiate a feedwater flow reduction to aid in an orderly ramp down of the steam supply system. Reactor power inputs to the reactor trip subsystem are derived from ex-vessel neutron flux detectors. Detector outputs are conditioned into linear signal components as required for the Special Nuclear Area Instrumentation and reactor trip module inputs.

The outer control rod pairs and the "safety-related" neutron detectors and detector electronics are protection subsystem equipment provided by the Neutron Control Subsystem.

2.2.2.2 Reactor Trip Using Reserve Shutdown Control Equipment

This "safety-related" trip subsystem actuates the reserve shutdown control equipment to perform reactor trip whenever the outer control rod reactor trip system fails to trip when commanded or when the positive reactivity of water ingress in the reactor core exceeds the negative reactivity of the outer control rods. A simplified one channel block diagram is shown in Figure 2-10. The reserve shutdown control equipment reactor trip inputs are:

1. Reactor neutron flux to main helium circulator speed ratio high (with appropriate delay time to allow the outer control rod reactor trip system to correct the transient).
2. Primary coolant pressure high.
3. Manual initiation (not required for safety).

The actuated equipment for this reactor trip subsystem are the reserve shutdown control equipment fusible links. Upon actuation the fusible links are energized, they open, causing the reserve shutdown hoppers to release the reserve shutdown material into receiver channels in fuel columns adjacent to the inner 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. Upon initiation of a reactor trip

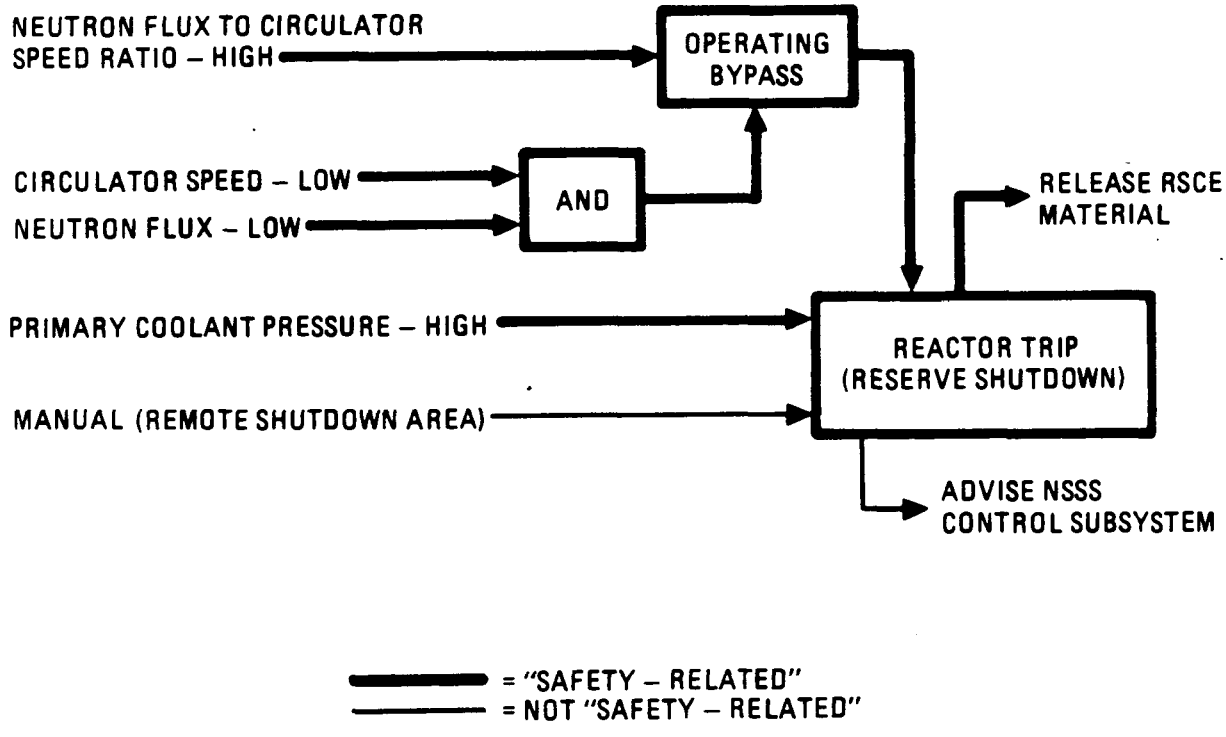


Figure 2-10
SIMPLIFIED BLOCK DIAGRAM, REACTOR TRIP - RESERVE SHUTDOWN CONTROL EQUIPMENT

using the reserve shutdown system, a signal is sent to the NSSS control subsystem to initiate a feedwater flow reduction to aid in an orderly rampdown of the steam supply system.

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

2.2.2.3 Main Loop Shutdown and Main Steam Isolation

This "safety-related" trip subsystem includes the main loop shutdown protective action and the main steam isolation protective action.

The main loop shutdown in conjunction with main steam isolation isolates the steam generator upon detection of a 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 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 in conjunction with main steam isolation the closure of the valves necessary to shut off the secondary side of the coolant loop.

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

1. Primary coolant pressure high.

2. Circulator speed high or low, compared to a nominal circulator speed setpoint programmed by feedwater flow and primary coolant helium density (not required for safety).

3. Steam generator isolation and dump signal (not required for safety).

4. Manual initiation (not required for safety).

The actuated equipment for main loop shutdown includes the feedwater block valves and circulator motor trip contactors.

The main steam isolation isolates the steam generator from the steam header and turbine-generator and allows the steam flow to be bypassed when the main steam temperature falls below the minimum acceptable temperature and quality required by the turbine. This protects the turbine from potential damage when low main steam temperature is detected. Main steam isolation is executed automatically by closing the main steam valves to the steam header. Main steam is then automatically diverted to the steam bypass.

The main steam isolation trip inputs, derived from four separate and redundant sensor channels are:

1. Main loop shutdown.
2. Main steam temperature low (not required for safety).
3. Manual initiation (not required for safety).

The actuated equipment for main steam isolation includes the superheater outlet valves.

A simplified one-channel block diagram of the main loop shutdown and main steam isolation subsystem is shown in Figure 2-11.

2.2.3 Special Nuclear Area Instrumentation Subsystem

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 and investment protection information display equipment consists of field mounted electronic multiplexer modules, redundant digital data highways, redundant microprocessor equipment, and instrumentation displays in the remote shutdown area and Reactor Building electrical area to provide the integration of protection sensor channel readouts, protection status (e.g., trip, alarm, normal, etc.) indication, and 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 actions have been completed after design basis events. The displays also are available for use in performing calibration, testing, and maintenance.

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

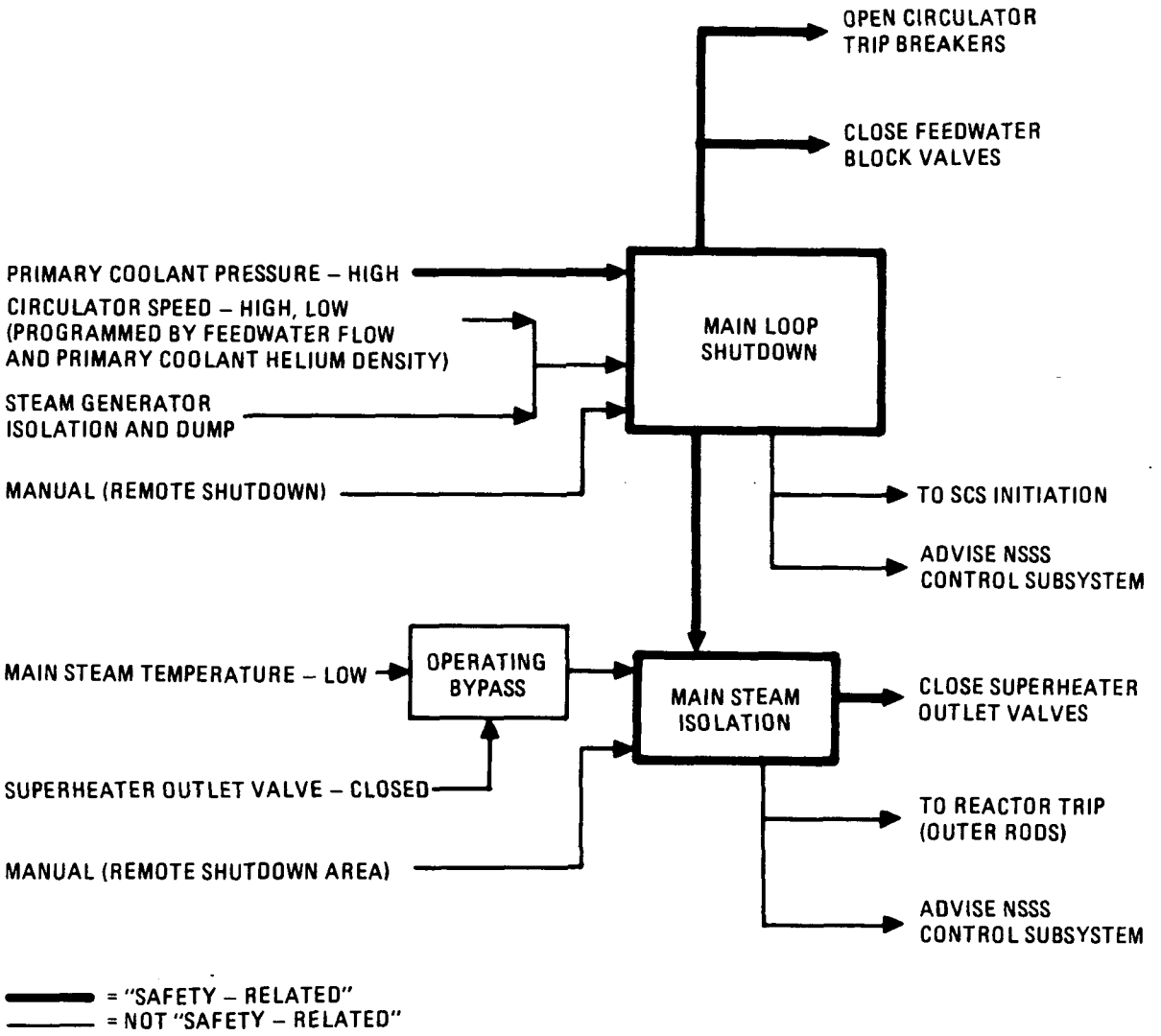


Figure 2-11
SIMPLIFIED BLOCK DIAGRAM, MAIN LOOP SHUTDOWN AND MAIN STEAM ISOLATION

The post-accident monitoring (PAM) instrumentation indicates plant information which is 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 processes data that provides information on the operation of plant "safety-related" systems and other systems that are required by the operating personnel during and 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.

2.2.3.1 Vessel System Pressure Relief Block Valve Closure Interlock

This trip 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 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.

2.2.3.2 Safety Protection Information Displays

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

1. Safety protection channel readouts.

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

3. 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 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 design basis events. 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.

2.2.3.3 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:

1. Investment protection channel readouts.

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

3. 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 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 operator to take manual actions from the Plant Protection and Instrumentation Subsystem equipment in the remote shutdown area which are important to protecting plant investment. These displays are provided by the Plant Protection and Instrumentation Subsystem to the Data Management Subsystem for display in the main control room by the Plant Supervisory Control Subsystem.

2.2.3.5 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 Special Nuclear Area Instrumentation 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.

2.3 SYSTEM PERFORMANCE CHARACTERISTICS

The design configurations outlined in Section 2.2 for the Investment and Safety Protection Subsystems will detect abnormal plant conditions and actuate equipment to maintain plant parameters within the plant damage thresholds established for the components listed in Table 1-4, preventing damage to components whose function is essential to meet top level regulatory requirements or for protection of the plant investment.

The duty cycle given in Table 1-3 governs the design of the Plant Protection and Instrumentation System.

The performance characteristics of major system elements are given in Tables 2-2, 2-3, and 2-4.

2.3.1 System Operating Modes

In general the trip portion of the Plant Protection and Instrumentation System is operable during all plant modes and the protection information display portions are operating during all plant modes. The status of the

Table 2-2 PLANT PROTECTION AND INSTRUMENTATION SYSTEM PROTECTIVE ACTIONS

Protective Action	Conditions for Completion of Protective Action	Time for Protection Action to Continue
Reactor trip using outer control rods	All outer control rods are inserted.	Sensor channel: until trip signal is sent. Execute features: indefinitely until manually reset.
Reactor trip using reserve shutdown control equipment	All reserve shutdown material is inserted.	Sensor channel: until trip signal is sent. Execute features: indefinitely until manually reset.
Reactor trip using inner control rods	All inner control rods are inserted.	Sensor channel: until trip signal is sent. Execute features: indefinitely until manually reset.
Steam generator isolation and dump	All steam generator isolation valves closed, dump valves cycled open to reduce SG pressure to {517 kPa (75 psid)}[a] above reactor vessel pressure and closed again.	Until dump and isolation is complete.
Main loop shutdown	All feedwater isolation valves closed and circulator motor trip contactors open.	Sensor channel: until shutdown signal is sent. Execute features: indefinitely until manually reset.
Main steam isolation	All main steam isolation valves closed.	Sensor channel: until isolation signal is sent. Execute features: indefinitely until manually reset.
Shutdown cooling initiation	Shutdown Cooling System start signal sent to shutdown cooling control subsystem.	Until shutdown cooling start signal is received by the SCS control subsystem.

Table 2-2 (Continued)

Protective Action	Conditions for Completion of Protective Action	Time for Protection Action to Continue
Primary coolant pumpdown	Primary coolant pumpdown start signal sent to helium purificacation system.	Sensor channel: until pumpdown signal is sent. Execute features: until primary coolant pumpdown start signal is received by helium purification subsystem.
Shutdown cooling heat exchanger isolation	All shutdown cooling heat exchanger isolation valves closed and drain valves cycled open to drain the shutdown heat exchanger and closed again.	Sensor channel: until isolation signal is sent. Execute features: indefinitely until manually reset.

(a)Numbers in { } estimated.

Table 2-3 PLANT PROTECTION AND INSTRUMENTATION SYSTEM SENSOR CHANNEL PARAMETERS

Monitored Variable - Sensor Parameters	Sensor Channel Parameters		
	Maximum Response Time	Minimum Accuracy	Minimum Range
Primary Coolant Pressure ("Safety-Related")	{2 s}[a]	{±1%} of span	{600-1100 psia}
Receptive Trip Subsystems: Reactor trip using outer control rods, reactor trip using reserve shutdown control equipment, main loop shutdown, primary coolant pressure pumpdown, steam generator isolation and dump (dump valve closure)			
Circulator Inlet Pressure Drop ("Safety-Related")			
Receptive Trip Subsystem: Reactor trip using outer control rods	{2 s}	{±1%} of span	{0-1.0 psid}
Primary Coolant High Moisture Concentration	{40 s} (at all loads and includes 20 s sample transit time and 5 s sensor time constant)	{±200 ppmv}	Not applicable
Receptive Trip Subsystems: Reactor trip using outer control rods, steam generator isolation and dump			
Steam Generator Inlet Helium Temperature	{20.0 s} time constant at 100% power	{±30°F}	{350°-2200°F}
Receptive Trip Subsystem: Reactor trip using outer control rods			

Table 2-3 (Continued)

Monitored Variable - Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Sensor Channel Parameters: Minimum Accuracy	Minimum Range
Reactor Neutron Flux ("Safety-Related")	{10.0 ms}	{±1%} of span	{2%-200%} of rated power
Receptive Trip Subsystem: Reactor trip using outer control rods			
Reactor trip using reserve shutdown control equipment			
Reactor Neutron Flux-to-Helium Mass Flow Ratio ("Safety-Related")	{2.0 s}	±[TBD] at full power	{0-2}
Receptive Trip Subsystem: Reactor trip using outer control rods			
This ratio is continuously calculated by dividing the reactor neutron flux by the helium mass flow rate			
Reactor Helium Mass Flow Rate ("Safety-Related")	{2.0 s}	±[TBD] at 100% flow	{8%-120%} (pressurized)
Receptive Trip Subsystem: Reactor trip using outer control rods		±[TBD] at 10% flow	
This parameter is continuously calculated from: circulator inlet differential pressure (ΔP) psi, main circulator inlet helium temperature (T) °F, primary coolant pressure (P) psia, and a constant, C			
Mass flow rate = $C \sqrt{\Delta P \; P/T}$			

Table 2-3 (Continued)

Monitored Variable - Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Sensor Channel Parameters: Minimum Accuracy	Minimum Range
Circulator Speed ("Safety-Related")	{10 ms}	{±1%} of span	{0-8000 rpm}
Receptive Trip Subsystems: Reactor trip using outer control rods, main loop shutdown			
Reactor Neutron Flux-to-Circulator Speed Ratio ("Safety-Related")			
Receptive Trip Subsystem: Reactor trip using reserve shutdown control equipment	{2.0 s}	±[TBD] at full power	{0-3 s}
Main Circulator Inlet Helium Temperature ("Safety-Related")	{20.0 s} (time constant)	{±9°F}	{300°-850°F}
Receptive Trip Subsystems: Reactor trip using outer control rods, main loop shutdown			
Sensors at the inlet of the circulator. This measurement is also used in the helium mass flow rate calculation above.			
Main Steam Temperature	{20 s} time constant at 100% power.	{±10°F}	{500°-1400°F}
Receptive Trip Subsystem: Main steam isolation	(Later) s time constant at 25% power		

Table 2-3 (Continued)

Monitored Variable - Sensor Parameters	Sensor Channel Parameters		
	Maximum Response Time	Minimum Accuracy	Minimum Range
Feedwater Flow Rate	{2 s}	{±[TBD] at 10% flow}	{5%-105%} flow
Receptive Subsystems: Main loop shutdown			
Superheat Steam Pressure	{2 s}	±[TBD] of full scale	{14-2800 psia}
Receptive Subsystem: Steam generator isolation and dump (dump valve closure)			
Reactor Building Radiation	[TBD]	[TBD]	[TBD]
Receptive Subsystem: Primary coolant pressure pumpdown			
Shutdown Cooling Heat Exchanger Leak	[TBD]	[TBD]	[TBD]
Receptive Trip Subsystem: Shutdown cooling heat exchanger isolation			

(a){ } = numbers are estimated.

Table 2-4
PLANT PROTECTION AND INSTRUMENTATION SYSTEM ACTUATED EQUIPMENT

Actuated Equipment	Maximum Response Time
Inner Control Rods	
Actuation Trip Subsystem: Reactor trip using inner control rods	{25 s}[a] for full insertion
Outer Control Rods ("Safety-Related")	
Actuating Trip Subsystem: Reactor trip using outer control rods	{25 s} for full insertion
Reserve Shutdown Control ("Safety-Related")	
Actuating Trip Subsystem: Reactor trip using reserve shutdown system	{40 s} for full insertion
Steam Generator Dump Valves	
Actuating Trip Subsystem: Steam generator isolation and dump Four dump valve matrix per steam generator (opening delayed to allow time for feedwater shutoff)	{5 s} to open {5 s} to close
Main Loop Isolation Valves and Circulator Trip Motor Contactors ("Safety-Related")	
Actuating Trip Subsystem: Main loop shutdown and main steam isolation	
The following valves for each steam generator:	
Feedwater block valves (two in series)	{5 s} to close
Superheater outlet valves (two in series)	{10 s} to close
Main circulator contactor opening (two contacts in series)	{1.0 s} to trip open
Helium Purification Primary Coolant Pressure Pumpdown Controls	
	[TBD] s to start
Shutdown Cooling System Controls	
	{5 s} to start

Table 2-4 (Continued)

Actuated Equipment	Maximum Response Time
Shutdown Cooling Heat Exchanger Isolation and Drain Valves	
Actuating Trip Subsystem: Shutdown cooling heat exchanger isolation	
The following valves for each shutdown cooling heat exchanger:	
Cooling water inlet block valves (two in series)	[TBD] s to close
Cooling water outlet block valves (two in series)	[TBD] s to close
Shutdown heat exchanger drain valves (two in parallel) (opening delayed to allow time for isolation)	[TBD] s to open

(a){ } = numbers are estimated.

plant is, therefore, monitored at all times and trip actions are initiated as required. Portions of the system may be bypassed for surveillance, testing, and maintenance; however, due to the system's redundancy this does not necessitate loss of the protective function. Operation of the plant with "safety-related" portions of the Plant Protection and Instrumentation System out of service is governed by the Plant Technical Specifications.

Table 2-5 gives the operating mode of the Plant Protection and Instrumentation System versus plant conditions.

2.3.2 System Steady State Performance

The steady-state performance is with the system operable, monitoring plant variables, and available for use if needed.

2.3.3 System Response to Plant Transients

Plant Protection and Instrumentation System trip parameters used during analysis of Anticipated Operational Occurrences (AOOs), Design Basis Events (DBEs), Safety-Related Design Conditions (SRDCs), and Emergency Planning Basis Events (EBBEs) are shown in Table 2-6.

The response of the Plant Protection and Instrumentation System to AOO and DBE plant transients and its performance subjected to SRDCs is described in the following subsections.

2.3.3.1 System Response to Anticipated Operational Occurrences (AOOs)

In this section only the response of the Plant Protection and Instrumentation System to AOOs is described. No other system's performance is described even though other systems may also respond to these AOOs.

Table 2-5
PLANT PROTECTION AND INSTRUMENTATION SYSTEM OPERATING MODE VERSUS PLANT CONDITION

	Plant Condition	Operating Mode[a]	Remarks[b]
1.1	Energy production	Operable	
1.2	Shutdown	Shutdown/operable	Portions of system may be shut down for maintenance. The reactor trip reserve shutdown and displays remain operating.
1.3	Refueling	Operable	
1.4	Startup and shutdown	Operable	
2.0	Maintain plant protected	Operable/operating[a]	Portions operating depends upon portion of plant in need of protection.
3.0	Radiological release controlled	Operable/operating[a]	Portions operating tend to relate to control of fission product barriers.
4.0	Emergency plan activated	Operable	

[a]Trip portions operate as necessary during abnormal plant events.
[b]Some portions of displays are operating during all plant conditions.

Table 2-6 PLANT PROTECTION AND INSTRUMENTATION TRIP PARAMETERS

PPIS Action	"Safety-Related"	Trip Parameter	DBE SRDC Analysis Setpoint	Nominal Setpoint	Measured Parameters	Delay Time to Measure Parameter	Instrument Time Constant	Calculation Delay	Command Action Delay	Actuated Equipment	Actuation Delay	Notes
Reactor trip outer control rods	Yes	Neutron flux to helium mass flow ratio high	1.50	[1.40]	Neutron flux (ϕ)	0 s	[10]* ms	1 s	1 s	Outer control rods	[25] s from full out to full in	
					Primary coolant helium pressure (P)	0 s	[2] s					Helium mass flow is calculated from $C\sqrt{\frac{P\Delta P}{T}}$ where C is a constant
					Circulator inlet pressure drop(ΔP)	0 s	[2] s					
					Circulator inlet temperature (T)	0 s	[20] s					
	Yes	Primary coolant pressure low and	825 psia	[835]psia	P (above)			0 s	1 s			
		Bypass at low neutron flux	Bypass at $\leq$12% neutron flux	Bypass at $\leq$10% neutron flux								
	Yes	Primary coolant pressure high	1025 psia	[1015]psia	P (above)			0 s	1 s			
	No	Primary coolant moisture high	1200 ppmv	[1000]ppmv	Moisture concentration (M)	[20] s	[5] s	0 s	1 s			Moisture concentration measurement from S/G isolation and dump
	No	Main loop shutdown/ main steam isolation	N/A	N/A	Main loop trip signal	N/A	N/A	0 s	1 s			
	No	S/G inlet helium temperature high	[1400] °F	[1375] °F	S/G inlet helium temature (T_{SG})	0 s	[20] s	0 s	1 s			

*[ ] = Number Tentative

Table 2-6 (Continued)

PPIS Action	"Safety-Related"	Trip Parameter	DBE SRDC Analysis Setpoint	Nominal Setpoint	Measured Parameters	Delay Time to Measure Parameter	Instrument Time Constant	Calculation Delay	Command Action Delay	Actuated Equipment	Actuation Delay	Notes
Steam generator isolation and dump	No	Primary coolant moisture concentration high	1200 ppmv	[1000] ppmv	Moisture concentration (M)	[20] s	[5]* s	0 s	1 s	Main loop shutdown	(See main loop shutdown)	
			7 s time delay	6 s time delay						Steam generator dump valves	[5] s to open	Dump valve opening delayed to allow for feedwater shutoff
Steam generator dump terminate	No	Main steam pressure to	[50] psid	[75] psid	Main steam pressure (P_{ms})	0 s	[2] s	0 s	1 s	Steam generator dump valves	[5] s to close	
		primary coolant pressure ΔP low			Primary coolant pressure (P)	0 s	[2] s					Helium pressure measurement from reactor trip pressure measurement
Primary coolant pressure pumpdown with helium purification system	No	Primary coolant pressure low	[800] psia	[810] psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s	Helium purification system	[TBD] s	
		and reactor building radiation high	TBD mR/h	TBD mR/h	Reactor building radiation (R)	TBD	TBD	TBD				
Shutdown cooling system (SCS) initiation	No	Main loop shutdown	N/A	N/A	Main loop shutdown signal	0 s	N/A	0 s	1 s	SCS control subsystem	[5] s to establish SCS cooling	
Shutdown cooling heat exchanger isolation	No	Shutdown cooling system leak	[TBD]	[TBD]	SCWS pressure (P_{cw})	Varies with leak size	[2] s	0 s	1 s	SCS heat exchanger isolation and drain valves	[ ] s to isolate water	Drain valve opening delayed to allow heat exchanger isolation; reclosing delayed to allow time for heat exchanger to drain

*[ ] = Number Tentative

Table 2-6 (Continued)

PPIS Action	"Safety-Related"	Trip Parameter	DBE SRDC Analysis Setpoint	Nominal Setpoint	Measured Parameters	Delay Time to Measure Parameter	Instrument Time Constant	Calculation Delay	Command Action Delay	Actuated Equipment	Actuation Delay	Notes
Reactor trip inner control rods	No	Reactor trip signal for outer control rods <u>and</u> inner control rods and one bank of outer control rods not fully withdrawn	N/A	N/A	Reactor trip signal for outer control rods	0 s	0 s		1 s	Inner control rods	25 s from full out to full in	

Table 2-6 (Continued)

PPIS Action	"Safety-Related"	Trip Parameter	DBE SRDC Analysis Setpoint	Nominal Setpoint	Measured Parameters	Delay Time to Measure Parameter	Instrument Time Constant	Calculation Delay	Command Action Delay	Actuated Equipment	Actuation Delay	Notes
Main loop (HTS) shutdown/ Main steam isolation	Yes	Primary coolant pressure high	1025 psia	[1015] psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s	Circulator motor contactors	[1] s to open	Helium pressure measurement from reactor trip pressure instrument
										Feedwater block valves	[5] s to close	
										Superheat outlet valves	[10] s to close	
	No	HTS circulator speed high or low programmed by feedwater flow and helium density	±[1487] rpm	±[1144] rpm	HTS circulator speed (s)	0 s	[10]*ms	1 s	1 s			Circulator speed measurement from reserve shutdown circulator speed measurement
					Feedwater flow (F)	0 s	[2] s					
					P (Above)							Circulator inlet temperature measurement from reactor trip circulator inlet temp. measurement
					Circulator inlet temp. (T)	0 s	[20] s					
	No	Main steam temperature low	≤[775]°F	≤[800]°F	Main steam temperature (T_{ms})	0 s	[20] s			Actuated equipment involves only superheat outlet valves		
	No	Steam generator isolation and dump signal	N/A	N/A	Steam generator isolation signal	0 s	N/A	0 s	1 s			

*[ ] = Number Tentative

Table 2-6 (Continued)

PPIS Action	"Safety-Related"	Trip Parameter	DBE SRDC Analysis Setpoint	Nominal Setpoint	Measured Parameters	Delay Time to Measure Parameter	Instrument Time Constant	Calculation Delay	Command Action Delay	Actuated Equipment	Actuation Delay	Notes
Reactor trip reserve shutdown control equipment	Yes	Neutron flux to HTS circulator speed ratio high and time delay ≤50 s and	1.90 and 50 s time delay	[1.80] and 30 s time delay	Neutron flux (ϕ)	0 s	[10]* ms	1 s	1 s	Reserve shutdown hopper release	5 s to open hopper 35 s to empty hopper	Time delay to allow reactor trip-outer rods to respond to event. Neutron flux measurement from reactor trip neutron flux measurement.
					HTS circulator speed (s)	0 s	[10] ms					
					time (t)	0 s	0 s					
		Bypass at low HTS circulator speed and low neutron flux	Bypass at ≤7% circulator speed and ≤14% neutron flux	Bypass at ≤5% circulator speed and ≤10% neutron flux								
	Yes	Primary coolant helium pressure high	1025 psia	[1015] psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s			Helium-pressure measurement from reactor trip pressure instrument

*[ ] = Number Tentative

AOO No. 1(A) Loss of Main Loop (HTS) Cooling. The initiating event for this plant transient is loss of HTS cooling caused by such events as loss of feedwater or helium circulator trip. Loss of HTS is detected as a high neutron flux to helium mass flow ratio and the PPIS commands a reactor trip using the outer control rods. An upset in HTS is also detected by the PPIS as a circulator speed to feedwater flow mismatch. When the measured circulator speed varies beyond a nominal setpoint compared to the programmed circulator speed based on feedwater flow, the PPIS commands a main loop shutdown and main steam isolation. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main steam isolation, in turn, causes a reactor trip using the outer control rods and the main loop shutdown signals for initiation of the Shutdown Cooling System.

The response of the Special Nuclear Instrumentation portion of the PPIS to all AOOs is as follows:

1. Monitors and displays all Safety Protection and Investment Protection Subsystem sensor channels before, during, and after all AOOs.

2. Monitors and displays Safety Protection and Investment Protection Subsystem actuated device states before, during, and after all AOOs.

3. Monitors and displays Safety Protection and Investment Protection Subsystem operability and status before, during, and after all AOOs.

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

AOO No. 1(B) Loss of Offsite Power and Turbine Trip. The initiating event for this plant transient causes loss of HTS cooling due to loss of electrical power to the HTS circulator and the feedwater pumps. The PPIS response to AOO No. 1(B) is identical to the response to AOO No. 1(A).

AOO No. 1(C) Spurious Reactor Trip With Cooling on HTS. The PPIS has no trip response to AOO No. 1(C) other than to continue to be operable. The PPIS Special Nuclear Area Instrumentation responds identically to all AOOs as explained for AOO No. 1(A).

AOO No. 1(D) Main Loop Transient Without Reactor Trip. The PPIS has no trip response to AOO No. 1(D) other than to continue to be operable. The PPIS Special Nuclear Area Instrumentation responds identically to all AOOs as explained for AOO No. 1(A).

AOO No. 2 Loss of Main Loop Cooling and Shutdown Cooling. The PPIS response to AOO No. 2 is identical to the response to AOO No. 1(A).

AOO No. 3 Rod Withdrawal With Reactor Trip and Cooling on HTS. An inadvertent control rod group withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint and the PPIS commands a reactor trip using the outer control rods. The PPIS Special Nuclear Area Instrumentation responds identically to all AOOs as explained for AOO No. 1(A).

AOO No. 4 Small Steam Generator Leak. The PPIS moisture monitor detects high primary coolant moisture concentration and the PPIS commands reactor trip using the outer control rods and steam generator isolation and dump. Steam generator isolation is performed by the steam generator isolation and dump commanding main loop shutdown. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and in conjunction with main steam isolation closes the superheat steam valves. The steam generator isolation and dump commands the steam generator dump valves to open, the steam generator inventory is dumped to a dump tank, and the dump

valves are reclosed. Main loop shutdown also commands for Shutdown Cooling System initiation. The PPIS Special Nuclear Area Instrumentation responds identically to all AOOs as explained for AOO No. 1(A).

AOO No. 5 Small Primary Coolant Leak. A small primary coolant leak causes a slow depressurization of the primary coolant. When the primary coolant pressure reaches the low pressure setpoint, the PPIS commands a reactor trip using the outer control rods.

When the primary coolant pressure decreases to the low setpoint and if high reactor building radiation is detected, the PPIS commands the Helium Purification System to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. When low main steam temperature is reached, the PPIS commands a main steam isolation to prevent low temperature steam from entering the main steam header and turbine(s). At this point in the transient main steam is automatically bypassed to the condenser.

The PPIS Special Nuclear Area Instrumentation responds identically to all AOOs as explained for AOO No. 1(A).

2.3.3.2 System Response to Design Basis Events (DBEs)

In this section only the response of the Plant Protection and Instrumentation System to DBEs is described. No other system's performance is described even though other systems may also respond to the DBEs.

DBE No. 1 Loss of HTS and SCS Cooling. The initiating event for DBE No. 1 is loss of offsite power and trip of both turbines. A loss of offsite power and turbine trip causes a loss of all primary ac power supplies. This causes the main loop helium circulator and feedwater pumps to coast down due to loss of power. This is initially detected as a high neutron flux to helium mass flow ratio and the PPIS commands a reactor trip using the outer control rods. The PPIS also detects this as a circulator speed

to feedwater flow mismatch and commands a main loop shutdown. The main circulator is tripped, the feedwater block valves are closed, and in conjunction with main steam isolation the superheat steam valves are closed. Main steam isolation in turn commands a reactor trip using the outer control rods. Main loop shutdown also commands Shutdown Cooling System (SCS) initiation but the SCS fails to start due to failure of standby ac power. If primary ac power is not restored and standby ac power is not available, the PPIS loses battery backup power after approximately one hour. At this time the PPIS fails "as is" as it has no further safety function to perform. Environmental conditions or other plant service conditions experienced during DBE No. 1 have no effect on the ability of the PPIS to perform its safety and investment protection functions. The response of the PPIS Special Nuclear Area Instrumentation to all DBEs is identical and is as follows:

1. Monitors and displays all Safety Protection and Investment Protection Subsystem sensor channels before, during, and after all DBEs.

2. Monitors and displays Safety Protection and Investment Protection Subsystem actuated device status before, during, and after all DBEs.

3. Monitors and displays Safety Protection and Investment Protection Subsystem operability and status before, during, and after all DBEs.

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

DBE No. 2 HTS Transient Without Control Rod Trip. The initiating event for DBE No. 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 and the PPIS commands a main loop shutdown. Main loop shutdown and high neutron flux to circulator speed ratio commands a reactor trip using the outer control rods. For this DBE, the outer control rods fail to trip. This situation 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 reserve shutdown control equipment is commanded. Main loop shutdown also signals for Shutdown Cooling System initiation.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1. Environmental conditions or other plant service conditions experienced during DBE No. 2 have no effect on the ability of the PPIS to perform its safety and investment protection functions.

DBE No. 3 Rod Withdrawal Without HTS Cooling. The initiating event for DBE No. 3 is an inadvertent control rod group withdrawal. An inadvertent control rod group withdrawal causes the neutron flux to helium mass flow measurement to exceed the PPIS high setpoint and the PPIS commands a reactor trip using the outer control rods.

DBE No. 3 also includes a main loop upset. This is detected as a circulator speed to feedwater flow mismatch and the PPIS commands a main loop shutdown. Main loop shutdown via main steam isolation separately signals a reactor trip using the outer control rods in addition to the "safety-related" trip previously commanded by the Safety Protection Subsystem. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1. Environmental conditions or other plant service conditions experienced during DBE No. 3 have no effect on the ability of the PPIS to perform its safety or investment protection functions.

DBE No. 4 Rod Withdrawal Without HTS and SCS Cooling. The PPIS response to DBE No. 4 is identical to the response to DBE No. 3 except as follows:

DBE No. 4 includes SCS failure to start. Core cooling on the Reactor Cavity Cooling System may cause the primary coolant pressure to exceed the PPIS high pressure setpoint and the PPIS may also command a reactor trip using the reserve shutdown control equipment. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods. The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1. Environmental conditions or other plant service conditions experienced during DBE No. 4 have no effect on the ability of the PPIS to perform its safety and investment protection functions.

DBE No. 5 Earthquake. The initiating event for DBE No. 5 is a large earthquake. It is assumed that the main cooling loop is upset. Trouble with the main cooling loop is detected by the PPIS as a high neutron flux to helium mass flow ratio which commands a reactor trip using the outer control rods and as a circulator speed to feedwater flow mismatch which commands a main loop shutdown. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation and in conjunction with main steam isolation separately signals for a reactor trip using the outer control rods.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

The PPIS and its auxiliary supporting features are qualified to withstand a safe shutdown earthquake (SSE) and perform their "safety-related" functions. No other environmental conditions or other plant service conditions experienced during DBE No. 5 have an effect on the ability of the PPIS to perform its safety or investment protection functions.

DBE No. 6 Moisture Inleakage. The initiating event for DBE No. 6 is a steam generator offset tube rupture and subsequent large moisture ingress rate.

The PPIS moisture monitor detects high primary coolant moisture concentration and commands reactor trip using the outer control rods and commands steam generator isolation and dump. Steam generator isolation is performed as a main loop shutdown and main steam isolation. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and in conjunction with main steam isolation closes the superheat steam valves. The steam generator dump valves open, the steam generator inventory is dumped to a dump tank, and the dump valves reclose. Main loop shutdown also signals for Shutdown Cooling System initiation.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

Environmental conditions or other plant service conditions experienced during DBE No. 6 have no effect on the ability of the PPIS to perform its safety and investment protection functions.

DBE No. 7 Moisture Inleakage Without SCS Cooling. The initiating event for DBE No. 7 is a moderate steam generator leak and subsequent moderate moisture ingress rate. The response of the PPIS to this event is identical to DBE No. 6 except the SCS fails to start. Core cooling on the Reactor Cavity Cooling System may cause the primary coolant pressure to exceed the PPIS high pressure setpoint and the PPIS may separately command a reactor trip using the reserve shutdown control equipment. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods.

DBE No. 8 Moisture Inleakage With Moisture Monitor Failure. The initiating event for DBE No. 8 is a small steam generator leak and subsequent

small moisture ingress rate. The PPIS moisture monitor is assumed to fail to detect the moisture ingress.

The moisture ingress causes the primary coolant pressure to slowly increase. The primary coolant pressure reaches the PPIS high pressure setpoint and the PPIS commands a reactor trip using the outer control rods and the reserve shutdown control equipment and a main loop shutdown. The operator performs a manual initiation of steam generator isolation and dump from the remote shutdown area.

Steam generator isolation is performed as a main loop shutdown and main steam isolation. The main loop shutdown trips the main helium circulator and closes the feedwater block valves. The main steam isolation closes the superheat steam valves. The steam generator dump valves open, the steam generator inventory is dumped to a dump tank, and the dump valves reclose. Main steam isolation also commands a reactor trip using the outer control rods. Main loop shutdown also signals for Shutdown Cooling System initiation.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

Environmental conditions or other plant service conditions experienced during DBE No. 8 have no effect on the ability of the PPIS to perform its safety or investment protection functions.

DBE No. 9 Moisture Inleakage With Steam Generator Dump Failure. The initiating event for DBE No. 9 is a small steam generator leak and subsequent small moisture ingress rate. The PPIS moisture monitor detects high primary coolant moisture concentration and commands reactor trip using the outer control rods and commands steam generator isolation and dump. Steam generator isolation is performed as a main loop shutdown and main steam isolation. The main loop shutdown trips the main helium circulator and closes the feedwater block valves. The main steam isolation closes the

superheat steam valves. The steam generator dump valves open, the steam generator inventory is dumped to a dump tank. DBE No. 9 assumes the steam generator dump valves fail to reclose. Main loop shutdown also signals for Shutdown Cooling System initiation.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

Environmental conditions or other plant service conditions experienced during DBE No. 9 have no effect on the ability of the PPIS to perform its safety or investment protection functions.

DBE No. 10 Primary Coolant Leak. The initiating event for DBE No. 10 is a moderate primary coolant leak which causes a rapid depressurization of the primary coolant. When the primary coolant pressure reaches the PPIS low pressure setpoint, the PPIS commands a reactor trip using the outer control rods.

When the primary coolant pressure decreases to the low PPIS setpoint and high reactor building radiation is detected, the PPIS commands the Helium Purification System to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. This pumpdown is assumed in DBE No. 10 to be ineffective because of the size of the primary coolant leak.

When low main steam temperature is reached, the PPIS commands a main steam isolation to prevent low temperature steam from reaching the turbine.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

Environmental conditions or other plant service conditions experienced during DBE No. 10 have no effect on the ability of the PPIS to perform its safety or investment protection functions.

DBE No. 11 Primary Coolant Leak Without HTS and SCS Cooling. The initiating event for DBE No. 11 is a small primary coolant leak and subsequent slow primary coolant depressurization.

When the primary coolant pressure reaches the PPIS low pressure setpoint, the PPIS commands a reactor trip using the outer control rods.

When the primary coolant pressure decreases to the low PPIS setpoint and high reactor building radiation is detected, the PPIS commands the Helium Purification System to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. This DBE also assumes that the main cooling loop is upset 15 h into the DBE.

The PPIS detects trouble with the main cooling loop as a circulator speed to feedwater flow mismatch and commands a main loop shutdown. The main circulator is tripped, the feedwater block valves are closed, and in conjunction with main steam isolation the superheat steam valves are closed. Main steam isolation signals a reactor trip using the outer control rods. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation but in this DBE the SCS fails to start.

The PPIS Special Nuclear Area Instrumentation responds identically to all DBEs as explained for DBE No. 1.

Environmental conditions or other plant service conditions experienced during DBE No. 11 have no effect on the ability of the PPIS to perform its safety or investment protection functions.

2.3.3.3 System Performance Under Safety-Related Design Conditions

Only the Safety Protection Subsystem of the PPIS is classified as "safety-related;" therefore, only the Safety Protection Subsystem performance must be analyzed under Safety-Related Design Conditions (SRDCs). No other system's performance is described even though other systems' designs may also be affected by these SRDCs.

SRDC No. 1 Pressurized Conduction Cooldown. SRDC No. 1 includes loss of offsite power and trip of both turbines. 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 due to loss of power. This loss of primary coolant flow is detected by the PPIS as a high neutron flux to helium mass flow measurement and the PPIS commands a reactor trip using the outer control rods. The Safety Protection Subsystem takes no further action for this SRDC. 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-related" function to perform. Environmental conditions or other plant service conditions experienced during SRDC No. 1 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 2 Pressurized Conduction Cooldown Without Control Rod Trip. SRDC No. 2 includes main loop cooling rampdown with a failure of reactor trip using the outer control rods to take place. This situation is detected by the PPIS 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, the PPIS commands a reactor trip using the reserve shutdown control equipment. Environmental conditions or other plant service conditions experienced during SRDC No. 2 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 3 Pressurized Conduction Cooldown With Control Rod Withdrawal. SRDC No. 3 includes an inadvertent control rod group withdrawal. An inadvertent control rod group withdrawal causes the neutron flux to helium mass flow measurement to exceed the PPIS high setpoint and the PPIS commands a reactor trip using the outer control rods.

Core cooling on the Reactor Cavity Cooling System may cause the primary coolant pressure to exceed the PPIS high pressure setpoint and the PPIS may command a reactor trip using the reserve shutdown control equipment. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods. Environmental conditions or other plant service conditions experienced during SRDC No. 3 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 4 Pressurized Conduction Cooldown With Control Rod Withdrawal. The performance of the Safety Protection Subsystem under SRDC No. 4 is identical to its performance under SRDC No. 3. Environmental conditions or other plant service conditions experienced during SRDC No. 4 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 5 Pressurized Conduction Cooldown with Earthquake. The initiating event for DBE No. 5 is a large earthquake. It is assumed that main loop cooling is eventually lost.

After loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high and the PPIS commands a reactor trip using the outer control rods.

The Safety Protection Subsystem and its "safety-related" auxiliary supporting features are qualified to with a safe shutdown earthquake (SSE) and perform their safety protection functions. No other environmental conditions or other plant service conditions experienced during SRDC No. 5 have

an effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 6 Depressurized Conduction Cooldown with Moderate Moisture Ingress. The initiating event for SRDC No. 6 is a steam generator offset tube rupture and subsequent large moisture ingress rate. The large water ingress rate causes the neutron flux to helium mass flow measurement to exceed the high setpoint and the PPIS commands reactor trip using the outer control rods. The primary coolant pressure also increases and when the high pressure setpoint is reached, the PPIS commands a reactor trip using the reserve shutdown control equipment and commands a main loop shutdown.

SRDC No. 7 Depressurized Conduction Cooldown with Moderate Moisture Ingress. The initiating event for SRDC No. 7 is a steam generator leak and subsequent moisture ingress. PPIS performance for SRDC No. 7 is identical to SRDC No. 6.

SRDC No. 8 Depressurized Conduction Cooldown with Small Moisture Ingress. The initiating event for SRDC No. 8 is a small steam generator leak and subsequent small moisture ingress rate. The moisture ingress causes the primary coolant pressure to slowly increase. When the primary coolant high pressure setpoint is reached, the PPIS commands a reactor trip using the outer control rods and reserve shutdown control equipment and commands main loop shutdown. Environmental conditions or other plant service conditions experienced during SRDC No. 8 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 9 Depressurized Conduction Cooldown with Small Moisture Ingress. The "safety-related" portions of the PPIS have no response to this SRDC since this SRDC assumes an initiating event where the moisture ingress is mitigated by the Investment Protection Subsystem.

SRDC No. 10 Depressurized Condition Cooldown With Moderate Primary Coolant Leak. The initiating event for SRDC No. 10 is a moderate primary coolant leak. A moderate primary coolant leak causes a rapid depressurization of the primary coolant. When the primary coolant pressure reaches the PPIS low pressure setpoint, the PPIS commands a reactor trip using the outer control rods. Environmental conditions or other plant service conditions experienced during SRDC No. 10 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 11 Depressurized Condition Cooldown With Small Primary Coolant Leak. The initiating event for SRDC No. 11 is a small primary coolant leak which causes a slow primary coolant depressurization. The performance of the Safety Protection Subsystem for SRDC No. 11 is identical to SRDC No. 10. Environmental conditions or other plant service conditions experienced during SRDC No. 11 have no effect on the ability of the Safety Protection Subsystem to perform its function.

2.3.4 System Failure Modes and Effects

The Plant Protection and Instrumentation system is a redundant single failure proof system of high reliability. Therefore, failure of a portion does not prevent the ability of the system to correctly respond when challenged. Failures within the system are either immediately alarmed or become apparent during the routine surveillance and testing of the system.

A detailed failure mode and effects analysis will be performed as part of the system design to help assure the system meets applicable availability and reliability criteria.

In general, the Plant Protection and Instrumentation System 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 energy.

In general, portions of the system, where power is required to perform an action and it is potentially detrimental to the plant safety or availability to spuriously initiate such actions (i.e., isolate a main cooling loop), utilize transmission logic (energize to initiate action). This means the logic must "turn on" to initiate protective action and no action occurs on loss of power or loss of signal.

Similarly, portions of the system where plant safety is of paramount concern or spurious actuation is tolerable in regards to plant availability utilize hindrance logic (de-energize to initiate action). This means action occurs on failures such as loss of power or loss of signal.

The failure modes of the Investment and Safety Protection Subsystems are given in Tables 2-7 and 2-8.

2.4 SYSTEM ARRANGEMENT

The Safety Protection Subsystem trips are arranged in modular electronic components with four separate channels. Each of the four MHTGR reactor modules has separate four channel protection systems. The components for each reactor module are associated with the reactor module. The operator interface equipment for the protection subsystems is provided by the Special Nuclear Area Instrumentation Subsystem.

The Special Nuclear Area Instrumentation Subsystem is arranged into modular electronic components. Each of the four 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 Reactor Building Electrical area and remote shutdown area (located in the

Table 2-7
FAILURE MODE AND EFFECTS - INVESTMENT PROTECTION SUBSYSTEM

Trip Subsystem: Reactor Trip - Inner Rods (Ref. Dwg. 029950/0 sheet 2)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Reactor Trip - Outer Rods	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test	
2. Input Channels For Bypass A,B	Control "Set" of Reactor Trip Bypass	Fails in Trip Mode	(Later)	Makes Bypass 1/1	Spurious Channel Trip	Immediate Detection, Makes Bypass 1/1
		Fails in Non-Trip Mode	(Later)	Bypass "Set" Inoperable	Surveillance Test, Comparison with Redundant Channel	Disables Ability to "Set" Bypass, Not of Concern to Plant Safety
3. Electric Power to Logic Div. I,II, III,IV	Provide Power to Logic	Fails Low OR Off	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection

Table 2-7 (Continued)

Trip Subsystem: Reactor Trip - Inner Rods (Ref. Dwg. 029950/0 sheet 2)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. Electric Power to Input Bypass Channel Div. I,II	Provide Power to Bypass Control Channel	Fails Low OR Off	(Later)	Bypass "Set" Inoperable	Surveillance Test	Disables Ability to "Set" Bypass, Immediate Detection
5. Logic Channel A,B,C,D	(Similar to Safety Protection Subsystem - Reactor Trip - Outer Rods)					
5a. Logic Channel Contactor Driver A1,A2,B1,B2, C1,C2,D1,D2	(Similar to Safety Protection Subsystem - Reactor Trip - Outer Rods)					
6. Contactor A1,A2,B1,B2, C1,C2,D1,D2	(Similar to Safety Protection Subsystem - Reactor Trip - Outer Rods)					

Table 2-7 (Continued)

Trip Subsystem: Steam Generator Isolation and Dump (Ref. Dwg. 029950/0 sheet 3)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variables, Convert to Electric Signals, Generate Channel Trip	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Channels	
2. Electric Power to Channel or Logic Div. I,II, III,IV	Provide Power to Instrument Loop and Logic	Fails Low OR Off	(Later)	Makes Trip 2/3	Surveillance Test	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection, Series Valve Prevents Spurious Dump
		Fails in Non-Trip Mode	(Later)	Trip Remains 2/4	Surveillance Test	Reduces System Reliability

Table 2-7 (Continued)

Trip Subsystem: Steam Generator Isolation and Dump (Ref. Dwg. 029950/0 sheet 3)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
		Generates Simultaneous Open and Close Signal	(Later)	Makes Valving 2/2	Surveillance Test	Dump Valve Closing Takes Precedence Over Opening, Concurrent Open and Close Signals Result in Valve Closing
4. Steam Generator Dump Valve A,B,C,D	Implements Dump	Fails in Trip Mode (Valve Opens)	(Later)	Makes Valving 1/1	Spurious Valve Opening	Immediate Detection, Series Valve Prevents Spurious Dump
		Fails in Non-Trip Mode	(Later)	Makes Valving 2/2	Surveillance Test	Reduces Dump Capability to 2/2 on Valves in Operable Dump Line

Table 2-7 (Continued)

Trip Subsystem: Steam Generator Isolation and Dump (Ref. Dwg. 029950/0 sheet 3)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
5. Steam Generator Dump Valve Power Div. I,II, III,IV	Power to Dump Valves (Valves Fail-as-is on Loss of Power)	Fails Low OR Off	(Later)	Makes Valving 2/2	Surveillance Test	Reduces Dump Capability to 2/2 on Valves in Operable Dump Line
Degraded Operation						
6. Logic Channel B,C,D [Plant Operation With One Channel (A) Out of Service]	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Valving 1/2 in Both Dump Lines	Spurious Valve Opening	Immediate Detection, Series Valve Prevents Spurious Dump
		Fails in Non-Trip Mode	(Later)	Makes Valving 2/2	Surveillance Test	Reduces Dump Capability to 2/2 on Valves in One Dump Line

Table 2-7 (Continued)

Trip Subsystem: Steam Generator Isolation and Dump (Ref. Dwg. 029950/0 sheet 3)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)

Notes: 1) Two dump lines (1/2) required to assure dump.
2) Two valves each line (2/2) required to prevent spurious dump on single valve opening.
3) Dump reclosure desirable but not mandatory.
4) Redundant actuator controls employed to allow uninhibited valve operation with one logic channel disabled.

Table 2-7 (Continued)

Trip Subsystem: Primary Coolant Pumpdown (Ref. Dwg. 029950/0 sheet 4)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variables, Convert to Electric Signals, Generate Channel Trip	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Channels	
2. Electric Power to Channel OR Logic Div. I,II, III,IV	Provide Power to Instrument Loop and Logic	Fail Low OR Off	(Later)	Makes Trip 2/3	Surveillance Test	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Output Control 1/1	Spurious Logic Channel Trip	Immediate Detection, Reduces Output Control to 1/1
		Fails in Non-Trip Mode	(Later)	Trip Remains 2/4 with 1/1 Outputs	Surveillance Test	Reduces System Reliability

Table 2-7 (Continued)

Trip Subsystem: Primary Coolant Pumpdown (Ref. Dwg. 029950/0 sheet 4)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. Output Control A,B	Control Contacts in Pumpdown Sequencer Control Circuit (Energize to Trip)	Fails in Trip Mode	(Later)	Spurious Trip	Spurious Trip	Immediate Detection, Initiates Primary Coolant Pumpdown Sequencer
		Fails in Non-Trip Mode	(Later)	Makes Output Control 1/1	Surveillance Test	
5. Electric Power to Outputs Div. I,II	Power Supply for Output Relays	Fails Low OR Off	(Later)	Makes Output 1/1	Surveillance Test	Immediate Detection, Reduces System Reliability

Table 2-7 (Continued)

Trip Subsystem: Shutdown Cooling System Initiation (Ref. Dwg. 029950/0 sheet 5)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Logic Channel A,B	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Spurious Trip	Spurious Trip	Immediate Detection, Initiates SCS Start However SCS Will Not Start Due to SCS Control Logic Unless Main Circulators are Off
		Fails in Non-Trip Mode	(Later)	Makes Output Control 1/1	Surveillance Test	Reduces System Reliability
2. Electric Power to Logic Channel Div. I,II	Power Supply for Output Relays	Fails Low OR Off	(Later)	Makes Output Control 1/1	Surveillance Test	Immediate Detection, Reduces System Reliability

Table 2-7 (Continued)

Trip Subsystem: Shutdown Cooling Heat Exchanger Isolation (Ref. Dwg. 029950/0 sheet 6)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variables, Convert to Electric Signals, Generate Channel Trip	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Channels	
2. Electric Power to Channel OR Logic Div. I,II, III,IV	Provide Power to Instrument Loop and Logic	Fails Low OR Off	(Later)	Makes Trip 2/3	Surveillance Test	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Output Control 1/1	Spurious Logic Channel Trip	Immediate Detection, Reduces Output Control to 1/1
		Fails in Non-Trip Mode	(Later)	Trip Remains 2/4 with 1/1 Outputs	Surveillance Test	Reduces System Reliability

Table 2-7 (Continued)

Trip Subsystem: Shutdown Cooling Heat Exchanger Isolation (Ref. Dwg. 029950/0 sheet 6)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. Output Control A,B	Control Contacts in Output Valve Control (Energize to Trip)	Fails in Trip Mode	(Later)	Spurious Trip	Spurious Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Output Control 1/1	Surveillance Test	
5. Electric Power to Outputs Div. I,II	Power Supply for Output Relays	Fails Low OR Off	(Later)	Makes Output 1/1	Surveillance Test	Immediate Detection, Reduces System Reliability

Table 2-8
FAILURE MODE AND EFFECTS - SAFETY PROTECTION SUBSYSTEM

Trip Subsystem: Reactor Trip - Outer Rods (Ref. Dwg. 029951/0 sheet 2)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variable, Convert to Electric Signal, Generate Channel Trip	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Channels	
2. Electric Power to Channel OR Logic Div. I,II, III,IV	Provide Power to Instrument Loop & Logic	Fail Low OR Off	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Dual Contactor Drivers (De-energize to Trip)	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test	

Table 2-8 (Continued)

Trip Subsystem: Reactor Trip - Outer Rods (Ref. Dwg. 029951/0 sheet 2) (cont)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
3a. Logic Channel Contactor Driver A1,A2,B1,B2, C1,C2,D1,D2	Control Contactor Coil Power (De-energize to Trip	Fails Off	(Later)	Makes Trip 2/3	Spurious Contactor Opening	De-energizes Two Contactors, System Operation Becomes 1/3 on Selected Channels.
		Single Relay Driver Removal	Intentional Driver Removal	Makes Trip 2/3		Immediate Detection, De-energizes One Contactor
		Fails On	(Later)	Makes Trip 3/4 (Output Trip Reduced to 1/1)	Surveillance Test	Keeps Two Contactors Closed, System Operation Becomes 2/4 on Selected Channels

Table 2-8 (Continued)

Trip Subsystem: Reactor Trip - Outer Rods (Ref. Dwg. 029951/0 sheet 2) (cont)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. DC Power Supply (Control Rod Holding Power A,B	Provides DC Hold Power to Control Rod Brakes	Fails On OR Off	(Later)	Plant Availability Reduces to 1 of 1 on Holding Power	Surveillance Test	Not of Concern to Plant Safety
5. Contactor A1,A2,B1,B2, C1,C2,D1,D2	Controls DC Holding Power to Control Rod Brakes (De-energize to Trip)	Fail Open	(Later)	Trip Remains 2/4	Surveillance Test	Immediate Detection
		Fail Closed	(Later)	Makes Trip 3/4 (Output Trip Reduced to 1/1)	Surveillance Test	Keeps One Contactor Closed, System Operation Becomes 2/4 on Selected Channels.

Table 2-8 (Continued)

Trip Subsystem: Reactor Trip - Reserve Shutdown (Ref. Dwg. 029951/0 sheet 3)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variables, Convert to Electric Signal, Generate Trip	Fails in Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Channels	
2. Electric Power to Input Channel OR Logic Div. I,II, III,IV	Provide Power to Instrument Loop & Logic	Fails Low OR Off	(Later)	Makes Trip 2/3	Surveillance Test	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Fuse Link Power Relays (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Output Control 1/1	Spurious Logic Channel Trip	Immediate Detection, Reduces Output Control to 1/1
		Fails in Non-Trip Mode	(Later)	Trip Remains 2/4 with 1/1 on Outputs	Surveillance Test	Reduces System Reliability

Table 2-8 (Continued)

Trip Subsystem: Reactor Trip - Reserve Shutdown (Ref. Dwg. 029951/0 sheet 3) (cont)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. Fuse Link Control A,B	Control Power to Fuse Links (Energize to Trip)	Fails in Trip Mode	(Later)	Spurious Trip	Spurious Trip	Immediate Detection, Releases RSC Material
		Fails in Non-Trip Mode	(Later)	Makes Output Control 1/1	Surveillance Test	
5. DC Power for Fuse Links 125 VDC ESS-A 125 VDC ESS-B	Power Supply for Fuse Links	Fails Low OR Off	(Later)	Makes Output 1/1	Surveillance Test	Immediate Detection, Fuse Link Continuity Monitors Detect Loss of Power

Table 2-8 (Continued)

Trip Subsystem: Main Loop Shutdown (Ref. Dwg. 029951/0 sheet 4)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Input Channel A,B,C,D	Sense Process Variable, Convert to Electric Signal, Generate Trip Signal	Fails In Trip Mode	(Later)	Makes Trip 1/3	Spurious Channel Trip	Immediate Detection
		Fails in Non-Trip Mode	(Later)	Makes Trip 2/3	Surveillance Test, Comparison with Redundant Chanels	
2. Electric Power to Channel OR Logic Div. I,II, III,IV	Provide Power to Instrument Loop and Logic	Fails Low OR Off	(Later)	Makes Trip 2/3	Surveillance Test	Immediate Detection
3. Logic Channel A,B,C,D	Logic to Drive Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Makes Output 1/1	Spurious Logic Channel Trip	Immediate Detection, Reduces Output Control to 1/1
		Fails in Non-Trip Mode	(Later)	Trip Remains 2/3 with 1/1 on Outputs	Surveillance Test	Reduces System Reliability

Table 2-8 (Continued)

Trip Subsystem: Main Loop Shutdown (Ref. Dwg. 029951/0 sheet 4) (cont)

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
4. Output Control A,B	Control Contacts in Output Control (Energize to Trip)	Fails in Trip Mode	(Later)	Spurious Trip	Spurious Trip	Immediate Detection, Results in Main Loop Shutdown
		Fails in Non-Trip Mode	(Later)	Makes Output Control 1/1	Surveillance Test	
5. Electric Power to Outputs Div. I,II	Power Supply for Output Control	Fails Low OR Off	(Later)	Makes Output 1/1	Surveillance Test	Immediate Detection, Reduces System Reliability

Reactor Service Building). These functional components of the Plant Protection and Instrumentation System and their locations are shown in Figure 2-12.

The vessel pressure relief block valve interlock utilizes interlock limit switches located on the valve actuator (gear/cam operated). (Alternately valve shaft mounted limit switches may be used.) The actuator relays are located in the motor control centers associated with the pressure relief block valves.

A list of and specific locations of the Plant Protection and Instrumentation System Equipment is given on Table 2-9.

2.5 INSTRUMENTATION AND CONTROL

[This section not used because this entire system is an Instrumentation and Control System.]

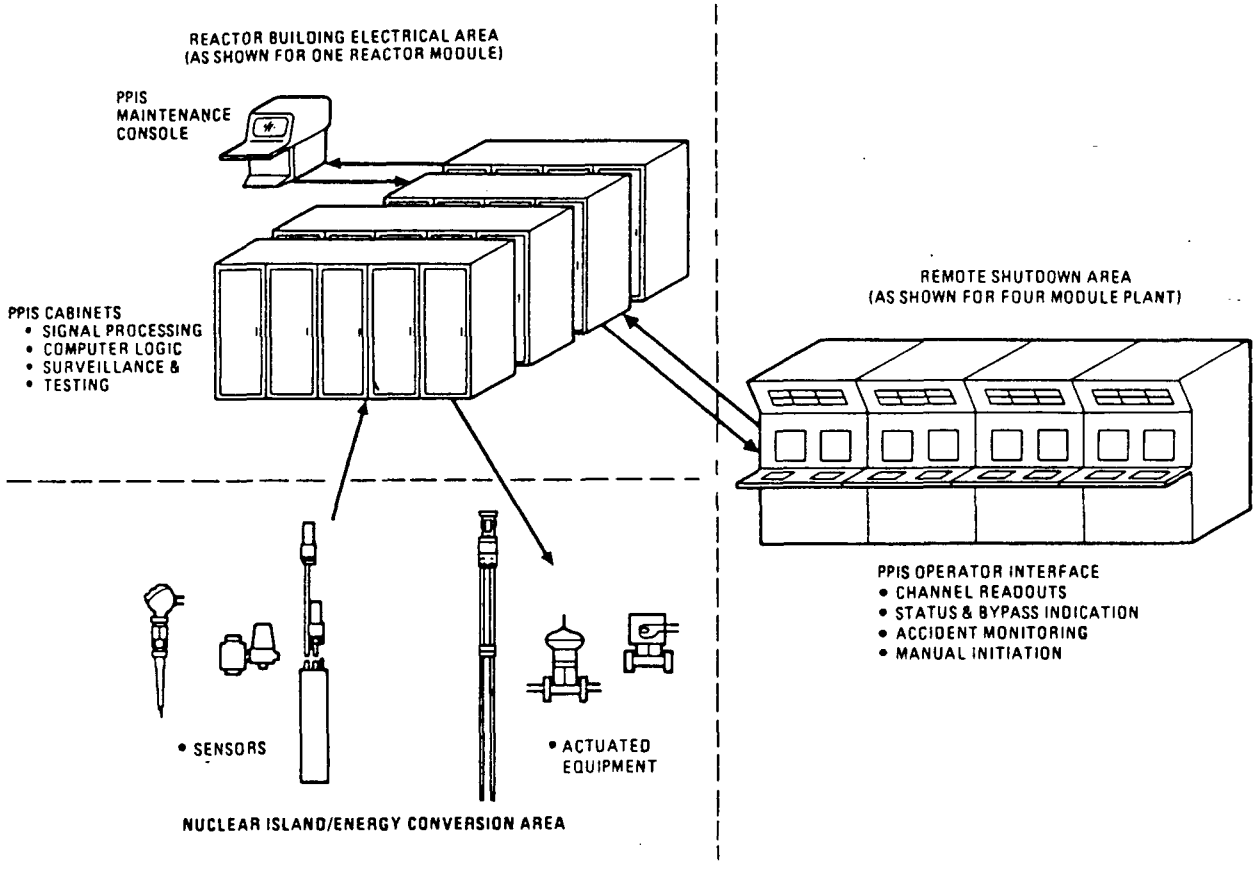


Figure 2-12
PLANT PROTECTION AND INSTRUMENTATION SYSTEM EQUIPMENT ARRANGEMENT

Table 2-9
GENERAL LOCATION OF PLANT PROTECTION AND INSTRUMENTATION SYSTEM EQUIPMENT

Equipment Number[a]	Equipment Name	Quantity Required for MHTGR Plant	Equipment Location
INVESTMENT PROTECTION SUBSYSTEM EQUIPMENT			
I-3216-1/4-A/D	Investment protection cabinet	16	Reactor building electrical area
I-3211-1/5-A/D	Investment protection local instrument cabinet	16 4	Reactor building energy conversion area
S-3201-A/D	Hygrometer module	4	Reactor building
S-3203-A/D	Nonmodule equipment	4 lots	Reactor building
Z-3201-1/4-A/D	Sensors, instruments, and hardware	16 lots	All of above
Z-3202-A/D	O&M hardware and software	4 lots	All of above
SAFETY PROTECTION SUBSYSTEM EQUIPMENT			
I-3202-1/4-A/D	Safety protection cabinets	16	Reactor building elec- area
I-3205-1/4-A/D	Safety protection local instrumentation cabinets	16	Reactor building
Z-3205-1/4-A/D	Sensors, instruments, and hardware	16 lots	All of above
I-3206-A/D	O&M hardware and software	4 lots	All of above
SPECIAL NUCLEAR AREA INSTRUMENTATION EQUIPMENT			
I-3201-A/D	PPIS maintenance consoles	4	Reactor building electrical area
I-3203-A/D	PPIS operator interface	4	Remote shutdown area

Table 2-9 (Continued)

Equipment Number[a]	Equipment Name	Quantity Required for MHTGR Plant	Equipment Location
I-3206/9-A/D	Special nuclear area instrumentation cabinet	16	Reactor building
I-3219-1/2-A/D	Special nuclear area instrumentation field multiplex cabinets	16	Reactor building
I-3220-1/2-A/D	Special nuclear area instrumentation field multiplex cabinets	16	Reactor building
I-3221-1/2-A/D	Special nuclear area instrumentation field multiplex cabinets	8	Reactor service building
I-3222-1/2-A/D	Special nuclear area instrumentation field cabinets	8	Energy conversion area
I-3217-1/2-A/D	Special nuclear area cabinet	8	Reactor building elec- area
Z-3217-1/2-A/D	Instruments and hardware	8 lots	All of above
Z-3218-A/D	O&M hardware and software	4 lots	All of above

[a]Equipment numbering scheme is temporary until a system is established for the MHTGR program.

SECTION 3
SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

3.1 SUBSYSTEM FUNCTIONS

3.1.1 Investment Protection Subsystem Functions

The function of the Investment Protection Subsystem is to provide the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant protective actions required to mitigate the consequences of events, thereby aiding the plant in meeting the investment risk goals.

3.1.2 Safety Protection Subsystem Functions

The function of the Safety Protection Subsystem is to provide the protection system sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant protective actions required to mitigate the consequences of design basis events, protecting the public health and safety.

3.1.3 Special Nuclear Area Subsystem Functions

The function of the Special Nuclear Area Instrumentation Subsystem is to provide preventive features interlocks, and instrumentation that monitors protection systems status and the plant under normal operating and accident conditions.

3.2 SUBSYSTEM DESIGN REQUIREMENTS

3.2.1 Investment Protection Subsystem Design Requirements

3.2.1.1 Subsystem Configuration and Essential Features Requirements

The Investment Protection Subsystem shall be compatible with a configuration whereby reactor modules are located within a Nuclear Island that is physically separated from the remaining portions of the plant. (3200.0302.001)

The Investment Protection Subsystem shall be functionally independent from plant process control systems. (3200.0302.003)

Protective action trip signals shall be transmitted to the NSSS Control Subsystem. (3200.0302.004)

The Investment Protection Subsystem shall consist of five supporting trip subsystems: (3200.0302.005)

1. Reactor trip - inner rods.
2. Steam generator isolation and dump.
3. Shutdown cooling system initiation.
4. Primary coolant pumpdown.
5. Shutdown cooling heat exchanger isolation (and drain).

Each trip subsystem shall consist of four separate (redundant) safety channels and redundant two-out-four coincidence solid-state logic to command initiation of a protective action. (3200.0302.006)

Each input channel shall include the field mounted process variable sensor (e.g., thermocouples, flow transducers, pressure transducers, neutron

detectors, etc.), electronic signal conditioning equipment, and trip setpoint computer to provide a trip signal when the process variable value reaches the trip setpoint. (3200.0302.007)

The two-out-four coincidence logic circuitry shall provide a protective action initiation signal when any two or more separate input channels reach the trip setpoint. (3200.0302.008)

The protective action initiation signal shall be sent to separate and redundant actuation devices. (3200.0302.009)

The boundaries of the Investment Protection Subsystem shall be from, and including, the sensors to the input terminals of the actuation devices. (3200.0302.010)

The Investment Protection Subsystem and its supporting subsystems and interfaces with actuated equipment shall be as shown in the Investment Protection Subsystem Instrument Block Diagram. (Ref. 1, Appendix B.) (3200.0302.011)

Sensor channel parameters shall be as given in Table 2-4. (3200.0302.012)

3.2.1.2 Operational Requirements

The Investment Protection Subsystem shall be designed for an operating life of 40 calendar years.

The Investment Protection Subsystem shall accommodate the performance and transient characteristics of the following additional reactor/turbine-generator combinations: (3200.0302.015)

1. Two reactor modules operating in parallel supplying steam to a single turbine-generator.

2. Four reactor modules operating in parallel supplying steam to a single turbine-generator.

The Investment Protection Subsystem shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in Figures 1-1 through 1-5, Tables 1-1 and 1-2, and in the NSSS Thermal Performance Requirements Report (Ref. 1-2). (3200.0302.016)

The Investment Protection Subsystem shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0302.017)

The design of the Investment Protection Subsystem shall provide for periodic functional testing that will not interfere with normal plant operation. (3200.0302.018)

The Investment Protection Subsystem shall sense process variables to detect abnormal plant conditions and actuate equipment to maintain plant parameters within the plant damage thresholds established for the components listed in Table 1-4, preventing damage to components essential for the protection of plant investment. (3200.0302.021)

The Investment Protection Subsystem shall be designed to contribute towards limiting the total (unrecovered) leakage of helium from the plant systems to less than 10% of plant inventory per year. (3200.0302.022)

3.2.1.3 Structural Requirements

The Investment Protection Subsystem shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0302.100)

The Investment Protection Subsystem shall be designed to meet the OBE seismic load requirements given in Appendix D. (3200.0302.105)

Failures of the Investment Protection Subsystem SSCs shall not cause failure of "safety-related" SSCs. (3200.0302.107)

3.2.1.4 Environmental Requirements

The Investment Protection Subsystem 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 shown in Tables 3-1, 3-2, and 3-3. (3200.0302.120)

The Investment Protection Subsystem design shall provide for individual personnel access to normally accessible areas of the facility for 40 h per week to allow performance of operational, maintenance, and inspection duties while limiting the total average, long-term whole body radiation exposure from all sources to no more than 100 man-rem/year. (3200.0302.121)

The Investment Protection Subsystem shall be designed in conformance with the Occupational Safety and Health Administration Department of Labor, "Occupational Safety and Health Standards, (29CFR1910)." (3200.0302.122)

3.2.1.5 Instrumentation and Control Requirements

Capability to operate the Investment Protection Subsystem shall be provided in the Remote Shutdown Area. (3200.0302.130)

Instrumentation shall be provided to assure control of individual Investment Protection Subsystem equipment items such that their design conditions are not exceeded. (3200.0302.131)

Table 3-1
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

Building/Area	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, electromagnetic inference (EMI), radio-frequency interference (RFI), gas composition, and acoustic.

Table 3-2
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Table 3-3
EXTERNAL ENVIRONMENTAL CONDITIONS
(Design Basis Event)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	Not applicable (defined as "mild" environment not subject to these DBEs)				
Remote Shutdown Area	Not applicable (defined as "mild" environment not subject to these DBEs)				

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the Investment Protection Subsystem. (3200.0302.132)

Human engineering techniques shall be employed in the design of the Investment Protection Subsystem controls and instrumentation/operator interface to enhance the operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD]. (3200.0302.133)

The Investment Protection Subsystem shall be located outside the control room with status indication provided to the NSSS Control Subsystem and Plant Supervisory Control Subsystem. (3200.0302.134)

3.2.1.6 Surveillance and In-Service Inspection Requirements

The design of the Investment Protection Subsystem shall include provisions for surveillance including periodic testing. (3200.0302.140)

3.2.1.7 Availability Assurance Requirements

The Investment Protection Subsystem shall be designed to meet its overall reliability allocation given in Table 3-4. (3200.0302.152)

Design modifications and improvements that allow exceeding the availability in the above availability requirements shall be considered for incorporation in the design, if a 1% increase in the total capital investment produces, at a minimum, a 0.7% improvement in the equivalent availability factor. (3200.0302.153)

3.2.1.8 Maintenance Requirements

The Investment Protection Subsystem shall be designed to meet its planned outage allocation given in Table 3-5. (3200.0302.155)

Table 3-4 RELIABILITY ALLOCATIONS TO INVESTMENT PROTECTION SUBSYSTEM

Subsystem or Feature	Mean Time to Failure (MTTF) of Operation	Probability of Failure to Start or Change	Mean Time to Repair (MTTR)	Equivalent Forced Outage Hours (h/yr)	Other Description
Investment protection	{33,000}[a] h		{65} h	{15.00}	
Moisture monitors		{1 x 10^{-3}}			Probability water ingress is not detected

[a]Numbers in { } are estimated and subject to change.

Table 3-5
SCHEDULED OUTAGE ALLOCATION TO INVESTMENT PROTECTION SUBSYSTEM

	Scheduled Outage Summary (h/yr)			
	Planned	Maintenance	Planned Derating	Allocation
Investment Protection Subsystem	[TBD]	[TBD]	[TBD]	[TBD]
Moisture Monitoring	[TBD]	[TBD]	[TBD]	[TBD]

The Investment Protection Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3200.0302.161)

The Investment Protection Subsystem shall be designed to facilitate hands-on maintenance. (3200.0302.162)

Components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory. (3200.0302.163)

Special maintenance tools shall be provided by the equipment vendor. (3200.0302.164)

3.2.1.9 Safety Requirements

The Investment Protection Subsystem is classified as not "safety-related." (3200.0302.180)

3.2.1.10 Industry Codes and Standards Requirements

The piping, valves, and mechanical components of the moisture monitor/detection equipment shall be designed in accordance with the ASME Boiler and Pressure Vessel Code, Section VIII, Division 1, and ANSI/ASME B31.1.* (3200.0302.200)

The design of the Investment Protection Subsystem shall meet the industry standards given in Table 3-6. (3200.0302.201)

*The actual issue date, edition, addenda, etc., of applicable industry codes and standards shall be specified at the time of plant site selection.

Table 3-6
INDUSTRY CODES AND STANDARDS APPLICABLE TO THE
INVESTMENT PROTECTION SUBSYSTEM DESIGN[a]

ANSI/ASME NQA-1	Quality Assurance Program Requirements for Nuclear Facilities.
DOE NE F2-10	Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1).

[a]The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

3.2.1.11 Quality Assurance Requirements

Items that are not "safety-related" shall come under a Quality Assurance Program which complies with selected basic requirements and appropriate supplements of ANSI/ASME NQA-1 and the four additional supplements from DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawing Lists (NE 02-1.3.5). (3200.0302.210)

3.2.1.12 Construction Requirements

The design of Investment Protection Subsystem shall be based upon parallel construction of the complete plant. Additionally, features shall be included to enable construction and startup in increments of two standard reactor modules and one turbine. (3200.0302.221)

Special installation equipment not commercially available shall be provided by the equipment vendor. (3200.0302.222)

3.2.1.13 Decommissioning Requirements

Until more specific criteria and/or rules are published, NUREG-0586, "Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities," January 1981, shall be used as guidance for anticipating NRC criteria concerning plant decommissioning. (3200.0302.230)

3.2.2 Safety Protection Subsystem

3.2.2.1 Subsystem Configuration and Essential Features Requirements

The Safety Protection Subsystem shall be compatible with a configuration whereby reactor modules are located within a Nuclear Island that is physically separated from the remaining portions of the plant. (3200.0302.301)

The plant control system and major equipment monitoring and protective systems of the Safety Protection Subsystem shall be functionally independent. (3200.0302.303)

Protective action trip signals shall be transmitted to the NSSS Control Subsystem. (3200.0302.304)

The Safety Protection Subsystem shall consist of three supporting trip subsystems: (3200.0302.305)

1. Reactor trip - outer rods.
2. Reactor trip - reserve shutdown.
3. Main loop shutdown/main steam isolation.

Each trip subsystem shall consist of four separate (redundant) safety channels and redundant two-out-four coincidence solid-state logic to command initiation of a protective action. (3200.0302.306)

Each channel shall include the field mounted process variable sensor (e.g., thermocouples, flow transmitters, pressure transducers, neutron detectors, etc.), electronic signal conditioning equipment, and trip setpoint computer to provide a trip signal when the process variable value reaches the trip setpoint. (3200.0302.307)

The two-out-four coincidence logic circuitry shall provide a protective action initiation signal when any two or more separate input channels reach the trip setpoint. (3200.0302.308)

The protective action initiation signal shall be sent to separate and redundant actuation devices. (3200.0302.309)

The boundaries of the Safety Protection Subsystem shall be from, and including, the protection system sensors to the input terminals of the protection system actuation devices. (3200.0302.310)

The Safety Protection Subsystem and its supporting subsystems and interfaces with actuated equipment shall be as shown in the Safety Protection Subsystem Instrument Block Diagram. (Ref. 2, Appendix B.)
(3200.0302.311)

Sensor channel parameters shall be as given in Table 2-3. (3200.0302.312)

3.2.2.2 Operational Requirements

The Safety Protection Subsystem shall be designed for an operating life of 40 calendar years. (3200.0302.321)

The Safety Protection Subsystem shall accommodate the performance and transient characteristics of the following additional reactor/turbine-generator combinations: (3200.0302.323)

1. Two reactor modules operating in parallel supplying steam to a single turbine-generator.

2. Four reactor modules operating in parallel supplying steam to a single turbine-generator.

The Safety Protection Subsystem shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in Figures 1-1 through 1-5, Tables 1-1 and 1-2, and in the NSSS Thermal Performance Requirements Report (Ref. 1-2). (3200.0302.324)

The Safety Protection Subsystem shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3.
(3200.0302.325)

The Safety Protection Subsystem shall sense process variables to detect abnormal plant conditions and actuate equipment to maintain plant parameters within the plant damage thresholds established for the components listed in Table 1-4, preventing damage to components essential for the protection of the public health and safety and plant investment. (3200.0302.326)

The Safety Protection Subsystem shall be designed to contribute towards limiting the total (unrecovered) leakage of helium from the plant systems to less than 10% of plant inventory per year. (3200.0302.327)

3.2.2.3 Structural Requirements

The Safety Protection Subsystem shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0302.500)

The Safety Protection Subsystem shall be designed to meet the OBE load requirements given in Appendix D. (3200.0302.510)

The "safety-related portions of the Safety Protection Subsystem shall remain functional during and after the SSE. The SSE load levels shall be twice the OBE values. (3200.0302.511)

Failures of Safety Protection Subsystem SSCs which are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE. (3200.0302.512)

3.2.2.4 Environmental Requirements

The Safety Protection Subsystem shall be capable of performing their functions before, during, and for an adequate time after being subjected to the

normal, abnormal, and design basis event environmental conditions shown in Tables 3-7, 3-8, and 3-9. (3200.0302.520)

The Safety Protection Subsystem design shall provide for individual personnel access to normally accessible areas of the facility for 40 h per week to allow performance of operational, maintenance, and inspection duties while limiting the total average, long-term whole body radiation exposure from all sources to no more than 100 man-rem/year. (3200.0302.523)

The Safety Protection Subsystem shall be designed in conformance with the Occupational Safety and Health Administration Department of Labor, "Occupational Safety and Health Standards, (29CFR1910)." (3200.0302.525)

3.2.2.5 Instrumentation and Control Requirements

Capability to operate the Safety Protection Subsystem shall be provided in the remote shutdown area. (3200.0302.530)

Instrumentation shall be provided to assure control of Safety Protection Subsystem individual equipment items such that design conditions are not exceeded. (3200.0302.531)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the Safety Protection Subsystem. (3200.0302.532)

Human engineering techniques shall be employed in the design of the Safety Protection Subsystem controls and instrumentation/operator interface to enhance the operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD]. (3200.0302.523)

The Safety Protection Subsystem shall be located outside the control room with status indication provided to the NSSS Control Subsystem and Plant Supervisory Control Subsystem. (3200.0302.534)

Table 3-7
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Table 3-8
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Table 3-9
EXTERNAL ENVIRONMENTAL CONDITIONS
(Design Basis Event)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	Not applicable (defined as "mild" environment not subject to these DBEs)				
Remote Shutdown Area	Not applicable (defined as "mild" environment not subject to these DBEs)				

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

3.2.2.6 Surveillance and In-Service Inspection Requirements

Surveillance is required for the "safety-related" portions of the Safety Protection Subsystem. This surveillance shall meet the criteria of IEEE Standard 603. The surveillance may be done in three parts: (1) every 10 s for pattern recognition, (2) monthly for logic channels function check, and (3) yearly for calibration check. (3200.0302.551)

3.2.2.7 Availability Assurance Requirements

The Safety Protection Subsystem shall be designed to meet its overall reliability allocation given in Table 3-10. (3200.0302.572)

Design modifications and improvements that allow exceeding the availability in the above availability requirements shall be considered for incorporation in the design, if a 1% increase in the total capital investment produces, at a minimum, a 0.7% improvement in the equivalent availability factor. (3200.0302.573)

3.2.2.8 Maintenance Requirements

The Safety Protection Subsystem shall be designed to meet its planned outage allocation given in Table 3-11. (3200.0302.581)

The Safety Protection Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3200.0302.587)

The Safety Protection Subsystem shall be designed to facilitate hands-on maintenance. (3200.0302.588)

Components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory. (3200.0302.591)

Table 3-10 RELIABILITY ALLOCATIONS TO SAFETY PROTECTION SUBSYSTEM

Subsystem or Feature	Mean Time to Failure (MTTF) of Operation	Probability of Failure to Start or Change	Mean Time to Repair (MTTR)	Equivalent Forced Outage Hours (h/yr)	Other Description
Safety protection	{10,000}[a] h		{12} h	{9.00}	

[a]Numbers in { } are estimated and subject to change.

Table 3-11
SCHEDULED OUTAGE ALLOCATION TO SAFETY PROTECTION SUBSYSTEM

	Scheduled Outage Summary (h/yr)			
	Planned Maintenance		Planned Derating	Allocation
Safety Protection Subsystem	[TBD]	[TBD]	[TBD]	[TBD]

Special maintenance tools shall be provided by the equipment vendor. (3200.0302.592)

3.2.2.9 Safety Requirements

The Safety Protection Subsystem equipment classification shall be as specified in the equipment classification list (Table 1-7). (3200.0302.610)

Portions of the Safety Protection Subsystem designated "safety-related" shall be designed to perform their safety function(s) for the Safety-Related Design Conditions (SRDCs) listed in Table 3-12. The transient design conditions for the SRDCs are included in Ref. 1-3. (3200.0302.611)

"Safety-related" portions of the Safety Protection Subsystem shall be located in their entirety within the Nuclear Island. (3200.0302.612)

Compliance with the safety requirements shall be ensured by designing the plant Safety Protection Subsystem to meet the reliability allocations for the Standard MHTGR (Table 1-5) and the safety performance requirements for the Standard MHTGR [TBD]. (3200.0302.613)

The plant shall be designed to meet 10CFR100 requirements without reliance on the control room, its contents, the automated plant control system, the operator, or his/her actions. (3200.0302.614)

The Safety Protection Subsystem shall assure that 10CFR100 radionuclide release limits are not exceeded for the Safety-Related Design Conditions in Table 3-12 by:

1. Sensing plant process variables to detect abnormal plant conditions and actuate reactor trip to control heat generation.

Table 3-12 SAFETY-RELATED DESIGN CONDITIONS

Pressurized Conduction Cooldown
(SRDC No. 1)

Pressurized Conduction Cooldown Without Control Rod Trip
(SRDC No. 2)

Pressurized Conduction Cooldown With Control Rod Withdrawal
(SRDC Nos. 3 and 4)

Pressurized Conduction Cooldown With Earthquake (SSE)
(SRDC No. 5)

Depressurized Conduction Cooldown With Moderate Moisture Ingress
(SRDC Nos. 6 and 7)

Depressurized Conduction Cooldown With Small Moisture Ingress
(SRDC Nos. 8 and 9)

Depressurized Conduction Cooldown With Moderate Primary Coolant Leak
(SRDC No. 10)

Depressurized Conduction Cooldown With Small Primary Coolant Leak
(SRDC No. 11)

2. Sensing plant process variables to detect large steam generator leaks and actuate main loop shutdown to isolate the steam generator to control chemical attack of the fuel. (3200.0302.615)

3.2.2.10 Industry Codes and Standards Requirements

The design of the Safety Protection Subsystem shall meet the industry standards given in Table 3-13. (3200.0302.631)

3.2.2.11 Quality Assurance Requirements

All structures, systems, and components designated "safety-related" shall come under a Quality Assurance Program which fully complies with the requirements of Title 10 Code of Federal Regulations Part 50 (10CFR50), Appendix B. The basic requirements and supplements of ANSI/ASME NQA-1 (as endorsed by Regulatory Guide 1.28, Revision 3) and the four additional supplements from DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawing Lists (NE 03-1.3.5) shall be implemented on activities that affect the quality of such items. Structures, systems, and components are not "safety-related" shall come under a quality assurance program which complies with selected basic requirements and appropriate supplements of NQA-1 and the four additional supplements from F2-10 identified above. (3200.0302.650)

3.2.2.12 Construction Requirements

The design of Safety Protection Subsystem shall be based upon parallel construction of the complete plant. Additionally, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3200.0302.671)

Special installation equipment not commercially available shall be provided by the equipment vendor. (3200.0302.672)

Table 3-13
INDUSTRY CODES AND STANDARDS APPLICABLE TO THE SAFETY PROTECTION SUBSYSTEM DESIGN[a]

ANSI/ASME NQA-1	Quality Assurance Program Requirements for Nuclear Facilities.
DOE NE F2-10	Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1).
ANSI/IEEE Standard 603	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations[b].

[a]The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

[b]IEEE-279 is required by 10CFR50.55a; however, it has been withdrawn by IEEE as IEEE-603 supersedes IEEE-279.

3.2.2.13 Decommissioning Requirements

Until more specific criteria and/or rules are published, NUREG-0586, "Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities," January 1981, shall be used as guidance for anticipating NRC criteria concerning plant decommissioning. (3200.0302.680)

3.2.3 Special Nuclear Area Instrumentation Subsystem

3.2.3.1 Subsystem Configuration and Essential Features Requirements

The Special Nuclear Area Instrumentation Subsystem shall be compatible with a configuration whereby reactor modules are located within a Nuclear Island that is physically separated from the remaining portions of the plant. (3200.0302.750)

The Special Nuclear Area Instrumentation Subsystem shall be functionally independent from plant process control systems. (3200.0302.752)

Fixed audible alarm annunciator points shall be restricted to those critical parameters which can lead to initiation of protective action for major plant components or the loss of electrical production. (3200.0302.753)

The Special Nuclear Area Instrumentation Subsystem shall include monitoring and diagnostics for the Reactor Cavity Cooling System. (3200.0302.754)

The Special Nuclear Area Instrumentation Subsystem shall provide preventive feature interlocks, and instrumentation that monitors protection systems status and the plant under normal operating and accident conditions. (3200.0302.755)

The preventive feature interlock shall be the vessel pressure relief block valve closure interlock. (3200.0302.756)

The vessel pressure relief block valve closure interlock shall consist of redundant electrical sensors, logic, and electrical interlocks to prevent the simultaneous closure of both reactor vessel pressure relief valve trains, thereby preventing the complete bypass of the vessel overpressure protection. (3200.0302.757)

The protection systems information displays shall consist of field mounted multiplex cabinets, redundant digital data highways, and remote shutdown area instrumentation displays to provide the integration of protection system sensor channel readouts, protection system status (e.g., trip, alarm, normal, etc.) indication, and protection system bypass indication. (3200.0302.758)

The Protection System Information Displays shall be configured as an integrated overall display subsystem. (3200.0302.759)

The Vessel Pressure Relief Block Valve Closure Interlock shall be powered from the same electrical power source which powers the vessel system pressure relief block valves. (3200.0302.760)

The Special Nuclear Area Instrumentation Subsystem shall provide source range neutron level and number of control rods withdrawn data to the refueling control console. (3200.0302.761)

3.2.3.2 Operational Requirements

The Special Nuclear Area Instrumentation Subsystem shall be designed for an operating life of 40 calendar years from start of operation. (3200.0302.763)

The Special Nuclear Area Instrument Subsystem shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0302.764)

3.2.3.3 Structural Requirements

The Special Nuclear Area Instrumentation Subsystem shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report (Ref. 1-3) for the number of cycles specified in Table 1-3. (3200.0302.765)

The Special Nuclear Area Instrumentation Subsystem shall be designed to meet the OBE seismic load requirements given in Appendix D. (3200.0302.770)

Failures of the Special Nuclear Area Instrumentation Subsystem SSCs which are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE. (3200.0302.772)

3.2.3.4 Environmental Requirements

The Special Nuclear Area Instrumentation Subsystem shall be capable of performing their functions before, during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions shown in Tables 3-14, 3-15, and 3-16. (3200.0302.790)

The Special Nuclear Area Instrumentation Subsystem design shall provide for individual personnel access to normally accessible areas of the facility for 40 h per week to allow performance of operational, maintenance, and inspection duties while limiting the total average, long-term whole body radiation exposure from all sources to no more than 100 man-rem/year. (3200.0302.791)

Table 3-14
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Turbine Building	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Table 3-15
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Remote Shutdown Area	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Turbine Building	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

Table 3-16
EXTERNAL ENVIRONMENTAL CONDITIONS
(Design Basis Event)

Building/Area	Ranges				
	Temperature [°C (°F)]	Pressure MPa Gauge (psig)	Humidity (%)	Radiation[a]	Other[b]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Service Building (by zone)	Not applicable (defined as "mild" environment not subject to these DBEs)				
Remote Shutdown Area	Not applicable (defined as "mild" environment not subject to these DBEs)				
Turbine Building	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

[a]Radiation data includes type, exposure rate, and integrated dose.

[b]Includes vibration, EMI, RFI, gas composition, and acoustic.

The Special Nuclear Area Instrumentation Subsystem shall be designed in conformance with the Occupational Safety and Health Administration Department of Labor, "Occupational Safety and Health Standards, (29CFR1910)." (3200.0302.792)

3.2.3.5 Instrumentation and Control Requirements

Instrumentation shall be provided to assure control of Special Nuclear Area Instrumentation individual equipment items such that their design conditions are not exceeded. (3200.0302.801)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the Special Nuclear Area Instrumentation Subsystem. (3200.0302.802)

Human engineering techniques shall be employed in the design of the Special Nuclear Area Instrumentation Subsystem controls and instrumentation/operator interface to enhance the operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD]. (3200.0302.803)

The Special Nuclear Area Instrumentation Subsystem shall be located outside the control room with status indication provided to the NSSS Control Subsystem and Plant Supervisory Control Subsystem. (3200.0302.804)

3.2.3.6 Surveillance and In-Service Inspection Requirements

The design of the Special Nuclear Area Instrumentation shall include provisions for surveillance including periodic testing. (3200.0302.850)

3.2.3.7 Availability Assurance Requirements

The Special Nuclear Area Instrumentation Subsystem shall be designed to meet its overall reliability allocation given in Table 3-17. (3200.0302.852)

3.2.3.8 Maintenance Requirements

The Special Nuclear Area Instrumentation Subsystem shall be designed to meet its planned outage allocation given in Table 3-18. (3200.0302.873)

The Special Nuclear Area Instrumentation Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3200.0302.876)

The Special Nuclear Area Instrumentation Subsystem shall be designed to facilitate hands-on maintenance. (3200.0302.877)

Components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory. (3200.0302.882)

Special maintenance tools shall be provided by the equipment vendor. (3200.0302.882)

3.2.3.9 Safety Requirements

The Special Nuclear Area Instrumentation Subsystem shall be as specified in the equipment classification list (Table 1-7). (3200.0302.900)

3.2.3.10 Codes and Standards Requirements

The design of the Special Nuclear Area Instrumentation Subsystem shall meet the industry standards given in Table 3-19. (3200.0302.903)

Table 3-17 RELIABILITY ALLOCATIONS TO THE SPECIAL NUCLEAR AREA INSTRUMENTATION

Subsystem or Feature	Mean Time to Failure (MTTR) of Operation	Probability of Failure to Start or Change	Mean Time to Repair (MTTR)	Equivalent Forced Outage Hours (h/yr)	Other Description
Special nuclear area instrumentation	{89,000}[a] h		{12} h	{1.00}	

[a]Numbers in { } are estimated and subject to change.

Table 3-18
SCHEDULED OUTAGE ALLOCATION TO SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM

	Scheduled Outage Summary (h/yr)			
	Planned	Maintenance	Planned Derating	Allocation
Special Nuclear Area Instrumentation	[TBD]	[TBD]	[TBD]	[TBD]

Table 3-19
INDUSTRY CODES AND STANDARDS APPLICABLE TO THE SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN[a]

ANSI/ASME NQA-1	Quality Assurance Program Requirements for Nuclear Facilities.
DOE NE F2-10	Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1).
ANSI/IEEE Standard 603 (Section 5.8)	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

[a]The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

3.2.3.11 Quality Assurance Requirements

Items that are not "safety-related" shall come under a Quality Assurance Program which complies with selected basic requirements and appropriate supplements of ANSI/ASME NQA-1 and the four additional supplements from DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawing Lists (NE 03-1.3.5). (3200.0302.910)

3.2.3.12 Construction Requirements

The design of Special Nuclear Area Instrumentation Subsystem shall be based upon parallel construction of the complete plant. Additionally, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3200.0302.921)

Special installation equipment not commercially available shall be provided by the equipment vendor. (3200.0302.925)

3.2.3.13 Decommissioning Requirements

Until more specific criteria and/or rules are published, NUREG-0586, "Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities," January 1981, shall be used as guidance for anticipating NRC criteria concerning plant decommissioning. (3200.0302.930)

SECTION 4
SYSTEM AND SUBSYSTEM INTERFACES

4.1 INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interface requirements imposed on other systems are presented in Table 4-1. These are given on a per reactor module basis as the Plant Protection and Instrumentation System is independent for each reactor module.

4.2 SUBSYSTEM BOUNDARY DEFINITION

The scope of the protection subsystems starts with and includes the process sensors through the input of the actuated equipment. Generally the boundaries of the protection subsystem include the sensor installation.

Output data from the Plant Protection and Instrumention System is transmitted to the NSSS Control Subsystem and Plant Supervisory Control Subsystem. Each of the protection subsystems, along with other plant systems, provide data inputs to the Special Nuclear Area Instrumentation Subsystem.

Each of the subsystems within the Plant Protection and Instrumentation System Communicates with each other. The intrasystem boundaries are at the output terminations of the instrumentation cabinets of the subsystem generating the signal.

Table 4-1
PLANT PROTECTION AND INSTRUMENTATION SYSTEM INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS
(Given on a per reactor module basis)

4.1.1 Identification of Interfaces Between Systems

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.1 Reactor System (1000)			
Neutron Control Subsystem (1012)	Provide control rod drive mechanisms to act as actuated equipment for the Reactor Trip Subsystem, including accepting separate and redundant signals to directly trip the mechanisms.	Function only.	Quantity: One control rod mechanism for each control rod. Maximum response time: {25}[a] s for full insertion. Diverse reserve shutdown control equipment response time: {40} s for full insertion. (3200.0401.001)
4.1.1.2 Heat Transport System (2100)			
Main Circulator Subsystem (2101)	Redundant electric signals.	Main circulator control cabinet.	Accept separate and redundant electric signals and redundantly trip the main circulator within {1.0} s. (3200.0401.040)
4.1.1.3 Shutdown Cooling System (5700)			
Shutdown Cooling Heat Removal Control Subsystem (5703)	Redundant electric signals.	Control cabinet.	Accept redundant electric signals and initiate shutdown cooling. (3200.0401.080)
Shutdown Cooling Water Subsystem (5704)	Redundant electric signals.	Control cabinet.	Accept separate and redundant electric signals and redundantly isolate and drain heat exchanger within [TBD] s. (3200.0401.082)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.4 Reactor Cavity Cooling System (5600)			
	Redundant electric signals.	Control cabinets.	Provide status and performance instrumentation signals including inlet and outlet temperatures and flows. (3200.0401.070)
4.1.1.5 Vessel System (1100)			
Pressure Relief Subsystem (1105)	Redundant electric signals (from the vessel pressure relief block valve closure lock to prevent the closure of one block valve if the other block valve is not fully open).	Relief valve block valve control cabinet.	Accept redundant electric signals and prevent relief valve block closure. (3200.0401.020)
4.1.1.6 Plant Protection and Instrumentation System (3200)			
Interfaces within this system are addressed at the subsystem level.			
4.1.1.7 Fuel Handling and Storage System (3400)			
No requirements imposed on this system.			
4.1.1.8 Reactor Service Group (2000)			
Helium Purification Subsystem (2023)	Redundant electric signals.	Helium purification control cabinet.	Accept separate and redundant electric signals and initiate primary coolant pumpdown. (3200.0401.030)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.9 Power Conversion Group (5000)			
Feedwater and Condensate System (5002)	Redundant electric signals.	Control cabinet.	Accept separate and redundant electric signals and redundantly shut off feedwater within {5} s. (3200.0401.060)
Main and Bypass Steam System (5004)	Redundant electric signals.	Control cabinet.	Accept separate and redundant electric signals and redundantly isolate main steam within {10} s. (3200.0401.065)
	Electric signals (superheater outlet valve closed position for use in operating bypass in main loop shutdown/main steam isolation).	Control cabinet.	Provide redundant (two per valve) superheater outlet valve closed position signals. (3200.0401.065)
Steam and Water Dump System (5013)	Redundant electric signals.	Control cabinet.	Accept separate and redundant electric signals and redundantly dump the steam generator with a four-valve matrix. Maximum valve response times are opening time {5} s; closing time {5} s. (3200.0401.068)
4.1.1.10 Heat Rejection Group (5200)			
No requirements imposed on this group.			

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.11 Plant Control, Data, and Instrumentation System (3700)			
NSSS Control Subsystem (3701)	Electric signals (indicates reactor trip inner rods, outer rods, reserve shutdown, main loop shutdown, main steam isolation, SG isolation and dump, SCS initiation, and primary pressure pumpdown).	NSSS control cabinet.	Accept electric signals and initiate control adjustments in response to trips. (3200.0401.050)
Data Management Subsystem (3735)	Electric signals representing data for use by operator.	Control cabinet.	Accept electric signals and transmit data and alarms to Plant Supervisory Control Subsystem. (3200.0401.052)
4.1.1.12 Electrical Group (9200)			
Essential Uninterruptible Power Supply System (9205)	Electric feeders.	Circuit breaker panel(s).	Provide {112} circuits. (3200.0401.100)
4.1.1.13 Miscellaneous Control and Instrumentation Group (3000)			
Radiation Monitoring System (3003)	Redundant electric signals (input to primary coolant pumpdown).	Control cabinet.	Provide four redundant reactor building radiation signals. (3200.0401.045)
4.1.1.14 Plant Service Group (9000)			
No requirements imposed on this group.			

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.15 Buildings, Structures, and Building Service Group (7000)			
Reactor Building (7001)	Equipment space and support.	Floor space.	Provide space and mounting for {24} equipment cabinets and one hygrometer module. (3200.0401.090)
Reactor Service Building (7002)	Equipment space and support.	Floor space.	Provide space and mounting for {4} equipment cabinets. (3200.0401.091)
Turbine Building (7001)	Equipment space and support.	Floor space.	Provide space and mounting for {4} equipment cabinets. (3200.0401.092)

SECTION 5
SYSTEM CONSTRUCTION

The construction of the Plant Protection and Instrumentation System will be planned and scheduled so that its subsystems and components will fit up properly with all its interfacing systems. This will require a detailed plan for installing the proper subsystem components at the proper time in the plant construction sequence.

5.1 PACKAGING AND SHIPPING

The design of the Plant Protection and Instrumentation System includes consideration for special packaging including as necessary handling fixtures for the packages and for the components to be inserted and removed from the packages. The packages and components are designed for handling, storage, and movement both horizontally and vertically with considerations for impact loading and shock absorbers due to inadvertent truck accidents. Shipping fixtures, attachments, welded lifting lugs, slings, etc., where provided on large items, receive the same design review, including materials and process approval prior to fabrication, as is applied to the component itself. The design of the initial shipping/handling fixtures on large items will be coordinated with the plant constructor to ensure that they are compatible with his lifting equipment which is not necessarily the plant equipment to be used after construction completion.

5.2 HANDLING AT DELIVERY

A specification/procedure will be written to describe the procedure for handling the components of the Plant Protection and Instrumentation System from the delivery point to the storage or installation location, including appropriate inspections at specified intervals. These instructions shall be followed.

5.3 RECEIVING INSPECTION

The equipment as delivered will have been thoroughly shop tested and inspected during fabrication.

Thorough receiving inspection shall be made for all of the Plant Protection and Instrumentation System. Inspection includes damage assessment, accounting for all items with or without tags, determining if any protective packaging is deteriorating, proper positioning, QA checks, etc. Such inspections shall be planned and documented on a receiving inspection plan which shall be retained in the quality assurance record system for the plant.

5.4 STORAGE

All Plant Protection and Instrumentation System equipment/components shall be stored in closed environmentally controlled buildings out of the weather. All components regardless of location shall be inspected weekly in accordance with the specification/procedure described under Section 5.2.

5.5 ACCESS

Access to the reactor building is required for Plant Protection and Instrumentation Subsystem components located in the reactor building. Access requirements in other buildings and lifting equipment requirements are [TBD].

5.6 INSTALLATION AND/OR FIELD FABRICATION

The installation of the Plant Protection and Instrumentation System will be described in several specifications/procedures. In addition to handling and inspections (see Sections 5.2 and 5.3), procedures are required for

connecting piping, electrical power and instrumentation leads to the components of the Plant Protection and Instrumentation System. These connections are preferably prefabricated with connectors, flanges, etc., to make for easy installation with a minimum of field fabrication.

5.7 CONSTRUCTION TESTING

A construction test procedure is required for the Plant Protection and Instrumentation System to describe visual and mechanical inspection, cleaning, pressure/leak testing, electrical continuity, insulation integrity, phase sequence, operability of moving equipment, etc. The procedure includes specific pressure levels, voltage levels, and boundaries for application of these test levels with specific precautions (such as double block and bleed valves) to prevent leakage or misapplication during cleaning and testing. If construction cleaning is required of components to be installed in the reactor vessel and to be operated in primary coolant helium, such cleaning shall conform to GA Reference Specification RC-2-2. The results of construction testing will be reported for a record of test performance and results.

5.8 AS-BUILT DRAWINGS

Permanent changes will be recorded for the master reproducible drawings of the Plant Protection and Instrumentation System for record purposes. All changes will be subject to the normal design review process for approval or restoration to the original design configuration.

SECTION 6
SYSTEM OPERATION

6.1 SYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

6.1.1 System Limitations and Setpoints

Trip setpoints are conservatively established to assure that component damage limits are not reached. Figure 6-1 illustrates the relationship between trip setpoints and damage limits. The limiting protection system settings (allowable values) conservatively bound component damage thresholds so that if the limiting protection 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 SRDC and DBE transient analysis is performed at the "analysis trip level."

The operating limits (limiting protection system settings) and setpoints (actual protection system settings) for the Plant Protection and Instrumentation System are shown in Table 6-1.

6.1.2 Precautions

Design features are included to assist the operator in verifying that a system degree of redundancy of at least one is always maintained. For example, whenever any protection system component is bypassed, such that a protection channel is inoperable, a status indication of the protection system bypass is presented in the main control room. Whenever one protection channel of the two-out-of-four logic is disconnected or bypassed, the

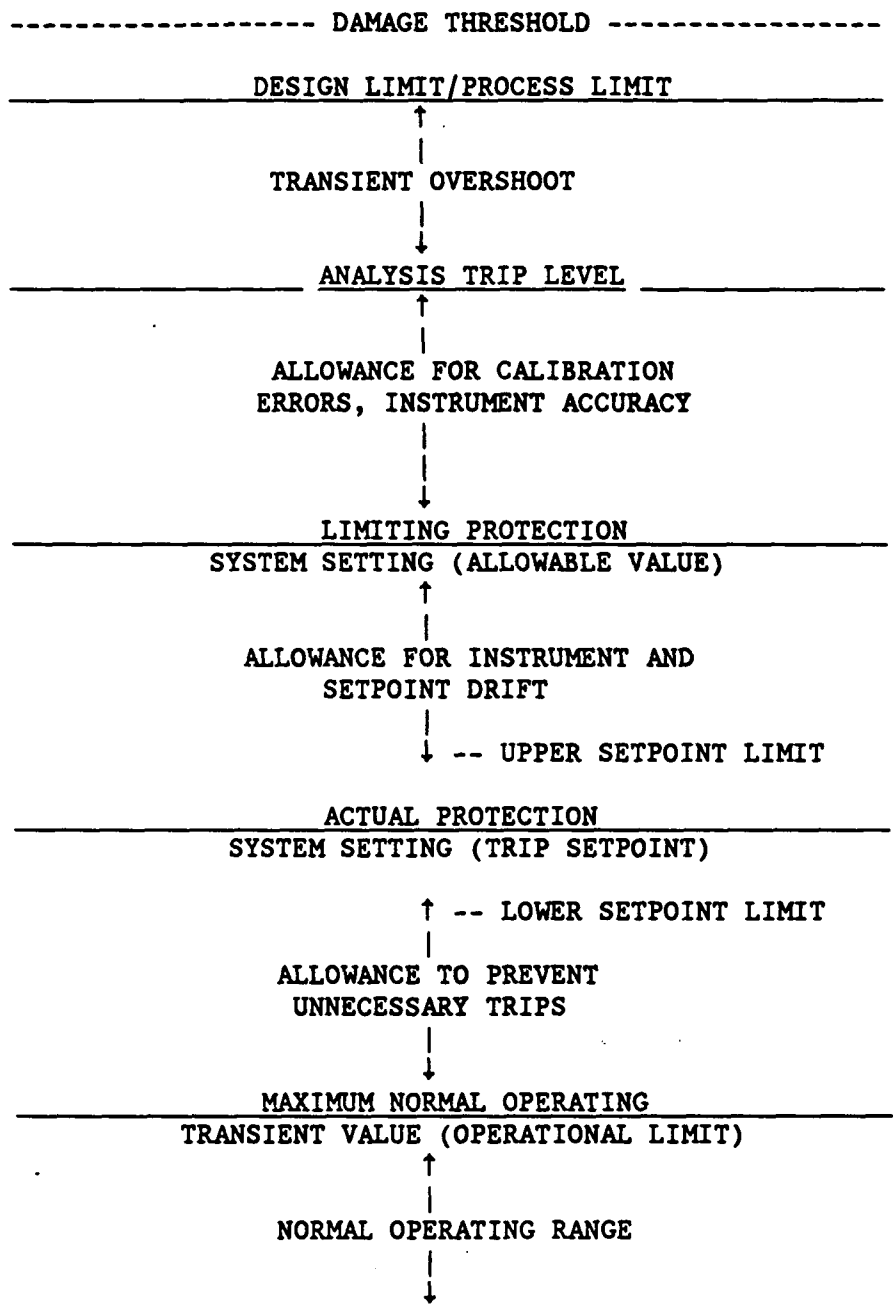


Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS AND COMPONENT DAMAGE LIMITS

Table 6-1 OPERATING LIMITS AND SETPOINTS FOR THE PLANT PROTECTION AND INSTRUMENTATION SYSTEM

Parameter	Operating Limit (Limiting Protection System Setting)	(Actual Protection System Setting)	Remarks
REACTOR TRIP			
Neutron flux to helium mass flow ratio	[TBD]	{1.4}[a]	
Neutron flux	[TBD]	{10%}	
Steam generator helium inlet temperature °C (°F)	[TBD]	{746 (1375)}	
Primary coolant pressure, MPa absolute (psia)	[TBD]	high {6.978 (1015)} low {5.757 (835)}	
Primary coolant moisture concentration, ppmv	[TBD]	{1000}	
RESERVE SHUTDOWN SYSTEM			
Reactor power to circulator speed ratio	[TBD]	{1.8}	
Primary coolant pressure, MPa absolute (psia)	[TBD]	{6.978 (1015)}	
MAIN LOOP (HTS) SHUTDOWN/ MAIN STEAM ISOLATION			
Circulator speed (programmed by feedwater flow)	[TBD]	{±1144 rpm}	

Table 6-1 (Continued)

Parameter	Operating Limit (Limiting Protection System Setting)	(Actual Protection System Setting)	Remarks
Primary coolant pressure MPa (psia)	[TBD]	{6.978 (1015)}	
Main steam temperature, °C (°F)	[TBD]	≥{393 (740)} ≤{427 (800)}	
STEAM GENERATOR ISOLATION AND DUMP			
Primary coolant moisture concentration, ppmv	[TBD]	{1000}	
Superheater steam pressure to primary coolant pressure (for steam generator dump terminate), kPa differential (psid)	[TBD]	{517 (75)}	
PRIMARY COOLANT PRESSURE PUMPDOWN (WITH HELIUM PURIFICATION SYSTEM)			
Primary coolant pressure, MPa absolute (psia)	[TBD]	{5.585 (810)}	
Reactor building radiation (mr/h)	[TBD]	[TBD]	

Table 6-1 (Continued)

Parameter	Operating Limit (Limiting Protection System Setting)	(Actual Protection System Setting)	Remarks
SHUTDOWN COOLING HEAT EXCHANGER ISOLATION			
Shutdown cooling system leak	[TBD]	[TBD]	

(a){ } = Numbers are estimated and subject to change.

remainder of the system reverts to two-out-of-three logic and maintains a degree of redundancy of one. Whenever a one-out-of-two protection system actuation device is disconnected or bypassed, the time of inoperability must be kept to a minimum and must be within acceptable reliability analysis constraints as specified in Section 1.2.7.

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

6.2 PREOPERATIONAL CHECKOUT

6.2.1 Initial Preoperational Checkout

After completion of the construction testing (see Section 5.7), a series of initial preoperational tests will be performed to verify the proper operation of the Plant Protection and Instrumentation System, its subsystems, and components prior to nuclear fuel loading and power operation.

Initial preoperational test procedures will be written to demonstrate operational and instrumentation capability for at least the following:

1. Reactor Trip - Outer Control Rods
2. Reactor Trip - Inner Control Rods
3. Reactor Trip - Reserve Shutdown
4. Main Loop Shutdown/Main Steam Isolation
5. Steam Generator Isolation and Dump
6. Primary Coolant Pressure Pumpdown
7. Shutdown Cooling System Initiation
8. Shutdown Cooling Heat Exchanger Isolation
9. Moisture Monitor/Detection Equipment

10. Vessel Pressure Relief Block Valve Closure Interlock
11. Protection System Information Displays

6.2.2 Routine Preoperational Checkout

The following prerequisites are required for routine preoperational checkout:

1. Remote Shutdown Area operable.
2. Reactor Building Instrument Equipment Area operable.
3. Uninterruptible power sources operable.
4. Plant Control, Data and Instrumentaion System operable.
5. Neutron Control Subsystem operable.
6. Vessel Pressure Relief Subsystem operable.
7. Heat Transport System Instrumentation operable.
8. Feedwater and Condensate System Instrumentation operable.
9. Main Steam and Turbine Bypass Instrumentation operable.
10. Shutdown Cooling System Instrumentation operable.

Checkout Procedure

In general, the following steps are governed by the Plant Technical Specifications. Some steps may be bypassed during any specific plant startup provided that the system is still current in accordance with the Plant Technical Specifications (for example, sensor calibration or actuation device exercising need not be performed upon each startup if the Technical Specification requirement is yearly calibration):

1. Check that any test instrumentation utilized has a current calibration.

2. Energize system, reset trips.

3. Calibrate sensors, record as-found and as-left data.

4. Calibrate readout instruments.

5. Confirm input channel operability.

6. Confirm channel trip operability, reset trip.

7. Check trip setpoints, record as-found as-left data, reset trips.

8. Check automatic logic test circuitry, run diagnostics programs.

9. Check all permutations and combinations of logic including interlocks, inhibits and bypasses, monitor automatic testing as provided, reset system as required.

10. Monitor outputs to actuators.

11. Exercise actuator or perform partial valve stroke tests (where such provisions are provided).

    The test sequence shall be complete, realistic and have sufficient overlap to assure all circuitry is tested and operable. The test sequence should also be chosen to minimize the wear and tear on electromechanical portions of the system (i.e., valves, contactors).

12. Check that all signals, actuators, etc., are returned to their correct positions and confirm that all redundant portions of the system are operable.

13. Repeat above applicable portions for other portions of the system/subsystem until all portions are tested.

6.3 STARTUP/SHUTDOWN

6.3.1 Startup to 25% Steam Flow

6.3.1.1 Prerequisites

The following prerequisites are required for plant startup:

1. Routine preoperational checkout performed.
2. System current per Plant Technical Specifications.
3. Electrical systems operating.
4. Heat Transport System operating.
5. Reactor Cavity Cooling System operating.
6. Heat Rejection Group operating.
7. Power Conversion Group operating.
8. Vessel System operating.
9. Shutdown Cooling System operable.
10. Reactor System operable.
11. Plant Control, Data and Instrumentation System operating.

6.3.1.2 Procedure

The startup procedure includes:

1. Reset Reactor Trip circuitry.

2. Reset any First-In Trip Annunciators.

3. Withdraw control rods in prescribed sequences as determined by Neutron Control Subsystem, equipment heatup rates, etc.

4. Ensure instrumentation readings increase appropriately throughout plant startup on all redundant channels.

6.3.2 Shutdown from 25% Steam Flow

The shutdown procedure includes:

1. Inserting control rods in prescribed sequences as determined by the Neutron Control Subsystem at a low power level.

2. Monitoring plant safety status periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

6.4 NORMAL OPERATION

The procedures for normal operation are as follows:

Periodically monitor systems to ensure that all portions are operating normally.

Perform periodic surveillance, testing, and calibration in accordance with the plant technical specifications and using the actual protection system settings and limiting protection system settings as given in Section 6.1.

6.5 REFUELING

Monitor plant status periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

The reactor trip contactors are to remain open during plant shutdowns (exclusive of any testing that may be performed). Control rod/drive mechanism removal for refueling, which requires powering of the control rod drive brake and motor to facilitate removal, can be accomplished on

a one-at-a-time basis using plug-in temporary controls provided on the reactor refueling floor as part of the Neutron Control Subsystem.

6.6 SHUTDOWN

A plant shutdown can be initiated either with the normal station controls (planned shutdown) or automatically by the Protection Subsystems (emergency shutdown). During plant shutdown the plant status must be monitored periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

Shutdown of the entire Plant Protection and Instrumentation System to perform maintenance is generally not required due to the redundancy of the channels. To the extent possible, maintenance and partial shutdown of the Plant Protection and Instrumentation System should be done during scheduled plant shutdowns. (Inadvertent shutdowns of redundant portions of the Plant Protection and Instrumentation System can result in a plant trip due to the fail-safe characteristics of the design.)

6.6.1 Automatic Plant Shutdowns

The Protection Subsystems automatically initiate reactor trips and shutdown of appropriate equipment upon detection of abnormal plant conditions. All automatic trips to the extent possible are preceded by early warning alarms. The operator should take immediate corrective action, where possible, to prevent a plant trip. This is not possible in all circumstances due to the nature of the various design basis events. Following automatic protective action, the following actions should be taken:

1. Verify that redundant portions of the Protection Subsystems have tripped. (Note any abnormal or suspicious Plant Protection and Instrumentation System behavior for future review.)

2. Verify that the protective actions derived have occurred or are occurring (i.e., are the control rods actually inserted and neutron flux decreasing upon a reactor trip). Manually initiate any action that has not occurred.

3. Ensure that reactivity, core cooling and fission product containment are satisfactory and under control.

4. Note the cause of the event and the need for additional actions.

5. Continue the plant shutdown per the plant emergency procedures.

6. Plant restart shall not be initiated until the cause for the trip has been positively established, necessary corrections, repairs have been performed, and it has been ascertained that the Plant Protection and Instrumentation System performance was per design.

6.6.2 Plant Protection and Instrumentation System Shutdown

Shutdown of the entire Plant Protection and Instrumentation System is not recommended and generally not required due to the redundancy within the system. Shutdown may in some situations be governed by the Plant Technical Specifications. Ensure the plant is shut down prior to shutting off electrical power in redundant load groups (loss of electrical power in more than one of a redundant group can cause a system trip.)

6.7 ABNORMAL OPERATION

Abnormal operation of the Plant Protection and Instrumentation System is limited to plant operation with the systems operating in a degraded mode (failed or inoperable equipment). Generally operation in a degraded mode is governed by the Plant Technical Specifications.

The Plant Protection and Instrumentation System is configured so as to not adversely affect plant safety or plant availability in conjunction with a single failure. Therefore, a single failed component or input channel will not cause an unwanted (spurious) system trip nor prevent a required one.

The cause for spurious channel trips should be determined, corrected, and the channel reset in a timely fashion. Continued plant operation with an input channel in a trip condition is undesirable because a second channel trip will result in an unwanted system trip. However, for Technical Specification purposes, a tripped channel is generally defined as operable and this may be employed in some instances to delay plant shutdown for a more appropriate time (i.e., the weekend, to receive spare parts, etc.). The protection system may usually be run in a degraded condition as long as a degree of redundancy of one is maintained.

Continued plant operation with the Plant Protection and Instrumentation System in a degraded mode can interfere with scheduled periodic surveillance testing.

Various provisions also exist in the design to allow, through reconnection, the use of additional spare sensors to regain operation in the event of selected sensor failure.

6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES

6.8.1 Casualty Events

Casualty events for the Plant Protection and Instrumentation System include the following:

1. Spurious trip (safe failure) of a single sensor channel.

2. Failure of a sensor.

3. Failure of component/module.

4. Failure of test units.

5. Electrical overload or loss of electrical power.

6. Detection of degraded performance (out of tolerance calibration/ trip setting).

7. Detection of an unsafe failure (detected during surveillance monitoring or testing).

6.8.1.1 Logic or Output Channel Failures

Logic or output actuating channel failures include:

1. Spurious trip (safe failures) of a single logic or output channel.

2. Failure of a component/module.

3. Failure of test units.

4. Electrical overload or loss of electrical power.

5. Detection of an unsafe failure (detected during surveillance testing).

6.8.1.2 System Failures

System failure generally involve common cause failure or multiple single failures. System failures include:

1. Spurious trips resulting in unwanted protection actions.

2. Failure of the system to perform upon command.

6.8.2 Design Features to Mitigate Effects of Casualty Events

Safe failures, those tending toward system trips, generally are self-revealing. Appropriate monitoring instrumentation and alarming is provided to immediately alert the operator to single channel trips and abnormal sensor deviation. Additionally, the problem area is identified via status indications, indicating lights and other diagnostic tools. Unsafe failures are addressed by the periodic surveillance and testing circuitry.

6.8.2.1 Input Sensing Channels

Input channels to the Protection Subsystems as well as data utilized in the computer-based Special Nuclear Area Instrumentation is automatically validated by comparison with redundant and/or diverse data channels.

Failure to validate data is alarmed and the data in question indicated to the operator. The computer-based instrumentation includes its own built-in self-testing diagnostics.

Loss of electrical power is alarmed.

Appropriate circuit protection is provided, on a coordinated basis, to minimize the circuitry disabled in the event of an electrical short or

overload. Circuit breakers or fuses with blown fuse indicators are provided.

The built-in periodic surveillance and testing circuitry is primarily directed towards detecting unsafe failures.

Various provisions also exist in the design to allow, through reconnection, the use of additional spare sensors to regain operation in the event of selected sensor failure.

6.8.2.2 Logic and Output Channels

Appropriate monitoring instrumentation and alarming is provided to immediately alert the operator to single channel trips. The problem area is identified by status indication indicating lights and other diagnostic tools.

Loss of electrical power is alarmed.

Appropriate electrical circuit protection is provided, on a coordinated basis, to minimize the circuitry disabled in the event of an electrical short or overload. Electrical circuit trip indicators are provided.

The built-in periodic surveillance and testing circuitry is primarily directed towards detecting unsafe failures.

This testing utilizes a combination of manually initiated testing and automatic logic testing. Detection of unsafe failures is readily apparent by built-in monitoring instrumentation or in the case of automatic testing by annunciation.

A key element included in this system is an analysis of the system behavior upon detection of a failed component to provide a design that will not yield an unacceptable plant availability.

Unlikely type failures (i.e., hot shorts) in the one-of-two transmission circuitry can cause a spurious system trip (defined as a safe failure), however this is either acceptable for the system or has been minimized to maintain an acceptable plant availability.

6.8.2.3 System Considerations

The Plant Protection and Instrumentation System is designed to meet the single failure criteria. Seismically and environmentally caused common cause failures are prevented by design and qualification to all conditions (normal, abnormal, and design basis events) during which operation is required.

The Plant Protection and Instrumentation System is a redundant system configured so that a single failure, particularly those related to an input measurement channel, will generally allow continued operation in a degraded mode. A single (safe) failure generally does not cause an inadvertent system trip and the system will still perform in the event of a single unsafe failure due to channel redundancy.

The Reactor Trip is designed with deenergize to trip logic so that loss of power or circuit interruptions tend towards a system trip. The bulk of the Plant Protection and Instrumentation System is designed with energize to trip logic where power is required to perform a protective action. Some of the actuation circuitry is a one-out-of-two configuration, however this is utilized on portions of the system where inadvertent actuation is acceptable and has been minimized to maintain acceptable plant availability.

Manual initiation is provided for all protective actions and the manual initiation is implemented to reduce the number of discrete operator manipulations and utilize a minimum of equipment.

Other plant provisions for addressing failure of a protection system are beyond the design scope of the Plant Protection and Instrumentation System.

6.8.3 Recovery Procedures

All recovery procedures need to be done in accordance with the Plant Technical Specifications.

6.8.3.1 Recovery from Sensor Channel Failures

Recovery procedures generally involve repair and reset of the sensor channel. In instances where repair cannot be implemented during the time allowed by the Plant Technical Specifications, an orderly plant shutdown is initiated.

6.8.3.2 Recovery from Logic and Output Channel Failures

Recovery procedures for logic and output channel failures is similar to that of Section 6.8.3.1.

6.8.3.3 Recovery from System Failures

Recovery from unwanted system trips involves first assuring safe plant operating status. The affected subsystems may then be restarted subsequent to failure diagnosis, repair, and preoperational checkout.

Failure of a protection system to perform upon command is unlikely. Manual initiation may be employed and efforts concentrate upon assuring that a safe plant status is maintained. The information and data systems are employed to assist in locating problem areas. On a longer term basis failure diagnosis, repair, and preoperational checkout is required.

SECTION 7
SYSTEM MAINTENANCE

7.1 MAINTENANCE APPROACH

The general Plant Protection and Instrumentation System maintenance approach is based upon utilizing a modular instrumentation system construction, standardizing each module to the extent practical, and minimizing the diversity of spare parts inventory. Additionally, maintenance involves disabling a relatively small portion of the system/subsystem, thereby reducing the amount of checkout/testing required following repair.

Due to the system configuration and redundancy provided, it is possible to perform a considerable amount of maintenance and repair with the plant operating; however, it is preferred that, where possible, routine maintenance be performed during plant outages scheduled for maintenance of other systems or reactor module refueling. The system design considers maintenance activities in the following order of preference:

1. Adjust in place.

2. Replace component with spare unit (and then repair the disabled unit).

3. Repair components in-place by contact maintenance to the extent permissible (consistent with personnel radiation exposure and safety needs).

7.2 CORRECTIVE MAINTENANCE

Corrective maintenance of the Plant Protection and Instrumentation System includes the following procedural steps:

1. Locate failed module, questionable channel, etc., utilizing the built-in surveillance and test instrumentation.

2. Ascertain what other, if any, maintenance is being performed and whether this proposed maintenance will include disabling a second channel of a redundant protection system. (A minimum degree of redundancy of one must be maintained during plant operation on a system level basis). The protection system status and bypass displays will assist in establishing any work in progress on redundant portions.

3. Obtain the shift supervisor's/reactor operator's clearance to disable appropriate portions of the circuitry.

4. Determine the system status to be maintained during maintenance period (i.e., should channel be tripped/untripped) to be consistent with Plant Technical Specifications.

5. Proceed and take channel/circuitry out of service.

6. Confirm with the reactor operator that bypass display reflects that maintenance is being performed.

7. Proceed with the repair/maintenance.

8. Perform necessary checkout and surveillance following repair/ maintenance.

9. Notify the operator following completion of maintenance/repair.

10. Ascertain that alarms/status indications are returned to their normal state.

7.3 PREVENTIVE MAINTENANCE

The Plant Protection and Instrumentation System is composed of electronic, electrical, electromechanical, and mechanical components. The electronic components require no specific preventive maintenance other than verification that electrical power supply and environmental requirements are maintained. Electrical components require inspection for degradation (including insulation). Electromechanical components such as trip contactors, relays, and valve actuators require adjustment of contact spring tension, contact cleaning, and lubrication of the mechanical mechanisms. Major mechanical components of this system such as valves and pumps require lubrication of moving parts, retightening of bolts, and inspection and replacement of seals, O-rings, and gaskets.

Preventive maintenance is performed on a schedule and by a methodology consistent with any assumptions made during equipment qualification. The qualified life of the equipment is maintained through the use of qualified lubricants and qualified replacement parts. Inspections performed during preventive maintenance are used to identify any age-related component degradation that may affect the component qualified life and corrective maintenance is performed or the component qualified life is adjusted accordingly.

7.4 IN-SERVICE INSPECTION

There is no ISI for the Plant Protection and Instrumentation System.

7.5 SURVEILLANCE

Surveillance testing is provided for in the design and is performed in accordance with the Plant Technical Specifications to include instrument checks, functional tests, calibration verification tests, and response time verification tests.

7.5.1 Instrument Checks

The operability of instrument channels which have channel readouts are verified by comparing readings on channels which monitor the same variable (e.g., two different neutron flux channels), comparing readings between channels which monitor the same variable and bear a known relationship between each other (e.g., overlap of startup and power range neutron flux channels), and comparing readings between channels which monitor different variables that bear a known relationship to one another (e.g., average core neutron flux and steam generator helium inlet temperature).

7.5.2 Functional Tests

Functional tests are performed to assure that electrical, electronic, electromechanical, and mechanical equipment is capable of performing its design function. Care must be exercised in performing these tests to ensure that spurious plant trips are not caused. Where possible, testing should be done during plant outages. All tested equipment must be returned to normal position (condition) after the test. The functional tests include:

1. Manual start of equipment (e.g., motor, pump) and verification of proper operation.

2. Manual control of electrically operated valves.

3. Injection of test signals to channel sensors to verify channel trip setpoints, readouts, and alarms.

4. Verification of proper electrical power bus sequencing and execute features sequencing.

5. Verification that trip setpoint algorithms are receiving the proper channel inputs.

6. Testing of protection system status and bypass indications.

7.5.3 Calibration Verification Tests

Calibration verification tests are performed to prove that with a known precision input the sensor channel gives the required output. If the required output is not obtained, the sensor channel is recalibrated. If the sensor channel fails to recalibrate, corrective maintenance is performed.

7.5.4 Response Time Verification Tests

Response time verification testing is performed on protection systems to verify that protective action response times are within the limits established by design basis analysis. The response time tests include as much of each protection system, from the sensor input to the actuated equipment, as is practicable in a single test. Where the entire set of equipment cannot be tested at once, discrete portions are tested and the overall response time is determined from the sum of the discrete response times.

SECTION 8
SYSTEM DECOMMISSIONING

[TBD]

SECTION 9
REFERENCES

1-1 Overall Plant Design Specification Modular High-Temperature Gas-Cooled Reactor, HTGR-86-004, Rev. 4, May 1987, (HFS-20100, Rev. 4) (908397, Rev. 4).

1-2 "NSSS Thermal Performance Requirements for the Modular High-Temperature Gas-Cooled Reactor," DOE-HTGR-86-030, Rev. 2, June 1987 (to be issued).

1-3 "MHTGR Plant Design Basis Transient Analysis," DOE-HTGR-86-121, Rev. 1, (908754, Rev. 1) April 1987.

1-4 "Vessels and Ducts Subsystem Design Description," HTGR-86-126, Rev. 1, (HFD-41106, Rev. 2) (908475, Rev. 1).

1-5 "Site Personnel Dose Assessment Report, Modular HTGR Plant," HTGR-86-089, September 1986.

1-6 "Top Level Regulatory Criteria for the Standard HTGR," HTGR-85-002, Rev. 2, (PC-000169, Rev. 1), October 1986.

APPENDIX A
TRACEABILITY OF REQUIREMENTS

1. INTRODUCTION

This appendix provides traceability of requirements to sources in external documents. the requirement traceability summary (Table A-1) identifies the requirements as outlined below and identifies the source. Table A-2 is a list of the references which are identified as sources in Table A-1. Traceability is given for requirements contained in Sections 1, 3, and 4. Traceability of requirements in the remaining sections has not been completed to a large extent and is therefore omitted.

Each requirement is given a traceability number which is composed of three groups of digits. The first group identifies the system (e.g., 3200); the second group identifies the section and subsection numbers of this document where the requirement is located (e.g., 0102 for SDD Section 1, Subsection 2); and the third group identifies the sequential requirement number (e.g., 001 for Requirement 1).

TABLE A-1
TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0102.010	Nuclear Island configuration	1	5.1.1
3200.0102.011	Standardized construction	1	5.1.1
3200.0102.012	Design to support certification	1	5.1.1
3200.0102.013	NI includes four reactor modules	1	5.1.1
3200.0102.014	ECA includes two steam turbine generators	1	5.1.1
3200.0102.015	Control and protection independence	1	5.7.1
3200.0102.016	Limited use of fixed alarm points	1	5.7.1
3200.0102.020	Outputs to NSSS Control Subsystem	10	4.1
3200.0102.021	Monitoring and diagnostics for RCCS	11	4.1
3200.0102.022	Reactor trip control for NCSS	4	4.1
3200.0102.023	Flux and rod data to Fuel Handling Subsystem	13	4.1
3200.0102.030	40-yr life	1	5.1.1
3200.0102.031	Reactor/turbine generator combinations	1	5.1.1
3200.0102.032	Load change capability	1	5.1.1
3200.0102.033	Reduced load operation	1	5.1.1
3200.0102.034	Plant systems performance	1	5.1.1
3200.0102.035	Design transient performance	1	5.1.1
3200.0102.036	Operability with reactor out of service	1	5.1.1

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0102.037	Operability with one turbine generator out of service	1	5.1.1
3200.0102.038	Periodic functional testing	1	5.7.2
3200.0102.039	Overall functional requirement for the design of PPIS	1	5.7.2
3200.0102.130	Graphite water reaction	3	4.1
3200.0102.200	Limit helium circulator blade temperature	5	4.1
3200.0102.201	Limit helium circulator speed	5	4.1
3200.0102.310	Steel vessels temperature limits	6	4.1
3200.0102.350	Steam generator tubesheet temperature	8	4.1
3200.0102.351	Steam generator tube bundle temperature	8	4.1
3200.0102.352	Steam generator support plates temperature	8	4.1
3200.0102.353	Steam generator bimetallic weld temperature	8	4.1
3200.0102.354	Steam generator tube bundle temperatures	8	4.1
3200.0102.355	Steam generator tubesheet temperature	8	4.1
3200.0102.357	Steam generator primary coolant flow	8	4.1
3200.0102.370	SCS helium leakage	9	4.1
3200.0102.380	Steam piping	12	4.1
3200.0102.400	Mechanical and thermal loads	1	5.1.3
3200.0102.410	Seismic design	1	5.1.3

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0102.411	Seismic response spectra	1	5.1.3
3200.0102.412	Failure of not "safety-related" SSCs	1	5.1.3
3200.0102.450	Operating environments		[TBD]
3200.0102.451	Personnel access	1	5.1.4
3200.0102.452	Dose level limits	1	5.1.4
3200.0102.453	Conformance OSHA	1	5.1.4
3200.0102.502	Requirement for remote shutdown	1	5.1.5
3200.0102.503	Individual equipment instrumentation	1	5.1.5
3200.0102.504	Internal diagnostic monitoring	1	5.1.5
3200.0102.505	Human engineering	1	5.1.5
3200.0102.506	Location of supporting controls and instruments	1	5.1.5
3200.0102.533	Surveillance of "safety-related" portions	1	5.1.6
3200.0102.550	Availability	1	5.1.7
3200.0102.551	System outage requirements allocation	1	5.1.7
3200.0102.552	Limit on long-term outages	1	5.1.7
3200.0102.553	System reliability requirements allocation	1	5.1.7
3200.0102.554	Design modifications for availability improvement	1	5.1.1
3200.0102.570	Scheduled outage time	1	5.1.8

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0102.571	Minimizing spare parts	1	5.1.8
3200.0102.573	Special maintenance tools	1	5.1.8
3200.0102.600	Design to top level regulatory criteria	1	5.1.9
3200.0102.601	Design to PAGs	1	5.1.9
3200.0102.602	Retention of radionuclides	1	5.1.9
3200.0102.603	Equipment safety classification	1	5.1.9
3200.0102.604	Design to SRDCs	1	5.1.9
3200.0102.605	"Safety-related" portions limited to Nuclear Island	1	5.1.9
3200.0102.606	Compliance with safety requirements	1	5.1.9
3200.0102.607	Design to meet 10CFR100 without reliance on control room	1	5.1.9
3200.0102.608	PPIS design to 10CFR100	1	5.1.9
3200.0102.620	Industry codes and standards	1	5.1.10
3200.0102.621	Piping codes	1	5.1.10
3200.0102.680	Quality assurance requirements	1	5.1.11
3200.0102.701	Parallel construction	1	5.1.12
3200.0102.702	Special installation equipment	1	5.1.12
3200.0102.703	Utilization of shop, factory or field fabricated parts	1	5.1.2
3200.0102.704	Arrangement features	1	5.1.2

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0102.705	Materials, processes and parts	1	5.1.2
3200.0102.720	Decommissioning	1	5.1.13
3200.0102.721	Decommissioning and refurbishment features	1	5.1.13
3200.0302.001	Nuclear island configuration	2	1.2.1
3200.0302.003	Control and protection independence	2	1.2.1
3200.0302.004	Interface with NSSS control subsystem	2	1.2.1
3200.0302.005	Investment protection subsystem configuration	2	2.2.1
3200.0302.006	Two-out-of-four sense and command logic	2	2.2.1
3200.0302.007	Investment protection subsystem configuration	2	2.2.1
3200.0302.008	Investment protection subsystem configuration	2	2.2.1
3200.0302.009	Investment protection subsystem configuration	2	2.2.1
3200.0302.010	Investment protection subsystem configuration	2	2.2.1
3200.0302.011	Investment protection subsystem configuration	2	2.2.1
3200.0302.012	Sensor channel requirements	2	2.2.1
3200.0302.015	Reactor/turbine generator combinations	2	1.2.2
3200.0302.016	Duty cycle events	2	1.2.2
3200.0302.017	Design transients	2	1.2.2
3200.0302.018	Periodic functional testing	2	1.2.2

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.019	Overall functional requirement for the design of the investment protection subsystem	2	1.2.2
3200.0302.100	Mechanical and thermal design requirements	2	1.2.3
3200.0302.105	Seismic design	2	1.2.3
3200.0302.107	Interaction with "safety-related" SCCs	2	1.2.3
3200.0302.120	Operating environments	2	1.2.4
3200.0302.121	Personnel access	2	1.2.4
3200.0302.122	Conformance with OSHA	2	1.2.4
3200.0302.130	Requirement for remote shutdown	2	1.2.5
3200.0302.131	Individual equipment design	2	1.2.5
3200.0302.132	Malfunctions detection	2	1.2.5
3200.0302.133	Human engineering requirements	2	1.2.5
3200.0302.134	Outside control room location	2	1.2.5
3200.0302.140	Surveillance testing	2	1.2.6
3200.0302.152	System reliability requirements allocation	2	1.2.7
3200.0302.153	Design modifications for availability improvement	2	1.2.7
3200.0302.154	Surveillance testing	2	1.2.6
3200.0302.155	Planned outage allocation	2	1.2.8
3200.0302.161	Arrangement to facilitate on-line maintenance	2	1.2.8

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.162	Design to facilitate hands-on maintenance	2	1.2.8
3200.0302.163	Parts interchangeability	2	1.2.8
3200.0302.164	Maintenance tools	2	1.2.8
3200.0302.180	Equipment classification	2	1.2.9
3200.0302.200	Codes and standards	2	1.2.10
3200.0302.201	Codes and standards	2	1.2.10
3200.0302.210	Quality assurance	2	1.2.11
3200.0302.221	Parallel construction	2	1.2.12
3200.0302.222	Installation tools	2	1.2.12
3200.0302.230	Decommissioning	2	1.2.13
3200.0302.301	Nuclear island configuration	2	1.2.1
3200.0302.303	Control and protection independence	2	1.2.1
3200.0302.304	Protection action signal transmission to NSSS control subsystem	2	1.2.1
3200.0302.305	Safety protection subsystem configuration	2	2.2.2
3200.0302.306	Two-out-of-four sense and command logic	2	2.2.2
3200.0302.307	Safety protection subsystem configuration	2	2.2.2
3200.0302.308	Safety protection subsystem configuration	2	2.2.2
3200.0302.309	Safety protection subsystem configuration	2	2.2.2

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.310	Safety protection subsystem configuration	2	2.2.2
3200.0302.311	Safety protection subsystem configuration	2	2.2.2
3200.0302.312	Sensor channel requirements	2	2.2.2
3200.0302.321	40-year life	2	1.2.2
3200.0302.323	Reactor/turbine generator combinations	2	1.2.2
3200.0302.324	Plant performance	2	1.2.2
3200.0302.325	Design transients	2	1.2.2
3200.0302.326	Overall functional requirement for the design of the safety protection subsystem	2	1.2.2
3200.0302.500	Mechanical and thermal design loads	2	1.2.3
3200.0302.510	Seismic design	2	1.2.3
3200.0302.511	Seismic response spectra	2	1.2.3
3200.0302.512	Not "safety-related" equipment failure	2	1.2.3
3200.0302.520	Operating environments	2	1.2.4
3200.0302.523	Personnel access	2	1.2.4
3200.0302.524	Design to OSHA	2	1.2.4
3200.0302.530	Requirement for remote shutdown	2	1.2.5
3200.0302.531	Instrumentation for control of equipment	2	1.2.5
3200.0302.532	Requirement for internal diagnostics	2	1.2.5

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.533	Human engineering techniques	2	1.2.5
3200.0302.534	Equipment locations	2	1.2.5
3200.0302.551	Surveillance requirements	2	1.2.6
3200.0302.572	System reliability requirements allocation	2	1.2.7
3200.0302.573	Design modifications for availability improvement	2	1.2.7
3200.0302.581	Planned outage allocation	2	1.2.8
3200.0302.587	Arrangement to facilitate on-line maintenance	2	1.2.8
3200.0302.588	Design to facilitate hands-on maintenance	2	1.2.8
3200.0302.591	Component standardization	2	1.2.8
3200.0302.592	Special maintenance tools	2	1.2.8
3200.0302.610	Equipment classification	2	1.2.9
3200.0302.611	Design to SRDCs	2	1.2.9
3200.0302.612	Location within Nuclear Island	2	1.2.9
3200.0302.613	Compliance with reliability allocations	2	1.2.9
3200.0302.614	Design to 10CFR100	2	1.2.9
3200.0302.615	SPS design to 10CFR100	2	1.2.9
3200.0302.631	Codes and standards	2	1.2.10
3200.0302.650	Quality assurance requirements	2	1.2.11

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.671	Parallel construction	2	1.2.12
3200.0302.672	Special installation equipment	2	1.2.12
3200.0302.680	Decommissioning	2	1.2.13
3200.0302.750	Nuclear island configuration	2	1.2.1
3200.0302.752	Independence from process controls	2	1.2.1
3200.0302.753	Use of fixed alarm points	2	1.2.1
3200.0302.754	Monitoring and diagnostics for RCCS	2	1.2.1
3200.0302.755	Special nuclear area instrumentation essential features	2	2.2.3
3200.0302.756	Essential preventive features	2	2.2.3
3200.0302.757	Preventive features configuration	2	2.2.3
3200.0302.758	Configuration of protection systems information displays	2	2.2.3
3200.0302.759	Integration of protection systems information displays	2	2.2.3
3200.0302.760	Reactor vessel pressure relief block valve closure interlock electrical power	2	2.2.3
3200.0302.761	Flux and rod position data for refueling	2	1.2.3
3200.0302.763	40-year life	2	1.2.2
3200.0302.764	Design transients	2	1.2.2
3200.0302.765	Mechanical and thermal design	2	1.2.3
3200.0302.770	Seismic design	2	1.2.3

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.772	Seismic interaction with not "safety-related" SSCs	2	1.2.3
3200.0302.790	Operating environments	2	1.2.4
3200.0302.791	Personnel access	2	1.2.4
3200.0302.792	Design to OSHA	2	1.2.4
3200.0302.801	Individual equipment instrumentation	2	1.2.5
3200.0302.802	Internal diagnostic monitoring	2	1.2.5
3200.0302.803	Human engineering techniques	2	1.2.5
3200.0302.804	Equipment location	2	1.2.5
3200.0302.850	Surveillance testing	2	1.2.6
3200.0302.852	System reliability requirements allocation	2	1.2.7
3200.0302.873	Planned outage allocation	2	1.2.8
3200.0302.876	Arrangement to facilitate on-line maintenance	2	1.2.8
3200.0302.877	Design to facilitate hands-on maintenance	2	1.2.8
3200.0302.882	Component standardization	2	1.2.8
3200.0302.883	Special maintenance tools	2	1.2.8
3200.0302.900	Equipment classification	2	1.2.9
3200.0302.903	Codes and standards	2	1.2.10
3200.0302.910	Quality assurance	2	1.2.11

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0302.921	Parallel construction	2	1.2.12
3200.0302.925	Special installation equipment	2	1.2.12
3200.0302.930	Decommissioning	2	1.2.13
3200.0401.001	Control rod and reserve shutdown trip response	2	2.3.3
3200.0401.020	Relief valve block valve closure interlock signal	2	2.2.3.1
3200.0401.030	Primary coolant system pumpdown	2	2.2.1.5
3200.0401.040	Circulator trip contactor	2	2.2.1.2
3200.0401.045	Radiation monitor inputs	2	2.2.1.5
3200.0401.050	Control system actions on PPIS trip	2	2.3.3
3200.0401.052	Transmission of data to operator	2	2.2.3
3200.0401.060	Feedwater shutoff valves	2	2.2.2
3200.0401.064	Superheater outlet valves	2	2.2.2
3200.0401.065	Superheater outlet valve position	2	2.2.2
3200.0401.068	Feedwater dump system valving	2	2.3
3200.0401.070	RCCS status and performance	2	2.2.3
3200.0401.080	SCS start signals	2	2.2.1.4
3200.0401.082	SCHE isolate and drain valving	2	2.3
3200.0401.090	Building space and structural support for PPIS equipment	2	2.4

TABLE A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference	
		Reference	Section
3200.0401.091	Building space and structural support for PPIS equipment	2	2.4
3200.0401.092	Building space and structural support for PPIS equipment	2	2.4
3200.0401.100	Electric power to PPIS equipment	2	2.4

TABLE A-2

TRACEABILITY SUMMARY REFERENCE LIST

1. "Overall Plant Design Specification Modular High-Temperature Gas-Cooled Reactor," HTGR-86-004, Rev. 4, (HFS-20100, Rev. 4) (908397, Rev. 4).

2. "Plant Protection and Instrumentation System Design Description," HTGR-86-047, Rev. 1, (HFD-33200, Rev. 2) (908444, Rev. 2).

3. "Reactor Internals Subsystem Design Description," HTGR-86-055, Rev. 1, (HFD-41017, Rev. 1) (908473, Rev. 2).

4. "Neutron Control Subsystem Design Description," HTGR-86-100, Rev. 1, (HFD-41012, Rev. 2) (908472, Rev. 2).

5. "Main Circulator Subsystem Design Description," HTGR-86-099, Rev. 1, (HFD-42101, Rev. 1) (908490, Rev. 2).

6. "Vessels and Ducts Subsystem Design Description," HTGR-86-126, Rev. 1, (HFD-41106, Rev. 2) (908475, Rev. 1).

7. "Pressure Relief Subsystem Design Description," HTGR-86-127, Rev. 1, (HFD-41105, Rev. 1) (908476, Rev. 1).

8. "Steam Generator Subsystem Design Description," HTGR-86-129, Rev. 1, (HFD-42102, Rev. 1) (908491, Rev. 1).

9. "Shutdown Cooling System Design Description," HTGR-86-028, Rev. 2, (HFD-35700, Rev. 1) (908443, Rev. 3)

10. "NSSS Control Subsystem Design Description," HTGR-86-051, Rev. 1, (HFD-43701, Rev. 2) (908468, Rev. 2).

11. "Reactor Cavity Cooling System Design Description," HTGR-(later), Rev. 0, (HFD-35600, Rev. 1) (908442, Rev. 1).

12. "Main and Bypass Steam System Description," HTGR-(later) (HFD-45004, Rev. 1) (908516, Rev. 1).

13. "Core Refueling Subsystem Design Description," HTGR-86-097, Rev. 1, (HFD-43413, Rev. 2) (908500, Rev. 2).

APPENDIX B

DRAWINGS LIST

Ref. No.	Drawing No.	Title
1	GA Drawing 029950	IB Diagram - MHTGR Investment Protection Subsystem (GA Proprietary Information)
2	GA Drawing 029951	IB Diagram - MHTGR Safety Protection Subsystem (GA Proprietary Information)
3	GA Drawing 030055	IB Diagram - MHTGR Plant Protection and Instrumentation Systems Equipment and Locations

APPENDIX C
TRANSIENTS

Plant transients do not directly affect the performance of the Plant Protection and Instrumentation System. The PPIS is environmentally qualified to assure performance of its functions during all plant transients. The performance of the PPIS affects the outcome of various plant transients. The results of these plant transients are shown in DOE-HTGR-86-121, Revision 1 (908754/1), "Modular High Temperature Gas-Cooled Reactor Plant Design Basis Transients Analysis," April 1987.

Unprotected transients that contribute to the designs of the PPIS are given in "Unprotected Transients for PPIS Designs," Document 908940/0.

APPENDIX D
DESIGN BASIS SEISMIC INPUTS

[LATER]

APPENDIX E
PLANT PROTECTION AND INSTRUMENTATION SYSTEM PARAMETERS AND MAJOR FEATURES

A. GENERAL

Number of subsystems = Three
Input logic = Two out of four

Equipment location = Local, reactor building equipment room, reserve shutdown area

Subsystems and classification

Investment Protection Subsystem - not "safety-related"
Safety Protection Subsystem - "safety-related"
Special nuclear area instrumentation - not "safety-related"

Applicable Industry Standards

Safety Protection Subsystem - IEEE-603

B. INVESTMENT PROTECTION SUBSYSTEM

Reactor Trip - Inner control rods

Trip Parameters:

1. Primary coolant moisture-high.
2. Manual initiation.

Actuated Equipment:

1. Release mechanisms - inner control rods.

Steam Generator Isolation and Dump

Trip Parameters:

1. Primary coolant moisture-high.
2. Manual initiation.

Actuated Equipment:

1. Steam generator dump valves (4).
2. Signal to main loop shutdown and main steam isolation.

Primary Coolant Pressure Pumpdown.

Trip Parameters:

1. Primary coolant pressure low and reactor building radiation high.

2. Manual initiation.

Actuated Equipment:

1. Purification system pumpdown sequencer.

Shutdown Cooling System Initiation

Trip Parameters:

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

2. Manual initiation.

Actuated Equipment:

1. Shutdown Cooling System start circuitry.

Shutdown Cooling Heat Exchanger Isolation.

Trip Parameters:

1. Shutdown cooling system helium leak.
2. Manual initiation.

Actuated Equipment:

1. Inlet water block valves (2).
2. Outlet water block valves (2).
3. Heat exchanger drain valves (2).

C. SAFETY PROTECTION SUBSYSTEM ("SAFETY-RELATED")

Reactor Trip - Outer Control Rods.

Trip Parameters:

1. Neutron flux to helium mass flow ratio high.

2. Primary coolant pressure low.

3. Primary coolant pressure high.

4. Primary coolant moisture concentration high (not required for safety).

5. Main loop shutdown and main steam isolation trip signal (not required for safety).

6. Steam generator inlet helium temperature high (not required for safety).

7. Manual initiation (not required for safety).

Actuated Equipment:

1. Release mechanisms - outer control rods.

Reactor Trip - Reserve Shutdown.

Trip Parameters:

1. Reactor neutron flux to main helium circulator speed ratio - high.

2. Primary coolant pressure high.

3. Manual initiation (not required for safety).

Actuated Equipment:

1. Release mechanisms - reserve shutdown material.

Main Loop Shutdown and Main Steam Isolation.

Trip Parameters:

1. Primary coolant pressure high.

2. Circulator speed high or low (programmed by feedwater flow and helium density) (not required for safety).

3. Main steam temperature low (not required for safety).

4. Steam generator dump and isolation signal (not required for safety).

5. Manual initiation (not required for safety).

Actuated Equipment:

1. Feedwater block valves (2).
2. Superheater outlet valves (2).
3. Circulator motor trip contactors (2).

D. SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM

Vessel Pressure Relief Block Valve Closure Interlock.

Inputs: Block valve limit switches.

Outputs: Interlocks to prevent block valve closing.

Logic: 1 of 2

Safety and Investment Protection Information Displays.

Readouts:

1. All protection system input sensors and channels.

2. All protection subsystem status indications including status indications for actuation devices, actuated equipment, and auxiliary supporting features.

3. All protection system bypass indications including bypass indications for actuation devices, actuated equipment, and auxiliary supporting features.

4. Post accident monitoring.

Integrated Display System Requirements

Number of Inputs	
Internal to protection system	[100]*
External - analog	[50]
External - digital	[50]
Frequency to Poll Parameters	[Once per 10 s]
Number of Displays (Overviews, Safety, and Investment Protection Subsystems' Status, Status of Bypasses, Plant Status, Accident Monitoring, etc.)	
Displays	Color CRTs
Historical Trending	
Time history of variables available for trending	[30 minutes]
Number of variables for trending	[100]
Recording Capability	Magnetic Tape
Interfacing Protocol	RS-232

*Value of brackets [ ] is tentative.

APPENDIX F
PROPRIETARY CLAIMS

[NONE]