DOE/HTGR-86-049

HTGR

INVESTMENT PROTECTION SUBSYSTEM DESIGN DESCRIPTION

~~APPLIED TECHNOLOGY~~

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

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

Distribtion of this report is Unlimited David Hamrin OSTI 3/10/21

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

SEPTEMBER 1986

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

HTGR–86–049
908497/1

INVESTMENT PROTECTION SUBSYSTEM
DESIGN DESCRIPTION

APPLIED TECHNOLOGY

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

NOTICE

This report contains information of a preliminary nature and was prepared primarily for internal use at the originating installation. It is subject to revision or correction and therefore does not represent a final report. It is passed to the recipient in confidence and should not be abstracted or further disclosed without the approval of the originating installation or USDOE Office of Scientific and Technical Information, Oak Ridge, TN 37830.

RELEASED FOR ANNOUNCEMENT IN HGF,
DISTRIBUTION LIMITED TO PARTICIPANTS
IN THE HTGR PROGRAM.
OTHERS REQUEST FROM HTR, DOE

MASTER

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

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

SEPTEMBER 1986

ROLL 2084

GA 1485 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY

TITLE	INVESTMENT PROTECTION SUBSYSTEM DESIGN DESCRIPTION	☐ R & D ☐ DV & S ☒ DESIGN	APPROVAL LEVEL 5

DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO.	ISSUE NO./LTR.
0	32 01	SSDD	6300	908497	1

QUALITY ASSURANCE LEVEL	SAFETY CLASSIFICATION	SEISMIC CATEGORY	ELECTRICAL CLASSIFICATION
QAL II	NNS	Non CAT I	Non 1E

INFO 1

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 Interface Assurance F.A.Silady	G.P.Connors	G.C.Bramblett		Initial issue (HFD-43201 Rev. 0) 6352-320-103

~~APPLIED TECHNOLOGY~~

~~Any Further Distribution by any Holder of this Document or 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

Cover Sheets = 2 (Unnumbered)

Issue Summary 1,1a	2		A-1 through A-8	8
ii through xvii	16		B-1	1
1-1 through 1-29	29		C-1	1
2-1 through 2-25	25		D-1	1
3-1	1		E-1	1
4-1 through 4-5	5		F-1	1
5-1 through 5-3	3			
6-1 through 6-11	11			
7-1	1		Total	110
8-1	1			
9-1	1			

NEXT INDENTURED DOCUMENTS

908444

(HFD-33200)

REV	1		0	←		→ 0																						
SH	1a		57	THRU		110																						
REV	0	←																										→ 0
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	1	0	←																									→ 0
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

GA 1485-1 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY CONTINUATION SHEET

INFO 1

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
INVESTMENT PROTECTION SUBSYSTEM DESIGN DESCRIPTION	908497	1

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: FUNDING PROJECT	APPROVAL: APPLICABLE PROJECT	ISSUE DESCRIPTION/ CWBS NO.
1	SEP 09 1986	J.Zgliczynski C. Rodriguez Jr J. Zgliczynski J. Bauer J Bauer	C Rodriguez C.Rodriguez Donald A Silady F.A.Silady R.D. Phelps Interface Assurance	G.P. Connors G.P.Connors	GCB G.C.Bramblett		HTGR cover added HTGR-86-049/0 (HFD-43201,Rev. 1) Class II Change 6301998201

LIST OF EFFECTIVE PAGES

SECTION	PAGE	REV.	DATE
	Cover		
--	ii through xvii	0	6/30/86
1	1-1 through 1-29	0	6/30/86
2	2-1 through 2-25	0	6/30/86
3	3-1	0	6/30/86
4	4-1 through 4-5	0	6/30/86
5	5-1 through 5-3	0	6/30/86
6	6-1 through 6-11	0	6/30/86
7	7-1	0	6/30/86
8	8-1	0	6/30/86
9	9-1	0	6/30/86
Appendix A	A-1 through A-8	0	6/30/86
Appendix B	B-1	0	6/30/86
Appendix C	C-1	0	6/30/86
Appendix D	D-1	0	6/30/86
Appendix E	E-1	0	6/30/86
Appendix F	F-1	0	6/30/86

CONTENTS

CONTENTS (Continued)

CONTENTS (continued)

CONTENTS (continued)

LIST OF APPENDICES

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CRT	Cathode Ray Tube
DBE	Design Basis Event
EMI	Electromagnetic Interference
HTS	Heat Transport System
HVAC	Heating Ventilating and Air Conditioning
IEEE	Institute of Electrical & Electronic Engineers
IB	Instrument Block
ISI	In-Service Inspection
LCO	Limiting Condition for Operation
MM	Moisture Monitor/Detection Equipment
NEMA	National Electrical Manufacturers Association
NNS	Nonnuclear Safety
OBE	Operating Basis Earthquake
PAM	Post-Accident Monitoring
PCDIS	Plant Control, Data, and Instrumentation System
PPIS	Plant Protection and Instrumentation System
QA	Quality Assurance
QAL	Quality Assurance Level
RFI	Radio Frequency Interference
SCS	Shutdown Cooling System
SDD	System Design Description
SHE	Shutdown Heat Exchanger
SSDD	Subsystem Design Description
SRDI	Safety-Related Display Instrumentation
SSE	Safe Shutdown Earthquake
TBD	To Be Determined

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: Non-Class 1E circuits not physically separated or electrically isolated from Class 1E circuits by acceptable separation distance, safety class 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.

*In general, definitions of terms used in this document (some of which are repeated herein) are defined in accordance with ANSI/IEEE Std. 279-1971, IEEE Std. 603-1980, and IEEE Std. 497-1981, unless otherwise specified herein.

DEFINITIONS (Continued)

Class 1E: The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, reactor core cooling, and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

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.

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.

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.

DEFINITIONS (Continued)

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.

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 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.

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 5 consecutive days a dose in excess of 1.0×10^{-3} Sv (100 millirems).

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.

Protection Group: A given minimal set of interconnected components, modules, and equipment that can accomplish a protection function.

NOTE: A group involves two sensing channels in a 2 of N system.

Safety System: Those systems or subsystems (e.g., the safety protection subsystem including all auxiliary supporting features) providing a safety function. A safety system is comprised of more than one protection group of which any one protection group can provide the safety function.

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
1.2 Maintain Safe Plant Shutdown
1.3 Maintain Safe Plant Refueling
1.4 Maintain Safe Plant Startup/Shutdown

2. Maintain Plant Protection (in the event that plant operation cannot be maintained in the normal operating envelope)
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 (in the low probability event of failure to maintain plant protection).
3.1 Control radiation
3.2 Control personnel access

4. Maintain Emergency Preparedness (in the extremely low probability of failure to maintain control of release of radionuclides).

The OPDS is the top-level technical document for the HTGR plant. The OPDS (based on owner requirements 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, SDDs and SSDDs are prepared which describe and control the individual system and subsystem designs. Traceability from plant-level requirements to equipment-level requirements is maintained throughout this hierarchy of design documents.

SUMMARY

The Plant Protection and Instrumentation System is one of the systems comprising the MHTGR plant. The design of this system has been developed through the Integrated Approach (Ref. 1.1) toward safe and economical production of electrical power. The Plant Protection and Instrumentation System has three subsystems (Safety Protection, Investment Protection, and Special Nuclear Area Instrumentation).

This document defines the functions of the Investment Protection Subsystem, subsystem design requirements derived from the functional analysis, and institutional requirements from the Overall Plant Design Specification (Ref. 1.1). A description of the subsystem design which satisfies the requirements is then presented. Lower-tier requirements at the component level are next defined. This document also includes information on aspects of subsystem construction, operation, and maintenance.

The Investment Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant 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. In so doing, it indirectly contributes to protecting the public health and safety but it is not required to prevent design basis events from exceeding 10CFR100 limits; therefore, it is not safety-related. The investment protection provides an integrated response to various plant upsets and events to ensure equipment damge limits are not exceeded. The subsystem uses redundancy and other system characteristics to meet plant investment and availability goals. Each reactor module has a separate and independent investment protection subsystem. The Investment Protection Subsystem is part of the Plant Protection and Instrumentation System and is separate and independent of all other plant instrumentation and controls.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 INTEGRATED APPROACH SUBSYSTEM FUNCTIONS

The function of the Investment Protection Subsystem is to monitor and protect plant systems and equipment for protection of plant investment. 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 plant investment risk.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Formal utility/user reviews of the Investment Protection Subsystem design shall be made and the results of and designer response to the review documented at the completion of conceptual, preliminary, and final design. Design reviews shall include consideration of plant operability, maintainability, fabricability, and constructability. (3201.0102.001)*

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. (3201.0102.002)

The Investment Protection Subsystem shall be responsive to minimizing the number of inaccessible areas due to high radiation levels during reactor operation to facilitate routine operational and maintenance activities. (3201.0102.003)

*Requirements traceability number.

The plant control system and major equipment monitoring and protective systems of the Investment Protection Subsystem shall be functionally independent. (3201.0102.004)

The Investment Protection Subsystem shall consist of five supporting trip subsystems: (3201.0102.005)

1. Reactor Trip - Inner Rods
2. Main Loop Shutdown
3. Steam Generator Isolation and Dump
4. Shutdown Cooling System Initiation
5. Primary Coolant Pumpdown

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. (3201.0102.006)

Each input channel shall include the field mounted process variable sensor (e.g., resistance thermometers, flow transducers, pressure transducers, neutron detectors, etc.), electronic signal conditioning equipment, and electronic trip setpoint comparator to provide a trip signal when the process variable value reaches the trip setpoint. (3201.0102.007)

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. (3201.0102.008)

The protective action initiation signal shall be sent to separate and redundant actuation devices. (3201.0102.009)

The boundaries of the Investment Protection Subsystem shall be from, and including, the sensors to the input terminals of the actuation devices.
(3201.0102.010)

The Investment Protection Subsystem and its supporting subsystems and interfaces with actuated equipment shall be as shown in the Functional Overview Protection Subsystem Drawing and Safety and Investment Protection Subsystem Instrument Block Diagram. (For drawings see Appendix B.) (3201.0102.011)

Sensor channel parameters shall be as given in Table 1-1. (3201.0102.012)

1.2.2 Operational Requirements

The design, development, fabrication/construction, and installation of the Investment Protection Subsystem shall accommodate a mid-1990s start-of-operation date. (3201.0102.015)

The Investment Protection Subsystem shall be designed for an operating life of 40 calendar years from start of operation while accommodating either base load operation or the weekly load cycle of Fig. 1-1. (3201.0102.016)

The Investment Protection Subsystem shall be designed to accommodate the transients resulting from the duty cycle events in Table 1-2. (3201.0102.017)

The Investment Protection Subsystem shall accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations: (3201.0102.018)

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.

3. Cogeneration configurations (TBD).

Table 1-1

INVESTMENT PROTECTION SENSOR CHANNEL PARAMETERS

Monitored Variable - Sensor Parameters	Sensor Channel Parameters		
	Maximum Response Time	Minimum Accuracy	Minimum Range
Primary Coolant Pressure Receptive Subsystems: Main loop shutdown, primary coolant pressure pumpdown, steam generator isolation and dump (dump valve closure)	{2 s}*	{±1%} of span	{600-1100 psia}
Primary Coolant High Moisture Concentration Receptive Subsystems: Steam generator isolation and dump	{40 s} (constant at all loads and includes 25 s sample transit time and 5 s sensor time constant)	{±140 ppmv}	Not Applicable
Circulator Speed Receptive Subsystems: Main loop shutdown	{10 ms}	{±1%} of span	{0-3600} rpm
Main Circulator Outlet Helium Temperature (Core Inlet Temp.) Receptive Subsystems: Main loop shutdown Sensors at the outlet of the circulator.	{20.0 s} (time constant)	{+9°F}	{300-850°F}

*N[illegible]s in { } are estimated and subject to change.

908497/0

Table 1-1 (Continued)

Monitored Variable → Sensor Parameters	Sensor Channel Parameters		
	Maximum Response Time	Minimum Accuracy	Minimum Range
Superheat Steam Temperature Receptive Subsystems: Main loop shutdown	{20 s} time constant at 100% power. (Later) sec time constant at 25% power	{±10°F}	{500-1400°F}
Feedwater Flow Rate Receptive Subsystems: Main loop shutdown	{2 s}	{±[TBD] @ 10% flow}	{5-105%} flow
Superheat Steam Pressure Receptive Subsystem: Steam generator isolation and dump (dump valve closure)	{2 s}	±[TBD] of full scale	{14-2800 psia}
Reactor Building Radiation Receptive Subsystem: Primary coolant pressure pumpdown	[TBD]	[TBD]	[TBD]

908497/0

Fig. 1-1 **Weekly Load Following Cycle**

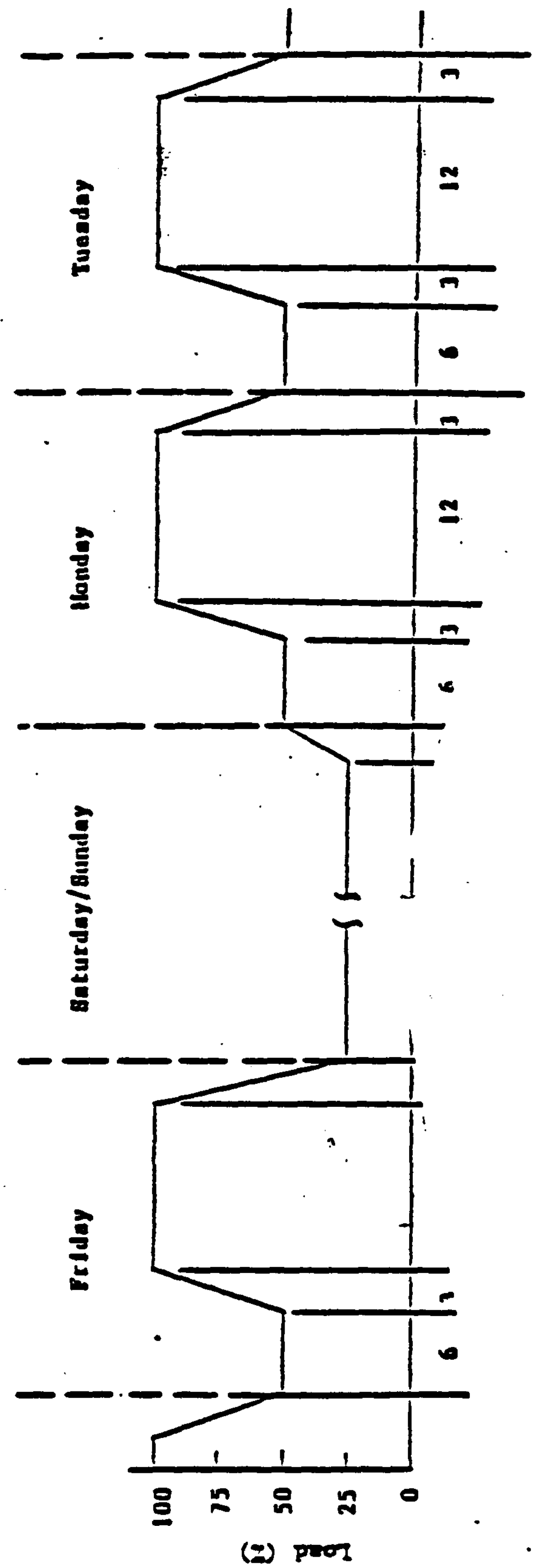

Table 1-2

DESIGN DUTY CYCLE EVENTS

	Event	Design No. of Occurrences (per Reactor Module)	ASME Boiler & Pressure Vessel Code Level of Service Limits
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 min) (25%-100%)	1000	A
6.	Normal Load Increase (0.5% per min) (25%-100%)	20800	A
7.	Rapid Load Decrease (5% per min) (100%-25%)	1000	A
8.	Normal Load Decrease (0.5% per min) (100%-25%)	17500	A
9.	Step Load Increase (+15%)	1000	A
10.	Step Load Decrease (-15%)	1000	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.	Reactor Trip from 100%	180(a)	B
16b.	Reactor Trip from 25%		

Table 1-2 (Continued)

Event	Design No. of Occurrences (per Reactor Module)	ASME Boiler & Pressure Vessel Code Level of Service Limits
17. Turbine Trip or Load Rejection	120	B
18. Sudden Reduction of FW Flow	30	B
19. Steam Generator Tube Leak (Small)	9	B
20. Control Rod Insertion	5	B
21. Main Loop Overcooling	10	B
22. Operating Basis Earthquake (OBE)	1	B
23. Slow Primary System Depressurization	8	B
24a. Rod Withdrawal (normal rod speed) (P/F Trip)	1	C
24b. Rod Withdrawal (slow) (SGIT Trip)	1	C
25. Failure of Circulator Speed Control	1	C
26. Circulator Trip with He Shutoff Valve Failure	1	C
27. Steam Generator Tube Rupture	1	C
28. SCS Heat Exchanger Tube Leak	1	C
29. Total Loss of FW 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. HTS Trip and Failure of SCS to Start (SRDC No. 1)	1	C
32. Loss of HTS Without Control Rod Insertion or SCS Operation (ATWS) (SRDC No. 2)	1	D[b]

Table 1-2 (Continued)

	Event	Design No. of Occurrences (per Reactor Module)	ASME Boiler & Pressure Vessel Code Level of Service Limits
33.	Control Rod Withdrawal Followed by P/F Trip and RCCS Cooling (SRDC No. 3, 4)	1	D[b]
34.	Large Earthquake Followed by RCCS Cooling [Safe Shutdown Earthquake (SSE)] (SRDC No. 5)	1	D[b]
35.	Steam Generator Tube Rupture Without Isolation (SRDC No. 6A)	1	D[b]
36.	Steam Generator Tube Rupture Without Isolation, Followed by RCCS Cooling (SRDC No. 6B)	1	D[b]
37.	Steam Generator Tube Leaks Without Isolation, Followed by RCCS Cooling (SRDC No. 7)	1	D[b]
38.	Small Steam Generator Tube Leak Without Isolation, Followed by RCCS Cooling (SRDC No. 8)	1	D[b]
39.	Small Steam Generator Tube Leak With Unterminated Dump Followed by RCCS Cooling (SRDC No. 9)	1	D[b]
40.	Rapid Depressurization Followed by RCCS Cooling (SRDC No. 10)	1	D
41.	Slow Primary System Depressurization With Loss of Forced Circulation (SRDC No. 11)	1	D[b]
42.	Main Steam Pipe Rupture	1	D

[a]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%.

[b]In general, level D service limits are assigned to SRDCs for specified safety functions of safety related SSCs. However, level D limits are intended primarily for guidance. The plant level requirement is that 10CFR100 dose requirements not be exceeded. Event No. 31 (SRDC No. 1) and 40 (SRDC No. 10) are exceptions to this. Their minimum service limit levels are C and D, respectively.

Accommodation of the above requirement shall be confirmed through analysis to verify that standard reactor module system and component design limits are not exceeded under anticipated transient and accident conditions.
(3201.0102.019)

The system shall function through the design transients provided in Table 1-3. (3201.0102.020)

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 the public health and safety and plant investment.
(3201.0102.021)

The Investment Protection Subsystem shall be designed to be administered, operated, and maintained by a minimum plant staff consistent with the plant availability and safety goals. (3201.0102.022)

1.2.3 Structural Requirements

1.2.3.1 Mechanical

Investment Protection Subsystem cabinets, control boards, racks, and panels shall meet or exceed the mechanical design requirements of ANSI/IEEE Std. 420, NEMA-ICS 1 (National Electrical Manufacturers Association) and NEMA-ICS 2. (3201.0102.100)

1.2.3.2 Seismic

The Investment Protection Subsystem shall be designed, fabricated, and erected to performance standards that will enable it to withstand the forces that might be imposed by an earthquake with ground acceleration levels corresponding to an Operating Basis Earthquake (OBE) with a maximum

Table 1-3

HTGR PLANT TRANSIENTS

[LATER]

Table 1-4

PLANT EQUIPMENT DAMAGE LIMITS FOR USE IN DESIGNING THE INVESTMENT PROTECTION SUBSYSTEM

Component	Requirements*
Graphite moderator, reflectors and core support	Limit graphite/water reaction to less than [TBD]. (3201.0102.023)
Fuel particles	Limit fuel/water reaction to less than [TBD]. (3201.0102.024)
	Maintain fuel particle temperature ≤{2912}°F with (3201.0102.025)
Movable metal clad poison rods	Maintain control rod structure and cladding temperature ≤{1700}°F for transient exposure duration (100 h). (3201.0102.026)
Helium circulator	Maintain helium circulator inlet temperature <{1100}°F. (3201.0102.030)
	Maintain helium circulator speed <[TBD] rpm. (3201.0102.031)
Welded steel vessels and concentric cross ducts	Maintain steel vessel's temperature <{700}°F. (3201.0102.035)
	Maintain primary coolant pressure <{1150} psia. (3201.0102.036)
Steel vessels relief valve setting	Maintain primary coolant pressure <{1041} psia. (3201.0102.040)

*Numbers in { } are estimated and subject to change.

908497/0

Table 1-4 (Continued)

Component	Requirements
Steam generator	Maintain helical bundle support plates <{1400}°F. (3201.0102.045)
	Maintain helical superheater tubes ≤{1400}°F. (3201.0102.046)
	Maintain bimetallic weld <{1150}°F. (3201.0102.047)
	Maintain straight tube superheater tube <{1400}°F. (3201.0102.408)
	Maintain steam generator temperature below 300°F before reintroduction of feedwater. (3201.0102.049)

908497/0

horizontal ground acceleration of 0.15 g and vertical acceleration of 0.15 g lasting {15}* s and a Safe Shutdown Earthquake (SSE) with a maximum horizontal ground acceleration of 0.30 g and vertical acceleration of 0.30 g lasting {25} s as defined in Ref. 1.1, and operate as required without undue risk to the reactor plant and ultimately to the health and safety of the public. (3201.0102.105)

The system components shall be designed to meet the seismic response spectra provided in [later]. (3201.0102.106)

The damping coefficients for the seismic response analysis shall be selected and justified. Representative values of damping coefficients for various types of structures are as follows: (3201.0102.107)

Type of Structure	Operating Basis Earthquake	Safe Shutdown Earthquake
Reactor Building	2%	5%
Auxiliaries and Diesel Building	4%	7%
Circulator	1%	2%
Other components and equipment	2%	3%
Steel piping systems	1%	2%
Miscellaneous structural items (welded)	2%	4%
Miscellaneous structural items (bolted)	4%	7%

1.2.3.3 Material

Materials shall be selected to minimize the production of radioactive materials due to activation and the generation of products of corrosion. (3201.0102.110)

*Numbers in { } are estimated and subject to change.

1.2.4 Environmental Requirements

The Investment 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 1-5, 1-6, 1-7. (3201.0102.120)

1.2.5 Instrumentation and Control Requirements

Controls and instrumentation capable of manually initiating a reactor trip, establishing and maintaining core cooling, and monitoring the achievement of these two functions shall be provided to permit and maintain a safe plant shutdown in the event the main control room becomes uninhabitable. No design basis event shall result in a simultaneous loss of control from the central control room and remote shutdown capability. (3201.0102.130)

1.2.6 Surveillance and In-Service Inspection Requirements

This section is not used as this subsystem is nonsafety-related.

1.2.7 Availability Assurance Requirements

The Investment Protection Subsystem operating availability shall be accomplished through provisions in the design for equipment reliability, equipment redundancy, maintenance support features and facilities, human factors, and identification of spare parts, material, and manpower requirements. (3201.0102.150)

The subsystem shall be designed to meet its planned outage allocation given in Table 1-8. (3201.0102.151)

The subsystem shall be designed to meet its overall reliability allocation given in Table 1-8. (3201.0102.152)

Table 1-5

EXTERNAL ENVIRONMENTAL CONDITIONS (NORMAL)

Building/Area	Ranges				
	Temperature °C (°F)	Pressure MPa gauge (psig)	Humidity %	Radiation*	Other**
Control Room	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

*Radiation data includes type, exposure rate, and integrated dose.
**Includes vibration, electromagnetic inference (EMI), radio-frequency interference (RFI), gas composition, acoustic.

908497/0

Table 1-6

EXTERNAL ENVIRONMENTAL CONDITIONS (ABNORMAL)

Building/Area	Ranges: Temperature °C (°F)	Pressure MPa gauge (psig)	Humidity %	Radiation*	Other**
Control Room	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

*Radiation data includes type, exposure rate, and integrated dose.
**Includes vibration, EMI, RFI, gas composition, acoustic.

Table 1-7

EXTERNAL ENVIRONMENTAL CONDITIONS (DESIGN BASIS EVENT)
(Where Applicable)

Building/Area	Ranges				
	Temperature °C (°F)	Pressure MPa gauge (psig)	Humidity %	Radiation*	Other**
Control Room	Not Applicable (Defined as "mild" environment not subject to these DBEs)				
Reactor Building (by zone)	[TBD]	[TBD]	[TBD]	[TBD]	[TBD]

*Radiation data includes type, exposure rate, and integrated dose.
**Includes vibration, EMI, RFI, gas composition, acoustic.

Table 1-8

UNAVAILABILITY/RELIABILITY ALLOCATIONS
(MAINTAIN PLANT PROTECTION AND MAINTAIN CONTROL OF RADIONUCLIDE RELEASE)

	Unavailability			Reliability		Allocation	
Subsystem	MTBF (h)	MTTR (h)	EFOH (h/yr)	Investment	Safety	EFOH	Other
Investment Protection	{33,000}*	{65}	{14.6}			{14.6}	

*Numbers in { } are estimated and subject to change.

Design modifications and improvements to achieve 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. (3201.0102.153)

1.2.8 Maintenance Requirements

The design of Investment Protection Subsystem protective features shall provide for periodic functional testing that will not interfere with normal plant operation. (3201.0102.154)

A Preventive Maintenance Plan shall be developed and documented based upon the plant final design. A first draft shall be issued at completion of preliminary design. This plan shall address the preventive maintenance requirements, tasks, methods, personnel skills and anticipated man-hour requirements on a system basis for mechanical, electrical and control, and instrumentation maintenance. Anticipated health physics man-hours shall be documented. (3201.0102.155)

A planned outage schedule shall be developed and maintained throughout the design process. The major maintenance and ISI activities are to be identified, durations determined, and a critical path established. Anticipated tasks, methods, personnel skills, and man-hours required to achieve the scheduled durations shall be determined and documented.

(3201.0102.156)

Anticipated tasks, methods, personnel skills, and man-hours requirements to accomplish unscheduled maintenance shall be documented for the Investment Protection Subsystem. Analysis shall be based upon industrial experience (mean time between failure and mean time to repair data) for like type systems and components. Estimated man-hours shall also include equipment/ system isolation, preparation for maintenance, and return to service. Anticipated health physics man-hours shall also be documented.

(3201.0102.157)

The use of standard "off-the-shelf" components and materials shall be used to reduce costs associated with the required spare parts. Components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings. (3201.0102.158)

A spare parts listing and recommended spare parts inventory shall be developed consistent with the Preventive Maintenance Plan, anticipated unscheduled maintenance and plant availability requirements. (3201.0102.159)

The design of Investment Protection Subsystem mechanical and electrical systems, components, and parts shall provide for reasonable and necessary interchangeability. (3201.0102.160)

The Investment Protection Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3201.0102.161)

The Investment Protection Subsystem shall be designed to facilitate hands-on maintenance. (3201.0102.162)

Provisions shall be made in the Investment Protection Subsystem for monitoring plant status, configuration, and performance as a basis for maintenance diagnostics and decision-making. (3201.0102.163)

The Investment Protection Subsystem shall support a plant design goal for the permanent maintenance staff of a maximum of 75 full-time personnel. This staff would include first line supervisors and personnel assigned in the categories of mechanical, electrical, electronic and instrument maintenance, quality control, and stores and warehouse activities. (3201.0102.164)

Remote maintenance technique shall be considered in the Investment Protection Subsystem design where improved availability may result from time savings. (3201.0102.165)

Where practicable, the design of the Investment Protection Subsystem and components shall incorporate those features required to implement in-service inspection functions with the unit or major component on-line. For those inspection activities that require the unit or major component be removed from service, design features shall be included to accomplish the inspection as one of those activities to be completed during the allotted plant planned downtime. (3201.0102.166)

1.2.9 Safety Requirements

Since the Investment Protection Subsystem does not perform any 10CFR100 related radionuclide control functions, no special classification is applied to it. However, the subsystem will have appropriate reliability to meet other top-level regulatory criteria and user requirements.

Equipment classification requirements shall be in accordance with Table 1-9. (3201.0102.180)

1.2.10 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.* (3201.0102.200)

The design of the Investment Protection Subsystem shall meet the industrial standards given in Table 1-10. (3201.0102.201)

---

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

Table 1-9

EQUIPMENT CLASSIFICATION
(INVESTMENT PROTECTION SUBSYSTEM)

	Equipment Classification	Seismic Category	QAL Level
Piping Valves and Mechanical Components for Moisture Monitor	Nonsafety-related	Non CAT I	QAL II
Investment Protection Circuitry and Electronics	Non 1E	[TBD]	QAL II

908497/0

Table 1-10

INDUSTRIAL CODES AND STANDARDS APPLICABLE TO THE INVESTMENT PROTECTION SUBSYSTEM DESIGN

[Later]

The design of the Investment Protection Subsystem shall consider the industrial standards given in Table 1-11. (3201.0102.202)

1.2.11 Quality Assurance Requirements

Items designated nonsafety-related, seismic category Non CAT I, or electrical class Non 1E are QAL II or QAL III. QAL II items shall come under a quality assurance program which complies with selected basic requirements and supplements of ANSI/ASME NQA-1 and the four additional supplements from NE F2-10, regarding engineering holds, engineering drawing lists, design review and management assessment. QAL III items shall come under a quality assurance program which complies with selected basic requirements of NQA-1 and the four additional supplements identified above. (3201.0102.210)

Subsystem-level documents are assigned the QAL classification that corresponds to the highest QAL of any item in the subsystem. Therefore, this SSDD is classified as QAL II.

1.2.12 Construction Requirements

A construction plan and schedule shall be developed by the end of preliminary design. The use of models should be considered to facilitate assessments of constructability, particularly in congested areas. (3201.0102.220)

The design of Investment Protection Subsystem shall be based upon parallel construction of the complete plant; however, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3201.0102.221)

The Investment Protection Subsystem design shall utilize shop factory, or field fabricated, assembled and erected components and subsystems to reduce erection costs and to enhance quality controls. (3201.0102.222)

Table 1-11

INDUSTRIAL CODES AND STANDARDS FOR CONSIDERATION IN THE INVESTMENT PROTECTION SUBSYSTEM DESIGN

IEEE Std. 308*	"Criteria for Class 1E Power Systems for Nuclear Power Generating Stations."
IEEE Std. 317	"Standard for Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations."
IEEE Std. 323	"Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
ANSI/IEEE Std. 334	"Type Tests of Continuous Duty Class 1E Motors for Nuclear Power Generating Stations."
ANSI/IEEE Std. 338	"Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems."
IEEE Std. 344	"Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
IEEE Std. 352	"Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems."
ANSI/IEEE Std. 379	"Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems."

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

Table 1-11 (Continued)

IEEE Std. 381	"Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations."
IEEE Std. 382	"Standard for Qualification of Safety-Related Valve Actuators."
ANSI/IEEE Std. 383	"Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations."
IEEE Std. 384	"Criteria for Independence of Class 1E Equipment and Circuits."
IEEE Std. 422	"Guide for the Design and Installation of Cable Systems in Power Generating Stations."
IEEE Std. 518	"Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources."
ANSI/IEEE Std. 577	"Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations."
IEEE Std. 627	"Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations."
ANSI/IEEE/ANS-7432	"Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."

Table 1-11 (Continued)

ANSI/ISA-S67.01	"Transducer and Transmitter Installation for Nuclear Safety Applications."
ISA-S67.02	"Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants."
ISA-S67.04	"Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."
ISA-S67.06	"Response Time Testing of Nuclear Safety-Related Instrument Channels in Nuclear Power Plants."
NEMA-ICS 1	"General Standards for Industrial Control and Systems."
NEMA-ICS 2	"Standards for Industrial Control Devices Controllers and Assemblies."

The Investment Protection Subsystem and its equipment and arrangement features shall facilitate installation, removal, and reinstallation. (3201.0102.223)

Materials, processes, and parts for civil, structural, mechanical, electrical, and instrumentation systems and their components shall be incorporated as required to meet all transportation, handling, storage, construction, and operational functions. Appropriate specifications, codes and code class specifications, and design categories shall be identified to meet safety and economic goals identified for the plant design. Maximum use shall be made of commercial practice typified by fossil-fired facilities. (3201.0102.224)

1.2.13 Decommissioning Requirements

An analysis shall be performed to estimate the cost of decontaminating and dismantling the Investment Protection Subsystem. (3201.0102.230)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The Investment Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant 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. In so doing, it indirectly contributes to protecting the public health and safety, but it is not safety-related equipment. 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 Investment Protection Subsystem consists of the following:

1. Reactor trip using inner control rods.
2. Main loop shutdown.
3. Steam generator isolation dump.
4. Shutdown cooling system initiation.
5. Primary coolant pressure pumpdown.

2.2 SUBSYSTEM CONFIGURATION

The Investment Protection Subsystem 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 plant investment.

The investment protection functions are implemented on a per reactor basis with a remote multiplexed, central controlled, microprocessor based modular protection system. The protection system architecture consists of multiple optical digital data highways from the local multiplex units (satellite modules) communicating with four centrally located, separate, redundant computers to implement the four channel protection subsystems for each reactor module as shown in Fig. 2-1.

The operator interfaces for the Investment Protection Subsystem are located in the control room, the PPIS equipment room, and the remote shutdown area. The operator interfaces include color video displays, function input devices, and keyboards. The remote shutdown area operator interfaces provide the reactor operators the capability of tripping the reactor and taking the necessary actions to shut down the plant, from a position remote from the main control room in the event the main control room becomes uninhabitable.

The design parameters of the Investment Protection Subsystem 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 five supporting trip subsystems. Each trip subsystem consists of four separate (redundant) instrument channels and redundant two-out-of-four coincidence solid-state logic to 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

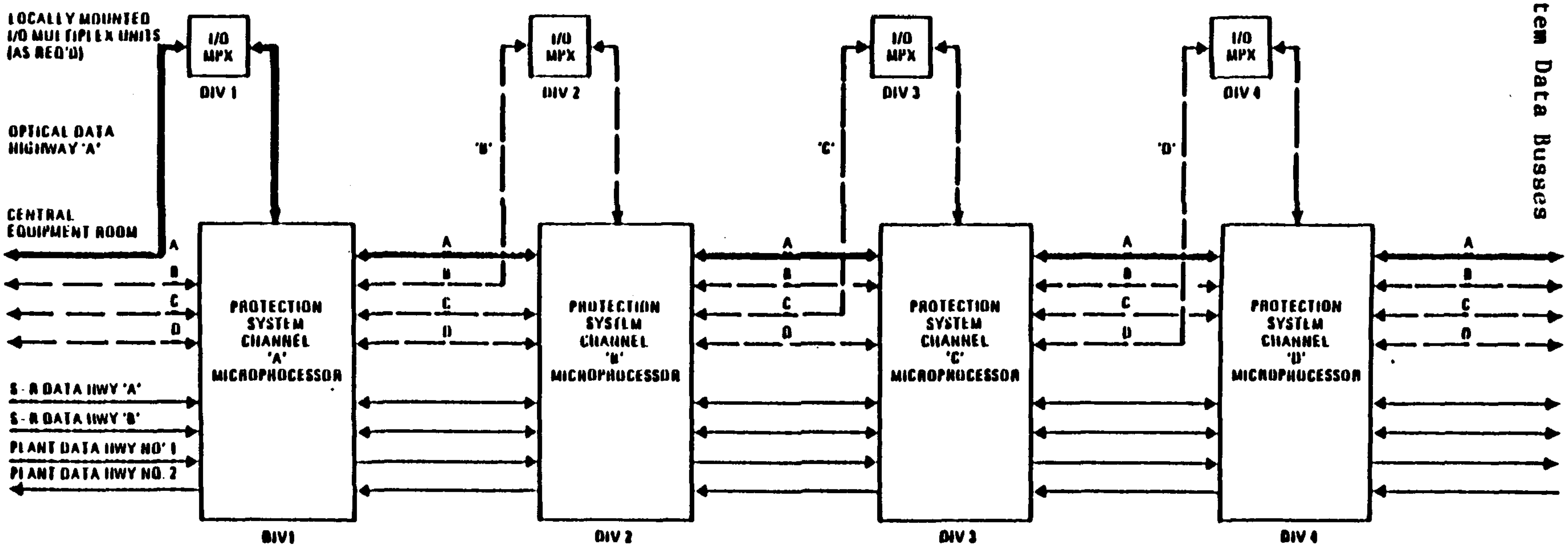

FIG. 2-1 Protection System Data Busses

908497/0

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 Class 1E associated circuits.

The Investment Protection Subsystem is composed of the following 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 nonsafety-related reactor trip subsystem for use during reactor startup and rise to power maneuvering. This subsystem initiates a rapid reduction in reactor power following the receipt of a reactor trip signal from the safety-related outer control rod reactor trip subsystem. The inner control rod reactor trip is inhibited once all six inner control rods are full out and one bank of three outer control rods are full out. This inhibit reduces the investment risk to the inner control rods of possible exposure to elevated conduction cooldown temperatures.

2.2.1.2 Main Loop Shutdown

The Main Loop Shutdown Subsystem limits the temperature of the steam generator tubes and tubesheets and limits the temperature and speed of the helium circulator to protect the steam generator, circulator, and the primary coolant boundary. The temperature and circulator speed are limited by automatically initiating the opening of the main helium circulator motor trip contactors and the closure of the valves necessary to shut off the secondary side of the coolant loop. The primary coolant loop shutoff valve on the circulator compressor inlet is mechanically self-actuating and closes by gravity and opposing pressure rise generated by the shutdown cooling system circulator. There is a separate and independent Main Loop Shutdown Subsystem for each of the reactor modules.

The Main Loop Shutdown Subsystem trip inputs, each derived from four separate and redundant sensor channels, are:

1. Circulator speed high or low (programmed by feedwater flow).
2. Primary coolant pressure low and main steam temperature <u>not</u> low.
3. Steam generator dump and isolation signal.
4. Manual initiation.

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

2.2.1.3 Shutdown Cooling System Initiation

The Shutdown Cooling System Initiation Subsystem starts the shutdown cooling system upon loss of main loop cooling thus reducing thermal cycling of large module components.

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

1. Main loop shutdown.
2. Manual initiation.

2.2.1.4 Steam Generator Isolation and Dump

This 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.

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

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

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

2.2.1.5 Primary Coolant Pressure Pumpdown

The Primary Coolant Pressure Pumpdown 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 radioactive helium into the reactor building. The trip inputs to this subsystem are primary coolant pressure low and reactor building radiation high, or manual initiation.

2.3 SUBSYSTEM PERFORMANCE

The design configuration outlined in Section 2.2 for the Investment Protection Subsystem will detect abnormal plant conditions and actuate equipment to maintain plant parameters within the plant damage thresholds established for the components listed in Table 2-1, preventing damage to components essential for the protection of the plant investment.

The duty cycles given in Table 1-2 govern the design of the Investment Plant Subsystem.

Table 2-1

PLANT DAMAGE LIMITS
FOR USE IN DESIGNING THE INVESTMENT PROTECTION SUBSYSTEM

Component	Damage Limit*
Graphite moderator, reflectors, and core support	Limit graphite/water reaction to less than [TBD].
Fuel particles (TRISO coatings)	Maintain fuel particle temperature ≤{2912}°F.
	Limit fuel/water reaction to less than [TBD].
Movable metal clad poison rods	Maintain control rod structure and cladding temperature ≤1700°F for transient exposure duration (100 h).
Helium circulator	Maintain helium circulator inlet temperature <{1100}°F.
Welded steel vessels	Maintain steel vessel temperature <{700}°F.
Concentric cross ducts	Maintain cross ducts <{1700}°F.
Steel vessel relief valve settings	Maintain primary coolant pressure <{1041} psia.
Steam generator	Maintain helical bundle support plates <{1400}°F.
	Maintain helical superheater tubes ≤{1400}°F.
	Maintain bimetallic weld <{1150}°F.
	Maintain straight tube superheater tube <{1400}°F.
	Maintain steam generator temperature below 300°F before reintroduction of feedwater.

*Numbers in { } are estimated and subject to change.

908497/0

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

2.3.1 Subsystem Operating Modes

In general the trip portion of the Investment Protection Subsystem is operable during all plant. The status of the 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 protection system portions of the Investment Protection Subsystem out of service is governed by the plant operating procedures.

Table 2-4 gives the operating mode of the Investment Protection Subsystem versus plant conditions.

2.3.2 Subsystem Steady State Performance

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

2.3.3 Subsystem Response to Plant Transients

The Investment Protection Subsystem design basis is the subject of continuing design basis analysis. The purpose of this design basis analysis is twofold:

1. To establish and confirm characteristics of the Investment Protection Subsystem (in particular, trip sensing measurements and actuator response).

2. To establish limiting transients that can be imposed on major equipment components.

Table 2-2

INVESTMENT PROTECTION SUBSYSTEM
PROTECTIVE ACTIONS

Protective Action	Conditions for Completion of Protective Action	Time for Protection Action to Continue
Reactor Trip Using Inner Control Rods	Insertion of enough negative reactivity to achieve a minimum 0.010Δk shutdown margin	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 psig)}* above reactor vessel pressure and closed again.	Until dump and isolation is complete
Main Loop Shutdown	All main loop isolation valves closed and circulator motor contactors open.	Sensor channel: Until shutdown signal 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.

*Numbers in { } are estimataed and subject to change.

908497/0

Table 2-3

INVESTMENT PROTECTION SUBSYSTEM
ACTUATED EQUIPMENT

Actuated Equipment	Maximum Response Time
Inner Control Rods	
Actuating Subsystem: Reactor Trip using inner control rods	{25 s}* for full insertion
Steam Generator Dump Valves	
Actuating Subsystem: Steam Generator Isolation & Dump Four dump valve matrix per steam generator	{5 s} to open {5 s} to close
Main Loop Isolation Valves and Circulator Trip Motor Contactors	
Actuating Subsystem: Main Loop Shutdown	
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

*{ } = Numbers are estimated and subject to change.

Table 2-4

INVESTMENT PROTECTION SUBSYSTEM
OPERATING MODE VERSUS PLANT CONDITION

Plant Condition	Operating Mode	Remarks[1]
1.1 Energy production	Operable	
1.2 Shutdown	Shutdown/operable	Portions of system may be shut down for maintenance
1.3 Refueling	Operable	Portions of system may be shut down for maintenance
1.4 Startup and shutdown	Operable	
2.0 Maintain plant protected	Operable/operating	Portion operating depends upon portion of plant in need of protection
3.0 Radiological release controlled	Operable/operating	
4.0 Emergency plan activated	Operable	

(1) Trip portions operate as necessary during abnormal plant events.

Investment Protection Subsystem trip parameters used during Design Basis Event (DBE) analysis are shown in Table 2-5.

2.3.3.1 AOO Performance

The response of the Investment Protection Subsystem to AOOs is described in this section. No other system's performance is described even though other systems may also respond to these AOOs.

AOO No. 1(A) Loss of Main Loop Cooling. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown is commanded. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown in turn signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for shutdown cooling system initiation.

AOO No. 1(B) Loss of Offsite Power and Turbine Trip. The response of the Investment Protection Subsystem to AOO No. 1(B) is identical to AOO No. 1(A).

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

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

Table 2-5 Investment Protection Subsystem Analysis 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 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	

9084970

Table 2-5 (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	No	HTS circulator speed high or low programmed by feedwater flow	±[1487] rpm	±[1144] rpm	HTS circulator speed (s)	0 s	[10]* ms	1 s	1 s	Circulator motor contactors	[1] s to open	Circulator speed measurement from reserve shutdown circulator speed measurement
					Feedwater flow (F)	0 s	[2] s			Feedwater block valves	[5] s to close	
										Superheat outlet stop/check valves	[10] s to close	
	No	Primary coolant pressure low and	[625] psia and	[640] psia and	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s			Helium pressure measurement from reactor trip pressure measurement
		main steam temperature not low	≥[725]°F	≥[740]°F	Main steam temperature (T_{ms})	0 s	[20] s					
	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 and Subject to Change

90849/0

Table 2-5 (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 <u>high</u>	1200 ppmv	1000 ppmv	Moisture concentration (M)	[20] s	[5]* s	0 s	1 s	Main loop shutdown	(See main loop shutdown)	
										Steam generator dump valves	[5] s to open	
Steam generator dump terminate	No	Main steam pressure to primary coolant pressure ΔP <u>low</u>	[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 (P)	0 s	[2] s					
Primary coolant pressure pumpdown with helium purification system	No	Primary coolant pressure <u>low</u> <u>and</u>	[800] psia	[810] psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s	Helium purification system	[TBD] s	
		reactor building radiation <u>high</u>	TBD mR/h	TBD mR/h	Reactor building radiation (R)	TBD	TBD	TBD				
Shutdown cooling system (SCS) start	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	

*[ ] = Number Tentative and Subject to Change

908497/0

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

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

AOO No. 4 Small Steam Generator Leak. The moisture monitor detects high primary coolant moisture concentration and commands reactor trip using the outer control rods and steam generator isolation and dump. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Steam generator isolation is performed by main loop shutdown. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and 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 close. Main loop shutdown also signals for shutdown cooling system initiation.

AOO No. 5 Small Primary Coolant Leak. When the primary coolant pressure decreases to the low setpoint and high reactor building radiation is detected the Helium Purification System is commanded to begin a primary coolant pumpdown to perform controlled depressurization of the primary coolant. When the primary coolant pressure reaches a lower setpoint and the main steam temperature has not reached saturation temperature, a main loop shutdown is commanded to prevent steam generator quench. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown also signals for Shutdown Cooling System initiation.

2.3.3.2 DBE Performance

The response of the Investment Protection Subsystem to DBEs is described in this section. No other system's performance is described even though other systems may also respond to these DBEs.

DBE No. 1 Loss of HTS and SCS Cooling. The initiating event for DBE No. 1 is loss of offsite power and turbine trip. A loss of offsite power and turbine trip causes a loss of all primary AC power supplies. This causes the main loop helium circulator to coastdown due to loss of power. This is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown in commanded. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown in turn signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for shutdown cooling system (SCS) initiation but the SCS fails to start due to failure of standby ac power.

DBE No. 2 HTS Transient Without Control Rod Trip. Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. For this DBE, the outer control rods fail to trip. Main loop shutdown also signals for Shutdown Cooling System initiation.

DBE No. 3 Control Rod Withdrawal Without HTS Cooling. The initiating event for DBE No. 3 is an inadvertent control rod bank withdrawal. DBE No. 3 also includes a main loop upset. This is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown is commanded. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation.

DBE No. 4 Control Rod Withdrawal Without HTS and SCS Cooling. The response of the Investment Protection Subsystem to DBE No. 4 is identical to DBE No. 3 but DBE No. 4 also includes SCS failure to start.

DBE No. 5 Large Earthquake With SCS Cooling. 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 as a circulator speed to feedwater flow mismatch and a main loop shutdown is commanded. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation.

The Investment Protection Subsystem and its auxiliary supporting features are designed to withstand a safe shutdown earthquake (SSE) and perform their functions.

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

The moisture monitor detects high primary coolant moisture concentration and commands reactor trip using the outer control rods and commands steam generator isolation and dump. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Steam generator isolation is performed as a main loop shutdown. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and 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.

DBE No. 7 Moisture Inleakage Without SCS Cooling. The response of the Investment Protection Subsystem to DBE No. 7 is identical to DBE No. 6 but DBE No. 7 also includes SCS failure to start.

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 moisture monitor is assumed to fail to detect the moisture ingress. The reactor operator performs a manual initiation of steam generator isolation and dump.

Steam generator isolation is performed as a main loop shutdown. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and 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 close. Main loop shutdown also commands a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for Shutdown Cooling System initiation.

DBE No. 9 Moisture Inleakage With Steam Generator Isolation and Failure to Reclose the Dump System. The initiating event for DBE No. 9 is a small steam generator leak and subsequent small moisture ingress rate. The moisture monitor detects high primary coolant moisture concentration and commands reactor trip using the outer control rods and commands steam generator isolation and dump. This reactor trip is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Steam generator isolation is performed as a main loop shutdown. The main loop shutdown trips the main helium circulator, closes the feedwater block valves, and 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 dump valve failure to reclose causes a slow primary coolant depressurization. When the primary coolant pressure decreases to the low setpoint and high reactor building radiation is detected, the Helium Purification System is commanded to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant.

DBE No. 10 Primary Coolant Leak With HTS Cooling. 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 decreases to the low setpoint and high reactor building radiation is detected the Helium Purification System is commanded to begin a primary coolant pumpdown to perform a controlled depressurization of the primary coolant. This pumpdown is assumed to be ineffective because of the size of the primary coolant leak.

When the primary coolant pressure decreases to a lower setpoint and main steam temperature is still above satuaration a main loop shutdown is commanded to prevent steam generator quench.

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. This DBE assumes that the main cooling loop is upset 15 h into the DBE.

Trouble with the main cooling loop is detected as a circulator speed to feedwater flow mismatch and a main loop shutdown is commanded. The main circulator is tripped, the feedwater block valves are closed, and the superheat steam valves are closed. Main loop shutdown signals a reactor trip using the outer control rods. This reactor trip signal is in addition to any safety-related reactor trip commanded by the Safety Protection Subsystem. Main loop shutdown also signals for Shutdown Cooling System (SCS) initiation.

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

2.3.3.3 <u>SRDC Performance</u>

The Investment Protection Subsystem is not classified as safety-related; therefore, this section is not applicable.

2.3.4 <u>Failure Modes and Effects</u>

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

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

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

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

The general failure modes of the system are given in Table 2-6.

Table 2-6

FAILURE MODES OF INVESTMENT PROTECTION SUBSYSTEM

Subsystem	Subsystem Design Characteristic
Reactor trip using inner control rods	De-energize to trip
Steam generator isolation dump	Energize to trip
Main loop shutdown	Energize to trip
Shutdown Cooling System initiation	Energize to trip

2.4 SUBSYSTEM ARRANGEMENT

The Investment Protection Subsystem is arranged into modular electronic components with four separate channels. Each of the four MHTGR reactor modules has a separate four channel Investment Protection Subsystem. The components for each reactor module are associated with that reactor module. The operator interface equipment for the Investment Protection Subsystem is provided by the Special Nuclear Area Instrumentation and is located in the control room, PPIS equipment room, and remote shutdown area. These functional components of the Plant Protection and Instrumentation System and their locations are shown in Fig. 2-2.

A list of and specific locations of the Investment Protection Subsystem equipment is given in Table 2-7.

2.5 INSTRUMENTATION AND CONTROL

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

Fig. 2-2 Arrangement of PPIS Equipment

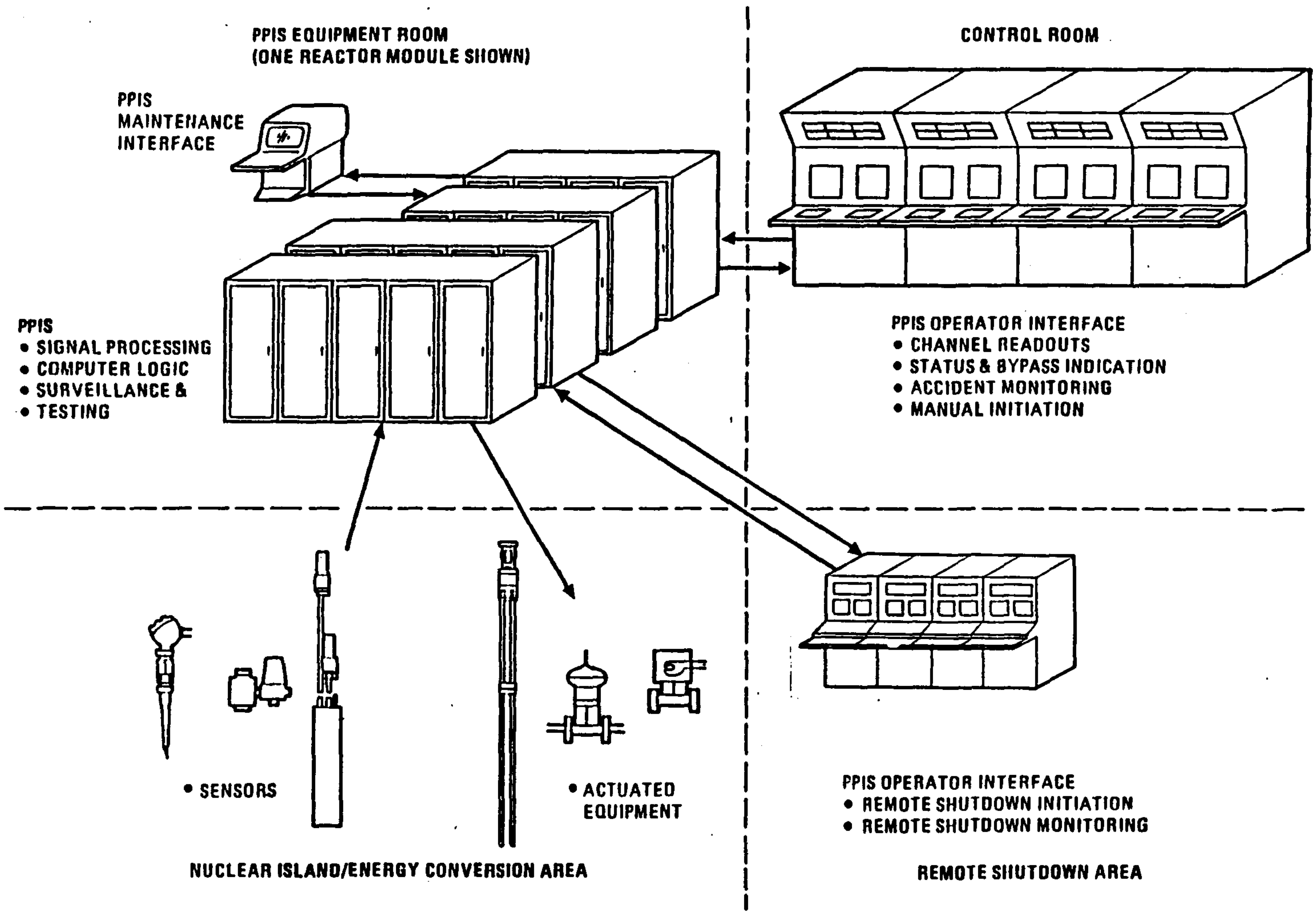

Table 2-7

INVESTMENT PROTECTION SUBSYSTEM EQUIPMENT

Equipment Number	Equipment Name	Quantity Required for MHTGR Plant	Equipment Location
I-3216-1/4-A/D	Investment protection modules	16	PPIS equipment room
I-3211/15-A/D	Investment protection satellite modules	20	Reactor building
S-3201-A/D	Hygrometer module assemblies	4	Reactor building
S-3202-A/D	Compressor modules	4	Reactor building
T-3201-A/D	Accumulator tanks	4	Reactor building
S-3203-A/D	Non-module equipment	4 lots	Reactor building
Z-3201-A/D	Instruments, hardware, and software	4 lots	All of above

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

3.1 COMPONENT FUNCTIONS

[Later]

3.2 COMPONENT DESIGN REQUIREMENTS

[Later]

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

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

4.2 COMPONENT BOUNDARY DEFINITION

The Investment Protection Subsystem is the sense and command portion of the protection systems. It interfaces with various plant systems which provide the actuate portion of the protection system.

The Investment Protection Subsystem (along with other plant systems) provides signal inputs to the Special Nuclear Area Instrumentation Subsystem.

Table 4-1

INVESTMENT PROTECTION SUBSYSTEM
INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS
(Given on a per reactor module basis)

4.1.1 Identification of Interfaces

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.1 Reactor Service Group (2000)			
Helium Purification Subsystem (2023)	Provide reprocessing of primary helium coolant extracted by the moisture monitors.	Piping.	Quantity: One sample line per module. (3201.0401.010)
Essential Cooling Water Subsystem (2042)	Provide cooling water to the moisture monitors.	Piping.	Quantity: Two coolers per module. (3201.0401.014)
Gaseous Radioactive Waste Subsystem (2064)	Provide gaseous radioactive waste management for the moisture monitors.	Piping.	Quantity: One waste line per module. (3201.0401.016)
4.1.1.2 Heat Transport System (2100)			
Main Circulator Subsystem (2101)	Provide for installation of moisture sample rake at the outlet of main circulator.	Piping.	Quantity: Four independent sample rakes. (3201.0401.020)
Steam Generator Subsystem (2102)	Provide for installation of protection system sensors to measure primary coolant parameters.	Piping.	Quantity: Four low range pressure transmitters to measure primary coolant pressure for use in steam generator dump termination. (3201.0401.024)

908497/0

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
	Provide steam generator penetrations to accommodate Investment Protection Subsystem sensors.	Steam generator penetrations.	<u>Quantity</u>: Four steam generator inlet thermowell access penetrations. (3201.0401.026)
4.1.1.3 <u>Miscellaneous Control and Instrumentation Group</u> (3000)			
Radiation Monitoring Subsystem (3003)	Provide signals for monitoring reactor building radiation to act as an input to the primary coolant pumpdown system.	Electrical signals.	<u>Quantity</u>: Four separate signals. (3201.0401.030)
4.1.1.4 <u>Plant Protection and Instrumentation System</u> (3200)			
Special Nuclear Area Instrumentation Subsystem (3203)	Provide monitoring of input channels and system status.	Isolated output electrical signals.	<u>Quantity</u>: Each input, each bypass, and output. (3201.0401.040)
4.1.1.5 <u>Plant Control, Data, and Instrumentation System</u> (3700)			
NSSS Control Subsystem (3701)	Adjust control system settings following investment protection trips.	Electrical signals.	<u>Quantity</u>: Five (reactor trip inner rods, main loop shutdown, SG isolation and dump, SCS initiation, and primary pressure pumpdown). (3201.0401.050)

908497/0

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.6 Power Conversion Group (5000)			
Feedwater and Condensate Subsystem (5002)	Provide for installation of feedwater flow transmitters monitoring the steam generator feedwater inlet line to act as an input sensor channel to the Investment Protection Subsystem.	Electrical signals.	Quantity: Four feedwater flow transmitters monitoring the steam generator feedwater inlet pipe. (3201.0401.060)
Main and Bypass Steam Subsystem (5004)	Provide for installation of thermowell assemblies in the superheater outlet lines to act as an input sensor channel to the Investment Protection Subsystem.	In pipe thermowell.	Quantity: Four resistance thermometers in the superheater outlet pipe. (3201.0401.064)
	Provide for installation of pressure transmitters in superheater outlet pipe to measure superheat steam pressure for use in steam generator dump termination.	Valved pressure tap in piping.	Quantity: Four pressure transmitters in the superheater outlet pipe. (3201.0401.066)
	Provide superheater outlet valves in the steam generator outlet pipe to act as actuated equipment for the main loop shutdown subsystem.	Electrical signals.	Quantity: Two superheater outlet valves for the steam generator. (3201.0401.068)

908497/0

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.7 <u>Building, Structures, and Building Service Group</u> (7000)			
Reactor Building (7001)	Provide building space and structural support to accommodate Investment Protection Subsystem	Floor mounting, piping, and electrcal.	<u>Quantity</u>: Nine cabinets, one hygrometer module, one compressor assembly, and one accumulator tank assembly. (3201.0401.090)
4.1.1.8 <u>Mechanical Service Group</u> (9000)			
HVAC (9011)	Provide HVAC to support the proper operation of the Investment Protection Subsystem.	None.	<u>Quantity</u>: Two. (3201.0401.100)
4.1.1.9 <u>Electrical Group</u> (9200)			
Non-Class 1E AC Distribution (9202)	Provide low-voltage ac distribution for the moisture monitor compressors.	Electric feeders.	<u>Quantity</u>: Two. (3201.0401.110)
Class 1E Uninterruptible Power Supply (9205)	Provide separate Class 1E uninterruptible power distribution channels to power the Investment Protection Subsystem as a 1E associated circuit.	Electric feeders.	<u>Quantity</u>: Four separate Class 1E sources. (3201.0401.112)

908497/0

SECTION 5

SUBSYSTEM CONSTRUCTION

The construction of the Investment Protection Subsystem will be planned and scheduled so that its components will fit up properly with all its interfacing systems, subsystems, and components. 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 Investment Protection Subsystem 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 Investment Protection Subsystem 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 Investment Protection Subsystem. 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 Investment Protection Subsystem equipment/components shall be stored in closed temperature 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 Investment Protection 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 Investment Protection Subsystem 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 Investment Protection Subsystem. 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 Investment Protection Subsystem 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 primary coolant 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 Investment Protection Subsystem 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

SUBSYSTEM OPERATION

6.1 SYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

6.1.1 Operating Limits and Setpoints

Trip set points are conservatively established to assure that component damage limits are not reached. Figure 6-1 illustrates the relationship between trip set points 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 set points) are conservatively bounded by the limiting protection system settings with allowance for instrument and set point drift. The lower set point 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 Investment Protection Subsystem are shown in Table 6-1.

6.1.2 Precautions

Design features are included to assist the operator in verifying that Investment Protection Subsystem degree of redundancy of at least one is always maintained. For example, whenever any essential protection system component is bypassed, such that a protection group is inoperable, a

DAMAGE THRESHOLD

DESIGN LIMIT/PROCESS LIMIT

TRANSIENT OVERSHOOT

ANALYSIS TRIP LEVEL

ALLOWANCE FOR CALIBRATION
ERRORS, INSTRUMENT ACCURACY

LIMITING PROTECTION
SYSTEM SETTING (ALLOWABLE VALUE)

ALLOWANCE FOR INSTRUMENT AND
SETPOINT DRIFT

-- UPPER SETPOINT LIMIT

ACTUAL PROTECTION
SYSTEM SETTING (TRIP SETPOINT)

-- LOWER SETPOINT LIMIT

ALLOWANCE TO PREVENT
UNNECESSARY TRIPS

MAXIMUM NORMAL OPERATING
TRANSIENT VALUE (OPERATIONAL LIMIT)

NORMAL OPERATING RANGE

Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS
AND COMPONENT DAMAGE LIMITS

Table 6-1

OPERATING LIMITS AND SETPOINTS FOR THE INVESTMENT PROTECTION SUBSYSTEM

	Operating Limit (Limiting Protection Subsystem Setting)	Nominal Setpoint (Actual Protection System Setting)
Reactor Trip Using Outer Control Rods		
Steam generator helium inlet temperature	[TBD]°F	{1375}°F*
Primary coolant moisture concentration	[TBD] ppmv	{1000} ppmv
Main Loop (HTS) Shutdown		
Circulator speed high or low (programmed by feedwater flow)	[TBD] rpm	{±1144} rpm
Primary coolant pressure	[TBD] psia	{640} psia
Main steam temperature	[TBD]°F	{740}°F
Steam Generator Isolation And Dump		
Primary coolant moisture concentration	[TBD] ppmv	{1000} ppmv
Superheater steam pressure to primary coolant pressure for steam generator dump terminate)	[TBD] psid	{75} psid
Primary Coolant Pressure Pumpdown (with Helium Purification System)		
Primary coolant pressure, MPa absolute	[TBD] psia	{810} psia
Reactor building radiation	[TBD] mr/h	[TBD] mr/h

*Numbers in { } are estimated and subject to change.

continuous protection system bypass indication/alarm is displayed in the main control room. Whenver one protection channel of the two-out-of-four logic is disconnected or bypassed, maintains a degree of redundancy of one. Whenever a one-out-of-two actuation device is disconnected or bypassed, the time of inoperability will be kept to a minimum and will be within acceptable protection system reliability analysis constraints as specified in Section 1.2.7.

Whenever the two-out-of-four logic protection system is operated with one channel tripped (i.e., the remaining channels in a one-out-of-three operating mode) extreme care 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 Investment Protection Subsystem 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. Steam Generator Isolation and Dump
2. Main Loop Shutdown
3. Shutdown Cooling System Initiation
4. Primary Coolant Pressure Pumpdown

5. Moisture Monitor/Detection Equipment

6.2.2 Routine Preoperational Checkout

The following prerequisites are required for routine preoperational checkout:

1. Control room operable.

2. Reactor building instrument equipment area operable.

3. Uninterruptible power sources operable.

4. Special Nuclear Area Instrumentation Subsystem operating.

5. Heat Transport System instrumentation operable.

6. Feedwater and Condensate System instrumentation operable.

7. Main steam and turbine bypass instrumentation operable.

Checkout Procedure

In general, the following steps are governed by the Plant O&M Procedures. Some steps may be bypassed during any specific plant startup provided that the system is still current in accordance with the Plant O&M Procedures (for example, sensor calibration or actuation device exercising need not be performed upon each startup if the plant procedures 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, etc.).

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. Electrical systems operating.
3. Heat Transport System operating.
4. Reactor Cavity Cooling System operating.
5. HVAC systems operating.
6. Heat rejection group operating.
7. Power conversion group operating (in particular feedwater and condensate; and steam and water dump subsystems).
8. Reactor Vessel System operating.
9. Shutdown Cooling System operable.
10. Reactor System operable.
11. Plant Control Data and Instrumentation System operating.
12. Helium Purification Subsystem operating.

6.3.1.2 Procedure

The startup procedure includes:

1. Reset trip circuitry as required.

2. Withdraw control rods in prescribed sequences as determined by reactivity control system, equipment heatup rates, etc.

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

4. Observe that the bypass of the reactor trip times rods operates as designed.

6.3.2 Shutdown from 25% Steam Flow

The shutdown procedure includes:

1. Inserting control rods in prescribed sequences as determined by the reactor control subsystem at a low power level.

2. Monitoring plant and protection system status periodically to ascertain that reactivity and core cooling 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 preestablished schedules.

6.5 REFUELING

Monitor plant and protection system status periodically to ascertain that reactivity and core cooling are being maintained.

6.6 SHUTDOWN

A plant shutdown can be initiated either with the normal station controls (planned shutdown) or automatically by the protection subsystem. During plant shutdown the plant status should be monitored by the operator periodically to ascertain that reactor shutdown and core cooling are being maintained.

Shutdown of the entire Investment Protection Subsystem to perform maintenance is generally not required due to the redundancy of the channels. To the extent possible, maintenance and partial shutdown of the Investment Protection Subsystem should be done during scheduled plant shutdowns. Inadvertent shutdowns of redundant portions of the Investment Protection Subsystem can result in unprotected plant operation due to the characteristics of the design.

6.6.1 Automatic Plant Shutdowns

The Investment Protection Subsystem automatically initiates reactor trip 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 may 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 events. Following automatic protective action, the following operator actions should be taken:

1. Verify that redundant portions of the investment protection subsystem have tripped. (Note any abnormal or suspicious investment protection subsystem behavior for review.)

2. Verify that the inner control rods actually have inserted and neutron flux is decreasing upon a reactor trip. Manually initiate any required actions that have not automatically occurred.

3. Ensure that reactivity and core cooling 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 procedures.

6. Plant restart will 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 Investment Protection Subsystem performance was per design.

6.6.2 Investment Protection Subsystem Shutdown

Ensure the associated equipment for which its protection is provided is shut down prior to shutting off electrical power to the instrumentation (loss of electrical power in more than one redundant channel can cause a reactor trip, conversely shutoff of redundant sources of electrical force may result in loss of protection to portions of the plant).

6.7 ABNORMAL OPERATION

Abnormal operation of the Investment Protection Subsystem is limited to operation with the subsystem operating in a degraded mode (failed or inoperable equipment).

The Investment Protection Subsystem is configured so as to not adversely affect plant safety or plant availability in conjunction with a single failure. Therefore, a single failed component of 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 undesireable because a second channel trip will result in an unwanted subsystem trip. The Investment Protection Subsystem may be run in a degraded condition as long as a degree of redundancy of one is maintained.

6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES

[Later]

SECTION 7

SUBSYSTEM MAINTENANCE

[TBD]

SECTION 8

SUBSYSTEM DECOMMISSIONING

[TBD]

SECTION 9

REFERENCES

1.1 Overall Plant Design Specification Modular Gas-Cooled Reactor, HTGR-86-004, Rev. 2, (HFS-20100, Rev. 2) (908397, Rev. 2), March 1986.

APPENDIX A

TRACEABILITY OF REQUIREMENTS

1. INTRODUCTION

This Appendix provides traceability of requirements to sources within the Investment Protection SSDD and to sources in external documents. The requirement traceability summary (Table A-1) identifies the requirement provides a summary description and identifies the source. A list of the references which are identified as sources in Table A-1 is included.

Each requirement is given a traceability number which is composed of three groups of digits. The first group identifies the subsystem (e.g., 3201); the second group identifies the section and subsection numbers of this document where the requirement is located (e.g., 0102 for SSDD Section 1, Subsection 2); and the third group identifies the sequential requirement number (e.g., 001 for Requirement 1).

Table A-1

PPIS TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

Traceability Number	Summary Requirement Description	Source Ref.	Description/Reference Section
3201.0102.001	Formal design	1	3.2.1
3201.0102.002	Nuclear island configuration	1	3.2.1
3201.0102.003	Minimize inaccessible areas	1	3.2.1
3201.0102.004	Control and protection independence	1	3.2.1
3201.0102.005	Protection subsystem configuration of investment	1	3.2.1
3201.0102.006	Two-out-of-four sense and command logic	1	3.2.1
3201.0102.007	Investment Protection Subsystem configuration	1	3.2.1
3201.0102.008	Investment Protection Subsystem configuration	1	3.2.1
3201.0102.009	Investment Protection Subsystem configuration	1	3.2.1
3201.0102.010	Investment Protection Subsystem configuration	1	3.2.1
3201.0102.011	Investment Protection Subsystem configuration	1	3.2.1
3201.0102.012	Sensor channel requirements	1	3.2.1
3201.0102.015	Mid 1990's start of operation	1	3.2.1
3201.0102.016	40-year load cycle	1	3.2.1
3201.0102.017	Duty cycle events	1	3.2.1
3201.0102.018	Reactor/turbine generator combinations	1	3.2.1
3201.0102.019	Confirmation through analysis	1	3.2.1

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3201.0102.020	Design transients	1	3.2.1
3201.0102.021	Overall functional requirement for the design of the Investment Protection Subsystem	1	3.2.1
3201.0102.022	Operation by minimum staff	1	3.2.1
3201.0102.023	Graphite moderator, reflectors, and core support graphite/water reaction	1	3.2.1
3201.0102.024	Fuel/water reaction	1	3.2.1
3201.0102.025	Fuel particle temperature limits	1	3.2.1
3201.0102.026	Control rod structure and cladding temperature limits	1	3.2.1
3201.0102.030	Limit helium circulator temperature	1	3.2.1
3201.0102.031	Limit helium circulator speed	1	3.2.1
3201.0102.035	Steel vessels temperature limits	1	3.2.1
3201.0102.036	Steel vessels pressure limits	1	3.2.1
3201.0102.040	Steel vessel relief valve setting	1	3.2.1
3201.0102.045	Heat exchanger helical bundle support plates	1	3.2.1
3201.0102.046	Heat exchanger helical superheater tubes temperature limits	1	3.2.1
3201.0102.047	Heat exchanger bimetallic weld temperature limits	1	3.2.1

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Ref.	Description/Reference Section
3201.0102.048	Heat exchanger straight tube superheater tubes temperature limits	1	3.2.1
3201.0102.049	Steam generator temperature limit for FW restart	1	3.2.1
3201.0102.100	Mechanical requirements for cabinet, rack, and panel design	1	3.2.1
3201.0102.105	Seismic design	1	3.2.1
3201.0102.106	Seismic response spectra	1	3.2.1
3201.0102.107	Seismic damping coefficients	1	3.2.1
3201.0102.110	Materials	1	3.2.1
3201.0102.120	Operating environments	1	3.2.1
3201.0102.130	Requirement for remote shutdown	1	3.2.1
3201.0102.150	Availability	1	3.2.1
3201.0102.151	System outage requirements allocation	1	3.2.1
3201.0102.152	System reliability requirements allocation	1	3.2.1
3201.0102.153	Design modifications for availability improvement	1	3.2.1
3201.0102.154	Provide functional testing	1	3.2.1
3201.0102.155	Hands-on maintenance	1	3.2.1
3201.0102.156	Planned outage schedule	1	3.2.1

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Ref.	Description/Reference Section
3201.0102.157	Man-hour requirements	1	3.2.1
3201.0102.158	"Off-the shelf" components	1	3.2.1
3201.0102.159	Spare parts listing	1	3.2.1
3201.0102.160	Parts interchangeability	1	3.2.1
3201.0102.161	Arrangement to facilitate on-line maintenance	1	3.2.1
3201.0102.162	Design to facilitate hands-on maintenance	1	3.2.1
3201.0102.163	Monitoring as basis for maintenance diagnostics	1	3.2.1
3201.0102.164	Plant staffing	1	3.2.1
3201.0102.165	Remote maintenance	1	3.2.1
3201.0102.166	On-line in-service inspection	1	3.2.1
3201.0102.180	Equipment classification	1	3.2.1
3201.0102.200	Codes and standards	1	3.2.1
3201.0102.201	Codes and standards	1	3.2.1
3201.0102.202	Codes and standards	1	3.2.1
3201.0102.210	Quality identification (QAL II, III)	1	3.2.1
3201.0102.211	Document QAL classification	1	3.2.1
3201.0102.220	Construction plan and schedule	1	3.2.1

908497/0

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3201.0102.221	Parallel construction	1	3.2.1
3201.0102.222	Utilization of shop, factory or field fabricated parts	1	3.2.1
3201.0102.223	Arrangement features	1	3.2.1
3201.0102.224	Materials, processes and parts	1	3.2.1
3201.0102.230	Decommissioning	1	3.2.1
3201.0401.010	Reprocessing of primary coolant from moisture monitor system	2	2.2.1.4
3201.0401.014	Cooling of moisture monitoring sample flow	2	2.2.1.4
3201.0401.016	Recovery of gaseous waste from moisture monitors	2	2.2.1.4
3201.0401.020	Installation of moisture monitor rake	2	2.2.1.4
3201.0401.024	Installation of pressure transmitters to steam generator	2	2.2.1.4
3201.0401.026	Thermowell penetrations in steam generator	2	2.2.1.2
3201.0401.030	Radiation monitoring inputs to primary coolant pumpdown	2	2.2.1.5
3201.0401.040	Status monitoring	2	2.2.1
3201.0401.050	NSSS Control Subsystem adjustment following trips	2	2.2.1
3201.0401.060	Installation provisions for feedwater flow transmitters	2	2.2.1.2
3201.0401.064	Thermowell assemblies in superheater piping	2	2.2.1.2

908497/0

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Ref.	Description/Reference Section
3201.0401.066	Pressure transmitter installation in superheater piping	2	2.2.1.4
3201.0401.068	Superheater outlet valves	2	2.3
3201.0401.090	Building space for Investment Protection Subsystem equipment	2	2.4
3201.0401.100	HVAC requirements for Investment Protection Subsystem equipment	2	2.2
3201.0401.110	Electric power for moisture monitor compressors	2	2.2.1.4
3201.0401.112	Uninterruptible power for Investment Protection Subsystem	2	2.2

Table A-2

TRACEABILITY SUMMARY REFERENCE LIST

1. "Plant Protection and Instrumentation System Design Description 4 x 350 MW(t) HTGR Side-by-Side Steel Vessel," HFD-33200, Rev. 0 (908444, Rev. 0).

2. "Investment Protection Subsystem Design Description," HFD-43201, Rev. 0 (908497, Rev. 0).

APPENDIX B

DRAWINGS

Drawing Number	Title
GA Drawing [later]	IB Diagram - MHTGR Functional Overview Protection Subsystems
GA Drawing [later]	IB Diagram - MHTGR Safety and Investment Protection Subsystems

APPENDIX C

TRANSIENTS

[LATER]

APPENDIX D

DESIGN BASIS SEISMIC INPUTS

[LATER]

APPENDIX E

PARAMETER LISTS

[LATER]

APPENDIX F

PROPRIETARY CLAIMS

[LATER]