VOLUME VII

HTGR

MHTGR CONCEPTUAL DESIGN PACKAGE PLANT CONTROL, PLANT PROTECTION & PLANT MONITORING SYSTEMS

[redacted]

ISSUED BY GAS-COOLED REACTOR ASSOCIATES FOR
THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

DECEMBER 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

MHTGR CONCEPTUAL DESIGN PACKAGE

Table of Contents

VOLUME I -PLANT LEVEL REQUIREMENTS AND LICENSING

	Foreword	09/87
- GCRA	MHTGR Design Document Index	09/87
- GCRA 86-002/3	Utility/User Requirements for the MHTGR	06/87
- HTGR-86-004/5	Overall Plant Design Specification -MHTGR	06/87
-	MHTGR Design Document Index	09/87
- HTGR-86-034/1	Licensing Basis Events for the Standard MHTGR	02/87
- HTGR-86-017/1	Applications of Bridging Methods for the Standard HTGR Licensing Basis	02/86
- HTGR-86-001/1	Licensing Basis Event Selection Criteria	02/86
- HTGR-85-002/2	Top Level Regulatory Criteria for the Standard HTGR	10/86
- HTGR-85-001/4	Licensing Plan for the Standard MHTGR (Draft)	11/86

VOLUME II - PLANT LEVEL ANALYSIS

- HTGR-86-105/1	Expected Module Performance for the MHTGR Plant	07/87
- HTGR-86-121/1	MHTGR Plant Design Basis Transient Analysis	04/87
- GA/908934	Plant Control System Design Report: NSSS Control Subsystem	09/86
- HTGR-86-069/1	Forced Outage Assessment for the MHTGR	07/87
- HTGR-86-119	FY-1986 Seismic Assessment 4 x 350 MW(t) Modular HTGR Plant	09/86
- HTGR-86-090	Radiological Dose Assessment Report	09/86
- HTGR-86-089	Site Personnel Dose Assessment Report Modular HTGR Plant	09/86
- HTGR-87-086	MHTGR Plant Capital and Busbar Generation Cost Estimate Report	09/87

VOLUME III - PLANT FUNCTIONAL ANALYSIS

- HTGR-86-002/3	Functional Analysis Report Standard Modular HTGR Plant	06/87

VOLUME IV - REACTOR & REACTOR VESSEL SYSTEMS

- HTGR-86-035/1	Reactor SDD	07/87
- HTGR-86-100/1	Neutron Control SSDD	07/87
- HTGR-86-055/1	Reactor Internals SSDD	07/87
- HTGR-86-036/1	Reactor Core SSDD	07/87
- HTGR-86-125/1	Reactor Vessel SDD	07/87

Table of Contents

VOLUME V - REACTOR VESSEL & REACTOR SERVICE SYSTEMS

- HTGR-86-126/1	Vessels and Duct SSDD	07/87
- HTGR-86-127/1	Pressure Relief SSDD	10/86
- HTGR-86-128/1	Vessel Support SSDD	07/87
- HTGR-86-102	Reactor Service Equipment SSDD	09/86
- HTGR-86-103/1	Helium Purification SSDD	09/87
- HTGR-87-069	Helium Storage and Transfer SSDD	07/87
- HTGR-87-070	Liquid Nitrogen SSDD	07/87
- HTGR-87-071	Reactor Plant Cooling Water SSDD	07/87
- HTGR-87-072	Hot Service Facility SSDD	07/87
- HTGR-87-073	Decontamination Service SSDD	07/87
- HTGR-87-021	Liquid Radioactive Waste SSDD	06/87
- HTGR-87-022	Gaseous Radioactive Waste SSDD	06/87
- HTGR-87-023	Solid Radioactive Waste SSDD	06/87

VOLUME VI - HEAT TRANSPORT & FUEL HANDLING SYSTEMS

- HTGR-86-020/3	Heat Transport SDD	07/87
- HTGR-86-099/1	Main Circulator SSDD	07/87
- HTGR-86-129/1	Steam Generator SSDD	07/87
- HTGR-86-098/1	Fuel Handling and Storage SDD	07/87
- HTGR-86-097/1	Core Refueling SSDD	07/87
- HTGR-87-076	Site Fuel Handling SSDD	07/87
- HTGR-87-077	Spent Fuel Cooling SSDD	07/87

VOLUME VII - PLANT CONTROL, PLANT PROTECTION & PLANT MONITORING SYSTEMS

- HTGR-86-051/1	NSSS Control SSDD	07/87
- HTGR-86-076	Plant Control, Data and Instrumentation SDD	06/87
- HTGR-86-052	NSSS Analytical Instrumentation SSDD	09/86
- HTGR-86-047/1	Plant Protection and Instrumentation SDD	07/87
- HTGR-86-049	Investment Protection SSDD	09/86
- HTGR-86-048	Safety Protection SSDD	09/86
- HTGR-86-050	Special Nuclear Area Instrumentation SSDD	09/86
- HTGR-87-074	Radiation Monitoring SSDD	07/87
- HTGR-87-075	Seismic Monitoring SSDD	07/87
- HTGR-87-024	Meteorological Monitoring SSDD	06/87
- HTGR-87-025	Fire Detection and Alarm SSDD	06/87
- HTGR-87-026	Security Monitoring SSDD	06/87

Table of Contents

VOLUME VIII - TURBINE PLANT SYSTEMS

- HTGR-87-027/2	Feedwater and Condensate SDD	06/87
- HTGR-87-028/1	Steam and Water Dump SDD	06/87
- HTGR-87-029/2	Main and Bypass Steam SDD	06/87
- HTGR-87-030	Startup and Shutdown SSDD	08/86
- HTGR-87-031	Turbine Generator and Auxiliaries SSDD	08/86
- HTGR-87-032	Extraction and Auxiliary Steam SSDD	06/86
- HTGR-87-033	Heater Drains and Condensate Returns SSDD	06/86
- HTGR-87-034	Condensate Polishing SSDD	06/86
- HTGR-87-035	Steam Vents and Drains SSDD	06/86
- HTGR-87-036	Turbine Plant Sampling SSDD	06/86
- HTGR-87-037	Chemical Feed SSDD	06/86
- HTGR-87-038	Turbine Building Closed Cooling Water SSDD	06/86

VOLUME IX - PLANT COOLING WATER SYSTEMS

- HTGR-86-028/2	Shutdown Cooling SDD	07/87
- HTGR-86-101/1	Shutdown Cooling Circulator SSDD	07/87
- HTGR-86-130/1	Shutdown Cooling Heat Exchange SSDD	07/87
- HTGR-87-078	Shutdown Cooling Water SSDD	07/87
- HTGR-87-039	Circulating Water SSDD	06/86
- HTGR-87-040	Circulating Water Makeup & Blowdown System SSDD	06/86
- HTGR-87-041	Service Water SSDD	06/86
- HTGR-87-068	Reactor Cavity Cooling SDD	07/87

VOLUME X - BUILDINGS & STRUCTURES SYSTEMS

- HTGR-87-065	Reactor Building DD	07/87
- HTGR-87-067	Reactor Auxiliary Building DD	07/87
- HTGR-87-066	Reactor Service Building DD	07/87
- HTGR-87-042	Operations Center DD	09/86
- HTGR-87-043	Turbine Building DD	09/86
- HTGR-87-044	Standby Power Bldg DD	07/86
- HTGR-87-045	Radioactive Waste Management Building DD	09/86
- HTGR-87-079	Personnel Service Building DD	07/87
- HTGR-87-046	Fire Pump House DD	06/86
- HTGR-87-047	Energy Conversion Area and Nuclear Island Warehouse Buildings DD	06/86
- HTGR-87-080	Helium Storage DD	07/87
- HTGR-87-048	Intake Pump House and Discharge Structure DD	06/86
- HTGR-87-049	Maintenance Building DD	06/86
- HTGR-87-050	Cooling Tower Basin and Circulating Water Pumphouse DD	06/86
- HTGR-87-051	Make-up Water Treatment and Auxiliary Boiler Building DD	06/86

Table of Contents

VOLUME XI - ELECTRICAL & MISCELLANEOUS MECHANICAL SYSTEMS

-	HTGR-87-057	Non-Class IE AC Distribution SSDD	08/86
-	HTGR-87-058	Uninteruptable Power Supply SSDD	06/87
-	HTGR-87-059	Class IE Uninteruptable Power Supply SSDD	06/86
-	HTGR-87-060	DC Power SSDD	06/87
-	HTGR-87-061	Class IE DC Power SSDD	06/86
-	HTGR-87-062	Lighting and Service Power SSDD	06/87
-	HTGR-87-052	Plant Fire Protection SSDD	06/86
-	HTGR-87-053	Auxiliary Boiler SSDD	06/86
-	HTGR-87-054	Raw Water Treatment SSDD	06/86
-	HTGR-87-055	HVAC SSDD	06/86
-	HTGR-87-056	Demineralized Water Makeup SSDD	06/86

DOE-HTGR-86-051
Revision 1

HTGR

NSSS CONTROL SUBSYSTEM DESIGN DESCRIPTION

[redacted]

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.

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

JULY 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

DOE–HTGR–86–051
Revision 1
HFD–43701
Revision 2
908468/2

NSSS CONTROL SUBSYSTEM DESIGN DESCRIPTION

[redacted]

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

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

JULY 1987

ROLL 2084

GA 1485 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY

TITLE					
NSSS CONTROL SUBSYSTEM DESIGN DESCRIPTION				☐ R & D ☐ DV & S ☒ DESIGN	APPROVAL LEVEL 5
DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO.	ISSUE NO./LTR.
I	37 01	SSDD	6300	908468	2
QUALITY ASSURANCE LEVEL	SAFETY CLASSIFICATION	SEISMIC CATEGORY	ELECTRICAL CLASSIFICATION		
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	JUL 07 1986	D.Giegler	C.Rodriguez	G.P.Connors		G.D.Bramblett	Initial issue 6352370202 (HFD-43701, Rev. 0)
			F.A.Silady Interface Assurance	R.D.Phelps			

CONTINUE ON GA FORM 1485-1

*See List of Effective Pages

NEXT INDENTURED DOCUMENTS

908437
(HFD-33700)
(DOE-HTGR-86-076)

[redacted]

☐ GA PROPRIETARY INFORMATION

THIS DOCUMENT IS THE PROPERTY OF GA TECHNOLOGIES INC. ANY TRANSMITTAL OF THIS DOCUMENT OUTSIDE GA WILL BE IN CONFIDENCE. EXCEPT WITH THE WRITTEN CONSENT OF GA, (1) THIS DOCUMENT MAY NOT BE COPIED IN WHOLE OR IN PART AND WILL BE RETURNED UPON REQUEST OR WHEN NO LONGER NEEDED BY RECIPIENT AND (2) INFORMATION CONTAINED HEREIN MAY NOT BE COMMUNICATED TO OTHERS AND MAY BE USED BY RECIPIENT ONLY FOR THE PURPOSE FOR WHICH IT WAS TRANSMITTED.

☒ NO GA PROPRIETARY INFORMATION

ROLL 2084

GA 1485-1 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY CONTINUATION SHEET

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
NSSS CONTROL SUBSYSTEM DESIGN DESCRIPTION	908468	2

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: FUNDING PROJECT	APPROVAL: APPLICABLE PROJECT	ISSUE DESCRIPTION/ CWBS NO.
1	SEP 09 1986	D.Giegler	C.Rodriguez F.A.Silady Interface Assurance	G.P.Connors	G.Bramblett		HTGR cover added HTGR-86-051/0 (HFD-43701,Rev. 1) Class II Change 6301998201
2	JUL 01 1987	R.D.Pfremmer	C.Rodriguez F.A.Silady Interface Assurance	G.P.Connors	G.Bramblett		Revised Issue 6352370301 DOE-HTGR-86-051, Rev. 1 (HFD-43701, Rev. 2) Class II Changes

INFO 1

INFO 1

LIST OF EFFECTIVE PAGES

Page Number	Page Count	Revision
i through xxi	21	2
1-1 through 1-22	22	2
2-1 through 2-35	35	2
3-1 through 3-20	20	2
4-1 through 4-9	9	2
5-1 through 5-3	3	2
6-1 through 6-7	7	2
7-1 through 7-2	2	2
8-1	1	2
9-1	1	2
A-1 through A-13	13	2
B-1	1	2
C-1 through C-6	6	2
D-1	1	2
E-1	1	2
F-1	1	2
Total pages	144	

CONTENTS

PAGE

LIST OF EFFECTIVE PAGES iv
CONTENTS v
LIST OF APPENDICES. ix
LIST OF ILLUSTRATIONS x
LIST OF TABLES x
LIST OF ABBREVIATIONS AND ACRONYMS xi
DEFINITIONS xii
PREFACE xvii
SUMMARY xix

1 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS 1-1

1.1 Subsystem Functions 1-1

1.2 Subsystem Design Requirements 1-2

1.2.1 System Configuration and Essential Features Requirements 1-2
1.2.2 Operational Requirements 1-3
1.2.3 Structural Requirements 1-12
1.2.4 Environmental Requirements 1-12
1.2.5 Instrumentation and Control Requirements 1-17
1.2.6 Surveillance and In-Service Inspection Requirements 1-19
1.2.7 Availability Assurance Requirements 1-19
1.2.8 Maintenance Requirements 1-20
1.2.9 Safety Requirements 1-21
1.2.10 Codes and Standards Requirements 1-21
1.2.11 Quality Assurance Requirements 1-22
1.2.12 Construction Requirements 1-22
1.2.13 Decommissioning Requirements 1-22

CONTENTS (Continued)

PAGE

2 DESIGN DESCRIPTION 2-1

2.1 Summary Description 2-1

2.2 Subsystem Configuration 2-5

2.2.1 Direction Acceptance 2-5
2.2.2 Status Observation 2-5
2.2.3 Automatic Control Decision Making 2-6
2.2.4 Command Outputs 2-18
2.2.5 Information Reporting/Data System 2-18

2.3 Subsystem Performance Characteristics 2-21

2.3.1 Subsystem Operating Modes 2-21
2.3.2 Subsystem Steady-State Performance 2-27
2.3.3 Subsystem Response to Plant Transients 2-28
2.3.4 Subsystem Failure Modes and Effects 2-29

2.4 Subsystem Arrangement 2-29

2.4.1 NSSS Systems Interface Stations 2-33
2.4.2 NSSS Operations Stations 2-33

2.5 Instrumentation and Control 2-35

CONTENTS (Continued)

PAGE

3 COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS 3-1

3.1 Component Functions 3-1

3.1.1 NSSS Operations Station 3-1

3.1.2 NSSS Systems Interface Station 3-2

3.1.3 NSSS Control Software 3-2

3.2 Component Design Requirements 3-3

3.2.1 NSSS Operations Station Component Design Requirements 3-3

3.2.2 NSSS Systems Interface Station Component Design Requirements 3-10

3.2.3 NSSS Control Software Component Design Requirements 3-14

4 SUBSYSTEM AND COMPONENT INTERFACES 4-1

4.1 Subsystem Interface Requirements 4-1

4.1.1 Interface Requirements Imposed on Building and Structures and on Other Systems and Subsystems Within Other Systems 4-1

4.1.2 Interface Requirements Imposed on Subsystem Within the Plant Control, Data, and Instrumentation System 4-8

4.2 Subsystem Boundary Definition 4-8

CONTENTS (Continued)

PAGE

5 SUBSYSTEM CONSTRUCTION 5-1

5.1 Packaging and Shipping 5-1
5.2 Handling at Delivery 5-2
5.3 Receiving Inspection 5-2
5.4 Storage 5-2
5.5 Access 5-2
5.6 Installation and/or Field Fabrication 5-3
5.7 Construction Testing 5-3
5.8 As-Built Drawings 5-3

6 SUBSYSTEM OPERATION 6-1

6.1 Subsystem Limitations, Setpoints, and Precautions 6-1

6.1.1 Subsystem Limitations and Setpoints 6-1
6.1.2 Precautions 6-1

6.2 Preoperational Checkout 6-2

6.2.1 Initial Preoperational Checkout 6-2
6.2.2 Routine Preoperational Checkout 6-3

6.3 Startup/Shutdown 6-3

6.3.1 Startup to 25% Steam Flow 6-3
6.3.2 Shutdown from 25% Steam Flow 6-3

6.4 Normal Operation 6-4

CONTENTS (Continued)

PAGE

6.5 Refueling 6-4

6.6 Shutdown 6-5

6.7 Abnormal Operation 6-5

6.8 Casualty Events and Recovery Procedures 6-6

6.8.1 Casualty Events 6-6

6.8.2 Design Features to Mitigate Effects of Casualty Events 6-6

6.8.3 Recovery Procedures 6-7

7 SYSTEM MAINTENANCE 7-1

7.1 Maintenance Approach 7-1

8 SUBSYSTEM DECOMMISSIONING 8-1

9 REFERENCES 9-1

LIST OF APPENDICES

A NSSS CONTROL SUBSYSTEM DESIGN REQUIREMENTS TRACEABILITY SUMMARY A-1

B DRAWING LIST B-1

C TRANSIENTS C-1

D [LATER] D-1

E EQUIPMENT LIST E-1

F PARAMETER LIST F-1

LIST OF ILLUSTRATIONS

FIGURE	TITLE	PAGE
1-1	HTS Operating Envelopes at 100% Feedwater Flow	1-7
1-2	HTS Operating Envelope About 25% Feedwater Flow	1-8
1-3	HTS Operating Envelopes at Refueling	1-9
1-4	Weekly Load Following Cycle	1-14
2-1	MHTGR Buildings and NSSS Control Subsystem	2-2
2-2	Control Systems Within PCDIS	2-3
2-3	NSSS Control Subsystem Architecture and Interfaces	2-4
2-4	NSSS Control Scheme and Interfaces	2-13
2-5	Independent Module Feedwater Control and Throttle Pressure Feedback to Throttle Valve	2-14

LIST OF TABLES

1-1	Design Point NSSS Performance at Rated (100%) Feedwater Flow	1-6
1-2	Steam/Feedwater Control and Instrument Accuracies	1-11
1-3	Design Duty Cycles	1-13
1-4	Site Characteristics	1-15
2-1	NSSS Control and Data Size	2-7
2-2	NSSS Transient Control Requirements	2-16
2-3	Circulator Characterizer Function	2-17
2-4	NSS Module Startup Sequence from Depressurized Conditions	2-24
2-5	Failure Modes and Effects Analysis	2-30
2-6	Distribution of Control Stations	2-34
3-1	NSSS Operations Station Design Requirements	3-5
3-2	NSSS Operations Station Environmental Requirements	3-6
3-3	Reference Control System Algorithm Gains for NSSS Control System	3-15
4-1	NSSS Control Subsystem Interfaces with Other Systems and Subsystems	4-2

LIST OF ABBREVIATIONS AND ACRONYMS

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CRT	Cathode Ray Tube
DMS	Data Management System
ECA	Energy Conversion Area
EMI	Electromagnetic Interference
FW	Feedwater
HTS	Heat Transport System
HVAC	Heating, Ventilating, and Air Conditioning
IEEE	Institute of Electrical & Electronic Engineers
IB	Instrument Block
MHTGR	Modular High-Temperature Gas-Cooled Reactor
MTBF	Mean Time Between Failure
MTR	Mean Time to Repair
NSSS	Nuclear Steam Supply System
NSSSCS	NSSS Control Subsystem
PCDIS	Plant Control, Data, and Instrumentation System
PPIS	Plant Protection and Instrumentation System
PSCS	Plant Supervisory Control Subsystem
QA	Quality Assurance
QAL	Quality Assurance Level
ROM	Read Only Memory
SCS	Shutdown Cooling System
SDD	System Design Description
SSDD	Subsystem Design Description
TBD	To be determined

DEFINITIONS

Activity: An identifiable set of human actions undertaken to accomplish a particular task within one of the more general industry activities of Design, Construction, Operation, Maintenance, and Decommissioning.

Design Criterion: A basis for judging the acceptability of a particular quantity, action, procedure, or design solution.

Design Value: The nominal value of a plant or system operating parameter plus an appropriate margin.

Energy Conversion Area: That portion of the plant not included within the Nuclear Island.

Equilibrium Plant: A commercial plant that incorporates a design that has matured through construction of replicate facilities and has accrued the benefits of standardization, learning, and optimal use of associated manufacturing facilities.

Equivalent Availability: Equivalent availability is mathematically defined as:

$$Ae = \int_{o}^{T_p} \frac{Pa(t)}{T_p} \, dt$$

where: $Pa(t)$ = available net electrical power expressed as a percentage of design power as a function of time (t)

t = time

T_p = time period (operational lifetime)

DEFINITIONS (Continued)

Function: A statement of what is to be achieved.

Functional Analysis: A systems engineering technique or method used to develop (1) functions required to meet established goals, (2) the relationship between functions and related requirements, and (3) the basis and justification for design selections through which the prescribed goals are met. [Functional analysis is one part of the Integrated Approach.]

Functional Independence: Design provisions which ensure that the safety-related functions of a system do not rely in whole or in part on another system to provide the design function.

Functional Requirement: A bounding quantification that is derived from a functional need versus being imposed by an institutional standard.

Goal: An endpoint or accomplishment towards which an effort is directed. The Integrated Approach has identified the following specific goals supporting the overall objective:

1. Safe economical power (top level - Goal 0).
2. Maintain plant operation (Goal 1).
3. Maintain plant protection (Goal 2).
4. Maintain control of radionuclide release (Goal 3).
5. Maintain emergency preparedness (Goal 4).

Institution: A significant practice, relationship, or organization in a society. Institutions include the utility/user, the federal government, industry codes and standards, the Department of Energy, and state and local governments.

Institutional Requirement: A bounding quantification that is imposed by an institution as opposed to a quantification derived from a functional need.

DEFINITIONS (Continued)

Integrated Approach: A systems engineering technique for establishing and defending a well-developed nuclear plant design.

Interface Requirement: A requirement imposed by a system, subsystem, or component on another system, subsystem, or component, which must be accomplished to facilitate satisfaction of a function(s) of the imposing system, subsystem, or component.

Nominal Value: Value of a quantity in name only, and thus not actual. Generally rounded for this usage.

Nuclear Island: That portion of the plant that has within its boundary the following:

1. The standard reactor modules and "safety-related" buildings, structures, systems, portions of systems, and components dedicated to ensuring reactor shutdown, decay heat removal, fission product retention, and security of vital areas including new (unirradiated) fuel.

2. At the designer's discretion, buildings, structures, systems, portions of systems, and components that support reactor operation or investment protection, and are not "safety-related."

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

Operating Life: The calendar time from receipt of the operating license to completion of plant power production.

DEFINITIONS (Continued)

Plant: All buildings, structures, systems, and components that together accomplish the process of energy production and conversion and support the human activities of administration, operation, and maintenance.

Plant Life: The calendar time from construction permit issuance to completion of plant power production.

Parameter: A specific measurable and quantifiable aspect of a physical item.

Plant State: The condition of the physical plant (or module) at a particular time and place, as described by a set of appropriate variables associated with a plant goal.

Principal Design Criteria: Qualitative statements which specify the design commitments made to ensure that the dose criteria of 10CFR100 will be met and, therefore, that public health and safety will be protected under accident conditions.

Rated Value: The nominal value of a parameter at 100% plant energy conditions.

Requirement: The bounding quantification (limits) of a function.

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

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

DEFINITIONS (Continued)

Standard Reactor Module: That portion of the Nuclear Island which is duplicated with the addition of each reactor. This would include, in part, the reactor, steam generator, helium circulator, Reactor Building, Reactor Cavity Cooling System, etc.

System: A collection of electrical, mechanical, and/or structural components and associated software and human actions treated as a unit for technical, administrative, or contractual purposes.

PREFACE

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

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

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

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

4. Maintain Emergency Preparedness.

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

In response to the OPDS, a series of lower tier documents, System Design Description (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDDs), Component Design Specifications

PREFACE (Continued)

(CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability of requirement source from plant-level requirements to equipment-level requirements shall be maintained throughout this hierarchy of design documents.

SUMMARY

The NSSS Control Subsystem (NSSSCS) is one of the systems comprising the MHTGR. The design of this system has been developed through the Integrated Approach toward safe and economical production of electrical power.

This document defines the functions of the NSSSCS, system design requirements derived from the functional analysis, and institutional requirements from the Overall Plant Design Specification (Ref. 2). A description of the subsystem design which satisfies the requirements is presented. These lower-tier requirements are derived at the system level and passed down to the NSSSCS. This document also includes information on aspects of system construction, operation, maintenance, and decommissioning.

The NSSSCS controls NSSS systems and monitors and evaluates the state of the NSSS modules. There are four (4) independent NSSSCS modules in the MHTGR plant. The system automatically controls the NSSS during energy production, shutdown, refueling, and startup/shutdown. The scope of the system starts with and includes the electronic interfaces with other MHTGR systems. These include input of the NSSSCS commands to the actuated equipment in the NSSS. The NSSS systems interface stations, which are located near the Reactor Buildings and which are part of the NSSSCS, physically attach to these electronic interfaces. The scope of the system ends with the NSSS operations stations which perform other functions including exchange of control and status information with a plant supervisory control system and interface with plant operating personnel at locations outside of the control room.

The NSSSCS monitors selected process variables through its data system and controls the state of the NSSS through command of actuated equipment. The process instrumentation is contained in the other NSSS systems. The NSSSCS provides continuous monitoring and automatic control of NSSS systems and reports information to a Plant Supervisory Control System (PSCS). Each NSSSCS module independently receives command information from the PSCS and

SUMMARY (Continued)

responds independently to PSCS commands. The NSSSCS and PSCS, along with the other subsystems shown below, make up the Plant Control Data and Instrumentation System. The complete document structure for the controls is shown below.

System	System No.	Document No.
Plant Control Data and Instrumentation	3700	HFD-33700

Subsystem	Subsystem No.	Document No.
Plant Supervisory Control	3707	HFD-43707
NSSS Control	3701	HFD-43701
Tech. Operation Support	3708	HFD-43708
Data Management	3735	HFD-43735

SECTION 1
NSSS CONTROL SUBSYSTEM DESIGN DESCRIPTION

1.1 SUBSYSTEM FUNCTIONS

The NSSS Control Subsystem consists of four identical sets of controls - one for each NSSS module. These operate under the supervision of the Plant Supervisory Control Subsystem or the operators.

The NSSS Control Subsystems functions are:

1. Accept Direction - Supervisory control commands are accepted from the supervisory Control Subsystem or the operators. These commands tell the NSSS module its state set point, such as for example, load level. Information requests are also received by the NSSS Control Subsystem.

2. Observe Status - Process information is acquired by each NSSS Control Subsystem from its NSSS module, converted to alternate forms, and stored.

3. Make Decisions - Based on the observed status and the accepted direction, the NSSS Control Subsystem makes control decisions about the actions that it needs to take on its NSSS module in order to reach or maintain its state set point.

4. Effect Control - The NSSS Control Subsystems outputs analog and digital control signals to carry out control decisions.

5. Report Information - Information about the status of the NSSS module is communicated to data highways for output to operator interfaces.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

The NSSS Control Subsystems shall be functionally independent from major component and equipment monitoring and protective features. The NSSS control subsystem shall be functionally independent of the PPIS. (3701.0102.001)*

NSSSCS alarm points to the control room shall be restricted to those critical parameters which can lead to initiation of protective action for major plant components or the loss of electrical production. (3701.0102.002)

NSSSCS features shall be included to facilitate operation of the reactor module at different power levels. (3701.0102.003)

The design of structures, systems, and components (SSCs) within the Nuclear Island shall be standardized. (3701.0102.004)

The NSSSCS shall be designed for a Nuclear Island that contains four (4) standard reactor modules. (3701.0102.005)

Human/machine interfaces and machine/machine communication interfaces shall be provided for the NSSSCS equipment outside the control room requiring human interaction during energy production, shutdown, refueling, and startup/shutdown. (3701.0102.006)

Features of the NSSSCS (e.g., intersystem communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of equipment and device interfaces. (3701.0102.007)

---

*Requirement traceability number

The NSSSCS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating de-energizing electronics or affecting the operation of other electronic equipment. (3701.0102.008)

Base the NSSSCS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process. (3701.0102.010)

1.2.2 Operational Requirements

The NSSSCS shall provide the capability to control and regulate the conditions of the nuclear steam supply so as to deliver 2400 psig, 1000°F steam to the high-pressure turbine admission valves. (3701.0102.011)

The NSSSCS shall provide the capability for roving operators to control, under supervision from the control room, selected processes and subsystems during energy production, shutdown, refueling, and startups/shutdowns not requiring direct control room operator interfacing and interaction. Communications and status information shall be made available at the locations involved in the operations outside the control room. (3701.0102.012)

The NSSSCS shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in Table 5.1-1 of Ref. 2. (3701.0102.013)

The NSSSCS design shall accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations:

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. Four (4) reactor modules operating in parallel supplying steam to two turbine-generators. (3701.0102.014)

The NSSSCS design shall permit for reloading at 5% of rated load per minute following:

1. Load rejection from full generator electric output to house electrical load without a reactor trip.

2. Turbine trip (except on low condenser vacuum) from any load level without a reactor trip, without the necessity for a mandatory hold except for those associated with the turbine-generators. (3701.0102.015)

The NSSSCS design shall provide sustained and controlled operation for the conditions listed below:

1. Step changes of ±15% in plant output caused by utility electrical transmission grid upsets. (3701.0102.016)

NSSSCS features shall be included as required to limit recovery time to resumption of reactor power operation when a protection trip occurs consistent with meeting the plant availability goal. (3701.0102.017)

The NSSSCS shall be capable of changing reactor output under automatic control at a rate of up to and including 5% of rated output per minute. (3701.0102.018)

The NSSSCS shall include features to enable automatic control during startups. (3701.0102.518)

The NSSSCS shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in Table 1-1. (3701.0102.019)

The NSSSCS shall control circulator speed not to exceed a speed 10% above the nominal value. (3701.0102.020)

The NSSSCS shall be designed to maintain the SG primary coolant inlet bulk temperature and primary coolant flow rate within the envelope shown in Figures 1-1 through 1-3. (3701.0102.021)

The NSSSCS shall maintain the circulator speed/feedwater flow schedule between 25% and 100% feedwater flow between ±15% of nominal values. (3701.0102.022)

The NSSSCS shall be designed to maintain the primary coolant cold leg temperature below 288°C (550°F). (3701.0102.023)

The NSSSCS control shall maintain long-term, stable steam generator outlet temperature below 557°C (1035°F). (3701.0102.024)

The NSSSCS shall accept PPIS signals and initiate control adjustments in response to trips. (3701.0102.405)

The NSSSCS shall provide setpoint signals to the neutron flux controller for use in automatically controlling the rods. (3701.0102.415)

The system shall be designed to control the helium mass flow through the active steam generator bundle between 25% and 100% of nominal feedwater flow for steady-state operation as specified in Table 1-1 and Table 5.12-2 of Ref. 2. (3701.0102.025)

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

NSSS Heat Balance, MW(t)	
Heat generated by core	350.00
Heat added by circulators	3.13
Total heat to helium	353.13
Loss to environment from helium	0.73
Loss of SCHE from helium	0.25
Net steam generator power	352.15
Reactor	
Inlet helium flow rate, lb/h	1,246,397.0
Inlet helium temperature, °F	497.4
Inlet helium pressure, psia	924.5
Loss to vessel from core, MW(t)	0.62
Outlet helium temperature, °F	1,267.7
Helium pressure drop, psi	8.00
Steam Generator	
Inlet helium flow rate, lb/h	1,248,100.0
Inlet helium temperature, °F	1,266.0
Inlet helium pressure, psia	915.8
Outlet helium temperature, °F	490.6
Helium pressure drop, psi	3.70
Inlet feedwater flow rate, lb/h	1,089,736.0
Inlet feedwater temperature, °F	380.0
Inlet feedwater pressure, psia	3,000.0
Inlet feedwater enthalpy, Btu/lb	357.60
Regenerative heat loss, MW(t)	0.33
Outlet steam temperature, °F	1,005.3
Outlet steam pressure, psia	2,515.0
Steam pressure drop, psia	485.0
Main Circulator	
Circulator helium flow rate, lb/h	1,254,372.0
Bypass helium flow rate, lb/h	6,272.0
Inlet helium temperature, °F	490.7
Inlet helium pressure, psia	911.8
Helium temperature rise, °F	6.85
Helium pressure rise, psi	13.20
Circulator speed ratio	1.00

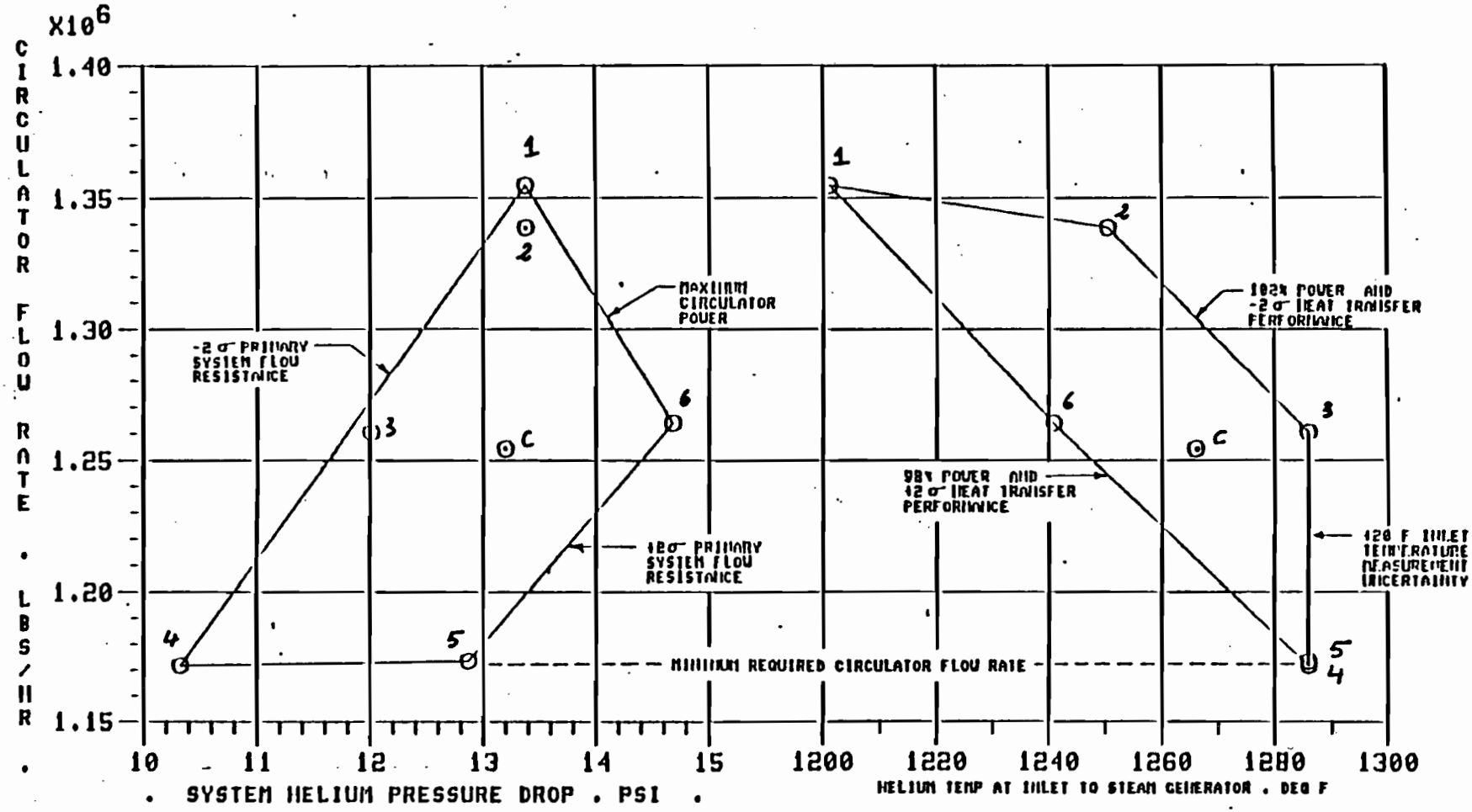
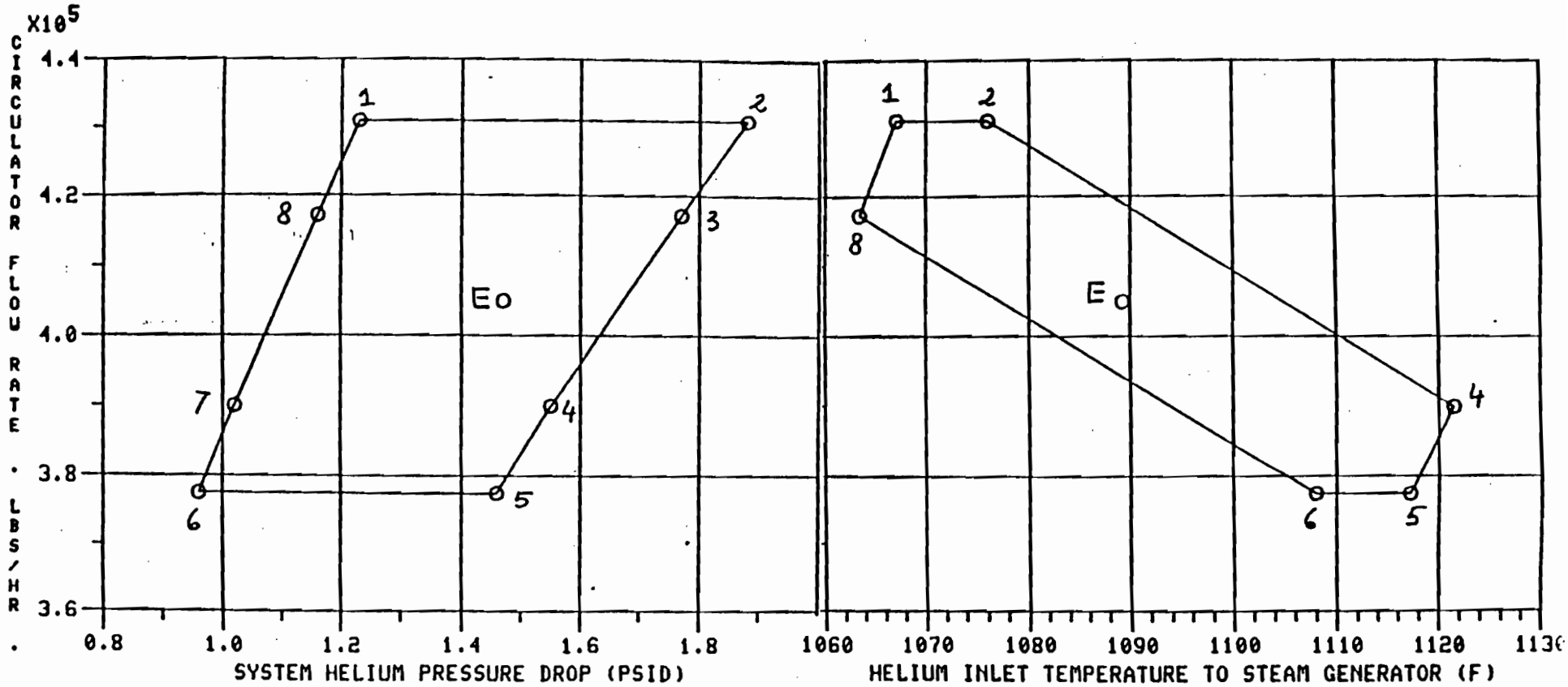


Figure 1-1 HTS OPERATING ENVELOPES AT 100% FEEDWATER FLOW


X10^5
CIRCULATOR FLOW RATE . LBS/HR .
4.4
4.2
4.0
3.8
3.6
0.8
1.0
1.2
1.4
1.6
1.8
SYSTEM HELIUM PRESSURE DROP (PSID)
Eo
1
2
3
4
5
6
7
8
1060
1070
1080
1090
1100
1110
1120
HELIUM INLET TEMPERATURE TO STEAM GENERATOR (F)
Eo
1
2
4
5
6
8

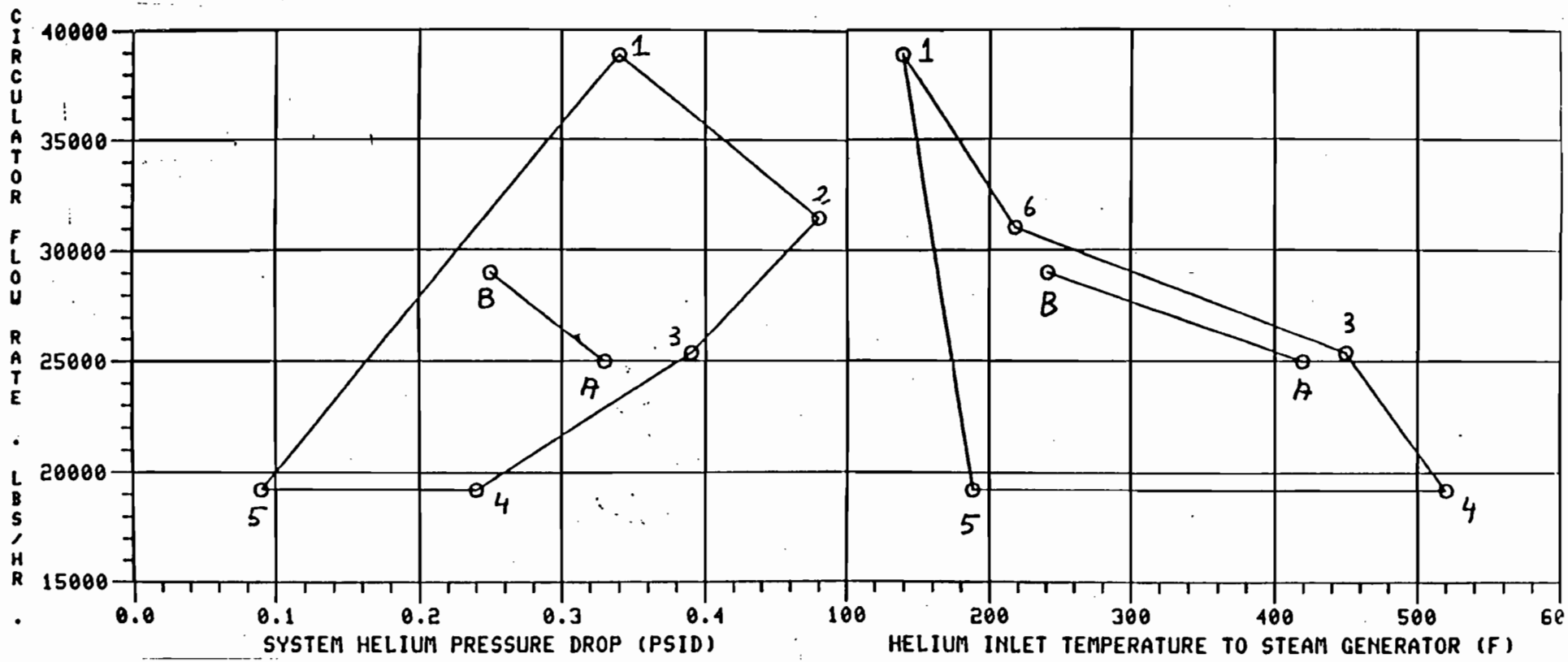


Figure 1-3 HTS OPERATING ENVELOPES AT REFUELING

Each individual reactor module shall be capable of continuous operation under automatic control between 25% and 100% of nominal module feedwater flow. (3701.0102.026)

The NSSSCS shall be designed to sustain continuous operation at reduced electrical output through and following transients associated with the loss or failure of a major component, system, or train, including an individual reactor. (3701.0102.027)

The NSSSCS shall be designed to measure and control the performance of the NSSS parameters at any point between 25% and 100% rated feedwater flow for steady-state operation as specified in Table 1-2. (3701.0102.028)

The NSSSCS shall include features to enable automatic control during plant operation. (3701.0102.029)

Reactor module startup shall range between 0% and 25% rated feedwater flow rate on a per reactor module basis. (3701.0102.030)

The NSSSCS shall be designed to accommodate one or more reactor modules starting up. (3701.0102.031)

Reactor module shutdown shall range between 25% and 0% rated feedwater flow rate on a per reactor module basis. (3701.0102.032)

The NSSSCS shall include features to enable automatic control during orderly shutdowns. (3701.0102.033)

The plant shall be designed to accommodate one or more modules shutting down. (3701.0102.034)

Provisions shall be made to remove a reactor from service, perform refueling, and return it to service with the remaining reactors and the turbine plant in operation. (3701.0102.035)

Table 1-2
STEAM/FEEDWATER CONTROL AND INSTRUMENT UNCERTAINTIES

Steam outlet temperature	±9°F
Steam outlet pressure	±1%
Feedwater inlet temperature	±2°F
Feedwater flow rate	±2%

The NSSSCS shall be designed for a plant operating life of 40 calendar years. (3701.0102.036)

Features shall be included in the NSSSCS to facilitate continual NSSS operation through the transients shown in Table 1-3 (except for shutdown) and at reduced electrical output upon loss of function of major subsystem components where more than one is employed. (3701.0102.037)

The NSSSCS shall be designed for base load operation and be capable of accommodating the weekly load cycle in Figure 1-4 over its design life. (3701.0102.038)

1.2.3 Structural Requirements

Nonsafety-related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum. (3701.0102.039)

Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE. (3701.0102.597)

OBE seismic response spectrum load level specifications for the NSSSCS shall be based on the plant seismic response spectra provided in the FY-86 MHTGR plant seismic assessment. (3701.0102.040)

The NSSSCS shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3. (3701.0102.041)

1.2.4 Environmental Requirements

Environmental qualification requirements pertaining to NSSSCS operation and structural design shall be based upon relevant plant site characteristics as specified in Table 1-4. (3701.0102.042)

Table 1-3 DESIGN DUTY CYCLES[a]

	Design Number of Occurrences for Plant Lifetime
1. Reactor/plant startup from cold conditions	160
2. Reactor/plant shutdown to cold conditions	160
3. Rapid load ramp (5%/min) (25% to 100%)/(100% to 25%)	1,000/1,000
4. Normal load ramp (0.5%/min) (100% to 25%)/(25% to 100%)	17,500/20,800
5. Step load changes (±15%)	2,000

[a]Additional duty cycle events and their frequency of occurrence are to be determined by the responsible designers for concurrence by the Utility/User (see Section 5.1, Ref. 2).

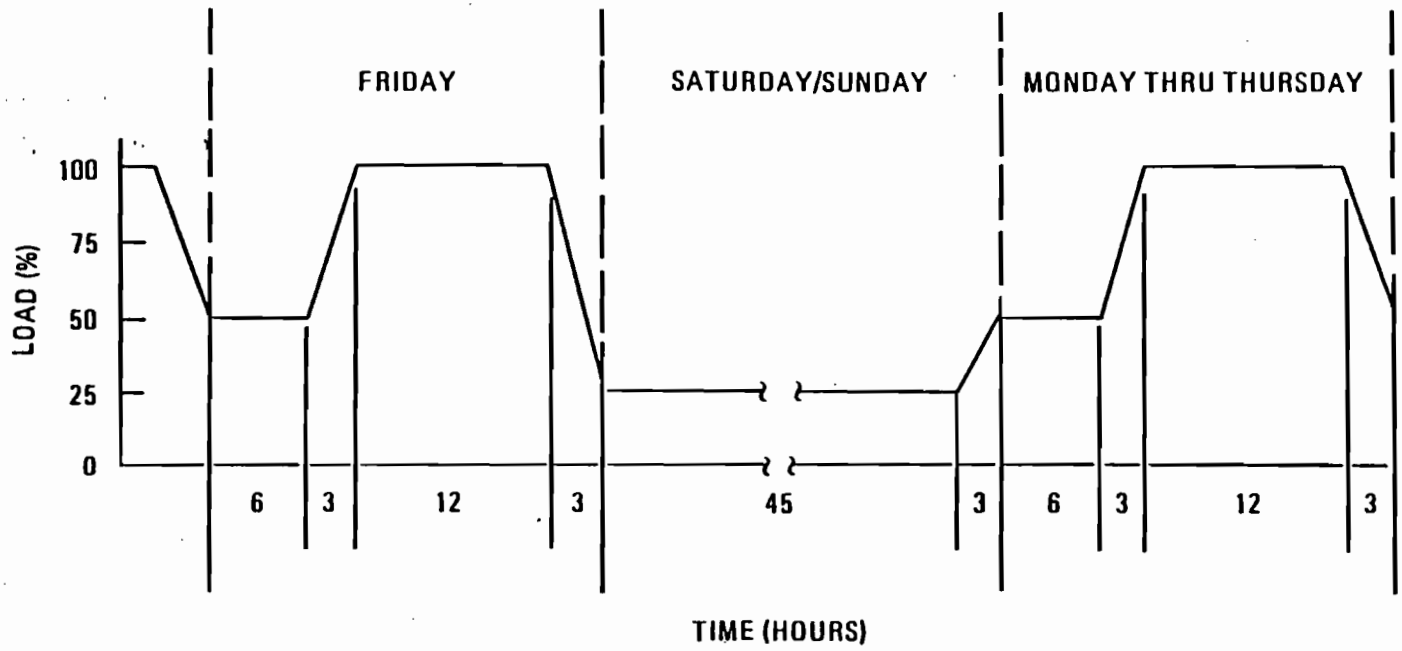


Fig. 1-4 WEEKLY LOAD FOLLOWING CYCLE

Table 1-4 SITE CHARACTERISTICS

This table provides the site characteristics to be used as a basis for the plant design. The characteristics include site parameters, which envelope 85% of the available U.S. sites.

1. Site Conditions	
1.1 Soil Characteristics[a]	
Shear wave velocity (fps)	1000 - 8000
Allowable static bearing capacity (KSF)	10[b]
1.2 Water Table	Normal groundwater elevation is approximately 8 ft below grade.
1.3 Precipitation (Snow)[a]	Snow load: 50 psf per ANSI A58.1.
1.4 Wind Velocity[a]	110 mph at and above a height of 33 ft (10 m) above grade per ANSI A58.1.
1.5 Air Temperature[a]	Dry Bulb / Wet Bulb 110°F / 82°F -45°F / N/A
1.6 Meteorological[a]	
Atmospheric dispersion X/Q values	Annual average at EAB: equivalent ground level release is 2×10^{-5} s/m^3. Accident evaluations are per NRC Regulatory Guides as appropriate.
1.7 Demography	
Population density	Uniform 500 people/mi^2 out to 30 miles, consistent with Reg. Guide 4.7 (tentative).

[a]Site characteristics which envelope 85% of prospective U.S. sites. Other characteristics are reference values.

[b]Value applicable to large mat foundations, not isolated footings.

Table 1-4 (Continued)

1.8 Boundaries[a]	
Exclusion area boundary (EAB)	425 m, minimum from reactor release point.
Protected area boundary (PAB)	To be determined by site layout.
Low population zone (LPZ)	425 m (same as EAB).
Emergency planning zone (EPZ)	425 m (same as EAB).
1.9 Water Sources	
Water	Nonbrackish river water (see Table 2.1-3 for analysis).
1.10 Elevation	
Nuclear Island[a]	100 to 6000 ft above mean sea level.
Energy Conversion Area	100 ft above mean sea level.
2. Site Events	
2.1 Seismic[a]	

Maximum ground acceleration:	Horizontal	Vertical
Safe shutdown earthquake	0.3 g	0.3 g
Operating basis earthquake	0.15 g	0.15 g

2.2 Tornado[a]	
Designation (RG 1.76)	Region I
Maximum wind speed	360 mph
Rotational speed	290 mph
Translational velocity	70 mph
External pressure drop	3.0 psi at 2.0 psi/s
2.3 Flooding	No special provisions required. Maximum probable flood level below plant grade.
2.4 Aircraft hardening	No specific provisions required. Plant considered to be outside of commercial flight paths.

[a]Site characteristics which envelope 85% of prospective U.S. sites. Other characteristics are reference values.

1.2.5 Instrumentation and Control Requirements

Provisions shall be made to automatically detect and document the sequence of significant events (e.g., control inputs, changes in operation of major systems and components, protective trips, etc.) that occur during plant operation. (3701.0102.043)

Portions and/or derivations of those observations required for controlling NSSS energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators. (3701.0102.044)

The NSSS control subsystem shall be capable of evaluating and determining the state of the NSSS and the corresponding module-level control state maneuvers required for energy production, shutdown, refueling and startup/shutdown control. (3701.0102.045)

The NSSS control subsystem shall provide the capability to automatically regulate conditions (e.g., pressure, flow, temperature, etc.) of the steam produced and delivered by each reactor module. (3701.0102.046)

The NSSS control subsystem shall provide the capability to control those actuators and devices required to effect a change in state in the NSSS during energy production, shutdown, refueling and startup/shutdown. (3701.0102.047)

The NSSS control subsystem shall be designed to accept directions corresponding to energy production and conversion load demand changes at rates anywhere from a minimum of [TBD % per minute] to a maximum of 5%/minute. (3701.0102.048)

The NSSSCS shall be capable of accepting plant energy production, shutdown, refueling and startup/shutdown instructions from the control room operators and operator workstations. (3701.0102.049)

The NSSS control subsystem shall acknowledge and process other subsystem variables, states, modes, performance limits, conditions, etc., in the energy production, shutdown, refueling and startup/shutdown analysis and decision making process. (3701.0102.050)

The NSSSCS shall provide the capability to communicate digital control and monitoring signals using non-hardwired, signal transmission techniques. (3701.0102.051)

The NSSSCS shall be designed to accept startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] % per minute to a maximum of [+TBD] % per minute. (3701.0102.052)

The NSSSCS shall be designed to accept shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD % per minute]. (3701.0102.053)

Provisions shall be made for monitoring NSSS status, configuration, and performance as a basis for maintenance diagnostics and decision making. (3701.0102.054)

The NSSSCS shall provide the capability to sense, process, and analyze those variables, states, modes, limits, conditions, etc., required for the NSSS to be observable. (3701.0102.055)

The NSSSCS shall monitor the SFSF temperature and report to the main control room if temperature exceeds [TBD]. (3701.0102.410)

The NSSSCS shall perform [TBD] calculations utilizing the signals from the neutron detection equipment. (3701.0102.420)

The NSSSCS shall monitor the number of control rods withdrawn during shutdown and issue an alarm report to the main control room if more than three are withdrawn. (3701.0102.425)

The NSSSCS shall monitor and report steam generator feedwater inlet temperatures in excess of 371°C (700°F) to the main control room. (3701.0102.450)

The NSSSCS shall monitor and report steam generator feedwater inlet pressure in excess of 25.4 MPa (3685 psia). (3701.0102.460)

The NSSSCS shall monitor and report steam generator outlet pressure in excess of 18.9 MPa (2750 psia). (3701.0102.465)

Human engineering techniques shall be employed in the design of the NSSSCS to enhance operator response and reduce the probability of human error as specified in the Human Factor Engineering Plan [TBD]. (3701.0102.056)

Supporting controls and instrumentation for systems, structures, or components whose failure would not have an immediate impact on plant output shall be located outside the control room in the proximity of the systems, structures, or component with status indication provided to the control room. (3701.0102.057)

1.2.6 Surveillance and In-Service Inspection Requirements

This subsystem does not perform a "safety-related" function and, therefore, no "safety-related" surveillance and/or in-service inspection is required.

Requirements in this category, needed to satisfy the Integrated Approach Goals 1, 2, and 3, are covered under "Maintenance Requirements" in Section 1.2.8.

1.2.7 Availability Assurance Requirements

The Effective Forced Outage Hour (EFOH) values specified for the NSSSCS in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to

repair data for like type or similar systems and/or components. The NSSSCS shall be designed to meet a planned outage allocation of [TBD] hours. (3701.0102.060)

The NSSSCS shall be designed to meet the reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The NSSSCS shall be designed to meet an overall reliability allocation of [TBD]. (3701.0102.061)

1.2.8 Maintenance Requirements

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the NSSSCS. (3701.0102.058)

Malfunctions within major plant control and electric systems shall be alarmed in the main control room. (3701.0102.059)

The NSSSCS shall provide self-test capabilities (i.e., monitoring, checking, and diagnosing) for key functional components. (3701.0102.560)

Provisions shall be made for monitoring NSSS status, configuration, and performance as a basis for maintenance diagnostics. (3701.0102.570)

The NSSSCS shall be designed and arranged, and equipment and components located in the plant to facilitate on-line maintenance. (3701.0102.062)

The NSSSCS components shall be designed to facilitate hands-on maintenance. (3701.0102.063)

The NSSSCS shall be configured to enable maintenance of NSSSCS equipment within a plant total scheduled outage time of less than 876 h per year averaged over the plant lifetime as defined in OPDS Table 5.1-4. (3701.0102.064)

NSSSCS components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory. (3701.0102.065)

Special NSSSCS maintenance and installation tools not commercially available shall be provided by the NSSSCS equipment vendor. (3701.0102.066)

The NSSSCS shall make provisions for removing a reactor from service, performing maintenance and returning it to service with the remaining reactors and the turbine plant in operation. (3701.0102.580)

1.2.9 Safety Requirements

[The NSSSCS is not a "safety-related" subsystem. Therefore, it has no nuclear "safety-related" requirements.]

The NSSSCS shall be designed to meet applicable top-level regulatory criteria. (3701.0102.590)

1.2.10 Codes and Standards Requirements

NSSSCS design, analysis, fabrication, and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in component design specifications and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justified in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities.

DOE NE F2-10, Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1). (3701.0102.067)

1.2.11 Quality Assurance Requirements

Items that are not "safety-related" 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 DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5). (3701.0102.068)

1.2.12 Construction Requirements

Shop, factory, or field fabricated, assembled, and erected components and subsystems shall be utilized as appropriate to reduce costs and enhance quality control. (3701.0102.069)

The NSSSCS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3701.0102.070)

1.2.13 Decommissioning Requirements

The NSSSCS shall include features that accommodate decommissioning or refurbishment of one reactor while maintaining others in operation. (3701.0102.080)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The NSSS Control Subsystem (NSSSCS) is a complete control, display, and information system. The MHTGR plant contains four such subsystems, each being a part of a particular NSSS module, and each being able to control the module steam conditions and flow independently of the other modules. Each subsystem contains redundant control processing hardware and software. Each subsystem provides distributed digital process control, information processing, display, and data storage capabilities. The scope of supply includes sensors for control and monitoring, hardware and software that provide control logic and outputs to final control elements, and equipment necessary to process, display, and store plant data. The NSSSCS communicates with a plant supervisory control system (PSCS) through an interface between the NSSSCS and the PSCS data highway. The NSSS data highway system, local microprocessors and cabinets are all part of the NSSSCS. Figure 2-1 shows the buildings where the NSSS control equipment is located. Signal processing, control logic execution and data processing for each NSSS module is performed in each reactor building. Limited operator interfaces are located in each reactor building. NSSS module operator interfaces are located in a separate building close to the reactor building.

Each NSSSCS processes approximately 1100 analog and digital variables as explained in Section 2.2.

The architecture within the Plant Control Data and Instrumentation system is shown in Figure 2-2. The architecture within the NSSSCS and its interface with the PSCS are shown in Figure 2-3.

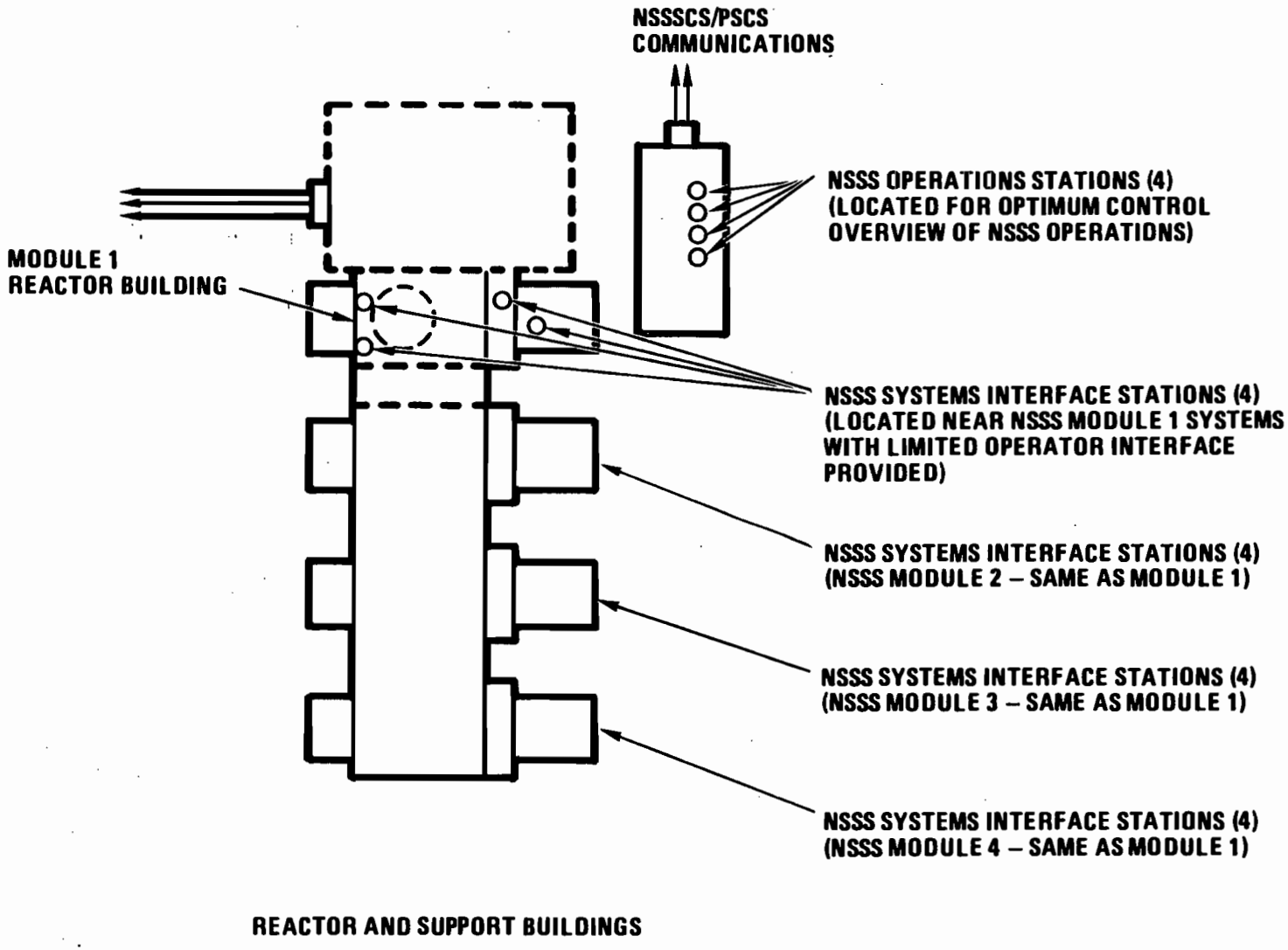


Fig. 2-1. MHTGR BUILDINGS AND NSSS CONTROL SUBSYSTEM

908468/2

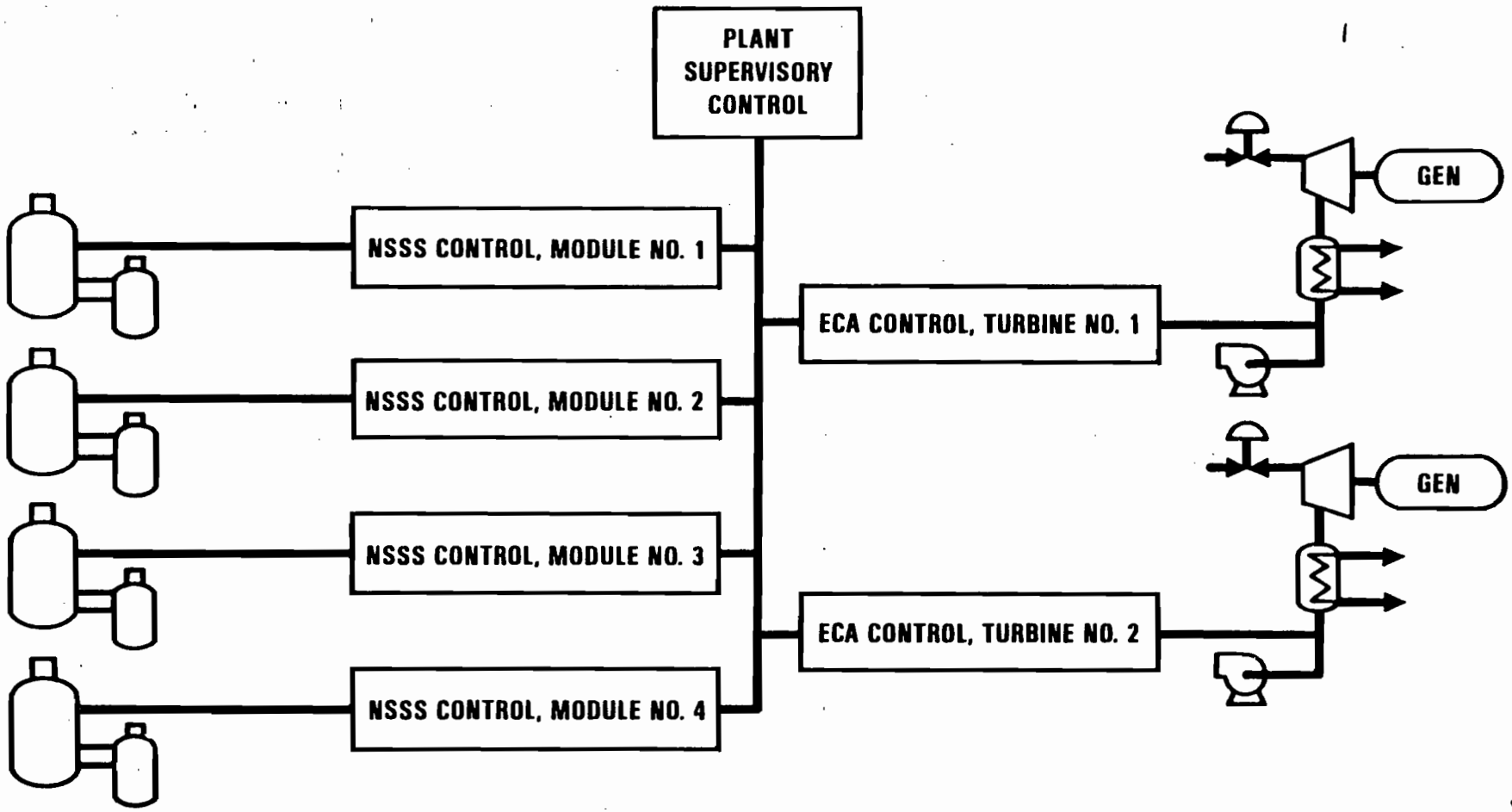


Fig. 2-2. CONTROL SYSTEMS WITHIN PCDIS

908468/2

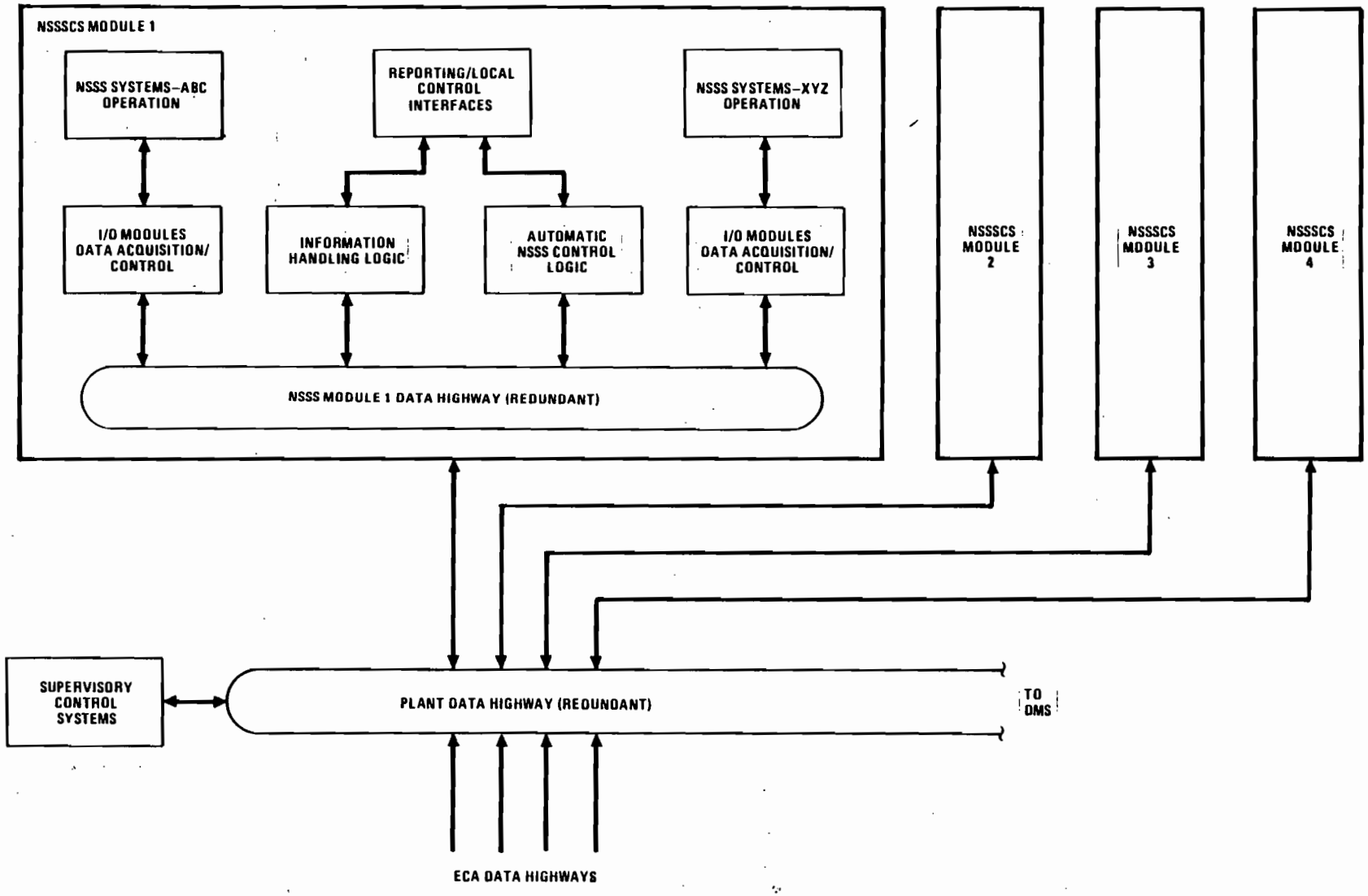


Fig. 2-3. NSSS CONTROL SUBSYSTEM ARCHITECTURE AND INTERFACES

The NSSSCS is functionally independent of the PPIS except that it is notified by the Plant Protection System via a unidirectional isolator of any equipment trips so that the NSSSCS can continue to adjust its parameters within acceptable operating ranges outside of trip ranges.

2.2 SUBSYSTEM CONFIGURATION

The five major functions of each NSSSCS are:

1. Accept direction from the PSCS or from operator.
2. Observe the status of the NSSS.
3. Make all control decisions for automatic NSSS response.
4. Provide output command signals to NSSS actuators and hardware control units.
5. Report information.

The design selections to perform these functions and the requirements they satisfy are discussed in the following sections.

2.2.1 Direction Acceptance

To follow direction from the plant supervisory control system or the operators, the NSSSCS automatically accepts load setpoints in the power operating range, or HOLD setpoints in the startup and shutdown range. These HOLD setpoints define the startup and shutdown sequences of the NSSS. Load setpoints and HOLD points are communicated over the data highways depicted in Figure 2-3.

2.2.2 Status Observation

The NSSSCS automatically detects and documents the sequence of significant operational events (e.g., changes in operation of major systems and

components), that occur during plant operation. It acknowledges and processes other NSSS system variables, states, modes, performance limits, conditions, etc., in the energy production, shutdown, refueling and startup/shutdown modes.

Table 2-1 shows the data parameters in each NSSS module that are monitored or controlled. There are about 1100 of these parameters in each module. The control variables are processed through control algorithms, and outputs are sent to the control actuators. The fastest cycle time required for this process is 500 ms.

Many of the parameters in Table 2-1 are measured, calculated, or actuated by devices that are part of other NSSS systems. However, they have been included in Table 2-1 for completeness in the total count of NSSS parameters to be monitored or controlled. For example, the Shutdown Cooling Control Subsystem is dedicated to and part of the Shutdown Cooling System; however, it has a reporting line to the NSSSCS. Therefore, Shutdown Cooling System information is passed to the NSSSCS via the Shutdown Cooling Control System Subsystem. Thus, there is a hierarchy of control which supports the modularity of the fluid and mechanical systems.

2.2.3 Automatic Control Decision Making

Based on the sensed data and the direction from the PSCS or the operator, the NSSS Control Subsystem automatically decides what control actions are used within each NSSS module to produce steam. The definition of these actions forms the control scheme. These actions are:

1. Control steam production process in accordance with plant electrical output and allocation of the total demand to each NSSS module.

Table 2-1 NSSS CONTROL AND DATA SIZE

	Monitored and Controlled Analog Variables	Monitored Analog Variables	Monitored On-Off Variables	Controlled On-Off Variables
1. Reactor:				
Core support deflection.		25		
Vessel temperature.		30		
Helium inlet temperature.		4		
Helium outlet temperature.		4		
Core pressure differential.		6		
Rod in.			60	
Rod out.			60	
Rod position.		60		
Cable tension.		60		
Rods motor on-off.			60	30
Rod holding voltage.		4		
Mechanism temperature.		36		
Wide range log power.		18		
Linear power.	1	12		
2. Steam Generator:				
Circulator motor exciter temperature.		6		
Circulator shaft vibration/displacement.		16		
Rotor axial position.		2		
Motor exciter voltage.		6		
Motor exciter current.		6		
Circulator buffer helium supply flow.		2		
Motor Cooling water flow.		2		
Motor control breaker position.			2	1

Table 2-1 (Continued)

	Monitored and Controlled Analog Variables	Monitored Analog Variables	Monitored On-Off Variables	Controlled On-Off Variables
Magnetic bearing current.		10		
Magnetic bearing voltage		2		
Circulator compressor ΔPs.		4		
Cooling water temperature, outlet.	1	1		
Cooling water temperature, inlet.		2		
Cooling water shutoff valve position.	2			
Module main steam temperature.	1	3		
Module steam pressure.	1	3		
Circulator RPM.	2	2	4	
FW flow, inlet.	1	3		
Primary coolant helium flow rate.		3		
Helium pressure, inlet	1	3		
Helium pressure, outlet.		3		
Helium temperature, circulator inlet		3		
Helium temperature, outlet		6		
Feedwater flow control valve position.	1	3		
Main loop shutoff valve position.		4		
Main loop shutoff valve actuation pressure		1		
Main loop shutoff valve actuation valve position		1		
FW header pressure, inlet.		4		
ΔP FW/steam.		4		
FW temperature, inlet.		4		
Isolation and startup valve positions.				20
Isolation and startup breaker positions.				20
3. Shutdown Cooling System:				
Helium pressure, inlet.		3		
Helium pressure, outlet.		3		
Flow ΔP.		3		
Motor bearing temperature.		3		

Table 2-1 (Continued)

	Monitored and Controlled Analog Variables	Monitored Analog Variables	Monitored On-Off Variables	Controlled On-Off Variables
Cooling water, temperature, inlet.		2		
Cooling water, temperature, outlet.	1	2		
Cooling water flow.		2		
Helium temperature, inlet		3		
Oil reservoir level.		3		
Cooling water pressure.		3		
SCS motor RPM.	1	3		
Shutdown loop shutoff valve position.	1	2		
CW valve position, inlet.			2	
Motor current.		2		
CW valve position, outlet.			2	
Motor control breaker position.			2	1
Motor voltage.		2		
Isolation and start-up valve positions.				20
Isolation and start-up breaker positions.				20
4. Helium Purifications System:				
Water temperature.		2		
Pressure, N_2.		2		
Water level.		2		
Heater status (on/off).			4	1
Relief valve position.			4	1
N_2 inlet valve position.			2	1
Water inlet valve position.			4	1
Helium storage pressure.		2		
Helium shutoff valves.	2		2	1

Table 2-1 (Continued)

	Monitored and Controlled Analog Variables	Monitored Analog Variables	Monitored On-Off Variables	Controlled On-Off Variables
5. Service Water System:				
Valve position, inlet.			4	1
Valve position, outlet.			4	1
Water flow.		2		
Water pressure.		2		
Service water temperature, inlet.		2		
Service water temperature, outlet.		2		
Isolation and startup valve, position.				20
Isolation and startup breaker position.				20
6. Reactor Cavity Cooling System:				
Air temperature, inlet duct.		12		
Air temperature, outlet duct.		12		
Flow, outlet duct.		6		
Air temperature in top of cavity.		6		
Air temperature on middle of cavity.		3		
Air temperature on floor of cavity.		3		
Pressure in cavity.		3		
8. Miscellaneous:				
Cross duct temperatures.		20		
Concrete temperatures pressures.		40		
Cross duct pressure.		20		
Helium purification pressures.	1	8		
Helium purification temperatures.		6		
Fuel handling, equipment position.	12	32	60	40
TOTALS	30	597	276	199

2. Adjust NSSS operating conditions to accommodate plant configuration changes.

3. Stabilize the NSSS module under transient conditions.

The design selections to accomplish the above three actions are discussed in the following sections. (Table 3-3 shows the design selection for automatic control. Since these design selections translate into component-level requirements, the table has been located in the component requirements section of this document.)

2.2.3.1 Regulation of Steam Conditions

Each NSSS module is required to deliver 2400 psig, 1000°F steam to the high pressure turbine admission valves. In order to meet this requirement, each NSSS control subsystem regulates circulator speed (helium flow), reactor power and module feedwater flow. By providing automatic and continuous control adjustment of these parameters, the NSSS control system meets its required capability to deliver the demanded amount of steam at the required temperature and pressure (1000°F, 2400 psig). The command signals for adjusting these parameters are the output of the control subsystem.

The plant is required to change reactor and plant output under automatic control at a rate of up to and including 5% of rated output per minute of those reactors on line: Therefore, each NSSS module is able to change its output at a rate up to and including 5% per minute of rated output.

Additionally, in order to enter or leave the power production mode, each reactor module must be controlled automatically through the range of 0% to 25% of rated feedwater flow. This control is accomplished also by adjusting module feedwater flow, circulator speed and reactor power, plus additional parameters which include the steam generator isolation valve positions (inlet and outlet), startup bypass valve positions, and control rod and control rod bank configurations.

Figure 2-4 shows the basic NSSS control scheme and the major interfaces with other systems. For simplicity, the diagram shows a single reactor control unit. The heavier lines show the process system.

The primary control outputs from the NSSS are the circulator motor speed setpoint, the reactor flux setpoint, the module feedwater flow setpoint and control valve position (in lower part of fluid flow system), the steam generator exit isolation valve position (directly above feedwater flow control valve) and the startup bypass valve (to right of exit isolation valve). The turbine throttle valve control referred to on Figure 2-4 is part of the ECA (see Ref. 7). The primary control input to the NSSS from the PSCS is the load index shown by the downward arrow at the top of Figure 2-4. The primary control sub-modules are identified by name in the boxes shown on Figure 2-4.

2.2.3.2 Adjustment to Plant Configuration

The control system must be able to operate reactor modules independently of one another. The plant Supervisory Control Subsystem or the operators can schedule the desired even or uneven load distribution, and each NSSS Control Subsystem drives its NSSS module to its allocated load regardless of the status of the other modules. Module-to-module control independence is achieved by manipulating module feedwater flow individually in each module and using module feedwater flow as a module load index. Figure 2-5 illustrates this feedback control concept, which passes throttle pressure feedback requirements to the ECA in Section 4 of this document. Decoupling of interactions between the ECA and the NSSS module via this method of control contributes to plant stability. As Figure 2-5 shows, control of each module is independent of other modules and the ECAs.

Similarly, the NSSS control design makes provisions for the automatic removal and return of one or more reactor modules from service to perform maintenance or refueling, and return it to service with other reactors and turbines in operation. This removal and return is through a sequence of hold points discussed in Section 2.3.1.1.

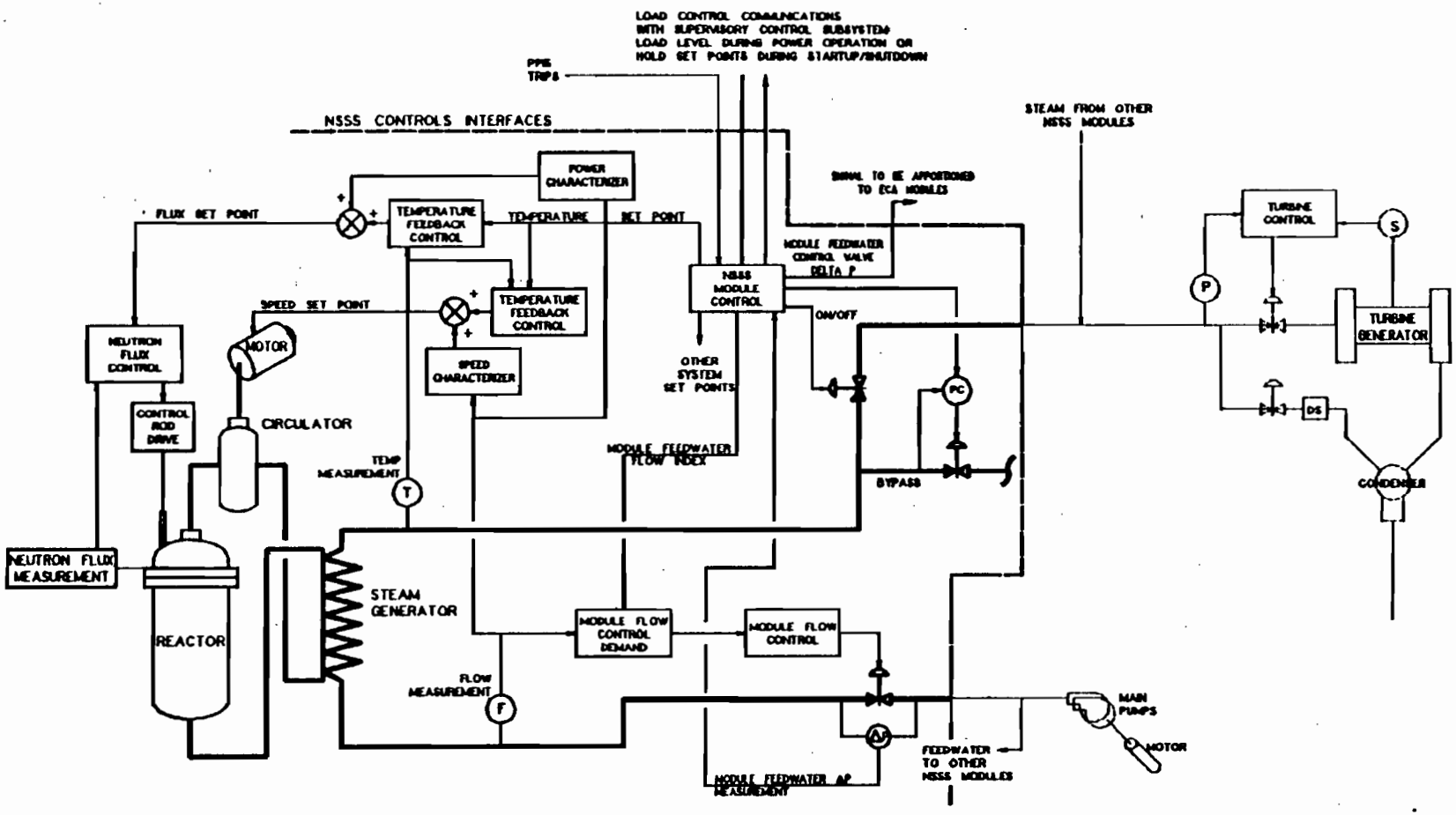


Fig. 2-4 NSSS CONTROL SCHEME AND INTERFACES

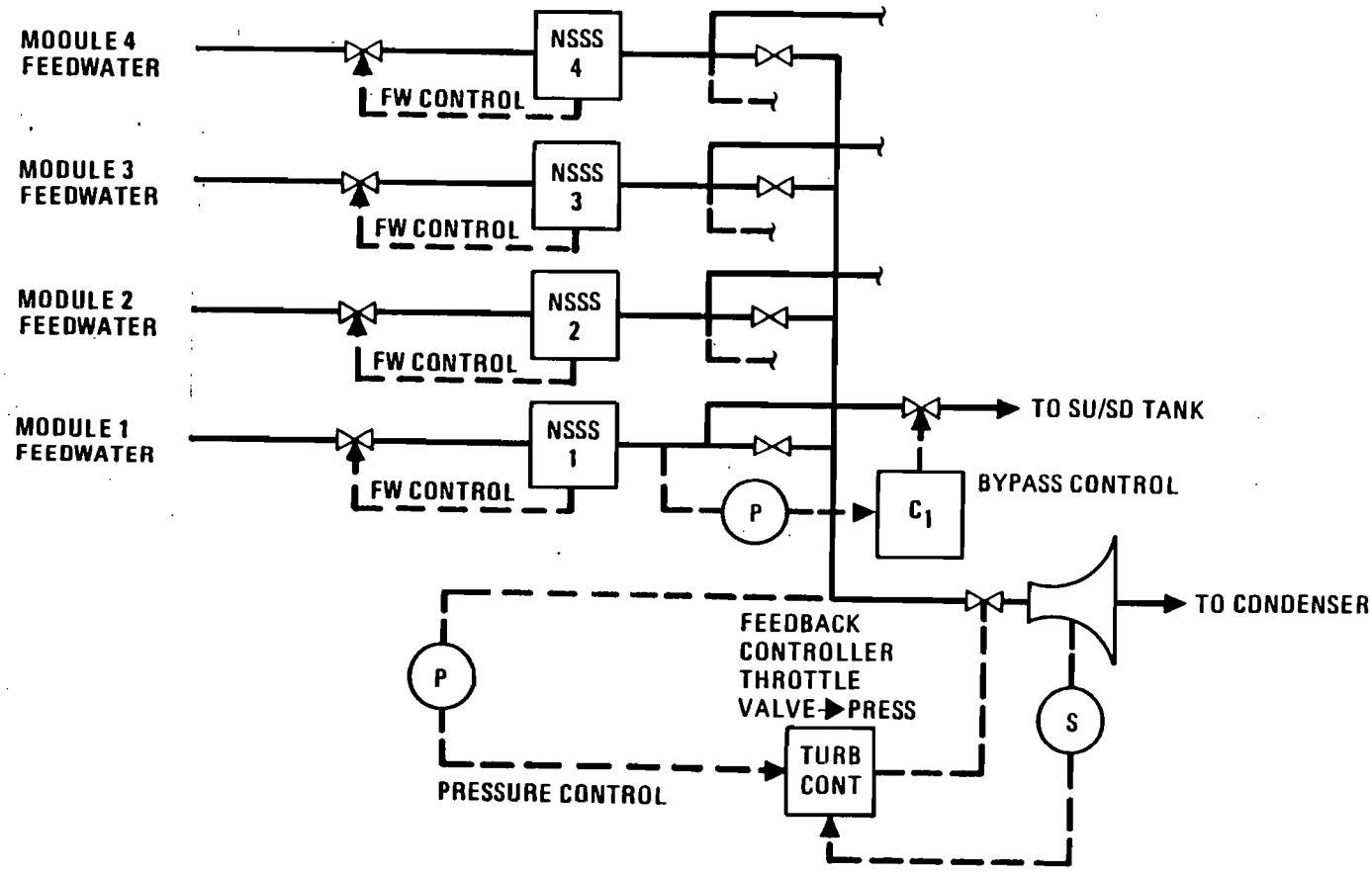


Fig. 2-5. INDEPENDENT MODULE FEEDWATER CONTROL, AND THROTTLE PRESSURE FEEDBACK TO THROTTLE VALVE.

2.2.3.3 Control System Stability

A detailed assessment of control system design selection trade-offs regarding true control stability provided by the control algorithms was provided during the conceptual design. The NSSS control scheme of Figure 2-4, along with specific control algorithms discussed in Section 3.0 and the interfacing ECA controller actions (Figure 2-5) provide the basic stability for the NSSS under any condition of change. The ability of the plant to provide sustained and controlled operation for the conditions below has been investigated and documented as part of the design process. Reference 1 contains the transient calculations which show plant stability with the NSSS Control Subsystem. The following specific requirements are satisfied by the NSSS control scheme:

1. Load rejection from full generator electric output to house electrical load without receiving a reactor trip signal.

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

3. Step changes of ±15% of plant output caused by utility electrical transmission grid frequency impacts.

Additionally, the NSSS controls are designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report.

In meeting the above requirements, the NSSS performs within the transient limitations specified in Table 2-2. These limitations are design selections which become requirements (see Section 3.2.3). The system is also designed to control the helium mass flow through the active steam generator bundle between 25% and 100% of nominal feedwater flow for steady-state operation as specified in Table 2-3 whenever a transient event

Table 2-2 NSSS TRANSIENT CONTROL REQUIREMENTS

Controller	Max Error from Setpoint	Range Limits	Rate Limits
Steam temperature	±40°F	25%-105%	--
Steam pressure	±50 psi	2200-2700 psia	--
Reactor power	±20%	10%-110%	4%/s
Circulator speed	±15%	5%-110%	4%/s
Turbine throttle valve	--	--	7.5%/s
Feedwater flow rate	[TBD]	15%-110%	2%/s

Table 2-3 CIRCULATOR CHARACTERIZER FUNCTION

Feedwater (% Design)	Circulator[a] Speed (% Design)
100	100.00
85	88.58
62.5	69.44
40	47.85
25	32.12

[a]Helium density correction = -2 rpm/% change in helium density at circulator inlet. Correction = 0.0 rpm at design condition.

occurs. These accommodations allow other plant systems to operate for the number of cycles specified in Table 5.1-3 of Ref. 2.

Each individual reactor module is capable of continuous operation under automatic control between 25% and 100% of nominal module feedwater flow and this supports the plant design requirement to sustain continuous operation through and following transients associated with the loss or failure of a major component, system, or train, including an individual reactor or turbine-generator.

2.2.4 Command Outputs

On the basis of the control decisions made, the NSSS Control Subsystem effects final control element action to bring steam conditions to desired levels. Figure 2-4 also shows the major NSSS control outputs: module feedwater flow control valve position, circulator motor speed input, and control rod position.

A preliminary design phase goal will be to develop detailed software interface requirements for the NSSS command/control hardware. Primary concerns will be maintenance and availability. The following design selections are directly applicable to requirements for the MHTGR design.

1. Systems will be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance.

2. Systems and components will be designed to facilitate hands-on maintenance.

2.2.5 Information Reporting/Data System

The NSSS Control Subsystem generates display information regarding NSSS status and conditions, and provides it to the supervisory control system and the operator stations. Communications and status information made

available at NSSS locations outside the control room as shown in Figure 2-1 allow for roving operators to control, under supervision from the control room, selected processes and control subsystems during energy production, shutdown, refueling, and startup/shutdown not requiring direct control room operator interfacing and interaction. The presentation formats for the data displays support the following activities:

1. Operations.
2. Test and Calibration.
3. Engineering Reporting.
4. Maintenance (hardware and software).
5. Management Reporting.

Each NSSS control subsystem module provides its own redundant data highway network which is be linked to the plant data highway network as shown in Figure 2-3. All failures of the data processing and control functions are automatically detected and reported.

NSSS information processing equipment includes computers for performance monitoring, status assessment, operator guidance, historical data base logs, calibration and equipment testing. Design selection trade-off studies to determine the hardware configuration were completed during the conceptual design. Two types of NSSS control system cabinets were determined and the functions of each are shown below.

	Display	Control	Print	Removable Magnetic Storage
NSSS Module Operator Interfaces	X	X	X	X
Limited Operator Interfaces (Four Locations per Module)	X	X		

The basic features described above meet the following top-level requirements from Section 1.

1. Capability of evaluating and determining the state of the NSSS and the corresponding module-level control state maneuvers required for simultaneous energy production, shutdown, refueling and startup/shutdown control.

2. Incorporation of internal diagnostic monitoring within the NSSS control subsystem to detect malfunctions.

3. Main control room alarming of malfunctions within major plant control and electric systems.

The NSSSCS concept supports the requirement to develop a reporting scheme that limits control room alarms to critical parameters leading to protective action for major plant components or loss of electrical production. This effort will incorporate the following utility/user goals for plant staffing determined in Ref. 2, Section 2.1.1.

1. Administration, operation, and maintenance by minimum plant staff consistent with the plant availability and safety goals.

2. Permanent operating staff maximum of 50 full-time personnel. This staff would include first line supervisors, operating, and operations maintenance support personnel.

3. Maximum shift staff of:

   a. 1 - senior licensed supervisor.
   b. 2 - licensed reactor operators in the control room.
   c. 4 - roving operators.

4. Evaluation of required operator response for each anticipated operating staff position. This evaluation shall be used to confirm that operator staffing is consistent with anticipated work loads and response times for normal, off-normal, and emergency conditions.

5. Permanent technical and security staff (excluding administrative and clerical staff) maximum of 70 full-time personnel. This staff would include first line supervisors and other personnel assigned in the categories of engineering, health physics, water and helium chemistry, laboratory staff, security, and other technical disciplines.

6. Permanent maintenance staff 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.

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

2.3.1 Subsystem Operating Modes

The NSSS control subsystem is in service during the following operations:

1. Startup and shutdown.
2. Normal operation.
3. Refueling.
4. Shutdown.
5. Abnormal operation.

The primary function is to control the NSSS to the required conditions during each of these operations.

2.3.1.1 Startup and Shutdown. Startup and shutdown covers the range of operating conditions encountered in the 0% to 25% module feedwater flow range. (See Table 5.3-3 of Ref. 2. Level of service "A" events 1 through 4.)

Dedicated equipment and provisions are used in the NSSS to startup and shutdown a module. For example, wide range nuclear flux instrumentation is provided to monitor and control core power from the source range up to the design power range. The total flux range spans several orders of magnitude (decades). Interfacing ECA actions are performed to startup and shutdown a reactor module. For example, the module steam bypass system allows hot water and steam produced during the startup and shutdown sequences to bypass the main steam header. To route the hot water and steam into this bypass, the module isolation valve, and bypass valve operate in a synchronized fashion. In order to allow independent operation of reactor modules, each module is equipped with its own bypass.

During startup or shutdown, the module main steam isolation and check valve is closed. This allows other reactor modules that may be on line to continue supplying steam to the turbine for power generation. Steam from the isolated module is passed via the module startup bypass valve to a flash tank. The bypass valve is modulated to control system pressure at the steam generator outlet through a pressure range of 700 to 2600 psia at the steam generator outlet.

The hot steam generator water and steam outlet temperatures during startup (and shutdown) ranges from 80°F subcooled liquid to rated 1005°F superheated steam. This temperature is controlled by the NSSS Control Subsystem by varying module feedwater flow, reactor power, and circulator speed. Feedwater inlet temperature is controlled by the ECA. During startup, the feedwater temperature ranges from 80°F to 380°F, while other modules operate with feedwater at the design temperature of 380°F. A startup feedwater system (part of the ECA) generates the appropriate feedwater temperature as demanded by the NSSS Control. The requirements for ECA control of this temperature are a control system interface which is identified in Section 4.

When a module reaches rated steam conditions in the startup sequence and it is requested by the Supervisory Control System to transfer its flow of

steam into the main steam header for use by the turbines, the NSSS Control Subsystem raises the module steam pressure via the startup bypass control valve control, above the main steam header pressure. This results in a slow closure of the module startup bypass valve and opening of the isolation check valve.

Table 2-4 shows the current planned startup sequence of a reactor module from depressurized helium conditions. The module is controlled automatically through a set of HOLD points that define the startup and shutdown sequences. During shutdown, special control gains are selected to allow automatic control of temperature with outlet steam conditions below rated values and feedwater flow less than 25%.

2.3.1.2 Normal Operation

Normal operation takes place in the load range between 25% and 100%. (See Table 5.1-3 of Ref. 2. Level of service "A" events 5 through 12 and level of service "B" events 15 and 16.) A brief description of steady state performance is contained in Section 2.3.2 and a description of response to plant transients is contained in Section 2.3.3. Reference 1 may also be consulted for information on transient events.

During normal operation, the NSSS load level setpoint is under continuous command from the PSCS. The NSSS Control Subsystem will respond automatically to this command. The NSSS control subsystem also allows operator command through consoles located within the nuclear island (see Section 2.4). This mode is under administrative control from the control room operators.

2.3.1.3 Shutdown

The NSSS Control Subsystem can enter one of two module shutdown modes; pressurized decay heat removal or depressurized decay heat removal. In the pressurized shutdown mode, the NSSS Control Subsystem automatically holds

Table 2-4
NSS MODULE STARTUP SEQUENCE FROM DEPRESSURIZED CONDITIONS

Time (h)	Action
STARTING POINT INITIATED FROM MAIN CONTROL ROOM	
0-0.5	Establish secondary pressure (startup bypass setpoint) to 1200 psia (17 psi/min)
0-5	Pressurize primary coolant vessel, perform precritical checks, and bring reactor to critical (0.5% power)
5-5.8	Increase feedwater flow to 15% (0.25%/min) Increase reactor power to 3% (0.053%/min) Increase circulator speed from 5% (minimum value) to 12.5% (0.16%/min)
6-10	(Hold at about 400°F steam generator secondary outlet temperature for feedwater cleanup and reactor vessel warmup as necessary)
HOLD TO ALLOW OPERATOR CLEARANCE TO CONTINUE	
10-10.5	Increase secondary pressure to 1800 psia (20 psi/min)
11.1-13.8	Increase feedwater temperature from 220°F to 380°F (1.0°F/min)
11.1-12.8	Increase power to 7% (0.039%/min)
HOLD TO ALLOW OPERATOR CLEARANCE TO CONTINUE	
12.8-13.3	Increase power to 16% (0.30%/min). Increase circulator speed to 30% (0.58%/min)
13.0-13.6	(Transition to boiling)
14.3-16.3	Decrease reactor power to 14.7% (0.011%/min)
14.5-18.6	(Hold at about 800°F main steam temperature for secondary component warm-up as necessary)
HOLD TO ALLOW OPERATOR CLEARANCE TO CONTINUE	
18.1	Place reactor power and circulator speed in automatic main steam temperature control (setpoint at 826°F)
18.6-20.1	Ramp main steam temperature setpoint to 1005°F (2.0°F/min)

Table 2-4 (Continued)

Time (h)	Action
19.1-20.1	Increase secondary pressure setpoint to 2450 psia (11 psi/min)
HOLD TO ALLOW OPERATOR CLEARANCE TO CONTINUE	
20.1-20.8	Stabilize module parameters and transfer steam flow from startup bypass to main steam header. Place feedwater flow in automatic control

circulator speed at 20% of design and feedwater flow at 15% of design. These conditions are sufficient to avoid core recirculation and to maintain subcooled conditions at the steam generator outlet.

In the depressurized shutdown mode, the NSSS Control Subsystem automatically holds circulator speed at 100% of design and supplies enough feedwater flow so boiling does not occur in the steam generator. The NSSS Control Subsystem is configured to allow core decay heat removal at subatmospheric reactor pressure. Helium is circulated through the module main loop in a balance with feedwater flow so that no boiling occurs in the steam generator and core outlet helium temperature remains less than 240°F. This is accomplished automatically by the NSSS Module Control Subsystem after reactor depressurization and on receipt of a refueling mode enable.

2.3.1.4 Refueling

The NSSS is configured to allow core decay heat removal via the SCS during refueling at subatmospheric reactor pressure. Helium is circulated and heat is extracted through the SCS heat exchanger. The SCS is placed on-line automatically by the NSSSCS after reactor depressurization and on receipt of a refueling mode enable.

When a reactor module is in the refueling mode, the primary function of the NSSSCS is data acquisition and information reporting to the PSCS. Many monitoring and control functions are administratively allowed at the reactor area. Most of the human interface are through the NSSS control console near the refueling area.

2.3.1.5 Abnormal Operation

Abnormal operation includes all operation not described above. Section 2.3.3 contains a brief description of NSSS control response to several abnormal events (e.g., B and C events identified in Table 5.3-3 of Ref. 2).

Reference 1 contains additional information on transient response to abnormal events.

In this mode of operation, the control hierarchy of the PSCS and the NSSCS can be reversed. The NSSSCS responds directly to keep the affected module within its operating range when it is notified of an abnormal event through the PPIS data interface (see Section 4). However, the PSCS is informed by the NSSCS of the situation simultaneously, and it may cause other unrestricted NSSS modules to make up for any loss of load in the affected module. The control system actions are entirely independent of the PPIS, and are not part of or necessary to the safety-related features of the plant.

Two additional features of the NSSSCS design address response to abnormal events. These are as follows:

1. Design features are included to facilitate continued plant operation if a control failure occurs.

2. Features are included to limit recovery time when a protection trip occurs.

The above features are necessary to meet the NSSSCS availability allocation discussed in Section 3.

2.3.2 Subsystem Steady-State Performance

The NSSSCS controls steam conditions within the tolerances listed in Table 5.12-1 of Ref. 2 during all steady state operation. The system also monitors the NSSS performance based on the measurements listed in Table 2-1. Each NSSS Control Subsystem module provides information regarding the NSSS module performance through the data highways. The operators have access to this information, as well as other plant information. The

NSSS information is also available at local operator interfaces within the reactor operations area.

2.3.3 Subsystem Response to Plant Transients

Control of module main steam temperature is accomplished by the NSSS Control Subsystem by manipulating reactor power and circulator speed. Steam temperature is kept between 990°F and 1014°F during a 100% to 25% load ramping maneuver. One hour after initiation of this maneuver, main steam temperature deviations are negligible and reactor power deviations are within the control algorithm deadband. (See transient response Figure 2-5 through 2.8 of Ref. 1.) During a 15% step load change from full load, module main steam temperature control maintains temperature between 99°F and 1025°F (e.g., see transient response Figure 2.10a of Ref. 1). Special steam temperature controls used following a module reactor trip significantly limit thermal transients in the steam generator: by ramping down main steam temperature setpoint at rates beginning at 1.0°F/s from 1005°F to saturation, then returning circulator speed to feedforward demand through a 30 s time constant, the NSSS Control Subsystem tightly controls the removal of stored heat from the core and heat transfer into the secondary fluid. Runback and steam bypass functions allow individual operation of the remaining, untripped MHTGR reactor modules by the NSSS Control Subsystems. Reference 1 shows examples of reactor trip response. In load range operation, if one or more reactor trips occur, the feedwater flow to each tripped module is ramped back on a schedule by its NSSS Control Subsystem to 15%. The schedule is given in Table 3-3. Simultaneously, the Supervisory Control System is notified, and it causes the other reactor modules or the turbine load to adjust on a matching schedule to make the turbine load compatible with available flow from the untripped modules.

Compatible ECA settings for bypass and relief valves are required to obtain the predicted response for turbine trip. (See Figure 2.15a in Ref. 1.) The turbine bypass and startup bypass setpoints for load range operation

are set for 2475 psig and 2575 psig, respectively in this example. The turbine bypass acts during turbine side upsets such as turbine trip, while the startup bypass acts during events such as startup, shutdown, and reactor trip. The isolation valve separates the module(s) from the main steam header on startup or shutdown.

2.3.4 Subsystem Failure Modes and Effects

Parts of the NSSS Control Subsystem are redundant and single failure proof. Therefore, a failure in one of these subsystem parts allows the system to respond correctly. A failure within the system is alarmed or identified during the routine surveillance testing of the system. The NSSS Control Subsystem is designed to operate correctly on disconnection of any failed parts of the system or loss of power.

Table 2-5 shows the preliminary failure modes and effects analysis for the major NSSS Control Subsystem loops.

2.4 SUBSYSTEM ARRANGEMENT

The location of NSSS control hardware and resulting requirements for access, HVAC, etc. which are imposed on nuclear island buildings come from the following requirements.

1. Location of controls in proximity of the system being controlled.
2. Controls and instrumentation/operator interface design to enhance operator response.
3. Individual personnel access for 40 h per week performance.
4. Seismic, site, and environmental requirements.

Based on the above requirements, plus the reliability and maintainability requirements of Section 1, the architecture design selection for the NSSS Control Subsystem is of the distributed digital type.

Table 2-5
FAILURE MODES AND EFFECTS ANALYSIS

Failure Mode	Failure Effect	Detection Method	Remarks
Module Main Steam Temperature Control Output Fails:			
High:	Reactor power or circulator speed increases. Possible PPIS reactor module trip on high power to flow ratio.	Measured neutron flux, circulator speed and primary coolant flow. High main steam temperature alarm in NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Low:	Reactor power or circulator speed decreases. Possible circulator speed to feedwater flow mismatch trip or main turbine trip on low steam temperature.	Measured neutron flux, circulator speed and main steam temperature. Low main steam temperature alarm in NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Module Feedwater Flow Control Output:			
High:	Reactor module output increases beyond load allocated by the supervisory control system. Possible PPIS action on exceeding module load output limits.	High module load alarm in the supervisory control system. High feedwater flow alarm in NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

Table 2-5 (Continued)

Failure Mode	Failure Effect	Detection Method	Remarks
Low:	Reactor module output decreases to less than load allocated by the supervisory control system. Possible PPIS action on module parameters decreasing to less than investment or safety limits.	Low module load alarm in the supervisory control system. Feedwater flow error high alarm in NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Reactor Power Control Command Output Fails:			
High:	Module reactor power increases. Group rod insertion occurs on high neutron flux. Possible PPIS action to trip module when parameters increase to investment or safety limits.	High measured neutron flux and main steam temperature alarm in the NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Low:	Module reactor power decreases. Module primary and secondary coolant temperatures decrease. Possible PPIS action to trip module when parameters decrease to investment or safety limits.	Low measured neutron flux and main steam temperature alarm in the NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.

Table 2-5 (Continued)

Failure Mode	Failure Effect	Detection Method	Remarks
Circulator Speed Control Output Fails:			
High:	Module circulator speed increases. PPIS speed-to-primary coolant flow mis-match trip.	Measured circulator speed high alarm in the NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Low:	Module circulator speed decreases. PPIS speed-to-primary coolant flow mis-match trip.	Measured circulator speed low alarm in the NSSS control system.	Possible loss of one reactor module output. Remaining modules can operate at full output. Control hardware and software fault tolerance may allow minimum decrease in affected module output.
Load Following Command Signal Failure:			
Load increase not received:	No change in module steam flow or steam conditions.	Measured feedwater flow.	Modules will stay on-line. Software may detect condition.
Load decrease not received:	No change in module steam flow or steam conditions.	Measured feedwater flow.	Modules will probably stay on line. Software may detect condition.

2.4.1 NSSS Systems Interface Stations

Four control stations are used for each reactor module for NSSS control. One of the four stations is used for SCS interface. (The SCS is provided with its own control systems.) All of these stations are connected to the NSSS data highway. Table 2-6 shows the distribution of data and command variables, and each of the locations is explained as follows:

1. The HTS station is located near the main circulator motor control. It provides command and instrumentation interfaces for the main circulator motor, the magnetic bearings, the motor cooling system and other HTS subsystems.

2. The Reactor System station is located in the reactor auxiliary building near the PPIS equipment. This station interfaces with the nuclear instrumentation cabinets and the PPIS. It sets reactor power levels in the power operating range and schedules rod run-in or withdrawal sequencing for startup or shutdown. It also acquires data from the PPIS via a unidirectional isolation

3. The NSSS Feedwater and Steam Bypass Station is located near the feedwater and main steam grade level entry/exit points of each reactor building.

4. The SCS station is located near the SCS circulator motor power supply. It interfaces with the SCS control and acquire SCS information.

2.4.2 NSSS Operations Stations

Each reactor module has an operator control station. The DMS interface for a particular reactor module is located at this station.

Table 2-6 DISTRIBUTION OF CONTROL STATIONS

Data Highway Station Description	Interfacing Systems	Command I/O Variables	Data I/O Variables
NSSS Operations Station	Plant Supervisory Control System Data Highway (PSCS)	100	250
HTS Station	Heat Transport System (HTS)	3	110
	Service Water System	--	60
	Other NSSS Systems	--	40
Reactor Systems Station	Reactor System	4	520
	Helium Purification System	8	220
	PPIS	--	100
NSSS Feedwater and Startup Bypass Station	Feedwater Supply System	4	40
	Turbine System	2	10
	Startup Bypass System	1	10
SCS Control Station	Shutdown Cooling System	3	80

This station provides the data management features necessary to accept direction from and report information to roving operators and to the PCDIS data highway. It also drives the redundant NSSS data highways, which carry data and control information to the four NSSS control stations discussed in Section 2.4.1.

Figure 2-1 shows the general arrangement of the reactor and support buildings where the NSSSCS stations are located.

2.5 INSTRUMENTATION AND CONTROL

The NSSS Control Subsystem is itself an instrumentation and control system. Therefore, it is described throughout this entire document.

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

3.1 COMPONENT FUNCTIONS

The functions that the NSSSCS components provide are:

1. Interfacing the operation of a particular NSSS module with the operation of other parts of the plant. This includes interfacing with Nuclear Island local operators, the PSCS, and ECA controls.

2. Controlling and communicating with NSSS module systems and subsystems, including acquiring the necessary data for reporting status of each NSSS module.

The control selection studies determined two types of distributed control hardware components and one software component for accomplishing these functions. These components are discussed next.

3.1.1 NSSS Operations Station

The NSSS operations station (one station provided for each NSSS module) provides the following functions.

1. Communicating with the plant data highway, the ECA controls, and the PPIS. (The PPIS is not part of the NSSSCS.)

2. Controlling data flow within the connecting control stations which comprise the distributed control system for a particular NSSS module.

3. Maintaining a reportable data base reflecting the state of the NSSS and the corresponding module-level control state maneuvers.

4. Accepting PSCS commands through the plant data highway and assurance of continuous operation through design transients and other events.

5. Interfacing and interacting with operators outside the control room during energy production, shutdown, refueling, and startup/shutdown.

3.1.2 NSSS Systems Interface Station

The NSSS systems interface station (four stations per module) provides the following functions:

1. Connection of digital or analog data sources from adjacent NSSS systems with the NSSSCS and processing these signals for control and for transmission to the NSSS data highway.

2. Automatic regulation of NSSS outlet conditions through command of actuators and devices under the control of adjacent NSSS subsystems.

3.1.3 NSSS Control Software

The NSSS control software provides all of the software features necessary to perform the NSSS operations station and NSSS system interface station functions. This includes NSSS information reporting, storage and display, and automatic NSSS control response to transients or energy production demands.

The software contains logic and algorithms which perform the functions described in Section 2.2.3.

3.2 COMPONENT DESIGN REQUIREMENTS

Component requirements for this subsystem arise from the system design requirements in Section 1.2, from design selection in Section 2, and from trade-off studies, which lead to those design selections.

3.2.1 NSSS Operations Station Component Design Requirements

3.2.1.1 Component Configuration and Essential Features Requirements

The NSSS operations station shall be independent of the PPIS. It shall receive protection information via a unidirectional isolator. (3701.0302.101)

Components shall be of solid state, standardized, modular, plug-in design. Any module may be easily removed from the system and replaced without breaking or making solder-type connections and without recourse to alteration, force selection, or wiring changes. (3701.0302.102)

Physically separated interconnecting cables shall be plug-connected at both ends wherever possible. (3701.0302.103)

A communication protocol that is recognized by the PCDIS data highway and by the distributed NSSS systems interface stations. (3701.0302.104)

The NSSS operations station shall operate the NSSS Control Subsystem data highway, which ties together a particular NSSS Control System. The data highway shall not be susceptible to electromagnetic noise or interference. (3701.0302.105)

3.2.1.2 Operational Requirements

The NSSS operations station shall provide the capability for operator control of its NSSS module outside of the control room during energy production, shutdown, refueling, and startup/shutdown. (3701.0302.106)

The NSSS operations station shall maintain a data base which is adequate for evaluating and determining the state of the NSSS and the corresponding module-level control state maneuvers. Design requirements shown in Table 3-1 shall be met during all possible combinations of events or plant states. (3701.0302.107)

3.2.1.3 Structural Requirements

Nonsafety-related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum. (3701.0302.108)

3.2.1.4 Environmental Requirements

The NSSS operations station shall be designed and built for continuous service under the environmental conditions shown in Table 3-2. (3701.0302.109)

The NSSSCS shall be configured to enable maintenance of NSSSCS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant lifetime as defined in OPDS Table 5.1-4. (3701.0302.110)

3.2.1.5 Instrumentation and Control Requirements

The NSSS operations station is an instrumentation and control component. Its requirements are distributed over the entire Section 3.2.1.

Table 3-1 NSSS OPERATIONS STATION DESIGN REQUIREMENTS

Control command acknowledge time	0.5 s
Maximum sampling period	0.5 s
Maximum control action period	0.5 s
Minimum automatic data storage time span	(TBD)
Data processing (mass, energy, nuclear balances, etc.)	5000 algebraic equations
Real time displays	20 pages

Table 3-2 NSSS OPERATIONS STATION OPERATING REQUIREMENTS

Power sources needed:

120 V, 60 Hz, 15 kVA

Equipment operating limits:

40°F to 120°F ambient temperature
10% to 90% relative humidity
≤0.15 g seismic acceleration at ground level

Nominal working conditions:

70°F to 80°F service building
65°F to 85°F reactor building
<(TBD) dB noise level
<(TBD) r/h radiation exposure level
>(TBD) lighting

(NOTE: TBD levels allow O&M access.)

3.2.1.6 Surveillance and In-Service Inspection Requirements

Refer to Section 1.2.6.

3.2.1.7 Availability Assurance Requirements

The NSSS operations station shall be designed to meet NSSSCS reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The NSSSCS shall be designed to meet an overall reliability allocation of <12 equivalent forced outage hours per year.

(3701.0302.113)

The NSSS operations station shall utilize diversity, redundancy, functional partitioning, or single failure proofing to meet its availability allocation. (3701.0302.114)

3.2.1.8 Maintenance Requirements

The NSSS operations station shall have automatic surveillance and announcement features. (3701.0302.112)

The NSSS Control Subsystem shall provide uninterruptible operation while equipment is serviced. This shall include redundant measurement inputs and equipment, and emergency standby units that bypass controllers for servicing without losing indication or ability to manipulate the final control elements. The NSSS operations station shall comply with this requirement. (3701.0302.115)

The NSSS operations station shall be serviceable with the plant on-line.

(3701.0302.116)

The NSSS operations station shall be provided with easy to follow preventive maintenance and equipment repair documentation, subsystem/equipment

failure clearing procedures, all spare parts needed to assure the required level of subsystem availability and training requirements. (3701.0302.117)

The NSSS operations station, components, and parts shall provide for interchangeability. This includes mechanical and electrical interchangeability. (3701.0302.118)

Special maintenance tools shall be provided by the equipment vendor. (3701.0302.119)

3.2.1.9 Safety Requirements

There are no safety requirements for the NSSS operations station.

3.2.1.10 Codes and Standards Requirements

NSSSCS design, analysis, fabrication, and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes, and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justified in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities.

DOE NE F2-10, Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1). (3701.0302.120)

3.2.1.11 Quality Assurance Requirements

The NSSS operations station shall come under the quality assurance program stated in Section 1.2.11. (3701.0302.122)

3.2.1.12 Construction Requirements

The NSSS operations station shall be constructed using materials and workmanship at least equal to the highest grade of industrial control equipment. (3701.0302.123)

Grounding, shielding, cabling, and wiring will not be susceptible to external electromagnetic and electrostatic interference and will not generate electromagnetic noise. (3701.0302.124)

All cabinets, racks, modules, cables, and terminal blocks shall be labeled in accordance with the schematics, wiring, an constructions drawings. (3701.0302.125)

The NSSS operations station design shall be based upon parallel construction of the complete plant as described in Section 5.1.2 of Ref. 2, however, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3701.0302.126)

3.2.1.13 Decommissioning Requirements

[Later]

3.2.2 NSSS Systems Interface Station Component Design Requirements

3.2.2.1 Component Configuration and Essential Features Requirements

The NSSS systems interface station shall be independent of the PPIS. It shall receive protection information via a unidirectional isolator. (3701.0302.201)

Components shall be of solid state, standardized, modular, plug-in design. Any module shall be easily removed from the system and replaced without breaking or making solder-type connections and without recourse to alteration, force selection, or wiring changes. (3701.0302.202)

Physically separated interconnecting cables shall be plug-connected at both ends wherever possible. (3701.0302.203)

A communication protocol that is recognized by the distributed NSSS systems interface stations and by the NSSS operations station shall be utilized. (3701.0302.204)

The NSSS systems interface station shall provide the capability to handle high- and low-level analog and digital I/O as required for NSSS system interfacing under all modes of plant operation. (3701.0302.205)

Data shall reference a common time base. (3701.0302.206)

The hardware configuration of every NSSS systems interface station shall be identical. (3701.0302.207)

3.2.2.2 Operational Requirements

The NSSS systems interface station shall provide the capability for limited operator interaction outside of the control room during energy production, shutdown, refueling, and startup/shutdown. (3701.0302.208)

3.2.2.3 Structural Requirements

Nonsafety-related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum. (3701.0302.209)

3.2.2.4 Environmental Requirements

The NSSS systems interface station shall be designed and built for continuous service under the environmental conditions shown in Table 3-2. (3701.0302.210)

The NSSSCS shall be configured to enable maintenance of NSSSCS equipment within a plant total scheduled outage time of less than 876 h per year averaged over the plant lifetime as defined in OPDS Table 5.1-4. (3701.0302.212)

3.2.2.5 Instrumentation and Control Requirements

The NSSS systems interface station is an instrument and control component. Its requirements are distributed over the entire Section 3.2.2.

3.2.2.6 Surveillance and In-Service Inspection Requirements

Refer to Section 1.2.6.

3.2.2.7 Availability Assurance Requirements

The NSSS systems interface station shall be designed to meet NSSSCS reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The NSSSCS shall be designed to meet an overall reliability allocation of <12 equivalent forced outage hours per year. (3701.0302.214)

The NSSS systems interface station shall utilize diversity, redundancy, functional partitioning, or single failure proofing to meet its availability allocation. (3701.0302.215)

3.2.2.8 Maintenance Requirements

The NSSS systems interface station shall have automatic surveillance and announcement features. (3701.0302.213)

NSSS systems interface station design shall provide uninterruptible operation while equipment is serviced. This shall include redundant measurement inputs and equipment, and emergency standby units that bypass controllers for servicing without losing indication or ability to manipulate the final control elements. (3701.0302.216)

The NSSS systems interface station shall be serviceable with the plant on-line. (3701.0302.217)

The NSSS systems interface station shall be provided with easy to follow preventive maintenance and equipment repair documentation, subsystem/equipment failure clearing procedures, all spare parts needed to assure the required level of subsystem availability and training requirements. (3701.0302.218)

The NSSS systems interface station, components, and parts shall provide for interchangeability. This includes mechanical and electrical interchangeability. (3701.0302.219)

Special maintenance tools shall be provided by the equipment vendor. (3701.0302.220)

3.2.2.9 Safety Requirements

There are no safety requirements for the NSSS systems interface station.

3.2.2.10 Codes and Standards Requirements

NSSSCS design, analysis, fabrication, and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes, and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justified in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities.

DOE NE F2-10, Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1). (3701.0302.221)

3.2.2.11 Quality Assurance Requirements

The NSSS systems interface station shall come under the quality assurance program stated in Section 1.2.11. (3701.0302.223)

3.2.2.12 Construction Requirements

The NSSS system interface station shall be constructed using materials and workmanship at least equal to the highest grade of industrial control equipment. (3701.0302.224)

Grounding, shielding, cabling, and wiring will not be susceptible to external electromagnetic and electrostatic interference and will not generate electromagnetic noise. (3701.0302.225)

All cabinets, racks, modules, cables, and terminal blocks shall be labeled in accordance with the schematics, wiring, an constructions drawings.
(3701.0302.226)

The NSSS system interface station design shall be based upon parallel construction of the complete plant as described in Section 5.1.2 of Ref. 2, however, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.
(3701.0302.227)

3.2.1.13 Decommissioning Requirements

[Later]

3.2.3 NSSS Control Software Component Design Requirements

3.2.3.1 Component Configuration and Essential Features Requirements

The software shall be of a standardized design. (3701.0302.301)

Four (4) identical software packages shall be utilized in the design. One software package shall be provided for each NSSSCS. (3701.0302.302)

The software shall provide data for other plant control algorithms. A calculated value of flow control valve ΔP shall be provided to the ECA.
(3701.0302.303)

3.2.3.2 Operational Requirements

[Table 3-3, should be referenced for further explanation of the design requirements given below.]

Table 3-3
4 x 350 MW(T) MHTGR
REFERENCE CONTROL SYSTEM ALGORITHM GAINS FOR NSSS CONTROL SYSTEM

	Proportional	Integral	Derivative
Throttle pressure (Valve-fract/psia)	-0.0015[a]	0.025	0.0
Main steam temperature (PWR-fract/°F)	3E-3 + 4E-3*FWN[b]	4E-4 + 4.3E-3*FWN	151.5 - 106*FWN
Main steam temperature (rpm/°F)	4.04+4.0*FWN	0.0	93.3-53.3*FWN
Main steam temperature (reactor trip) (rpm/°F)	3.33+6.67*FWN	0.0069	16.667
Neutron flux	On-off control	On=±0.004*VA	Off=±0.001*VA
Shim rod insertion	On-off control	On=-0.015	Off=-0.008
Auto control rod shim	Regulating rod bank is reshimmed if position is less than 15% inserted or more than 85% inserted		
Circulator speed	Equal to demand unless torque or power limited		
Steam temperature meas. time const.	17.5667-2.667*FSN FWN = FW/FWD (1.0 < FWN < 0.25) FW = feedwater flow rate (lbm/s) FWD = design feedwater flow rate FSN = FS/FSD FS = SG outlet flow rate (lbm/s) FSD = design main steam flow rate VA = load index (fract) (0.25 < VA < 1.0)		

[a] The negative sign on the proportional gain in the throttle pressure control loop accounts for the phase reversal inherent in valve closing resulting in increased throttle pressure and valve opening resulting in decreased throttle pressure.

[b] If temperature control of circulator inactive (i.e., loop open, control limited, or circulator motor power limited), gain is attenuated by 3.5 dB.

Table 3-3 (Continued)

	AFF	FFSIG	CAL	TCDEP (s)	TCF (s)	TCMESI (s)	TCF2	VCONS	VMIN	VMAX	VRATE	FCT
Throttle-press./ admission valve	0.95 (fract)	VA (load index)	25.0[7]	0.0	0.0	0.0	0.0	2415 (psia)	0.0 (valve-fract)	1.0 (valve-fract)	0.075[6] (valve-fract/s)	∞[7]
MS temp.-reactor power	Funct	FV2(1) + VCONC(5)	0.5	5.0	20.0	14.9 (Adapt)[5]	30.0	1005°F (Sched)[4]	0.1 (Fract) (Adapt)[1]	1.10 (Fract) (Adapt)[1]	0.04 (Fract/s)	5.0
MS temp.-circulator speed	Funct	FL(1,1,1)	0.0	2.0	20.0	14.9 (Adapt)[5]	30.0	1005°F (Sched)[4]	286.0 (rpm) (Adapt)[2]	6292.0 (rpm) (Adapt)[2]	228.8 (rpm/s)	N/A
Feedwater flow	302.46 (lbm/s)	VA[3]	0.0	3.0	0.0	2.0	0.0	Sched	45.37[3] (lbm/s)	332.71 (lbm/s)	6.049 (lbm/s^2)	N/A

Definitions:

- AFF = feedforward gain characterizer
- FFSIG = feedforward signal
- CAL = deadband for gain attenuaton
- FCT = deadband, gain attenuation factor
- TCDEP = actuator time constant
- TCF = FFSIG filter time constant
- TCMES1 = measurement time constant
- VCON/VCONS = design/setpoint
- VMIN/VMAX = control algorithm output range
- VCONC = char. coeff.
- VRATE = rate limit
- FL(1,1,1) = module feedwater flow
- TCF2 = feedforward lead time constant
- FSN = normalized steam flow fraction

(1)Controller output limited to ±20% of nominal reactor power (= ±0.2 fract.) in addition to VMIN and VMAX absolute limits.

(2)Controller output limited to ±15% of nominal circulator speed (= ±858 rpm) in addition to VMIN and VMAX absolute limits.

(3)Load runback rate following a reactor trip: 0.7%/s (= 2.1 lbm/s^2) to 25%, then 0.1% (= 0.3 lbm/s^2) to min. Runback held at 25% until MS measured decreases below 950°F. Load runback rate following a turbine trip: 0.25% (= 0.756 lbm/s^2). Feedwater minimum setpoint following reactor trip: 15% (= 45.37 lbm/s); feedwater minimum setpoint following turbine trip: 25% (75.615 lbm/s).

(4)MS temperature setpoint schedule following reactor trip: = -1.0°F/s from 1005°/F to 920°F, then = -0.30°F/s to saturation. Runback at first ramp rate is held at 920°F until MS measured decreases below 950°F. Second ramp is continuous to saturation. The runback is delayed until a SG helium inlet temperature tracker has released. The tracker is engaged when the SG helium inlet temp. rises within 20°F of PPIS trip. It releases when the temperature drops 10°F below a peak condition. When demand reaches saturation, speed is returned to feedforward setpoint through a 30 s time constant.

(5)17.5667-2.667*FSN.

(6)Fast valving (e.g., unit trip) rate limit is 5.0.

(7)Note: CAL = 10.0; FCT = 10 in FY87 design basis analysis. Table shows FY87 agreements for ECA control interface which have not been evaluated.

The control algorithms shall use integral control with accuracy sufficient to regulate the NSSS steam conditions required in Table 1-2. Column 2 of Table 3-3 gives the integral terms required in the control algorithms. (3701.0302.304)

The control algorithms shall be tested using simulation under each of the [TBD] design basis events given in Table 5.1-3 of Ref. 2. (3701.0302.305)

The module feedwater flow shall be commanded in proportion to the module load and used by the NSSSCS as a lead parameter in scheduling other NSSS control parameter load changes and plant configuration changes. (3701.0302.306)

The NSSS control software shall utilize scheduling algorithms to accommodate load rejection, turbine trip, or step changes in plant output up to ±15% per notes 1 through 6 on Table 3-3. The NSSS reactor module shall normally be controlled to avoid reactor trip if one of these events occurs. (3701.0302.307)

The recovery strategy shall allow resumption of reactor power following a protection trip within [TBD]. (3701.0302.308)

The NSSS control software shall maintain hardware scheduling rates (and hardware interface requirements) capable of meeting the maximum load scheduling rate (5%/min). (See VRATE and other data in Table 3-3.) (3701.0302.309)

The NSSS control software shall include limiters and other appropriate means to allow NSSS systems to meet the transient control requirements given in Table 2-2. This requirement has two purposes during normal operation with module feedwater flow between 25% and 100% as follows:

1. The NSSS shall operate within protection system trip settings.

2. The NSSS shall operate within design basis transient limitations needed to achieve the number of operating cycles specified in Table 5.1-3 of Ref. 2.

(3701.0302.310)

The NSSS control software shall schedule the relationship between module feedwater flow and helium flow for steady-state operations given in Table 2-3. (3701.0302.311)

The NSSS control software shall utilize feedforward and feedback control to assure continuous automatic control between 25% and 100% of nominal module feedwater flow. (3701.0302.312)

The NSSS control software shall utilize the scheme defined in Table 3-3 to assure continuous operation of the HTS following a reactor trip.

(3701.0302.313)

The NSSS control software shall utilize adjustment of gains based on module feedwater flow rate and shall combine the effects of circulator control and reactor control and assure continuous stability of the main steam temperature in all modes of operation. (See main steam temperature control, Table 3-3). (3701.0302.314)

The NSSS control software shall have design features which allow transition to a stable condition following a reactor or turbine trip. A reactor trip control for main steam temperature shall provide cooling rates satisfactory to the HTS and other NSSS systems during shutdown. Table 3-3 specifies the reactor trip control algorithms for main steam temperature.

(3701.0302.315)

3.2.3.3 Structural Requirements

The NSSS control software has no structural requirements.

3.2.3.4 Environmental Requirements

The NSSS control software has no environmental requirements.

3.2.3.5 Instrumentation and Control Requirements

The NSSS control software is an instrumentation and control component. Therefore, requirements are distributed over this entire section.

3.2.3.6 Surveillance and In-Service Inspection Requirements

Refer to Section 1.2.6.

3.2.3.7 Availability Assurance Requirements

The NSSS control software has no availability assurance requirements.

3.2.3.8 Maintenance Requirements

The NSSS control software shall support the self-checking and announcement features of the NSSS operations station and the NSSS system interface station. (3701.0302.317)

The NSSS control software shall support all of the maintenance requirements in Sections 3.2.1.8 and 3.2.2.8. (3701.0302.318)

3.2.3.9 Safety Requirements

The NSSS control software has no safety requirements.

3.2.3.10 Codes and Standards Requirements

NSSSCS software design analysis shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated

Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes, and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justified in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities.

DOE NE F2-10, Quality Assurance Program Requirements (Supplement to ANSI/ASME NQA-1). (3701.0302.319)

3.2.3.11 Quality Assurance Requirements

The NSSS control software shall come under the quality assurance program stated in Section 1.2.11. (3701.0302.320)

3.2.3.12 Construction Requirements

The NSSS control software shall be based upon parallel construction of the complete plant as described in Section 5.1.2 of Ref. 2, however, features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine. (3701.0302.321)

3.2.3.13 Decommissioning Requirements

The NSSSCS software shall include features that accommodate decommissioning or refurbishment of one reactor while maintaining others in operation. (3701.0302.322)

SECTION 4
SUBSYSTEM AND COMPONENT INTERFACES

The NSSS Control Subsystem receives direction from the Plant Supervisory Control Subsystem (PSCS) or operator, senses conditions within its NSSS module, makes control decisions and effects control actions within the module, and reports status within the NSSS module to the Supervisory Control System or to operators. In performing these functions, the NSSS Control Subsystem has top interfaces with the Supervisory Control System and the Plant Control Data Highway, horizontal interfaces with ECA control system, and interfaces with NSSS fluid and mechanical systems and components. Also, it receives protection action information from the Plant Protection and Instrumentation System via a unidirectional isolator, so that the NSSS Control Subsystem can independently adjust to changes brought on by the Plant Protection and Instrumentation System and maintain conditions in the NSSS module systems that are not affected by the PPIS.

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

4.1.1 Interface Requirements Imposed on Building and Structures and on Other Systems and Subsystems Within Other Systems

Each NSSS Control Subsystem requires space in four locations of the buildings associated with the particular NSSS module that it controls. In each of these locations, 200 ft^2 of space is required for signal conditioning, multiplexing, control logic, and command sending units. The ambient temperature is required to be in the 40°F to 120°F, and the relative humidity in the 10% to 90% range.

In addition, 500 ft^2 of space for complete operator overview of the NSSS at a location outside of the main control room is required, as shown in Figure 2-1, for the four local man-machine interfaces for each NSSS Control Subsystem. Temperature and humidity ranges are above.

Interfaces with other systems and subsystems within those systems and listed on Table 4-1.

Table 4-1
NSSS CONTROL SUBSYSTEM INTERFACES WITH OTHER SYSTEMS AND SUBSYSTEMS

4.1.1 Identification of Interfaces

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.1 Reactor System (1000)			
Neutron Control Subsystem (1012)	Provides capability for measurement and command of neutron flux level	Electrical signals	NSSS data and control information shall be exchanged with the NSSSCS through a compatible data interface (3701.0401.020)
	Provides instrumentation listed in Table 2.0-1 under group 1 and group 8	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface (3701.0401.030)
			Instrumentation shall allow detection of changes in operation of major systems and components that occur during plant operation (3701.0401.040)
4.1.1.2 Heat Transport System (2100)			
Main Circulator Subsystem (2101)	Provides capability for measurement and command of circulator speed	Electrical signals	NSSS data and control information shall be exchanged with the NSSSCS through a compatible data interface. (3701.0401.020)
	Provides instrumentation listed in groups 2 and 5 of Table 2.0-1	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface. (3701.0401.030)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
			Instrumentation shall allow detection of changes in operation of major systems and components that occur during plant operation. (3701.0401.040)
4.1.1.3 Shutdown Cooling System (5700)			
Shutdown Heat Removal Control Subsystem (5703)	Provide instrumentation listed in Table 2.0-1 under group 3	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface (3701.0401.030)
			Instrumentation shall allow detection of changes in operation of major systems (3701.0401.040)
	Provides control command interface	Electrical signals	NSSS data and control information shall be exchanged with the NSSSCS through a compatible data interface. (3701.0401.020)
4.1.1.4 Reactor Cavity Cooling System (5600)			
	Provides instrumentation listed in Table 2.0-1 under group 6	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface. (3701.0401.030)
			Instrumentation shall allow detection of changes in operation of major systems and components that occur during plant operation. (3701.0401.040)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.5 Vessel System			
No interfaces identified at this time (see instrumentation under 4.1.1.8 below).			
4.1.1.6 Plant Protection and Instrumentation System (3200)			
	Provides detection of PPIS actions	Electrical signals	NSSS data and control information shall be exchanged with the NSSSCS through a compatible data interface (3701.0401.020)
4.1.1.7 Fuel Handling and Storage System (3400)			
No interfaces identified at this time.			
4.1.1.8 Reactor Service Group (2000)			
Helium Purification Subsystem (2023)	Provides instrumentation listed in Table 2.0-1 under group 4	Electrical signals	NSSS data and control information shall be exchanged with the NSSSCS through a compatible data interface (3701.0401.020) Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface (3701.0401.030) Instrumentation shall allow detection of changes in operation of major systems and components that occur during plant operation. (3701.0401.040)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.9 Power Conversion Group (5000)			
Turbine Generator and Auxiliaries Subsystem (5001)	Transmission of turbine load droop caused by electric grid frequency variations	Optical or electrical interface into module data highways	Turbine control information shall be made available to the NSSSCS for use in NSSS module control during load changes or turbine trip. (3701.0401.060)
	Provides control stability	Pressure control algorithm	Main steam pressure control shall be maintained by action of the throttle valve. (3701.0401.070)
Feedwater and Condensate Subsystem (5002)	Provides capability for measurement and command of feedwater flow rate under controlled feedwater flow valve pressure drop	Electrical signals	Data and control information shall be exchanged with the NSSSCS through a compatible data interface (3701.0401.025)
	Provides capability for module feedwater temperature control while module starts up/shuts down	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface (3701.0401.030)
			Instrumentation shall allow detection of changes in operation of major systems and components that occur during plant operation (3701.0401.040)

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Main and Bypass Steam Subsystem (5004)	Provides steam pressure to NSSSCS	Electrical signals	Instrumentation for evaluating and determining the state of the NSSS shall be provided and made available to the NSSSCS through a compatible data interface (3701.0401.030)
	Provides thermocouple wells for main steam temperature sensors	Instrumentation and attachment fixtures	Main and bypass steam subsystem shall provide thermocouple wells for instrumentation of control parameters for individual reactor modules (3701.0401.050)
4.1.1.10 Heat Rejection Group (5200)			
No interfaces identified at this time.			
4.1.1.11 Plant Control, Data, and Instrumentation System (3700)			
PSCS (3707)	Transmits NSSS control information to the main control room operators	Data link between the NSSS module data highways and the PSCS	PSCS command and control information shall be passed to NSSSCS through a compatible data interface (3701.0401.010)
4.1.1.12 Electrical Group (9200)			
	Provides compatible electrical power to NSSS controls	Electric feeders	Redundant power circuits with UPS backup shall be provided for NSSSCS. (3701.0401.100)
4.1.1.13 Miscellaneous Control and Instrumentation Group (3000)			
No interfaces identified at this time.			

Table 4-1 (Continued)

Interfacing System (With Subsystem/ Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.14 Plant Service Group (9000)			
No interfaces identified at this time.			
4.1.1.15 Buildings, Structures, and Building Service Group (7000)			
	Provides Nuclear Island building space, structural and environmental support to accommodate NSSSCS	Equipment cabinets and communication hardware	Controls and instrumentation shall be located in proximity of system being controlled. Specific locations [TBD]. (3701.0401.080)
	Provides operational space	Control consoles	Space shall be provided to allow operator capability for NSSS operations outside the main control room (3701.0401.090)

4.1.2 Interface Requirements Imposed on Subsystem Within the Plant Control, Data, and Instrumentation System

The NSSS Control Subsystem interfaces with the other subsystems via communication interfaces to each of their data highways.

Specifically, the NSSS Control Subsystem receives direction from the Supervisory Control Subsystem or operators in the form of a load allocation and a load allocation weighting factor for the NSSS module when the module is in the power range (25% to 100% load, and module steam flowing to the main steam header). In the startup or shutdown range (0% to 25% reactor power level, and module steam flowing only to the startup bypass), the NSSS Control Subsystem receives direction from the same sources in the form of predefined HOLD points (or states) to which the NSSS Control Subsystem drives its NSSS module and holds.

The NSSS Control Subsystem reports states within the NSSS module to the Supervisory Control Subsystem and to operators via the system data highway.

Each NSSS Control Subsystem sends the pressure drop across the feedwater flow control valve in its module to the two feedwater trains in the ECA. The ECAs are required to maintain the lowest of the four pressure drops at 100 psid.

The NSSS Control Subsystem receives from the ECAs the turbine load droops caused by electric grid frequency variations.

4.2 COMPONENT BOUNDARY DEFINITION

Sensors: The boundary for each sensor that monitors or controls process conditions shall be the point at which the sensor touches or penetrates the process pipe or vessel. For temperature or other measurements requiring thermowells, the thermowells may be specified with the process pipe or vessel. Each case will be treated individually.

Communications Transmission Boundaries: There are two types of communication boundaries. One is a multiplexing panel that connects the NSSS Control Subsystem data highway to the Plant Control Data and Instrumentation data highway. The other type connects the NSSS Control Subsystem data highway to other NSSS systems. In these cases, the boundary is the connector at the data highway or at the system where the wires or digital communication lines are connected to the NSSS Control Subsystem.

Other: Other boundaries are defined by the brackets and mechanical attachments of electronic or optical cabinets to building floors or walls, and by electric power connectors.

SECTION 5
SUBSYSTEM CONSTRUCTION

The NSSS Control Subsystem architecture generally matches the modularity of the fluid and mechanical systems. Therefore, the subsystem is fabricated and packaged in a set of modules that are delivered to the plant with prefabricated.

5.1 PACKAGING AND SHIPPING

The NSSS Control Subsystem signal conditioning, control logic, man-machine interfaces, etc., is packaged as follows: for each NSSS module there are four cabinets of local signal conditioning and control logic, plus a fifth cabinet for man-machine function. There are four sets of these five cabinets, one for each reactor.

1. Sensors and data highways are packaged separately.
2. Software that is not burned in ROM is also packaged separately.
3. Environmental limitations for shipping are TBD.

The design of the NSSS Control 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 NSSS Control 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 the entire NSSS Control 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 NSSS Control 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 NSSS Control 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 NSSS Control 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 NSSS Control 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 NSSS Control 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 reactor vessel and to be operated in primary coolant helium, such cleaning shall conform to GA Reference Specification RC-2-2. A specific site acceptance test will be conducted to determine that the NSSSCS is installed and configured correctly. This test will repeat and be expected to duplicate a similar factory acceptance test that will be completed before the NSSSCS is shipped to the site. 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 NSSS Control 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 SUBSYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

The NSSS Control Subsystem is designed to operate the NSSS module within the operating ranges of all NSSS components. Any deviations from these ranges are detected and corrected by the independent Plant Protection and Instrumentation System. The operating limits and setpoints required for NSSS operations are given in Table 3-3. The NSSSCS itself has electronic equipment settings such as power supply voltage levels, etc., which are factory set and checked during periodic maintenance of the equipment.

6.1.1 Subsystem Limitations and Setpoints

Limitations and setpoints for control of NSSSCS equipment are entered through the NSSS operations station. The required setpoints or setpoint schedules, min/max limits, rate limits, and deadband range limits shown in Table 3-3 must be entered prior to any operation of the NSSS using the NSSSCS. Controller gains settings which must also be put into the NSSSCS data base before operating the plant, are specified in Table 3-3 as well.

Equipment calibration procedures for setting voltage regulators and other similar equipment in the NSSSCS will be developed during the preliminary and final design. These procedures are also executed before using the NSSSCS to operate the plant.

6.1.2 Precautions

The procedures for NSSSCS operation should be followed, especially when on-line maintenance is being done. Design features to assist the operator in verifying the system degree of redundancy are also included. These features, combined with administrative control of maintenance activities,

protect the plant against loss of both redundant control channels in one of the NSSS modules.

6.2 PREOPERATIONAL CHECKOUT

6.2.1 Initial Preoperational Checkout

After completion of the construction testing, a series of initial preoperational tests will be performed to verify the proper operation of the NSSSCS prior to nuclear fuel loading and power operation.

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

1. Main steam temperature control logic.
2. Feedwater flow control logic.
3. Neutron flux command logic.
4. Circulator speed command logic.
5. Load following control logic.
6. Control logic following a turbine trip.
7. Control logic following a reactor trip.

In addition, the following instrumentation and operator interfaces will be tested:

1. NSSS/PSCS operations interface and control.
2. Reactor instrumentation and operations interface.
3. HTS instrumentation and operations interface.
4. Feedwater and main steam instrumentation.
5. SCS instrumentation and operations interface.

6.2.2 Routine Preoperational Checkout

The following are required for routine preoperational checkout of the control system prior to placing the control system online after a shutdown.

1. Control Room operable.
2. Reactor Building Equipment operable.
3. Uninterruptible power sources operable.
4. Annunciator System operable.
5. Voice communication systems operable.
6. Reactor Operations Facility operable.
7. Neutron Control System operable.
8. SCS instrumentation and control operable.
9. Heat Transport System Instrumentation operable.
10. Feedwater and Steam System Instrumentation operable.
11. Reactor Systems Instrumentation operable.
12. Control system status to be placed on-line.

6.3 STARTUP/SHUTDOWN

6.3.1 Startup to 25% Steam Flow

When the preoperational checkout is completed, the NSSS Control Subsystem is placed in service. Then, the NSSS module is automatically started through the NSSS startup sequence shown in Table 2-3. Operator action is required to verify that each HOLD point has been successfully reached, and to release the NSSS Control Subsystem to take the NSSS module to its next HOLD point.

6.3.2 Shutdown from 25% Steam Flow

Normal shutdown is done automatically through the sequence of HOLD points in Table 2-3 in reverse, with operator participation to verify that each

HOLD point has been successfully reached, and to release the NSSS Control Subsystem to take the NSSS module to its next HOLD point.

The control system automatically regulates feedwater flow rate, steam temperature and steam pressure during shutdown. Special control gains (see Table 3-3) are selected automatically in order to stabilize the steam conditions and slow the cooling rates in the steam generator tubesheet and elsewhere when the shutdown is due to module isolation or reactor trip. The control system operates the circulator and FW flow valves to satisfy the requirements in Section 3.2.3. If the reactor vessel is depressurized the circulator speed is automatically increased to 100%. The NSSSCS continues to monitor data from NSSS subsystems and, if necessary, interact with the NSSS operators.

6.4 NORMAL OPERATION

Normal operation takes place in the load range between 25% and 100%, also known as the load range, or power range since this is the range in which the NSSS module actively contributes steam to the main steam header for turbine-generator operation. (See Table 5.1-3 of Ref. 2, Level of service "A" events 5 through 12 and level of service "B" events 15 and 16). In this range, the NSSS automatically follows the load demand allocated by the Supervisory Control Subsystem or the operator. References 1 and 7 may be consulted for NSSS performance information on these transient events. Appendix C contains control system information regarding control system transient performance that is typically expected during normal operation.

6.5 REFUELING

The NSSS is configured to allow core decay heat removal via the SCS during refueling at subatmospheric reactor pressure. Helium is circulated and heat is extracted through the SCS heat exchanger. The SCS is placed online automatically by the NSSSCS after reactor depressurization and on receipt

of a refueling mode enable. The NSSSCS monitors NSSS systems during this period and accomplishes its data reporting function.

6.6 SHUTDOWN

The transition to the reactor subcritical conditions in shutdown mode is described in Section 6.3. Beyond that, the NSSS Control Subsystem operates the other NSSS subsystems within their decay heat removal operating ranges.

6.7 ABNORMAL OPERATION

The NSSSCS is responsive to abnormal events and will respond in a particular fashion to such events. Abnormal operation pertaining to the NSSSCS itself includes all events involving control system failures which cause abnormal plant operation. The NSSSCS design includes features that enhance plant availability and minimize abnormal control operation. These are as follows:

1. Redundant processing of all data and control algorithms -- single failures of processing hardware do not disrupt normal operation of the plant other than within the affected control module. Maintenance design features, in turn, allow recovery from such an event.

2. Range limiting of controller outputs -- the ranges are generally satisfactory to provide load following but limit the outputs if a sensor or processing hardware component fails. In some cases, the energy production process is not interrupted because the NSSS is maintained within its operating range without challenging the independent PPIS. Also, the capability to adjust unaffected modules to accommodate abnormal operation of one NSSS module is assured by the module-to-module independence required of the NSSSCS design.

3. Feedforward synchronization of primary control elements -- module feedwater flow is controlled within the NSSS module and is the only index command input to other primary control loops. If the load level inputs to the NSSSCS from other plant controls are mismatched or incorrect, the NSSSCS still maintains reactor power consistent with NSSS heat removal through feedwater-flow-based feedforward command.

6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES

6.8.1 Casualty Events

Casualty events for the NSSS Control Subsystem include the following:

1. Events that cause PPIS protective action.

2. Events that cause the NSSS to drop below the energy production range (25% to 100% of rated output).

6.8.2 Design Features to Mitigate Effects of Casualty Events

The design features to reduce the frequency of casualty events are:

1. NSSSCS preventive maintenance and surveillance features to assure satisfactory capability for control component maintenance while the NSSSCS is on-line.

2. Module-to-module independence of NSSSCS control functions.

3. Automatic rate and range limiting of primary control variables.

Features which mitigate the effect of casualty events are:

1. Automatic reconfiguration of the control to retain HTS heat removal following a reactor trip. This feature reduces recovery

time that would be lost if NSSS/ECA feedwater supplies had to be replaced then reinstated following the event.

2. Module-to-module independence during startup/shutdown. This feature prevents loss of more than one module if the trip was initiated by an NSSS parameter and allows restart of the module independently of load adjustments in other modules following the event.

6.8.3 Recovery Procedures

Detailed recovery procedures are to be prepared in the preliminary and final design phases based on the features of Section 6.7.

In general, this will involve developing detailed procedures to place the NSSS module in one of the states defined as a HOLD point in the startup/shutdown regime, accomplishing heat removal to allow required maintenance to be performed, and allowing the NSSS Control Subsystem to take the NSSS module through the sequence of HOLD points in the startup range with operator acknowledge and release of each HOLD point.

SECTION 7
SYSTEM MAINTENANCE

7.1 MAINTENANCE APPROACH

The NSSSCS is designed to reduce or minimize the mean time to repair (MTR). One-half hour has been established as the design goal for MTR. A nominal level of expertise is required by operating and maintenance personnel when maintenance or calibration activities are performed. Only standard electronic equipment and very few special tools are required.

The NSSS Control Subsystem maintenance approach utilizes a modular instrumentation system construction, standardized modules to the extent practical, and a minimum of spare part diversity.

In both the NSSS operations station and the NSSS systems interface station all replaceable modules and subassemblies are made accessible from the front of the equipment enclosure. All terminal blocks and connectors are accessible without removal of modules, subassemblies, or chassis because of the use of swing-away panels or other electrical equipment construction techniques. Additionally, diagnostic programs have been incorporated into the software design to aid in detecting faults in communication channels or power supplies.

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

1. Adjust in place.

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

3. Repair components in place by available means to the extent permissible (consistent with personnel radiation exposure and availability requirements).

SECTION 8
SUBSYSTEM DECOMMISSIONING

The primary support of the decommissioning requirement is the independence of each NSSS control module. One control system can be removed without affecting the others.

SECTION 9
REFERENCES

1. "MHTGR Plant Design Basis Transient Analysis," DOE-HTGR-86-121, Rev. 1, (GA Document 908754/1), April 1987.
2. "Overall Plant Design Specification Modular High-Temperature Gas-Cooled Reactor," HTGR-86-004, Rev. 4, (HFS-20100, Rev. 4), (GA Document 908397/4), May 1987.
3. "NSSS Thermal Performance Requirements for the Modular High-Temperature Gas-Cooled Reactor," DOE-HTGR-86-030, Rev. 2, (GA Document 908755/2), June 1987.
4. "FY86 Seismic Assessment Report," 4 x 350 MW(t) Modular HTGR Plant," HTGR-86-119, Rev. 0, September 1986.
5. "Reliability Allocations for the Standard MHTGR," DOE-HTGR-87-008, Rev. 0, (GA Document 909279/0), February 1987.
6. "Plant Control, Data, and Instrumentation System Design Description," DOE-HTGR-86-076/2, (HFD-33700, Rev. 2), (GA Document 908437/2), July 1987.
7. "Main and Bypass Steam System Design Description," HFD-45004, Rev. 1, (GA Document 908516/1), September 1986.

APPENDIX A

Table A-1
NSSS CONTROL SUBSYSTEM DESIGN REQUIREMENTS TRACEABILITY SUMMARY

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.001	NSSS functionally independent of PPIS.	2/3.2.2/3700.0322.490
3701.0102.002	Audible alarms restricted to critical parameters.	2/3.2.2/3700.0322.220
3701.0102.003	Control features to operate reactors and turbines at different power levels.	2/3.2.2/3700.0322.080
3701.0102.004	Systems in Nuclear Island of standardized design.	2/3.2.2/3700/0322.015
3701.0102.005	Each NSSS module has independent control system.	2/3.2.2/3700.0322.129
3701.0102.006	Human-machine interfaces for NSSSCS equipment outside control room.	2/3.2.2/3700.0302.030
3701.0102.007	Data communications not restricted to location.	2/3.2.2/3700.0302.040
3701.0102.008	New control and data communication interfaced allowed.	2/3.2.2/3700.0302.050
3701.0102.009	One percentage increase in capital investment allowance versus 7/10 percentage availability.	2/3.2.2/3700.0302.070
3701.0102.010	Base design on proven technology.	2/3.2.2/3700.0302.090
3701.0102.011	Nuclear steam supply shall deliver 2400 psig, 1000°F steam.	2/3.2.2/3700.0322.285
3701.0102.012	Provide capability to control NSSS modules outside the control room.	2/3.2.2/3700.0322.110

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.013	Design control to operate through specified design transients.	2/3.2.2/3700.0322.160
3701.0102.014	Design control to accommodate reactor/turbine-generator combinations.	2/3.2.2/3700.0302.010
3701.0102.015	Controlled operation allowing load rejection or turbine trip without reactor trip.	2/3.2.2/3700.0322.330
3701.0102.016	±15% load step in plant output.	2/3.2.2/3700.0322.340
3701.0102.017	Features to limit recovery time after protection trip occurs.	2/3.2.2/3700.0322.320
3701.0102.018	Each NSSS module able to change output at rate up to 5% per minute.	2/3.2.2/3700.0322.320
3701.0102.518	Features to enable automatic startup.	2/3.2.2/3700.0322.148
3701.0102.019	NSSS transient control requirements to meet NSSS thermal requirements.	2/3.2.2/3700.0322.120
3701.0102.020	Maximum circulator speed requirement.	7/4.1.1/2100.0401.090
3701.0102.021	NSSSCS design maintain hot helium temperature.	7/4.1.1/2100.0401.091
3701.0102.022	NSSSCS control speed to flow ratio.	7/4.1.1/2100.0401.092
3701.0102.023	NSSSCS design maintain cold helium temperature.	7/4.1.1/2100.0401.093
3701.0102.024	NSSSCS maintain stable steam generator outlet temperature regulation.	7/4.1.1/2100.0401.094
3701.0102.025	Control of helium mass flow through steam generator bundle.	2/3.2.2/3700.0322.115

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.026	Continuous automatic control between 25% and 100% feedwater flow.	2/3.2.2/3700.0322.310
3701.0102.027	Ability to sustain continuous operation following failure of major component.	2/3.22/3700.0322.170
3701.0102.028	NSSSCS steady-state control accuracy.	2/3.2.2/3700.0322.117
3701.0102.029	NSSSCS automatic control during plant operation.	2/3.2.2/3700.0322.125
3701.0102.030	Startup -- 0% to 25% of rated feedwater flow.	2/3.2.2/3700.0322.150
3701.0102.031	Accommodate one or more modules starting up.	2/3.2.2/3700.0322.145
3701.0102.032	Shutdown -- 25% to 0% of rated feedwater flow.	2/3.2.2/3700.0322.130
3701.0102.034	Accommodate one or more modules shutting down.	2/3.2.2/3700.0322.129
3701.0102.035	Capability for removal of a reactor from service for refueling and return to service with remaining plant in operation.	2/3.2.2/3700.0322.140
3701.0102.036	40-yr operating life.	2/3.2.2/3700.0322.420
3701.0102.037	Design duty cycles.	2/3.2.2/3700.0322.190
3701.0102.038	Weekly load cycle.	2/3.2.2/3700.0322.300
3701.0102.039	Seismic design requirement.	2/3.2.2/3700.0322.200
3701.0102.040	OBE seismic response spectrum.	2/3.2.2/3700.0322.205
3701.0102.041	Operation of NSSS systems by NSSSCS within transient margins for total duty cycles.	2/3.2.2/3700.0322.195
3701.0102.042	Site environmental table.	2/3.2.2/3700.0322.207

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.043	Provide automatic detection and documentation of significant events.	2/3.2.2/3700.0322.225
3701.0102.044	NSSSCS provide data to control room.	2/3.2.2/3700.0322.260
3701.0102.045	NSSSCS capable of evaluating and determining control action for module-level maneuvers.	2/3.2.2/3700.0322.270
3701.0102.046	NSSSCS automatic control capability.	2/3.2.2/3700.0322.280
3701.0102.047	NSSSCS control actuators and devices required for change in NSSS state.	2/3.2.2/3700.0322.290
3701.0102.048	NSSSCS follow PSCS load demand at rates up to ±5%/minute.	2/3.2.2/3700.0322.350
3701.0102.049	Ability to control NSSS at work stations outside control room.	2/3.2.2/3700.0322.360
3701.0102.050	NSSSCS ability to process data from NSSS systems and subsystems.	2/3.2.2/3700.0322.370
3701.0102.051	NSSSCS use of digital communication techniques to interface with PSCS.	2/3.2.2/3700.0322.400
3701.0102.052	Accept startup directions corresponding to rated load demand change.	2/3.2.2/3700.0322.380
3701.0102.053	Accept shutdown directions corresponding to rated load demand change.	2/3.2.2/3700.0322.390
3701.0102.054	Provisions for monitoring NSSS status.	2/3.2.2/3700.0322.240
3701.0102.055	NSSSCS capability to sense, process, and analyze.	2/3.2.2/3700.0322.250
3701.0102.410	Report excessive SFSF temperature to control room.	8/4.1.1/3400.0401.048

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.420	Perform neutron calculations.	6/4.1.1/1012.0401.080
3701.0102.425	Issue alarm to control room if more than three control rods.	6/4.1.1/1012.0401.081
3701.0102.450	Report excessive SG feedwater inlet temperature.	7/4.1.1/2100.0401.094
3701.0102.460	Report excessive SG feedwater inlet pressure.	7/4.1.1/2100.0401.096
3701.0102.465	Report excessive steam pressure.	7/4.1.1/2100.0401.097
3701.0102.056	Reduction of human error through design of operator interface.	2/3.2.2/3700.0322.060
3701.0102.057	Locate controls outside control room in proximity of system.	2/3.2.2/3700.0322.020
3701.0102.058	Provide internal diagnostic monitoring to detect malfunctions.	2/3.2.2/3700.0322.230
3701.0102.059	Malfunction alarming in control room.	2/3.2.2/3700.0322.060
3701.0102.560	NSSSCS have self-test capability	2/3.2.2/3700.0322.470
3701.0102.510	Provisions for monitoring NSSS status, configuration and performance.	2/3.2.2/3700.0322.480
3701.0102.060	Meet reliability allocation for MHTGR.	2/3.2.2/3700.0322.410
3701.0102.061	NSSSCS reliability design requirement.	2/3.2.2/3700.0322.430
3701.0102.062	Design, arrange, and locate components to facilitate on-line maintenance.	2/3.2.2/3700.0322.450
3701.0102.063	Design for hands-on maintenance.	2/3.2.2/3700.0322.440
3701.0102.064	NSSSCS configured to maintain within availability hours.	2/3.2.2/3700.0322.445
3701.0102.065	Reduction of spare parts inventory.	2/3.2.2/3700.0322.530

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.066	Special maintenance tools provided by vendor.	2/3.2.2/3700.0322.447
3701.0102.580	Provisions for removing reactor from service.	2/3.2.2/3701.0102.580
3701.0102.590	Top-level regulatory criteria.	2/3.2.2/3700.0322.590
3701.0102.067	Codes and standards requirement.	2/3.2.2/3700.0322.510
3701.0102.068	QAL requirements.	2/3.2.2/3700.0322.520
3701.0102.069	Shop fab/assembly requirement.	2/3.2.2/3700.0322.540
3701.0102.080	Parallel construction requirement.	2/3.2.2/3700.0322.550
3701.0102.081	Decommissioning requirement.	2/3.2.2/3700.0322.560
3701.0302.101	NSSS operations station independent of PPIS.	4/1.2.1/3701.0102.001
3701.0302.102	NSSS operations station components of standardized electronic design.	4/1.2.1/3701.0102.004
3701.0302.103	Plug-connected cables.	4/1.2.1/3701.0102.004
3701.0302.104	Consistent communication protocol between connected control hardware.	4/1.2.5/3701.0102.051
3701.0302.105	Data communications not susceptible to electromagnetic noise or interference.	4/1.2.1/3701.0102.061
3701.0302.106	NSSSCS provide capability to control NSSS modules outside of control room.	4/1.2.2/3701.0102.012; 4/1.2.2/3701.0102.035
3701.0302.107	Maintain data base adequate for evaluating and determining state of NSSS.	4/1.2.2/3701.0102.012; 4/1.2.5/3701.0102.045
3701.0302.108	NSSS operations station seismic design requirement.	4/1.2.3/3701.0102.039

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0302.109	NSSS operations station designed and built for continuous service.	4/1.2.3/3701.0102.042
3701.0302.110	NSSSCS configured for maintenance within scheduled outage time.	4/1.2.4/3701.0102.064
3701.0302.112	NSSS operations station automatic surveillance and announcement features.	4/1.2.5/3701.0102.058
3701.0302.113	NSSS operations station meet [TBD]% of NSSSCS reliability allocation.	4/1.2.7/3701.0102.060
3701.0302.114	NSSS operations station reliability design methods.	4/1.2.7/3701.0102.060
3701.0302.115	Uninterruptible operation while equipment is serviced.	4/1.2.8/3701.0102.062
3701.0302.116	Serviceable with plant on-line.	4/1.2.8/3701.0102.062
3701.0302.117	NSSS operations station service and spare parts plan.	4/1.2.8/3701.0102.063
3701.0302.118	Parts interchangeability.	4/1.2.1/3701.0102.065
3701.0302.119	NSSS operations station special tools provided by vendor.	4/1.2.8/3701.0102.066
3701.0302.120	Codes and standards requirement.	4/1.2.10/3701.0102.067
3701.0302.122	QAL requirement.	4/1.2.11/3701.0102.068
3701.0302.123	General quality of materials requirement.	4/1.2.11/3701.0102.067 4/1.2.9/3701.0102.069
3701.0302.124	External electromagnetic and electrostatic interference requirement.	4/1.2.11/3701.0102.056 4/1.2.11/3701.0102.050
3701.0302.125	General equipment labeling requirement.	4/1.2.11/3701.0102.067 4/1.2.11/3701.0102.069
3701.0302.126	Parallel construction requirement.	4/1.2.12/3701.0102.070

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0302.201	NSSS systems interface station independent of PPIS.	4/1.2.1/3701.0102.001
3701.0302.202	NSSS systems interface station components of standardized electronic design.	4/1.2.1/3701.0102.004
3701.0302.203	Plug connected cables.	4/1.2.1/3701.0102.004
3701.0302.204	Consistent communication protocol between connected control hardware.	4/1.2.1/3701.0102.051
3701.0302.205	Capability to handle analog and digital I/O.	4/1.2.5/3701.0102.045
3701.0302.206	Common time base.	4/1.2.5/3701.0102.044
3701.0302.207	Hardware configuration of stations identical.	4/1.2.1/3701.0102.051
3701.0302.208	NSSS systems interface station limited operator interaction capability.	4/1.2.2/3701.0102.012
3701.0302.209	NSSS systems interface station seismic design requirement.	4/1.2.3/3701.0102.039
3701.0302.210	NSSS systems interface station designed and built for continuous service.	4/1.2.3/3701.0102.042
3701.0302.212	NSSSCS configured for maintenance within schedule outage time.	4/1.2.4/3701.0102.064
3701.0302.213	NSSS systems interface station automatic surveillance and announcement features.	4/1.2.5/3701.0102.058
3701.0302.214	NSSS systems interface station meet [TBD]% of NSSSCS reliability allocation.	4/1.2.7/3701.0102.060
3701.0302.215	NSSS systems interface station reliability design methods.	4/1.2.7/3701.0102.060

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0302.216	Uninterruptible operation while equipment is serviced.	4/1.2.8/3701.0102.062
3701.0302.217	Serviceable with plant on-line.	4/1.2.8/3701.0102.062
3701.0302.218	NSSS systems interface station service and spare parts plan.	4/1.2.8/3701.0102.063
3701.0302.219	Parts interchangeability.	4/1.2.1/3701.0102.065
3701.0302.220	NSSS systems interface station special tools provided by vendor.	4/1.2.8/3701.0102.066
3701.0302.221	Codes and standards requirement.	4/1.2.10/3701.0102.067
3701.0302.222	QAL requirement.	4/1.2.11/3701.0102.068
3701.0302.224	General quality of materials requirement.	4/1.2.11/3701.0102.067 4/1.2.11/3701.0102.069
3701.0302.225	External electromagnetic and electrostatic interference requirement.	4/1.2.11/3701.0102.067 4/1.2.11/3701.0102.069
3701.0302.226	General equipment labeling requirement.	4/1.2.11/3701.0102.067 4/1.2.11/3701.0102.069
3701.0302.227	Parallel construction requirement.	4/1.2.12/3701.0102.070
3701.0302.301	Software of standardized design.	4/1.2.1/0100.0102.004
3701.0302.302	Software provided for each NSSSCS.	4/1.2.1/3701.0102.005
3701.0302.303	Software functions to calculate ECA control inputs.	4/1.2.1/3701.0102.011
3701.0302.304	Control algorithm integral gains.	4/1.2.2/3701.0102.046
3701.0302.305	Software testing via simulation.	4/1.2.2/3701.0102.013 4/1.2.2/3701.0102.037
3701.0302.306	Feedwater flow versus load command requirement.	4/1.2.2/3701.0102.014 4/1.2.2/3701.0102.021 4/1.2.2/3701.0102.023

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0302.307	Control algorithms to accommodate load rejection, turbine trip or load step change.	4/1.2.2/3701.0102.015 4/1.2.2/3701.0102.022
3701.0302.308	Recovery strategy following protection trip.	4/1.2.2/3701.0102.017
3701.0302.309	Hardware scheduling rates compatible with ±5% per minute load change.	4/1.2.2/3701.0102.018
3701.0302.310	Operation of NSSS within (1) protection trip settings and (2) within ranges needed for total duty cycles.	4/1.2.2/3701.0102.518 4/1.2.2/3701.0102.041 4/1.2.2/3701.0102.021
3701.0302.311	Coordination of feedwater flow and helium flow.	4/1.2.2/3701.0102.025 4/1.2.2/3701.0102.021
3701.0302.312	Control design methods to maintain continuous automatic control.	4/1.2.2/3701.0102.026 4/1.2.2/3701.0102.029
3701.0302.313	Reactor trip control.	4/1.2.2/3701.0102.027
3701.0302.314	Adjust gains automatically to maintain control stability.	4/1.2.2/3701.0102.028 4/1.2.2/3701.0102.024
3701.0302.315	Reactor or turbine trip control stable, with main steam cooling rates satisfactory for NSSS systems.	4/1.2.2/3701.0102.041 4/1.2.2/3701.0102.024
3701.0302.317	Software provide NSSSCS self-checking and failure announcement features.	4/1.2.5/3701.0102.058 4/1.2.5/3701.0102.059
3701.0302.318	Software support maintenance functions.	4/1.2.7/3701.0102.060
3701.0302.319	Software codes and standards requirement.	4/1.2.10/3701.0102.067
3701.0302.320	QAL requirement.	4/1.2.11/3701.0102.068
3701.0302.321	Parallel construction requirement.	4/1.2.11/3701.0102.080

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0302.322	Accommodate decommissioning one reactor while others in operation.	4/1.2.13/3701.0102.080
3701.0401.010	Command/data exchange with PSCS.	2/1.2.5/3700.0322.260
3701.0401.020	Command information sent to NSSS control actuators.	2/1.2.5/3700.0322.290
3701.0401.025	Command information sent to feedwater actuators.	2/1.2.5/3700.0322.270
3701.0401.030	Instrumentation for evaluating and determining state of NSSS.	2/1.2.5/3700.0322.270
3701.0401.040	Instrumentation to detect changes in major systems and components.	2/1.2.5/3700.0322.225
3701.0401.050	Main steam and bypass steam instrumentation for NSSSCS.	2/1.2.5/3700.0322.280 2/1.2.5/3700.0322.290
3701.0401.060	Turbine system control information sent to NSSSCS.	2/1.2.5/3700.0322.320 2/1.2.5/3700.0322.330 2/1.2.5/3700.0322.340
3701.0401.070	Capability to automatically regulate conditions of steam produced.	2/1.2.5/3700.0322.290
3701.0401.080	Location of controls and instrumentation in proximity of system.	2/1.2.5/3700.0322.020
3701.0401.090	Capability for operators to control outside of control room.	2/1.2.5/3700.0322.110
3701.0401.100	NSSSCS required to meet overall reliability allocation.	2/1.2.5/3700.0322.430
3701.0102.405	NSSSCS response to PPIS trip.	5/4.1.1/3200.0401.050
3701.0102.410	NSSSCS monitor and report SFSF temperature.	8/4.1.1/3400.0401.048
3701.0102.415	NSSSCS issue setpoint command to NCSS.	6/4.1.1/1012.0401.079
3701.0102.420	NSSSCS perform neutron flux calculations.	6/4.1.1/1012.0401.080

Table A-1 (Continued)

Traceability No.	Summary Description of Requirement	Source Reference/Section/ Traceability No.
3701.0102.425	NSSSCS monitor and alarm if more than three control rods withdrawn.	6/4.1.1/1012.0401.081
3701.0102.430	NSSSCS control circulator speed below maximum.	7/4.1.1/2100.0401.090
3701.0102.435	NSSSCS designed to maintain helium temperature at SG inlet within envelope.	7/4.1.1/2100.0401.091
3701.0102.440	NSSSCS control circulator speed to feedwater flow ratio.	7/4.1.1/2100.0401.092
3701.0102.445	NSSSCS designed to limit maximum temperature at SG outlet.	7/4.1.1/2100.0401.093
3701.0102.450	NSSSCS monitor and report feed-water temperature too high at SG inlet.	7/4.1.1/2100.0401.094
3701.0102.455	NSSSCS maintain stable steam outlet temperature below 1035°F.	7/4.1.1/2100.0401.095
3701.0102.460	NSSSCS monitor and report feedwater pressure too high at SG inlet.	7/4.1.1/2100.0401.096
3701.0102.465	NSSSCS monitor and report steam pressure too high at SG outlet.	7/4.1.1/2100.0401.097

TRACEABILITY STUDY SUMMARY REFERENCE LIST

1. This reference number not used.
2. "Plant Control, Data, and Instrumentation System Design Description," DOE-HTGR-86-076/2, (HFD-33700, Rev. 2), (GA Document 908437/2).
3. This reference number not used.
4. "NSSS Control Subsystem Design Description," DOE HTGR-86-051, Rev. 1, (HFD-43701, Rev. 2), (GA Document 908468/2), July 1987.
5. "Plant Protection and Instrumentation System Design Description," DOE-HTGR-86-047/1, (HFD-33200, Rev. 2), (GA Document 908444/2).
6. "Neutron Control Subsystem Design Description," DOE-HTGR-86-100/1, (HFD-41012, Rev. 2), (GA Document 908472/2).
7. "Heat Transport System Design Description Modular HTGR Plant," DOE-HTGR-86-020/3, (HFD-32100, Rev. 4), (GA Document 908441/4).
8. "Fuel Handling and Storage System Design Description," DOE-HTGR-86-098/1, (HFD-33400, Rev. 2), (GA Document 908445/2).

APPENDIX B

DRAWING LIST

Drawing No.	Title
GA 029900	Communications Between NSSS and ECA Control Modules
GA 029993	NSSS Control Scheme and Interfaces IB Diagram

APPENDIX C
TRANSIENTS

This appendix shows typical NSSS control system transient response during the following design events:

1. Load Ramp -- The NSSS control changes the output of the module at rates up to 5% per minute in order to change plant output. Load can change up to 75% (100% to 25% or 25% to 100%).

2. Load Step -- The NSSS control adjusts module steam flow up to 15% of the total design flow to change plant output automatically following a change in grid frequency.

3. Turbine Trip -- The NSSS control automatically reduces NSSS module steam flow at a rate of 15% per minute following a turbine trip. The reactor does not trip and the NSSS module continues to supply steam at rated temperature after the trip. If both turbines trip, the total NSSS steam flow will be reduced to 25%.

4. Reactor Trip -- The NSSS control automatically reduces feedwater flow and steam temperature following a reactor trip. The steam temperature feedback loop for circulator speed control is opened when the steam temperature reaches the saturation value and HTS cooling is continued via feedforward control of feedwater flow and circulator speed.

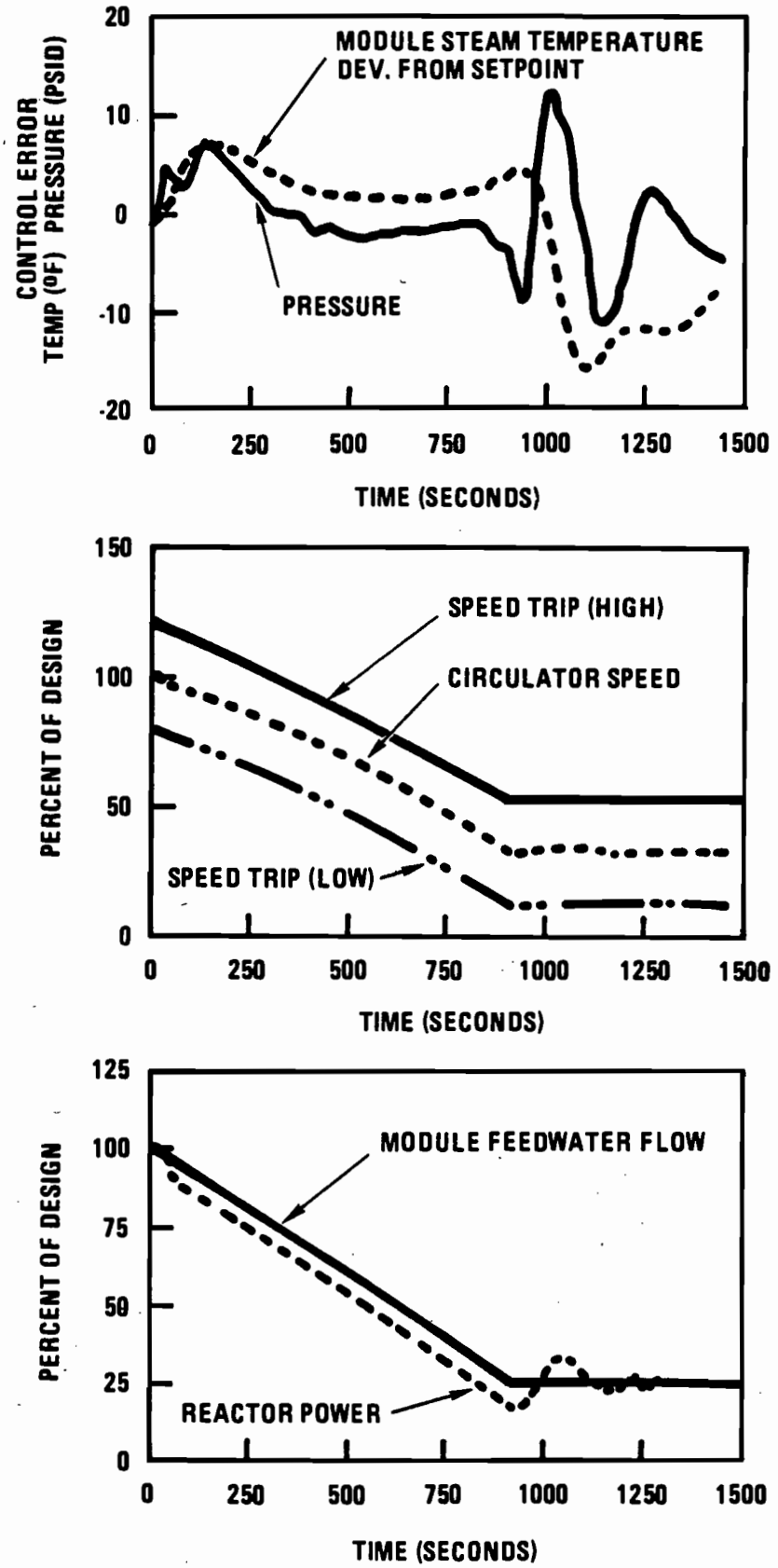


Fig. C-1. FIVE PERCENT PER MINUTE LOAD RAMP - 100% LOAD TO 25% LOAD

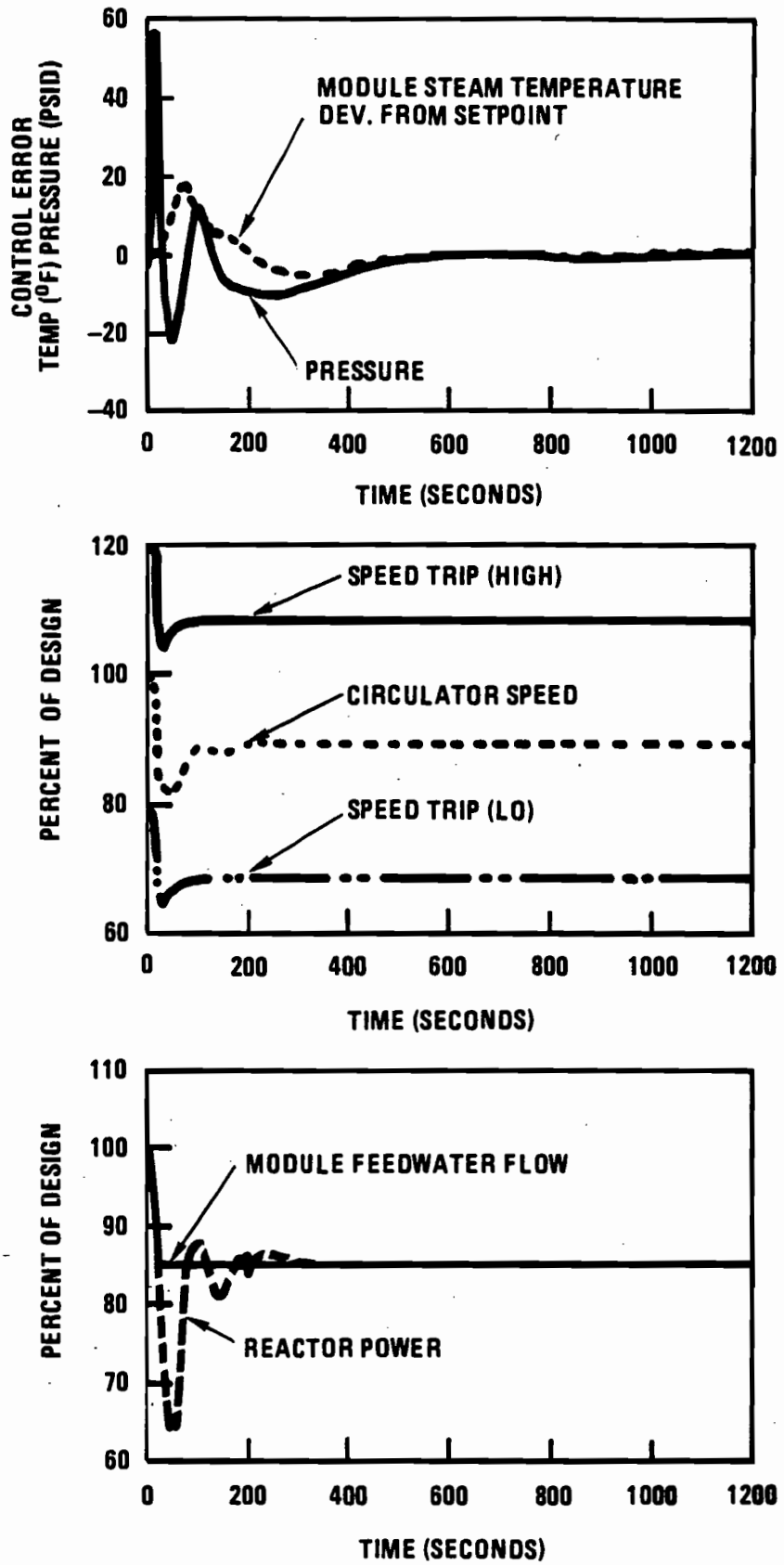


Fig. C-2. FIFTEEN PERCENT LOAD STEP - 100% LOAD TO 85% LOAD

908468/2

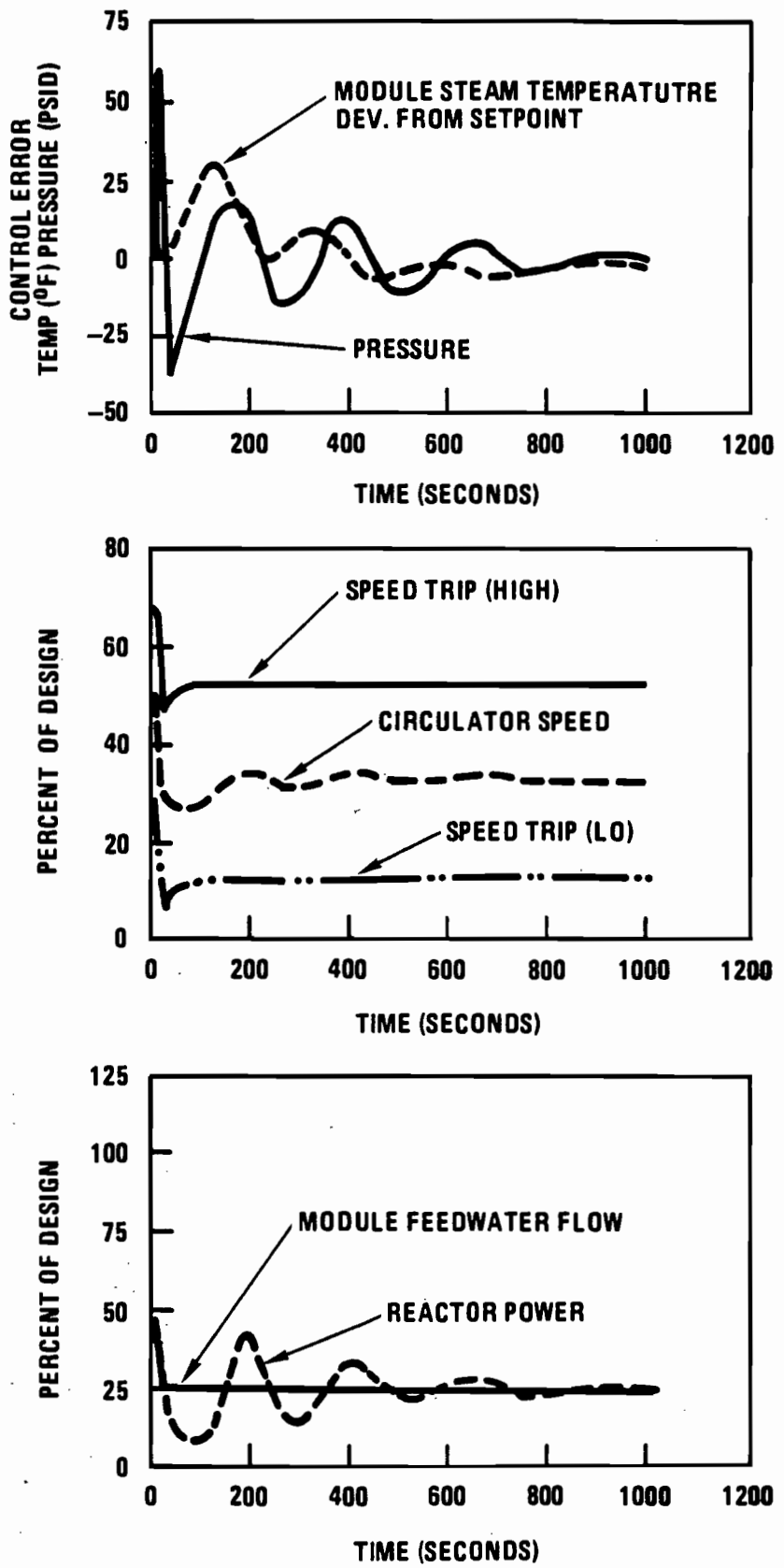


Fig. C-3. FIFTEEN PERCENT LOAD STEP - 40% LOAD TO 25% LOAD

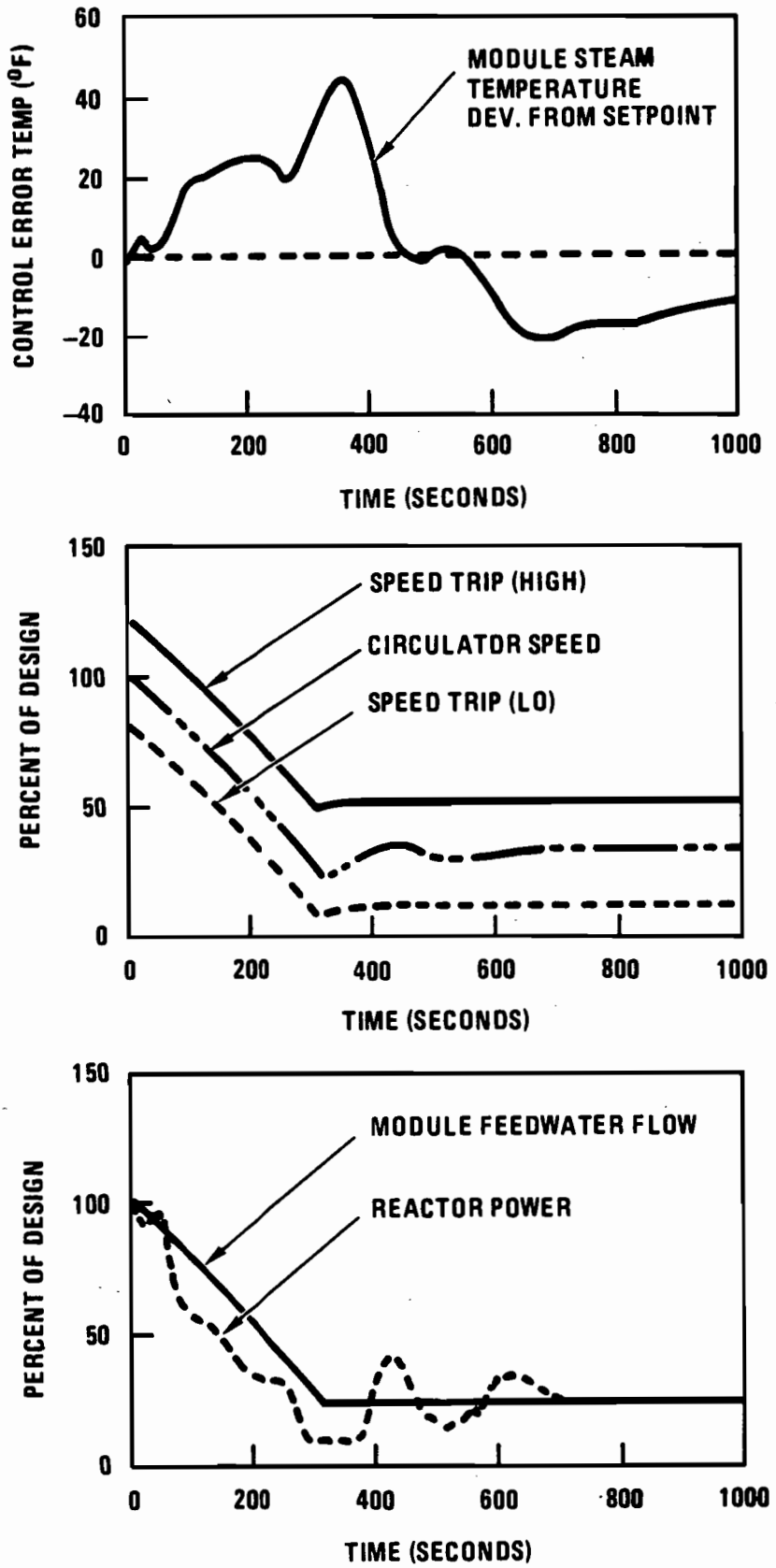


Fig. C-4. TURBINE TRIP RESPONSE OF NSSS MODULE FROM 100% LOAD TO MINIMUM STEAM FLOW

908468/2

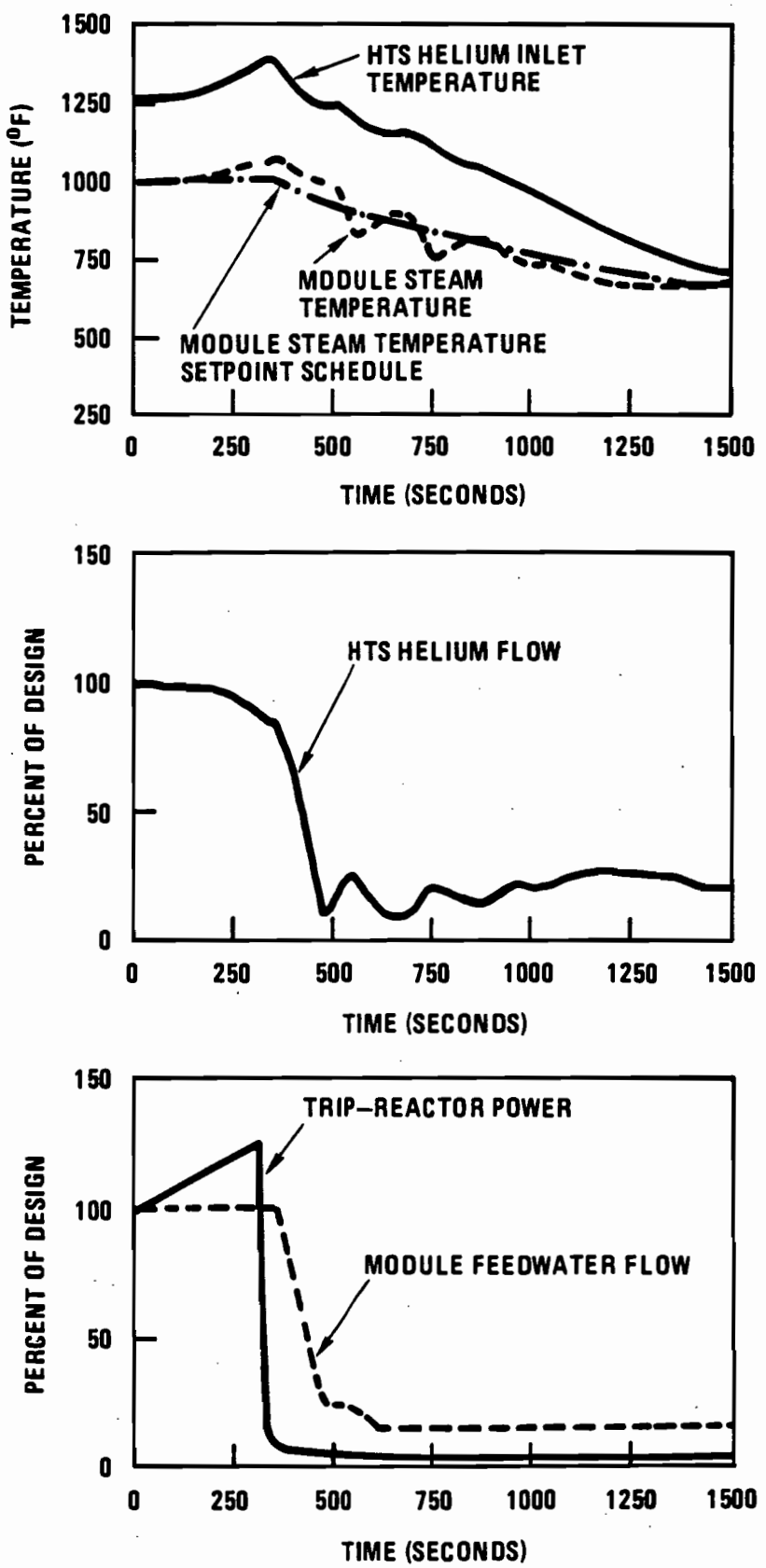


Fig. C-5. REACTOR TRIP RESPONSE AFTER POWER INCREASES ABOVE 100%

APPENDIX D

[LATER]

APPENDIX E
EQUIPMENT LIST

The following is a list of major equipment contained in the NSSS Control Subsystem (NSSSCS) equipment module. One NSSSCS equipment module is supplied with each NSSS module.

Equipment	Quantity
NSSS Operations Station	(1)
cables	
consoles	
cabinets	
printer	
operation manuals	
service equipment package	
maintenance tools	
maintenance manuals	
NSSS Control Software	(1)
disks	
manuals	
NSSS Systems Interface Station	(4)
cables	
consoles	
cabinets	

APPENDIX F
PARAMETER LIST

The following is a list of major parameters utilized by the NSSS Control Subsystem for control of its NSSS module.

Primary measurements:

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

Other measurements:

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

A count of parameters at the next level of detail is included in Section 2.2.2.

DOE-HTGR-86-076

HTGR

PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

[redacted]

AUTHORS/CONTRACTORS

GENERAL ELECTRIC CO.

ISSUED BY GENERAL ELECTRIC COMPANY
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-80ET34034

JUNE 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

DOE-HTGR-86-076
Rev. 2

HFD - 33700

PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

[redacted]

[redacted]

Authors/Contractors

GENERAL ELECTRIC CO.

Issued By: General Electric Company
For the Department of Energy
Contract DE-AC03-80ET34034

JUNE 1987

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, nor any of their contractors, subcontractors, or 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.

LIST OF EFFECTIVE PAGES

SECTION	PAGE	REVISION No.	DATE
---	Cover i through xv	2	6/26/87
1	All	2	6/26/87
2	All	2	6/26/87
3	All	2	6/26/87
4	All	2	6/26/87
5	All	2	6/26/87
6	All	2	6/26/87
7	All	2	6/26/87
8	All	2	6/26/87
9	All	2	6/26/87
Appendix A	All	2	6/26/87
Appendix B	All	2	6/26/87
Appendix C	All	2	6/26/87
Appendix D	All	2	6/26/87
Appendix E	All	2	6/26/87
Appendix F	All	2	6/26/87
Appendix G	All	2	6/26/87
Appendix H	All	2	6/26/87
Appendix I	All	2	6/26/87

TABLE OF CONTENTS

PAGE

LIST OF EFFECTIVE PAGES..... i

CONTENTS..... ii

LIST OF APPENDICES..... viii

LIST OF ILLUSTRATIONS..... ix

LIST OF TABLES..... x

LIST OF ABBREVIATIONS AND ACRONYMS..... xi

LIST OF DEFINITIONS..... xii

PREFACE..... xiv

SUMMARY..... xv

1.0 SYSTEM FUNCTIONS AND DESIGN REQUIREMEENTS..... 1 - 1

1.1 System Functions..... 1 - 1

1.2 System Design Requirements..... 1 - 1
1.2.1 System Configuration and Essential Features Requirements..... 1 - 2
1.2.1.1 System Configuration Requirements..... 1 - 2
1.2.1.2 Essential Features Requirements..... 1 - 3

1.2.2 Operational Requirements..... 1 - 4
1.2.2.1 Operational Staffing Requirements..... 1 - 4
1.2.2.2 Normal Operational Requirements..... 1 - 4
1.2.2.2.1 Operational Performance Requirements.... 1 - 5
1.2.2.2.2 Energy Production Requirements..... 1 - 5
1.2.2.2.3 Shutdown Requirements..... 1 - 5
1.2.2.2.4 Refueling Requirements..... 1 - 5
1.2.2.2.5 Startup Requirements..... 1 - 6
1.2.2.2.6 Main Control Room Operational Requirements..... 1 - 6
1.2.2.3 Off-Normal Operational Requirements..... 1 - 7
1.2.3 Structural Requirements..... 1 - 7
1.2.3.1 Seismic Tolerance Requirements..... 1 - 7

TABLE OF CONTENTS
(cont'd)

PAGE

1.2.4 Environmental Requirements..... 1 - 8
1.2.4.1 Environmental Qualification Requirements..... 1 - 8
1.2.5 Instrumentation and Control Requirements..... 1 - 8
1.2.5.1 Instrumentation Requirements..... 1 - 8
1.2.5.1.1 Monitoring Requirements..... 1 - 8
1.2.5.1.2 Analytic Requirements..... 1 - 9
1.2.5.2 Control Requirements..... 1 - 9
1.2.5.2.1 Plant Loading Requirements..... 1 - 10
1.2.5.2.2 Load Change Requirements..... 1 - 12
1.2.5.2.2.1 Ramp Load Change Requirements..... 1 - 12
1.2.5.2.2.2 Step Load Change Requirements..... 1 - 12
1.2.5.2.3 Control Transfer Requirements..... 1 - 12
1.2.5.2.4 Subsystem Coordination Control Requirements 1 - 12
1.2.5.3 Electrical Requirements..... 1 - 13
1.2.5.4 Data Communication Requirements..... 1 - 13
1.2.5.5 Software Requirements..... 1 - 13
1.2.5.6 Information Presentation Requirements..... 1 - 13

1.2.6 Surveillance and
In-Service Inspection Requirements..... 1 - 13

1.2.7 Availability Assurance Requirements..... 1 - 13
1.2.7.1 Availability Requirements..... 1 - 13
1.2.7.1.1 Operating Life Requirements..... 1 - 14
1.2.7.2 Reliability Requirements..... 1 - 14

1.2.8 Maintenance Requirements..... 1 - 14
1.2.8.1 On-Line Maintenance Requirements..... 1 - 14
1.2.8.2 Testing Requirements..... 1 - 14
1.2.8.3 Diagnostic Requirements..... 1 - 15

1.2.9 Safety Requirements..... 1 - 15
1.2.9.1 Safety Requirements..... 1 - 15
1.2.9.2 Licensing Requirements..... 1 - 15

1.2.10 Codes and Standards Requirements..... 1 - 15
1.2.10.1 Code Requirements..... 1 - 16
1.2.10.1.1 Code of Federal Regulations..... 1 - 16
1.2.10.1.2 Regulatory Guides..... 1 - 16
1.2.10.2 Standards Requirements..... 1 - 16
1.2.10.2.1 Government Standards and Specifications.... 1 - 16
1.2.10.2.1.1 RDT Standards..... 1 - 16
1.2.10.2.2 Industry and Institutional Standards..... 1 - 16
1.2.10.2.2.1 ANSI Standards..... 1 - 16
1.2.10.2.2.2 IEEE Standards..... 1 - 16

TABLE OF CONTENTS
(cont'd)

PAGE

1.2.11 Quality Assurance Requirements..... 1 - 17
1.2.11.1 Quality Assurance and Control Program..... 1 - 17
1.2.11.2 Materials..... 1 - 17
1.2.12 Construction Requirements..... 1 - 17
1.2.13 Decommissioning Requirements..... 1 - 17

2.0 DESIGN DESCRIPTION..... 2 - 1

2.1 Summary Description..... 2 - 1
2.1.1 Plant Supervisory Control Subsystem..... 2 - 2
2.1.2 Nuclear Steam Supply Control Subsystem..... 2 - 2
2.1.3 Energy Conversion Area Controls..... 2 - 3
2.1.4 Data Management Subsystem..... 2 - 4
2.1.5 Technical Operations Support Subsystem..... 2 - 4
2.1.6 Role of the MHTGR Plant Operators..... 2 - 5
2.1.6.1 Role of the Control Room Operators..... 2 - 5
2.1.6.2 Role of the Roving Operators..... 2 - 8

2.2 System Configuration..... 2 - 10
2.2.1 PSCS Configuration..... 2 - 10
2.2.1.1 PSCS Data Acquisition Software..... 2 - 11
2.2.1.2 PSCS Operator Interface Software..... 2 - 11
2.2.1.3 PSCS Control and Analysis Software..... 2 - 11
2.2.1.4 PSCS Command Generation Software..... 2 - 12
2.2.1.5 PSCS Information Processing Software..... 2 - 13
2.2.2 NSSCS Configuration..... 2 - 13
2.2.3 DMS Configuration..... 2 - 13
2.2.4 TOSS Configuration..... 2 - 13

2.3 System Performance Characteristics..... 2 - 14
2.3.1 System Operating Modes..... 2 - 15
2.3.1.1 Normal Control Modes (Goal 1)..... 2 - 15
2.3.1.1.1 Normal Energy Production Control (Goal 1, State 1)..... 2 - 15
2.3.1.1.1.1 Equal Load Apportioning..... 2 - 16
2.3.1.1.1.2 Unequal Load Apportioning..... 2 - 16
2.3.1.1.2 Normal Shutdown Control (Goal 1, State 2)..... 2 - 17
2.3.1.1.3 Normal Control During Refueling (Goal 1, State 3)..... 2 - 17
2.3.1.1.4 Normal Startup/Shutdown Control (Goal 1, State 4)..... 2 - 18
2.3.1.1.4.1 Startup Operational Sequence..... 2 - 18
2.3.1.1.4.2 Transition To Shutdown..... 2 - 19

TABLE OF CONTENTS
(cont'd)

PAGE

2.3.2 System Steady-State Performance..... 2 - 20
2.3.2.1 PSCS Steady-State Performance..... 2 - 20
2.3.2.2 NSSSCS Steady-State Performance..... 2 - 20
2.3.2.3 DMS Steady-State Performance..... 2 - 20
2.3.2.4 TOSS Steady-State Performance..... 2 - 20

2.3.3 System Response to Plant Transients..... 2 - 21
2.3.3.1 Off-Normal Control (Goal 2)..... 2 - 21
2.3.3.1.1 Off-Normal Energy Production Control (Goal 2, State 1)..... 2 - 22
2.3.3.1.2 Off-Normal Shutdown Control (Goal 2, State 2)..... 2 - 23
2.3.3.1.3 Off-Normal Control During Refueling (Goal 2, State 3)..... 2 - 23
2.3.3.1.4 Off-Normal Startup/Shutdown Control (Goal 2, State 4)..... 2 - 23
2.3.3.2 System Response to Specific Plant Transient Events..... 2 - 23

2.3.4 System Failure Modes and Effects..... 2 - 24
2.3.4.1 PSCS Failure Modes and Effects..... 2 - 24
2.3.4.1.1 PSCS Computers..... 2 - 25
2.3.4.1.2 Control Room Operator Workstation..... 2 - 25
2.3.4.2 NSSSCS Failure Modes and Effects..... 2 - 26
2.3.4.3 DMS Failure Modes and Effects..... 2 - 26
2.3.4.4 TOSS Failure Modes and Effects..... 2 - 26

2.4 System Arrangement..... 2 - 27
2.4.1 PSCS Arrangement..... 2 - 27
2.4.1.1 PSCS Computers..... 2 - 27
2.4.1.2 Operator Workstations..... 2 - 27
2.4.1.2.1 Control Room Operator Workstation..... 2 - 27
2.4.1.2.2 Control Room Assistant Workstation..... 2 - 28
2.4.1.2.3 Communication and Display Generation Equipment..... 2 - 28
2.4.1.2 NSSSCS Arrangement..... 2 - 29
2.4.1.3 DMS Arrangement..... 2 - 29
2.4.1.4 TOSS Arrangement..... 2 - 29

2.5 Instrumentation and Control..... 2 - 29

TABLE OF CONTENTS
(cont'd)

PAGE

3.0 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS..... 3 - 1

3.1 Subsystem Functions..... 3 - 2
3.1.1 PSCS Functions..... 3 - 2
3.1.1.1 PSCS Computers..... 3 - 2
3.1.1.2 PSCS Operator Workstations..... 3 - 3
3.1.1.2.1 Control Room Operator Workstation..... 3 - 3
3.1.1.2.2 Control Room Assistant Workstation..... 3 - 4
3.1.2 NSSSCS Functions..... 3 - 5
3.1.3 DMS Functions..... 3 - 6
3.1.4 TOSS Functions..... 3 - 7

3.2 Subsystem Requirements..... 3 - 8
3.1.1 PSCS Requirements..... 3 - 8
3.1.2 NSSSCS Requirements..... 3 - 22
3.1.3 DMS Requirements..... 3 - 35
3.1.4 TOSS Requirements..... 3 - 44

4.0 SYSTEM AND SUBSYSTEM INTERFACES..... 4 - 1
4.1 Interface Requirements Imposed on Other Systems..... 4 - 1
4.2 Subsystem Boundary Definition..... 4 - 1

5.0 SYSTEM CONSTRUCTION..... 5 - 1
5.1 Packaging and Shipping..... 5 - 1
5.2 Handling at Delivery..... 5 - 1
5.3 Receiving Inspection..... 5 - 1
5.4 Storage..... 5 - 1
5.5 Access..... 5 - 1
5.6 Installation and/or Field Fabrication..... 5 - 1
5.7 Construction Testing..... 5 - 1
5.8 As-Built Drawings..... 5 - 1

6.0 SYSTEM OPERATION..... 6 - 1
6.1 System Limitations, Setpoints and Precautions..... 6 - 1
6.2 Preoperational Checkout..... 6 - 3
6.3 Startup/Shutdown..... 6 - 4
6.4 Normal Operation..... 6 - 5
6.5 Refueling..... 6 - 7
6.6 Shutdown..... 6 - 8
6.7 Abnormal Operation..... 6 - 9
6.8 Casualty Events and Recovery Procedures..... 6 - 13

TABLE OF CONTENTS
(cont'd)

PAGE

7.0 SYSTEM MAINTENANCE..... 7 - 1
7.1 Maintenance Approach..... 7 - 2
7.2 Corrective Maintenance..... 7 - 4
7.3 Preventive Maintenance..... 7 - 6
7.4 In-Service Inspection..... 7 - 7
7.5 Surveillance..... 7 - 7

8.0 SYSTEM DECOMMISSIONING..... 8 - 1

9.0 REFERENCES..... 9 - 1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability of Requirements	A - 1
B	Drawings List	B - 1
C	Transients	C - 1
D	Design Basis Seismic Inputs	D - 1
E	Parameter Lists	E - 1
F	Proprietary Claims	F - 1
G	Equipment and Facilities	G - 1
H	Allocation of Functions to PCDIS Subsystems	H - 1
I	Alternate Load Allocation Strategies	I - 1

LIST OF ILLUSTRATIONS

ILLUSTRATION		PAGE
2 - 1	PCDIS Integrated Control Overview	2 - 73
2 - 2	MHTGR Integrated Control and Interface Scheme	2 - 74
2 - 3	PSCS Configuration Overview	2 - 75
2 - 4	Functional Configuration of PSCS Computers	2 - 76
2 - 5	[Reserved for future revisions]	
2 - 6	[Reserved for future revisions]	
2 - 7	[Reserved for future revisions]	
2 - 8	MHTGR Single Control Room Arrangement	2 - 77
2 - 9	Control Room Operator Workstation	2 - 78
7 - 1	PCDIS Maintenance Approach	7 - 8

LIST OF TABLES

TABLE		PAGE
1 - 1	Applicability of Regulatory Guides to the PCDIS	1 - 18
2 - 1	[Reserved for future revisions]	
2 - 2	[Reserved for future revisions]	
2 - 3	[Reserved for future revisions]	
2 - 4	Orderly Startup of 2 NSSS Modules and 1 ECA	2 - 60
2 - 5	[Reserved for future revisions]	
2 - 6	[Reserved for future revisions]	
2 - 7	[Reserved for future revisions]	
2 - 8	Shutdown Following a Module Feedwater Valve Leak	2 - 68
4.1-1	Identification of Interfaces for the PCDIS	4 - 2
4.1-2	Interface Requirements Imposed on the ECAC	4 - 28
6 - 1	PCDIS Parametric Control Variable Limits and Setpoints (Steady State)	6 - 14
6 - 2	PCDIS Parametric Control Variable Limits and Setpoints (Startup)	6 - 15
6 - 3	PCDIS Parametric Control Variable Limits and Setpoints (Normal Energy Production Transitions)	6 - 16
6 - 4	PCDIS Parametric Control Variable Limits and Setpoints (Transient Conditions)	6 - 17
A - 1	PCDIS Requirements Traceability Index	A - 3
A - 2	PCDIS Subsystem Requirements Traceability Index	A - 16
H - 1	Functions of the PCDIS	H - 3
I - 1	Alternate Load Allocation Strategies	I - 2

LIST OF ABBREVIATIONS AND ACRONYMS

ABBREVIATIONS

[LATER]

ACRONYMS

ANSI	American National Standards Institute
CFR	Code of Federal Regulations
CRAW	Control Room Assistant Workstation
CROW	Control Room Operator Workstation
DMS	Data Management Subsystem
EC	Energy Conversion
ECA	Energy Conversion Area
ECAC	Energy Conversion Area Controls
EP	Energy Production
IA	Integrated Approach
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronic Engineers
MCR	Main Control Room
MHTGR	Modular High Temperature Gas-Cooled Reactor
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NSSSCS	NSSS Control Subsystem
OPDS	Overall Plant Design Specification
PCDIS	Plant Control, Data and Instrumentation System
PPIS	Plant Protection and Instrumentation System
PSCS	Plant Supervisory Control Subsystem
RG	Regulatory Guide
SDD	System Design Description
SSDD	Subsystem Design Description
T/G	Turbine Generator
TOSS	Technical Operations Support Subsystem

LIST OF DEFINITIONS

ALLOCATED REQUIREMENT -

A requirement (functional in nature) established most commonly by simple modification of its superordinate form (e.g., system-level requirement) to reflect the application at the subordinate level (e.g, subsystem-level requirement). The only form of analysis and/or trade study used to establish the requirement is function allocation. For example, a plant-level requirement such as "The PCDIS shall be designed to automatically accept, with concurrence by the operating staff, baseload and load following net electrical output load demands allocated to the plant by the utility grid dispatcher." is modified to a subsystem-level requirement such as "The PSCS shall be designed to automatically accept.....".

CONTROL STRATEGY -

Refers to the process of using knowledge and available information about the plant or controlled process to identify and select a set of instructions (this set represents a substrategy) whose execution achieves objectives consistent with established goals and requirements. The selected instructions, whether mentally derived by an operator or automatically determined by the control system, are intended to ensure that requirements, and thus plant-level goals, are met within the limits which the operator or the control system has been allocated such responsibility.

With respect to human operators, the instructions represent tasks or procedures performed by an operator which initiate and/or accomplish control actions (e.g., insert a bank of control rods 0.5 inches). With respect to an automatic control system, the instructions are requests for subordinate control systems or actuators to execute specific functions or achieve an operating mode or condition according to measurable performance metrics (e.g., transition from 40% load to 100% load at a rate of 4.5% per minute, start pump 30 seconds after opening valve, etc.).

DERIVED REQUIREMENT -

Any requirement developed or evolved as an outcome from analysis and/or trade study beyond function allocation.

LIST OF DEFINITIONS (cont'd)

FUNCTIONAL INDEPENDENCE -

Features of a system design whereby the availability and reliability of a particular function are not dependent on the availability and reliability of another function. If human actions are a part of the particular function, the design must also ensure the capability to perform those human actions reliably. The features are achieved by any design approach which ensures the particular functions are executed in a manner that meets associated requirements should any or all other functions become unavailable. The selected design approach should also ensure that the success in meeting requirements is not significantly impacted as a consequence of the unavailability of other functions.

PREFACE

The objective of the Standard MHTGR 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 Standard MHTGR 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, SDD's and SSDD's 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 Control, Data and Instrumentation System (PCDIS) is one of the systems comprising the Standard 4x350 MW(t) Modular, High Temperature, Gas-Cooled Reactor plant (Standard MHTGR). The design of this system has been developed through the Integrated Approach toward safe, economical production of electrical power. This document defines the PCDIS functions, design requirements, and the system design features selected to perform the functions and satisfy the requirements. Subsystem functions and design requirements are defined and allocated to PCDIS subsystems. This document also includes design information on system operation, maintenance, construction, (de)commissioning, etc.

The PCDIS is an integrated, yet functionally hierarchical, set of hardware (digital computers, control initiators and monitoring devices) and software that enables the multiple-reactor, multiple-turbine plant to be automatically controlled and operated. The PCDIS is not "safety-related"; it does not perform any 10CFR100 related radionuclide control functions and no special classification is applied to it.

The PCDIS performs control, monitoring and data management functions given automatic and/or plant operator generated commands. Automatic control is implemented with a single Plant Supervisory Control Subsystem (PSCS) that coordinates overall plant energy production and energy conversion through interactions with an NSSS Control Subsystem (NSSSCS) and Energy Conversion Area (ECA) controls. The NSSSCS provides four sets of NSSS controls, one for each reactor module. The ECA includes automatic controls for two steam turbine-generators and associated feedwater trains. A Technical Operations Support Subsystem (TOSS) provides workstations for engineering and other technical operations staff personnel. A Data Management Subsystem (DMS) provides digital communication links between the PSCS, NSSSCS and ECA controls to achieve a distributed control architecture. With these automatic controls, the MHTGR plant is normally operated by a single operator from a single control room.

SECTION 1

SYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 System Functions

Per the Integrated Approach, five system-level functions have been defined for what is collectively referred to as overall plant control. The five functions, from which all subordinate PCDIS subfunctions are derived from, are the following:

- o Accept control direction
- o Observe plant status
- o Make control decisions
- o Effect control of the plant
- o Report information

These five general functions are performed during normal and off-normal plant energy production, shutdown, refueling and startup/shutdown operations.

Logical groupings have been identified for the subfunctions of these five functions. These logical groupings are the basis for the allocation of subfunctions to PCDIS subsystems and the ECA controls made in Appendix H and described in Section 3. The subfunctions are logically grouped according to one of the following functional categories:

- o Supervising and coordinating plant control and operation
- o Controlling energy production (nuclear steam supply)
- o Controlling energy conversion (turbine plant)
- o Managing plant data
- o Supporting plant technical operations

1.2 System Design Requirements

This section describes the PCDIS design requirements. These requirements are

- o program-level requirements applicable, as judged by the system designer, to the PCDIS. These are Utility/User and institutional requirements from OPDS Section 2 (Ref. 2); they are not derived,
- o derived plant-level requirements passed down from OPDS Section 5,
- o system-level requirements derived from analyses and/or trade studies on the program-level requirements and the plant-level requirements, and
- o interface requirements imposed on the PCDIS by other plant systems.

All requirements are followed by a traceability number whose use and coding scheme is prescribed in Reference 1. This traceability number has been used to index each requirement in Appendix A. Appendix A, in turn, provides references to the source (origin) of each requirement. In some cases the original wording from the reference document has been modified to reflect the system designers' interpretation of the requirement's applicability to the PCDIS.

1.2.1 System Configuration and Essential Features Requirements

1.2.1.1 System Configuration Requirements

The PCDIS shall accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations:

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

(3700.0102.020)

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

(3700.0102.040)

The PCDIS shall be designed for a Nuclear Island that includes four (4) standard reactor modules.

(3700.0102.042)

The PCDIS shall be designed for an Energy Conversion Area that includes two (2) steam turbine-generators.

(3700.0102.044)

Human-machine interfaces and machine-machine communication interfaces shall be provided for PCDIS subsystem equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.

(3700.0102.045)

The PCDIS configuration shall provide the capability to interface subsystem equipment distributed throughout the plant. Features of the PCDIS (e.g., inter-system communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.

(3700.0102.050)

The PCDIS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating deenergizing electronics or affecting the operation of other electronic equipment.

(3700.0102.055)

1.2.1.2 Essential Features Requirements

Human engineering techniques shall be employed in the PCDIS controls and instrumentation/operator interfaces to enhance operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD].

(3700.0102.060)

Design modifications and improvements which enable the plant to exceed availability requirements shall be considered for incorporation into the design, if a one percentage increase in the total capital investment produces, at a minimum, a seven tenths percentage improvement in the equivalent plant availability factor.

(3700.0102.065)

PCDIS features shall be included to facilitate operation of reactor modules and turbine-generators at different power levels.

(3700.0102.070)

Base the PCDIS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.

(3700.0102.072)

The design of structures, systems and components within the Nuclear Island shall be standardized.

(3700.0102.092)

1.2.2 Operational Requirements

1.2.2.1 Operational Staffing Requirements

The PCDIS shall provide the capability for roving operators to control, under supervision from the control room, selected processes and control subsystems during energy production, shutdown, refueling and startups/shutdowns not requiring direct control room operator interfacing and interaction. Communications and status information shall be made available at the locations involved in the operations outside the control room.

(3700.0102.095)

Design the PCDIS such that its operations staffing requirements support meeting the plant permanent operating staff goal of 50 full time personnel maximum (including first line supervisors and operating and operations support personnel).

(3700.0102.105)

The PCDIS design basis shall include an evaluation of required operator responses for normal, off-normal and emergency plant conditions for each anticipated operating staff position. This evaluation shall be used to confirm that operator staffing is consistent with anticipated work loads and response times.

(3700.0102.110)

At least one of the licensed control room operators per shift shall be a senior licensed operator.

(3700.0102.115)

As a design goal, the plant shall be designed to be operated by a maximum shift staff of:

a) 1 - senior licensed supervisor
b) 2 - licensed reactor operators in the control room
c) 4 - roving operators

(3700.0102.120)

1.2.2.2 Normal Operational Requirements

The PCDIS controls shall facilitate the normal duty cycle events specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0102.128)

1.2.2.2.1 Operational Performance Requirements

The PCDIS shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in OPDS Figures 5.1-1 through 5.1-5, Tables 5.1-1 and 5.1-2, and in the NSSS Thermal Performance Requirements Report.

(3700.0102.130)

The PCDIS shall provide the capability to concurrently coordinate energy production, shutdown, refueling and startup/shutdown operations for different reactor modules and T/G's in a manner consistent with optimizing the economics of each.

(3700.0102.132)

1.2.2.2.2 Energy Production Requirements

The PCDIS shall be designed to automatically accept, with concurrence by the operating staff, baseload and load following net electrical output load demands allocated to the plant by the utility grid dispatcher.

(3700.0102.135)

The PCDIS shall include features to enable automatic control during plant operation.

(3700.0102.138)

1.2.2.2.3 Shutdown Requirements

The PCDIS shall be designed to accommodate one or more reactor modules shutting down.

(3700.0102.139)

Reactor module shutdown shall range between 25% and 0% rated feedwater flow rate on a per reactor module basis.

(3700.0102.145)

The PCDIS shall include features to enable automatic control during orderly shutdowns.

(3700.0102.148)

1.2.2.2.4 Refueling Requirements

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

(3700.0102.155)

1.2.2.2.5 Startup Requirements

Reactor module startup shall range between 0% and 25% rated feedwater flow rate on a per reactor module basis.

(3700.0102.160)

The PCDIS shall be designed to accommodate one or more modules starting up.

(3700.0102.164)

The PCDIS shall include features to enable automatic control during startups.

(3700.0102.168)

1.2.2.2.6 Main Control Room Operational Requirements

The control room operator workstation shall be human engineered to concurrently accept those inputs from a single operator required to control plant energy production, shutdown, refueling and startup/shutdown operations.

(3700.0102.170)

The control room shall incorporate features necessary to facilitate startup, shutdown, monitoring and control and shall provide for the shutdown of major systems and components by the operator in order to limit investment risk and assure personnel protection.

(3700.0102.175)

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

(3700.0102.180)

The operator workstations to initiate and monitor all actions and information, respectively, requiring operator interaction from within the main control room shall be human-engineered and designed as a functional entity of one PCDIS subsystem.

(3700.0102.185)

1.2.2.3 Off-Normal Operational Requirements

The PCDIS controls shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0102.190)

The PCDIS shall be designed to sustain continuous plant operation at reduced electrical output through and following transients associated with the loss or failure of a major component, system or train, including an individual reactor or turbine-generator.

(3700.0102.195)

Features shall be included as required to limit recovery time to resumption of reactor power operation when a protection trip occurs consistent with meeting the plant availability goal.

(3700.0102.200)

Features shall be included in the PCDIS to facilitate continual plant operation through the transients of OPDS Table 2.1-1 (except for shutdown) and at reduced electrical output upon loss of function of major plant components where more than one is employed.

(3700.0102.205)

1.2.3 Structural Requirements

The PCDIS shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0102.210)

1.2.3.1 Seismic Tolerance Requirements

Failure of structures, systems and components (SSCs) which are not "safety-related" shall not cause failure of "safety-related" SSCs during a Safe Shutdown Earthquake (SSE).

(3700.0102.212)

Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.

(3700.0102.215)

OBE seismic response spectrum load level specifications for the system shall be based on the plant seismic response spectra provided in the FY86 MHTGR plant seismic assessment.

(3700.0102.217)

1.2.4 Environmental Requirements

1.2.4.1 Environmental Qualification Requirements

Environmental qualification requirements pertaining to PCDIS operation and structural design shall be based upon relevant plant site characteristics as specified in OPDS Table 2.1-2.

(3700.0102.220)

1.2.5 Instrumentation and Control Requirements

The PCDIS shall provide the controls, monitors and instrumentation for automatically controlling energy production and conversion, startups and shutdowns, coordinating with refueling operations, and maintaining shutdown of the plant or portions thereof.

(3700.0102.250)

1.2.5.1 Instrumentation Requirements

1.2.5.1.1 Monitoring Requirements

Malfunctions within major plant control and electric systems shall be alarmed in the main control room.

(3700.0102.252)

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

(3700.0102.255)

Provisions shall be made to automatically detect and document the sequence of significant events (e.g., control inputs, changes in operation of major systems and components, protective trips, etc.) that occur during plant operation.

(3700.0102.260)

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

(3700.0102.265)

Provisions shall be made for monitoring plant status, configuration and performance as a basis for decision-making.

(3700.0102.270)

PCDIS subsystems shall provide the capability to sense, process and analyze those variables, states, modes, limits, conditions, etc., required for the processes and subsystems to be observable.

(3700.0102.275)

Portions and/or derivations of those observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.

(3700.0102.280)

The control room operator workstation shall be human engineered to provide the capability for a single operator to concurrently observe plant energy production, shutdown, refueling and startup/ shutdown status.

(3700.0102.285)

1.2.5.1.2 Analytic Requirements

The PCDIS shall provide the capability to assist that energy production, shutdown and startup/shutdown decision making responsibility allocated to the operators.

(3700.0102.290)

The PCDIS shall be capable of evaluating and determining the state of the plant and the corresponding plant-level control state maneuvers required for concurrent energy production, shutdown, refueling and startup/shutdown control of different modules and turbine-generators.

(3700.0102.295)

The PCDIS shall provide control subsystems capable of evaluating and determining the state of the NSSS and the ECA and the corresponding module-level and turbine-plant level control state maneuvers required for concurrent energy production, shutdown, refueling and startup/shutdown control.

(3700.0102.300)

1.2.5.2 Control Requirements

The PCDIS shall provide the capability to control and regulate the conditions of the nuclear steam supply so as to deliver 2400 psig, 1000°F steam to the high pressure turbine admission valves.

(3700.0102.302)

The PCDIS shall be designed to measure and control the performance of the steam and feedwater parameters at any point between 25% and 100% rated feedwater flow for steady-state operation as specified in OPDS Table 5.12-1.

(3700.0102.306)

The PCDIS shall be designed to control the helium mass flow through the active steam generator bundle between 25% and 100% of rated feedwater flow for steady-state operation as specified in OPDS Table 5.12-2.

(3700.0102.308)

The PCDIS shall provide the capability to automatically regulate conditions (e.g., pressure, flow, temperature, etc.) of the following:

main steam supplied to the turbine-generators
feedwater supplied to each module
the steam produced and delivered by each module

(3700.0102.310)

The PCDIS control subsystems shall provide the capability to control those actuators and devices required to effect a change in state in the energy production and conversion processes during energy production, shutdown, refueling and startup/shutdown.

(3700.0102.315)

1.2.5.2.1 Plant Loading Requirements

The PCDIS controls shall facilitate the normal duty cycle events specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3. For plant load maneuvers, these are

5. Rapid Load Increase (+5%/min.)
6. Normal Load Increase (+0.5%/min.)
7. Rapid Load Decrease (-5%/min.)
8. Normal Load Decrease (-0.5%/min.)
9. Step Load Increase (+15%)
10. Step Load Decrease (-15%)

(3700.0102.320)

PCDIS controls shall be designed for base load operation and be capable of accommodating the weekly load cycle of OPDS Figure 2.1-1 over its design life.

(3700.0102.325)

Each individual reactor module shall be capable of continuous operation under automatic control between 25% and 100% of nominal module feedwater flow.

(3700.0102.330)

1.2.5.2.2 Load Change Requirements

1.2.5.2.2.1 Ramp Load Change Requirements

The PCDIS shall be capable of changing reactor and plant output under automatic control at a rate up to and including 5% of rated output per minute of those reactors on-line.

(3700.0102.335)

The design shall permit for reloading at 5% of rated load per minute following

a) load rejection from full generator output to house electrical load without a reactor trip, and
b) turbine trip (except on low condenser vacuum) from any load level without a reactor trip,

without the necessity for a mandatory hold except for those associated with the turbine-generators.

(3700.0102.340)

1.2.5.2.2.2 Step Load Change Requirements

The PCDIS shall provide sustained and controlled operation for step changes of ±15% in plant output caused by utility electrical transmission grid upsets.

(3700.0102.345)

1.2.5.2.3 Control Transfer Requirements

The control room operator workstation shall be designed to accept direction from the operators to transfer control of auxiliary processes to a mode of operation that can be supervised at locations outside the control room during energy production, shutdown, refueling and startups/shutdowns.

(3700.0102.350)

1.2.5.2.4 Subsystem Coordination Control Requirements

PCDIS control subsystems shall be designed to accept directions corresponding to energy production and conversion load demand changes at rates anywhere from a minimum of ± [TBD] %/minute to a maximum of ±5%/minute.

(3700.0102.355)

Roving operators and subsystems located outside the control room shall be capable of accepting plant energy production, shutdown, refueling and startup/shutdown instructions from the control room operators and operator workstation.

(3700.0102.360)

The PCDIS shall provide the capability to automatically allocate demands for individual energy production (module) and energy conversion (T-G's) sources. These demands shall be the energy production and coversion equivalents of baseload and load following plant net electrical output load demands from the utility grid dispatcher.

(3700.0102.365)

Load demands shall be distributed, during normal plant energy production, among the energy production (modules) and the energy conversion (turbine-generators) sources in operation consistent with plant economic and availability requirements.

(3700.0102.370)

The PCDIS shall provide the capability to automatically determine and allocate equivalent rates of change in energy production and conversion required for a rate of change in net plant electrical output anywhere from a minimum of ± [TBD] %/minute to a maximum of ±5%/minute.

(3700.0102.375)

The PCDIS control subsystems shall acknowledge process and other plant subsystem variables, states, modes, performance limits, conditions, etc., in the energy production, shutdown, refueling and startup/shutdown analysis and decision making process.

(3700.0102.380)

PCDIS control subsystems shall be designed to accept startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] %/minute to a maximum of [+TBD] %/minute.

(3700.0102.385)

PCDIS control subsystems shall be designed to accept shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD] %/minute to a maximum of [-TBD] %/minute.

(3700.0102.390)

The PCDIS shall provide the capability to automatically allocate startup and shutdown demands for individual energy production (module) and energy conversion (T-G's) sources. These demands shall be equivalent rates of change in energy production and energy conversion of ±1%/minute for startup and shutdown, respectively.

(3700.0102.395)

1.2.5.3 Electrical Requirements

[LATER]

1.2.5.4 Data Communication Requirements

PCDIS control subsystems and the control room operator workstation shall provide the capability to communicate digital control and monitoring signals using non-hardwired signal transmission techniques.

(3700.0102.400)

1.2.5.5 Software Requirements

[LATER]

1.2.5.6 Information Presentation Requirements

The PCDIS shall provide the capability and the associated operator workstations to concurrently and automatically report information required for observation and use in the control room and elsewhere as required.

(3700.0102.600)

1.2.6 Surveillance and In-Service Inspection Requirements

[Refer to Requirements 3700.0102.265 and 3700.0102.655]

1.2.7 Availability Assurance Requirements

1.2.7.1 Availability Requirements

The Effective Forced Outage Hour (EFOH) values specified in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. The PCDIS shall be designed to meet a planned outage allocation of [49.5 hours].

(3700.0102.610)

1.2.7.1.1 Operating Life Requirements

The PCDIS shall be designed for a plant operating life of forty calendar years.

(3700.0102.615)

1.2.7.2 Reliability Requirements

Plant systems shall be designed to meet the reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The PCDIS shall be designed to meet an overall reliability allocation of [TBD].

(3700.0102.620)

1.2.8 Maintenance Requirements

The PCDIS shall be configured to enable maintenance of PCDIS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant life as defined in OPDS Table 5.1-4.

(3700.0102.630)

Special PCDIS maintenance and installation tools not commercially available shall be provided by the PCDIS equipment vendors.

(3700.0102.635)

The PCDIS shall be designed to facilitate hands-on maintenance.

(3700.0102.640)

1.2.8.1 On-Line Maintenance Requirements

The PCDIS shall be designed and arranged, and equipment and components located, to facilitate on-line maintenance.

(3700.0102.645)

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

(3700.0102.650)

1.2.8.2 Testing Requirements

PCDIS subsystems shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.

(3700.0102.655)

1.2.8.3 Diagnostics Requirements

Provisions shall be made for monitoring plant status, configuration and performance as a basis for maintenance diagnostics.

(3700.0102.660)

1.2.9 Safety Requirements

1.2.9.1 Safety Requirements

[The PCDIS is not "safety-related". Therefore, it has no nuclear safety-related requirements.]

1.2.9.2 Licensing Requirements

The plant process controls shall be functionally independent from major component and equipment monitoring and protective features.

(3700.0102.665)

The PCDIS shall be designed to meet applicable top-level regulatory criteria.

(3700.0102.670)

1.2.10 Codes and Standards Requirements

The PCDIS shall be designed to comply with or meet the intent of, in part or in whole, each of the following codes, standards and guidelines to the extent they are determined applicable. Details of the application and conformance requirements with the following codes and standards shall be provided in PCDIS specifications.

Design, analysis, fabrication and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justifed in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, QA Program Requirements for Nuclear Facilities
DOE NE F2-10, QA Program Requirements (Supplement to ANSI/ASME NQA-1)

(3700.0102.680)

1.2.10.1 Code Requirements

1.2.10.1.1 Code of Federal Regulations

10CFR50 Domestic Licensing of Production and Utilization Facilities

10CFR55 Operators' Licenses

1.2.10.1.2 Regulatory Guides

The applicability of Regulatory Guides to the PCDIS design is indicated in Table 1-1.

(3700.0102.700)

1.2.10.2 Standards Requirements

1.2.10.2.1 Government Standards and Specifications

1.2.10.2.1.1 RDT Standards

RDT F1-2T (3700.0102.710)

1.2.10.2.2 Industry and Institutional Standards

1.2.10.2.2.1 American National Standards Institute (ANSI)

ANSI A58.1 (see 3700.0102.215)

1.2.10.2.2.2 IEEE Standards

[TBD]

1.2.11 Quality Assurance Requirements

1.2.11.1 Quality Assurance and Control Program

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

(3700.0102.760)

1.2.11.2 Materials

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

(3700.0102.785)

1.2.12 Construction Requirements

Shop, factory, or field fabricated, assembled and erected components and subsystems shall be utilized as appropriate to reduce costs and enhance quality control.

(3700.0102.795)

The PCDIS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.

(3700.0102.800)

1.2.13 Decommissioning Requirements

The PCDIS shall include features that enable decommissioning or refurbishment of one reactor while maintaining others in operation.

(3700.0102.805)

TABLE 1-1

APPLICABILITY OF REGULATORY GUIDES TO THE PCDIS

	REGULATORY GUIDE NUMBER AND TITLE	APPLICABILITY	NOTE* #
1.8	PERSONNEL SELECTION AND TRAINING	NO	3
1.11	INSTRUMENT LINES PENETRATING PRIMARY REACTOR CONTAINMENT	NO	
1.16	REPORTING OF OPERATING INFORMATION	YES	3
1.17	PROTECTION OF NUCLEAR POWER PLANTS AGAINST INDUSTRIAL SABOTAGE	YES	3
1.22	PERIODIC TESTING OF PROTECTION SYSTEM ACTUATION FUNCTIONS	NO	
1.23	METEOROLOGICAL MEASUREMENT PROGRAM FOR NUCLEAR POWER PLANTS	NO	
1.26	QUALITY GROUP CLASSIFICATION AND STANDARDS	[TBD]	4
1.28	QA PROGRAM REQUIREMENTS (DESIGN & CONSTRUCTION)	[TBD]	4
1.29	SEISMIC DESIGN CLASSIFICATION	NO	
1.30	QA REQUIREMENTS FOR THE INSTALLATION, INSPECTION, AND TESTING OF INSTRUMENTATION AND ELECTRIC EQUIPMENT	[TBD]	4
1.33	QA PROGRAM REQUIREMENTS (OPERATION)	[TBD]	3
1.38	QA REQUIREMENTS FOR PACKAGING, SHIPPING, RECEIVING STORAGE AND HANDLING OF ITEMS FOR WATER COOLED PLANTS	[TBD]	4
1.39	HOUSEKEEPING REQUIREMENTS FOR WATER COOLED NUCLEAR PLANTS	NO	2,3
1.40	QUALIFICATION TEST OF CONTINUOUS DUTY MOTORS INSTALLED INSIDE CONTAINMENT OF WATER COOLED NUCLEAR POWER PLANTS	NO	

* Notes provided at the end of this table.

TABLE 1-1
(continued)

APPLICABILITY OF REGULATORY GUIDES TO THE PCDIS

	REGULATORY GUIDE NUMBER AND TITLE	APPLICABILITY	NOTE #
1.47	BYPASSED AND INOPERABLE STATUS INDICATION FOR NUCLEAR POWER PLANT SAFETY SYSTEMS	YES	1
1.53	APPLICATION OF THE SINGLE-FAILURE CRITERION TO NUCLEAR POWER PLANT PROTECTION SYSTEMS	YES	1
1.58	QUALIFICATION OF NUCLEAR POWER PLANT INSPECTION, EXAMINATION AND TESTING PERSONNEL	YES	3
1.62	MANUAL INITIATION OF PROTECTIVE ACTIONS	NO	1
1.63	ELECTRIC PENETRATION ASSEMBLIES IN CONTAINMENT STRUCTURES FOR LIGHT WATER COOLED NUCLEAR PLANTS	NO	
1.64	QA REQUIREMENTS FOR THE DESIGN OF NUCLEAR POWER PLANTS	[TBD]	4
1.68	PRE-OP AND INITIAL STARTUP TEST PROGRAMS FOR WATER COOLED NUCLEAR POWER REACTORS	NO	2,4
1.68.2	INITIAL STARTUP TEST PROGRAM TO DEMONSTRATE REMOTE SHUTDOWN CAPABILITY FOR WATER COOLED NUCLEAR POWER PLANTS	NO	2
1.68.3	PRE-OP TESTING OF INSTRUMENT AND CONTROL AIR SYSTEMS	[TBD]	
1.70	STANDARD FORMAT AND CONTENT OF SAR'S	[TBD]	4
1.73	QUALIFICATION TESTS OF ELECTRIC VALVE OPERATORS INSTALLED INSIDE THE CONTAINMENT OF NUCLEAR POWER PLANTS	NO	
1.74	QA TERMS AND DEFINITIONS	[TBD]	4
1.75	PHYSICAL INDEPENDENCE OF ELECTRIC SYSTEMS	YES	
1.78	ASSUMPTIONS FOR EVALUATING THE HABITABILITY OF A NUCLEAR POWER PLANT CONTROL ROOM DURING A POSTULATED HAZARDOUS CHEMICAL RELEASE	[TBD]	2

TABLE 1-1
(continued)

APPLICABILITY OF REGULATORY GUIDES TO THE PCDIS

	REGULATORY GUIDE NUMBER AND TITLE	APPLICABILITY	NOTE #
1.88	COLLECTION, STORAGE AND MAINTENANCE OF NUCLEAR POWER PLANT QA RECORDS	[TBD]	4
1.89	QUALIFICATION OF CLASS 1E EQUIPMENT FOR NUCLEAR POWER PLANTS	NO	
1.97	INSTRUMENTATION FOR LIGHT WATER COOLED NUCLEAR POWER PLANTS TO ASSESS PLANT AND ENVIRONS CONDITIONS DURING AND FOLLOWING AN ACCIDENT	YES	1,2
1.100	SEISMIC QUALIFICATION OF ELECTRIC EQUIPMENT FOR NUCLEAR POWER PLANTS	NO	1
1.105	INSTRUMENT SETPOINTS	NO	
1.114	GUIDANCE ON BEING OPERATOR AT THE CONTROLS OF A NUCLEAR POWER PLANT	YES	
1.118	PERIODIC TESTING OF ELECTRIC POWER AND PROTECTION SYSTEMS	NO	1
1.120	FIRE PROTECTION GUIDELINES FOR NUCLEAR POWER PLANTS	YES	4
1.123	QA REQUIREMENTS FOR CONTROL OF PROCUREMENT OF ITEMS AND SERVICES FOR NUCLEAR POWER PLANTS	[TBD]	4
1.131	QUALIFICATION TESTS OF ELECTRIC CABLES, FIELD SPLICES AND CONNECTIONS FOR LWR'S	YES	1
1.134	MEDICAL EVALUATION OF NUCLEAR POWER PLANT PERSONNEL REQUIRING OPERATOR LICENSES	YES	3
1.144	AUDITING OF QA PROGRAMS FOR NUCLEAR PLANTS	[TBD]	4
1.146	QUALIFICATION OF QA PROGRAM AUDIT PERSONNEL FOR NUCLEAR PLANTS	[TBD]	4
1.149	NUCLEAR POWER PLANT SIMULATOR FOR USE IN OPERATOR TRAINING	YES	3

TABLE 1-1
(continued)

APPLICABILITY OF REGULATORY GUIDES TO THE PCDIS

	REGULATORY GUIDE NUMBER AND TITLE	APPLICABILITY	NOTE #
1.151	INSTRUMENT SENSING LINES	NO	
1.152	CRITERIA FOR PROGRAMMABLE DIGITAL COMPUTER SYSTEM SOFTWARE IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS	YES	1
1.153	CRITERIA FOR POWER, INSTRUMENTATION, AND CONTROL PORTIONS OF SAFETY SYSTEMS	YES	1
5.65	VITAL AREA ACCESS CONTROLS, PROTECTION OF PHYSICAL SECURITY EQUIPMENT, AND KEY AND LOCK CONTROLS	NO	

Notes:

(1) The intent of this Regulatory Guide (which addresses safety-related systems only) should be met by the non-safety-related PCDIS as part of the PCDIS system design practice and/or to meet interface requirements, if any, with safety systems for which this guide is applicable.

(2) An equivalent guide for a Standard MHTGR plant would be applicable to the PCDIS.

(3) This Regulatory Guide is related to actions normally performed by the licensee.

(4) This Regulatory Guide has plant-wide applicability.

SECTION 2

DESIGN DESCRIPTION

2.1 Summary Description

The Plant Control, Data and Instrumentation System (PCDIS) is an integrated, yet functionally hierarchical, set of hardware (digital computers, control initiators and monitoring devices) and software that enables the multiple-reactor, multiple-turbine plant to be automatically controlled and operated. The PCDIS is not "safety-related"; it does not perform any 10CFR100 related radionuclide control functions and no special classification is applied to it.

The PCDIS consists of a plant-level controller with an interactive operator interface, NSSS process controls, and a control and data communication network. A special set of workstations supports the ancillary activities of the plant technical operations staff. The PCDIS also includes numerous interfaces with energy conversion area controls. These control and instrumentation components and interfaces function in an integrated manner to accomplish overall control and operation of the plant. The components and equipment make up the following PCDIS subsystems, respectively:

- o Plant Supervisory Control Subsystem (PSCS)
- o Nuclear Steam Supply System Control Subsystem (NSSSCS)
- o Data Management Subsystem (DMS)
- o Technical Operations Support Subsystem (TOSS)

The PCDIS performs control, monitoring and data management functions given automatic and/or plant operator generated commands. Automatic control is implemented with a single PSCS that coordinates overall plant energy production and energy conversion through interactions with the NSSSCS and the Energy Conversion Area Controls (ECAC)[footnote]. The NSSSCS provides four sets of NSSS controls, one for each reactor module. The ECAC includes automatic controls for two steam turbine-generators and associated feedwater trains. The DMS provides communication links between the PSCS, NSSSCS and ECAC to achieve a distributed control architecture. With these automated controls, the MHTGR plant is normally operated by a single operator from a single control room.

The overall PCDIS configuration is aimed at producing a cost-effective, modular yet integrated implementation of modern control, monitoring and data management systems. An overview of the integrated PCDIS controls (i.e., excluding DMS data processing and the TOSS) is illustrated in Figure 2-1.

Footnote:
ECAC is the name used in this document to refer collectively to the controls for the energy conversion processes (e.g., main steam, bypass and feedwater systems, turbine-generator and auxiliaries systems, etc.).

2.1.1 Plant Supervisory Control Subsystem (PSCS)

The computer control portion of the PSCS illustrated at the top of Figure 2-1 coordinates overall operational control of the plant during normal and off-normal energy production, shutdown, refueling and startup/shutdown states. The PSCS computers automatically supervise and coordinate matching of load (power) levels between the energy production (NSSS) and energy conversion areas (ECA).

The PSCS automatically determines what contribution each NSSS will make to the ultimate delivery of steam for the energy conversion process. Likewise, the PSCS automatically determines what contribution each feedwater train and turbine-generator (T/G) will make to the main feedwater supply and overall plant electrical output, respectively. First stage pressures of the turbine-generators are used as a feedback signal to the PSCS for the load apportioning function. The PSCS also monitors the performance, response and limitations of each NSSS and the ECA. An optimum balance is maintained among the operational loads, equipment duty cycling, fuel burnup, etc. of each reactor module and turbine-generator.

The other components of the PSCS are the operator workstations, which consist of all the control initiators and monitors required in the plant's single control room. The workstations consist of the hardware, software and devices necessary to meet the operational requirements of the operators. The workstation shown at the top of Figure 2-1 provides the interactive operator-to-process interface required for a single licensed operator to operate the plant from the single control room.

2.1.2 Nuclear Steam Supply System Control Subsystem (NSSSCS)

There are individual sets of NSSS controls, one for each reactor module, that regulate reactor power and module steam conditions and the supply of steam to the main steam header. The control subfunctions of the NSSSCS module steam temperature control function are the following:

1. Module feedwater flow control

2. Module circulator speed control

3. Module neutron flux and thermal power control

The module steam temperature control function is block diagrammed in the upper left portion of Figure 2-~~3~~2. The NSSSCS automatically controls the pressure, temperature and flow of steam generated by each reactor module up to the point of main steam headering. This subsystem also controls reactor conditions during startup, shutdown and refueling. It preprocesses and provides NSSS-related data and information to the PSCS via the DMS.

For power generation, individual NSSS control is accomplished by a mixed-mode control scheme that combines characteristics of boiler-follow-turbine and turbine-follow-boiler control schemes to meet the required response and control stability requirements. Reactor module steam conditions (at the steam generator outlet regions) are regulated by controlling reactor module thermal power (via control rods), helium flow (via circulator speed), and feedwater admitted to the steam generators. Circulator speed is normally controlled by the combination of a feedforward signal based on module feedwater demand and a feedback control signal based on main steam temperature.

During power generation the NSSSCS performs its function by accomplishing five operations. The NSSSCS automatically accepts apportioned module load demands and permissives (during operational sequences such as startups) prescribed by the PSCS and the operators, respectively. The NSSSCS senses, processes, and analyzes NSSS variables, limits and conditions. Each of the four reactor module controllers within the NSSSCS determine what module feedwater demand is required to meet its allocated load demand and module steam conditions. On the basis of the decision made, the NSSSCS effects final control element action to regulate reactor power, circulator speed and module feedwater flow which govern module steam production and conditions (temperature and pressure).

2.1.3 Energy Conversion Area Controls (ECAC)

The ECAC is the name used in this document to refer to the controls associated with each process and set of major components (i.e., deaerators, condensers, feedwater pumps, turbine-generators, etc.) within the energy conversion area. These controls regulate the main steam flow acquired from the main steam header and admitted to the turbines. They also regulate the individual supplies of feedwater to the main feedwater header from the two feedwater trains.

Main steam pressure is controlled by a combination of feedwater pump speed, turbine throttle valve position, and bypass valve position, depending on the particular operating mode and conditions. The deviation of main steam header pressure with respect to its setpoint is used as a feedback signal and combined with the feedforward load demand signal from the PSCS to generate the turbine throttle valve position control signal. The feedwater supply available to the reactor modules is governed by feedwater pump speed and the lowest measured feedwater valve differential pressure.

The ECAC includes operator interfaces at ECAC equipment locations outside the main control room. These operator interfaces facilitate O&M activities which do not interrupt energy conversion and electrical power generation. The ECAC reports ECA status to the PSCS and the control room via the DMS.

2.1.4 Data Management Subsystem (DMS)

The DMS serves two plant-level functions in the PCDIS; these two functions are (plant-wide) data communication and (centralized) data processing and information management. The DMS consists of distributed data communication controllers and high-speed digital computers that perform these two principal DMS functions, respectively. A distributed communication network and data processing architecture is utilized to best meet the functions and requirements of the DMS. The communication network portion of the DMS is depicted as the set of data highways in Figure 2-1. The DMS interfaces directly with the PSCS and it is required for continuous control of the plant, particularly on a long-term basis and during off-normal plant operating conditions. However, the DMS does not initiate any plant control or protective functions.

The DMS communication network provides the principal means of physically interconnecting systems with the PCDIS when electrical signals can be exchanged between them using non-hardwired, digital communication techniques (e.g., multiplexed signal transmission). The DMS acquires, transmits and distributes to the NSSSCS and the ECAC all control initiating signals originating from the PSCS and within the main control room. The DMS acquires and transmits all monitoring signals originating from the NSSSCS and the ECAC including other plant systems such as the PPIS. Lastly, the DMS records, stores, monitors, processes, transmits, distributes, diagnoses and outputs data for both on-site, off-site, immediate and future use.

2.1.5 Technical Operations Support Subsystem (TOSS)

The Technical Operations Support Subsystem is the name given to the collection of computer-based workstations used by the plant engineering and technical staff whose presence in the main control room is not required. The principal function of the TOSS is to provide computational, analytical and monitoring capabilities so that engineering and technical staff personnel can perform their duties without being present in the MCR. The activities performed at these workstations are supervised under authority of the plant technical management staff. Operations and activities carried out using the TOSS supplement the plant operating requirements of the control room operators. The facilities housing the TOSS workstations provide for the following:

- centralized normal and emergency assembly location for plant engineering, technician and operations staff
- technical work environment in support of plant emergency response technical personnel
- support the control of personnel access to the main control room
- integration of group technical tasks. These tasks include required maintenance, surveillance, testing and calibration that occur during the various plant operating modes and states.

2.1.6 Role of the MHTGR Plant Operators

The MHTGR control room operators perform plant mission management tasks (Ref. 12). The tasks are those that coordinate energy production, shutdown, refueling and startup/shutdown operations so that the plant meets its electrical output demand efficiently, economically and reliably. The roving operators oversee activities performed outside the control room which include plant in-service inspection and surveillance, maintenance, refueling operations, and (pre)startup/(post)shutdown activities. Sections 2.1.6.1 and 2.1.6.2 summarize the control room operator and roving operator roles and responsibilities, respectively, for energy production, shutdown, refueling and startup/shutdown operations.

2.1.6.1 Role of the Control Room Operators

2.1.6.1.1 Energy Production Operations

1. Verifies proper execution and performance of the automatic energy production controls.

2. Acknowledges their acceptance of automatic energy production control actions being monitored and the resultant energy production conditions using operational directives (e.g., permissives for automated energy production control sequences to proceed).

3. Observes plant energy production status and performance (primarily observation of trends extending from several minutes to days).

4. Communicates with administrative, operations and maintenance staff as necessary to accomplish energy production operations concurrent with portions of the plant that may be shut down or starting up.

5. Performs administrative energy production tasks that have not been automated and tasks which have been delegated to the operator in accordance with institutional requirements.

6. Executes discretionary, manual operating tasks during abnormal conditions. The abnormal conditions may arise, for example, if the automatic controls of a main energy production or conversion process, system or component fail to achieve stable operating conditions and/or fail to temporarily suspend operation for diagnosis and maintenance. The operator removes the process, system or component from the energy production and conversion conversion mode of operation.

2.1.6.1.2 Shutdown Operations

1. Observes shutdown status and performance (primarily observation of trends extending from several hours to days).

2. Acknowledges their acceptance of shutdown conditions being monitored.
   - Verify proper valve/switch lineups, equipment stops (those not driven by the process dynamics)
   - Secure services

3. Performs administrative shutdown tasks that have not been automated and tasks which have been delegated to the operator in accordance with institutional requirements.

4. Directs roving operations personnel during shutdown activities involving service, support and auxiliary systems.
   - Filling, charging, purging, venting, draining, (de)pressurizing, (de)energizing, etc.
   - Establishing initial valve lineups
   - Instrument calibrations
   - Control system functional tests
   - Securing for maintenance
   - Acceptance tests for maintenance (e.g., establishing test valve/switch lineups, preparing for operation, equipment/system startups, completion of test procedures, accept for normal operation or re-secure for maintenance)

2.1.6.1.3 Refueling Operations

1. Performs administrative tasks related to refueling operations that have not been automated and tasks which have been delegated to the operator in accordance with institutional requirements.

2. Communicates with administrative, operations and maintenance staff as necessary to accomplish refueling concurrent with portions of the plant that may be shut down, starting up or in operation.

3. Observes refueling operations status and resulting core geometry.

4. Acknowledges their acceptance of the activities performed in preparation for refueling. For example, the operator verifies completion of necessary interlocks and grant permissives for refueling operations to begin.

5. Directs roving operations personnel in assuring that service, support and auxiliary systems are available as required to support refueling operations.

2.1.6.1.4 Startup/Shutdown Operations

1. Performs diagnostic tasks which require the activation of main energy production and conversion components and/or equipment.

2. Verifies proper execution and performance of the automatic startup/shutdown controls.

3. Acknowledges their acceptance of automatic startup/shutdown control actions being monitored and the resultant startup/shutdown conditions using operational directives (e.g., permissives for automated startup sequences to proceed).

4. Observes startup/shutdown status and performance (primarily observation of trends extending from several minutes to hours).

5. Communicates with administrative, operations and maintenance staff as necessary to accomplish startups/shutdowns (e.g., pre-operation and post-operation tests) concurrent with portions of the plant that may be shut down or in operation.
   - Verify startup valve/switch lineups
   - Establishing and checking equipment services
   - Verifying satisfactory local operating conditions (e.g., motor ventilation flow, oil ring operation and lubrication, bearing vibration, re-circulation flow, service systems flows, temperatures and pressures, and leaks)

6. Performs administrative startup/shutdown tasks that have not been automated and tasks which have been delegated to the operator in accordance with institutional requirements.

7. Executes discretionary, manual operating tasks during abnormal startup/shutdown.

8. Initiates the startup of major components and equipment in the energy production and conversion process.

9. Directs roving operations personnel in the startup/shutdown of service, support and auxiliary systems.

2.1.6.2 Role of the Roving Operators

2.1.6.2.1 Energy Production Operations

1. Verifies proper execution and performance of local automatic instrumentation and control during routine surveillance checks.

2. Observes status and performance of components and equipment in service, support auxiliary systems.

3. Performs administrative operational tasks that either
   a) have not been automated and which can be performed outside the control room without impacting operations for the remainder of the plant, or
   b) have been delegated to the roving operators in accordance with institutional requirements.

4. Communicates with control room operators and maintenance staff as necessary to accomplish 1., 2., and 3. above.

2.1.6.2.2 Shutdown Operations

1. Observes shutdown status and performance of components and equipment in service and support systems.

2. Acknowledges their acceptance of shutdown conditions being monitored.
   - Verify proper valve/switch lineups
   - Verify equipment stops (those not driven by the process dynamics)
   - Secure services

3. Communicates activity status to control room operators during post-shutdown or prestartup activities with service, support and auxiliary systems.

4. Performs administrative operational tasks that either
   a) have not been automated and which can be performed outside the control room without impacting operations for the remainder of the plant, or
   b) have been delegated to the roving operators in accordance with institutional requirements.
      - Filling, charging, purging, venting, draining, (de)pressurizing, (de)energizing, etc.
      - Establishing initial valve lineups
      - Instrument calibrations
      - Control system functional tests
      - Securing for maintenance
      - Acceptance tests for maintenance (e.g., establishing test valve/switch lineups, preparing for operation, equipment/system startups, completion of test procedures, accept for normal operation or re-secure for maintenance)

2.1.6.2.3 Refueling Operations

1. Verifies that service and support systems are available as required to support refueling operations.

2. Observes refueling operations status.

3. Communicates with control room operators and refueling personnel as necessary to accomplish 1. and 2. above.

2.1.6.2.4 Startup/Shutdown Operations

1. Performs diagnostic tasks which do not require the activation of components and/or equipment in the main energy production and conversion systems.

2. Verifies proper execution and performance of local automatic instrumentation and controls.

3. Acknowledges their acceptance of local automatic instrumentation and control status being monitored and the resultant startup/shutdown conditions using operational directives (e.g., permissives for local automated control action sequences to proceed and control room operator instructions).

4. Observes status and performance of components and equipment in service and support systems.

5. Communicates with administrative, operations and maintenance staff as necessary to accomplish startup/shutdown operations (e.g., pre-operation and post-operation tests).
   - Verify startup valve/switch lineups
   - Establishing and checking equipment services
   - Verifying satisfactory local operating conditions (e.g., motor ventilation flow, oil ring operation and lubrication, bearing vibration, re-circulation flow, service flow, temperature and pressure, leaks)

6. Executes discretionary, manual actions during abnormal startup/shutdown conditions. The abnormal conditions may arise, for example, if
   a) the local automatic controls of a service, support or auxiliary system fail to perform startup sequencing properly, or
   b) the automatic controls fail to achieve stable low-load operating conditions.
   c) the component under control fails upon startup, or

   The roving operators terminate startup of the process, system or component.

7. Communicates activity status to control room operators during the startup/shutdown of service, support and auxiliary systems.

2.2 System Configuration

Figure 2-2 depicts the MHTGR integrated control and interface scheme (configuration) with respect to the normal plant energy production state (25-100% rated plant output). The PCDIS uses a hierarchy of subsystem controllers and communications for controlling and monitoring the plant. This configuration enables the PSCS to coordinate the operations of available NSSS and ECAs independently of NSSS modules and ECAs that may not be available.

2.2.1 PSCS Configuration

This section describes the internal functional configuration of the PSCS (i.e., the functional elements of the automated supervisory controller). These internal functions are implemented and executed using hardware, software and user (e.g., operator, maintainer, etc.) interfaces. The integrated operation of hardware, software and user interfaces prescribes how the PSCS meets its requirements for automatic plant-level control and operation.

Figure 2-3 provides one functional block diagram of the PSCS configuration. Figure 2-3 emphasizes the configuration used to interface the operator with the plant (i.e., a workstation) and meet the majority of PSCS functional requirements (i.e., software). PSCS control requirements related to the five general PSCS functions (i.e., observing status, accepting inputs, making decisions, effecting control and reporting information) are met, in part, by the PSCS controller software shown in Figure 2-3. The controller software is structured for modular functionality and consists of the following software elements:

1. Data acquisition software (for observing plant status)
2. User interface software (for accepting operator inputs)
3. Control and analysis software (for making decisions)
4. Command generation software (for effecting control of the plant)
5. Information processing software (for reporting information)

Figure 2-4 provides another block diagram of the PSCS configuration. Figure 2-4 emphasizes the functional configuration of the PSCS computers with respect to the DMS and the control room operator workstation. The computer elements shown in Figure 2-4 are a combination of hardware and software.

2.2.1.1 PSCS Data Acquisition Software

The PSCS observes (monitors) the status of plant components and processes and determines the operational and control states of the plant. Data acquisition software manages the acquisition of data from the subordinate subsystems (i.e., the NSSSCS, ECA, DMS, and TOSS). The intermediary source of the data is the DMS. The DMS provides the PSCS with digital data containing original source identification and time tagging information. The source of the data and the data itself are validated before data archives are updated and made accessible by other internal PSCS software elements. Data is validated by comparing the sampled data against archived records of data acquired from previous communications. If discrepancies are observed, the data is flagged for subsequent analyses. Once validated, the data is aggregated (grouped logically and meaningfully) and processed into plant-level information for the operators.

2.2.1.2 PSCS Operator Interface Software

The plant operator has a role in making plant level decisions and information must be reported to the operator for this purpose. The operator interface software includes the capability to assist the decision making responsibility allocated to the operator. The operator interface software manages the reporting of results from the plant diagnosis and internal system diagnostic functions of the information processing software. Special information presentation routines using inputs from the information processing software provide real-time plant data in a manner that is intelligible and coherent for the operator. These routines alert the operator of vital plant symptoms and conditions.

2.2.1.3 PSCS Control and Analysis Software

The control and analysis software has a major role in coordinating plant control, making plant control decisions, effecting plant control, and accepting plant direction. The control software is the embodiment of control logic used to meet requirements for:

- operation of modules and turbines at different power levels,
- sustaining operation through plant maneuvers under loss of a major component or system,
- responding to off-normal service limit events,
- automatically accepting load demands from the grid dispatcher,
- determining plant state maneuvers, and
- allocating demands for, and rates of change in, energy production and conversion.

The control software reaches decisions based on predefined logic, inputs from the operator, results from the analysis software and information from data archives. The data archives contain information regarding operational capabilities (and limitations) of plant equipment and components. The control

software uses this information to determine feasible process and component configurations. The control software first identifies which strategies and directions are achievable based upon the current configuration of the plant components and processes. The control software resolves conflicting control decisions and selects the corresponding control strategy to meet the control and operating directions that are given precedence. The process of selecting a control strategy with respect to feasible configurations is executed according to a prioritized scheduling scheme.

The analysis software monitors and analyzes the performance of startup, shutdown and energy production maneuvers, the economics of reactor modules and turbines operating at different power levels, and it evaluates the state of the plant. The analysis software uses numerical algorithms to assess overall plant performance and operational trends.

2.2.1.4 Command Generation Software

The command generation software provides a check-before-execute capability to validate all control commands input by the operator or associated with the selected control strategy. The command generation software compares an expected plant state with the current and desired plant states. This validation process is one that provides an accurate indication of whether or not the control commands can be met (within established operating requirements) using the selected strategy and plant configuration. Making this indication available to operators and other software elements of the PSCS is a reporting function handled by the PSCS user interface software.

If a control command is invalid, the source/originator of the command is alerted to cancel the command or provide an alternate command for subsequent validation. This iterative validation process continues until the command is validated or until the operator is delegated full validation responsibility. The commands are generated in their final form upon validation.

The command generation software formulates a detailed set of control commands for subsystems based upon validated control instructions from the control software. The command generation software retrieves a set of predefined, subordinate instructions and corresponding system components or device destinations. Each set of command instructions selected is compared against the originating request prior to issue. If a discrepancy occurs, a discrepancy message is used to indicate that subordinate instructions cannot be validated for that command.

2.2.1.5 Information Processing Software

The information processing software performs plant diagnosis and internal system diagnostic functions. The information processing software provides for timely fault identification and anomaly diagnosis so that the control software can select alternate strategies. The plant diagnosis includes plant sequence-of-events monitoring. This software has a key role in meeting the requirements to sustain plant operation during off-normal conditions.

Invalid data, discrepancies between expected and actual performance, and anomalies or failures detected by self-tests are verified, analyzed and evaluated. The information processing software determines if the anomaly detected is an incipient failure, a faulted component, a false alarm, is a process upset, an inaccuracy with instrumentation, or a pertubation caused by equipment/component aging. The cause or condition is identified and routed to the control software for a control decision.

The information processing software also has access to the plant maintenance database. Typical maintenance database information includes the following:

- historical records
- ongoing preventive maintenance activities
- service records
- current maintenance schedules
- instruction manuals
- training aids
- maintenance and troubleshooting aids
- personnel exposure history
- parts inventory
- maintenance task durations
- master parts and spare parts lists
- equipment performance limits

2.2.2 NSSSCS Configuration

[LATER - Refer to NSSSCS SSDD]

2.2.3 DMS Configuration

[LATER - Refer to NSSSCS SSDD]

2.2.4 TOSS Configuration

[LATER - Refer to NSSSCS SSDD]

2.3 System Performance Characteristics

Optimal plant performance is achieved by a PCDIS control and operational strategy which enables the automatic controls, in conjunction with the plant operators, to accomplish the following and meet the PCDIS design requirements.

a) operate reactor modules and T/Gs in equal (balanced) or unequal (unbalanced) load configurations

b) meet plant load demand (i.e., maximizing plant availability, capacity factor, time operating efficiency, etc.)

c) avoid unnecessary or undesirable changes in plant electrical output to the grid

d) optimize core fuel burnup (including extending the fuel cycle of a reactor module)

e) limit integrated thermal stresses, corrosion, etc.

f) maximize main power generation loop efficiency

g) limit the frequency of challenges to investment and safety protection

h) minimize plant response time to load increases. Provided the plant output demand is being met, an unbalanced load configuration can establish the desired preparedness (initial conditions) to respond to rapid plant load increases if any units have reduced rate limits. For example, units without reduced rate limits can be operated at larger differentials from maximum load than those with reduced rate limits. Upon a demand for rapid load increase, the units without reduced rate limits can be allocated larger load demands while the rate-limited units can contribute according to their rate limit and smaller differential from maximum load.

i) avoid operation of reactor modules and T/Gs at marginally stable load levels.

j) reduce the potential for, and thereby the probability of, human error.

2.3.1 System Operating Modes

2.3.1.1 Normal Control Modes (Goal 1)

2.3.1.1.1 Normal Energy Production Control (Goal 1, State 1)

The PSCS derives a total plant electrical load (power) demand from the grid dispatcher's plant electrical power demand and the current plant total electrical power output. Comparisons are made with limits (if any) of generator electrical power output, module steam production, and feedwater supply to arrive at an achievable, total plant load demand. The PSCS then converts this total plant load demand into NSSS and ECA load demands. Within the energy production range of 25 percent to 100 percent rated plant output, the primary control function of the PSCS is to apportion and allocate these NSSS and ECA load demands for individual NSSS modules and ECA trains in the following form:

- o ECA demands
  - T/G throttle Valve Position Demand Indices (VPDI)
    (one to each T/G)
  - FeedPump Speed Demand Indices (PSDI)
    (one to each feedwater train)
  - Proportioned Feedpump Response Indices (PFRI)
    [associated with ECA feedwater control valve differential pressure trim function]
    (one to each feedwater train)
- o NSSS demands
  - Module Load Demand Indices (MLDI)
    (one to each reactor module)

These demand indices are depicted in Figure 2-2. The ECA load demand indices are used by the ECAC to determine turbine throttle valve positions and feedwater pump speeds. The NSSS load demand indices are used by the NSSSCS to determine module feedwater demands, helium circulator speeds and reactor power levels which will produce module steam at the required temperature and pressure.

Eighteen (18) alternate load allocation strategies are available for use by the PSCS. The selection of a particular strategy depends on the plant's condition/status, achievable process/component configurations, grid dispatcher requests, and discretionary decisions by the operators. Table I-1 in Appendix I lists these alternate strategies.

2.3.1.1.1.1 Equal Load Apportioning

Energy production and conversion load demands are normally allocated such that all available and non-limited (i.e., no operating constraints) units equally contribute their share of the EP and EC loads to meet the overall plant electrical load demand. "Available and non-limited" is taken to mean that irrespective of the performance limitations of any unit, each unit contributes to the overall demand equally as long as their respective performance limits are not exceeded. Thus, non-limited units are maneuvered to equal final load levels while limited units operate at their respective load limits (with margin). The strategy also involves equal changes (magnitude and rate) in load among the non-limited units from a balanced load configuration. Appendix I contains graphical illustrations of the equal load allocation strategies listed in Table I-1.

2.3.1.1.1.2 Unequal Load Apportioning

The PCDIS is designed to control reactor module and turbine-generators independently and at different load levels. There are plant operating modes and conditions when unequal (unbalanced) partitioning and allocation of load demands is made by the PSCS. The PSCS normally apportions loads unequally due to component operational limits; however, the PSCS is also designed for apportioning loads unequally to optimize the plant operating performance.

The strategy for unequal load allocation involves maneuvering the plant into a configuration whereby different units operate at different load levels. It also involves concurrent, unequal changes in unit loads from an initial load configuration that may be equalized or unequal among the units. For example, given a demand to increase the MHTGR plant output by 30% of rated capacity (say from 320 MWe to 500 MWe), the PSCS may determine that Module 1 contribute 40% of the increase (72 MWe), Module 2 contribute 30% of the increase (54 MWe), Module 3 contribute 20% of the increase (36 MWe), and Module 4 contribute 10% of the increase (18 MWe). Similarly, the electrical load increase may be unequally allocated to each T/G and associated feedwater train. The PSCS determines the rates of change in the individual NSSS and ECA loads and the final load levels for each NSSS and ECA.

When plant load demand is sufficiently less than plant power generating capability, load levels of limited modules are maintained approximately 10% below their respective load limits provided stable module operation can be maintained (e.g., above 25% rated load). This permits a higher rate of response to a plant load increase than the rate allowable (i.e., 5/4%/min. times the number of non-limited modules in operation) if limited module(s) were at its(their) upper load limits.

Appendix I contains graphical illustrations of the unequal load allocation strategies listed in Table I-1.

2.3.1.1.2 Normal Shutdown Control
(Goal 1, State 2)

[LATER]

2.3.1.1.3 Normal Control During Refueling
(Goal 1, State 3)

[LATER]

2.3.1.1.4 Normal Startup/Shutdown Control (Goal 1, State 4)

Startup from a total plant shutdown condition is normally performed in increments of two reactors and one ECA at a time when both turbines are available. The reactor modules are brought on-line in sequential order. Reactor module startups from depressurized shutdown conditions are accomplished by operationally sequencing each module up to minimum stable operating conditions. Concurrent startup of four reactors and two turbines is an infrequent occurrence (e.g., 0.1 per year, conservatively). However, reactor module startups from pressurized shutdown conditions can be performed in parallel.

Module load levels are adjusted in parallel to a common average load level at normal load ramp rates of +1/2 percent per minute. Modules are normally connected to the main steam line one at a time. The maximum perturbations in the main steam header occur when a second module is added with only one module on line. The steam generator outlet pressure for the reactor module to be connected is regulated at 2575 psia (160 psi higher than the main steam header pressure setpoint) by bypassing steam flow through the reactor module startup bypass valve. The reactor module isolation valve is then opened which results in automatic closure of the startup bypass valve due to the pressure difference between the bypass and the main steam header. As the isolation valve is opened, the steam generator outlet pressure decreases rapidly. However, this pressure drop results in a negligible increase in the feedwater flow for the reactor module being connected and a negligible decrease in the steam temperature. The steam temperature is regulated by adjusting the reactor power.

Each operational sequence has a set of logical hold points requiring operator acknowledgement. These hold points reduce the probability of automatic controls challenging normal operation, investment protection and safety protection. They also permit the operator to exercise discretionary actions during plant operation. The operator renders permissives to the automatic controls at predefined stages of the startup operational sequence. The permissives (i.e., logical removal of a temporary suspension in automatic sequencing) indicate to the automatic controls that the operator has acknowledged proper automatic control actions and confirmed that plant conditions permit proceeding to the next stage of the startup sequence. Operational hold points are also used during prestartup or shutdown phases (venting, filling, draining, etc.).

2.3.1.1.4.1 Startup Operational Sequence

Table 2-4 first lists the initial conditions and operational objectives of the startup operational sequence. This is followed by the tabulated list of operational sequence activities (OSAs) for startup of two reactor modules and one turbine. Stages of the sequence requiring operator permissives are indicated by asterisks (*) in Table 2-4.

2.3.1.1.4.2 Transition to Shutdown

From a control standpoint, the logistics of bringing a module to (de)pressurized shutdown conditions is essentially the reverse of that used for startup control. The modules are maneuvered sequentially in order to keep the turbines on-line as long as possible; otherwise the modules are shutdown in a step-wise parallel manner.

Reactor modules are disconnected from the main steam header one at a time. For example, with respect to one feedwater train operating at full capacity (i.e., two modules and one turbine operating at 100 percent load) a reactor module to be disconnected is maneuvered down to a 25 percent load level. At 25 percent load, the reactor module steam isolation valve closes. Reactor module steam is bypassed upon opening of the reactor module startup bypass valve. The other reactor module in operation remains at 100 percent load and the turbine operates at 62 1/2 percent capacity. The main steam header pressure is stabilized to its setpoint established by the NSSS control subsystem. Main steam flow to the turbine is gradually reduced from the initial 62 1/2 percent level to a final level of 50 percent as the reactor module at 25 percent power (corresponding to 12 1/2 percent turbine load) is disconnected from the main steam header.

2.3.2 System Steady-State Performance

2.3.2.1 PSCS Steady State Performance

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

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

2.3.2.2 NSSSCS Steady State Performance

[LATER - Refer to NSSSCS SSDD]

2.3.2.3 DMS Steady State Performance

[LATER]

2.3.2.4 TOSS Steady State Performance

[LATER]

2.3.3 System Response to Plant Transients

Section 2.3.3.1 describes the control strategies and actions of the PCDIS in response to off-normal occurrences and conditions. Section 2.3.3.2 describes in more detail the PCDIS responses to specific plant transient events.

2.3.3.1 Off-Normal Control (Goal 2)

The basic PCDIS control strategy executed in response to partial losses of energy production (EP) and/or energy conversion (EC) capability is to sacrifice plant operating efficiency and capacity factor on a short-term basis to support power distribution network (grid) availability over the long term. The PCDIS avoids potentially greater losses of plant electrical output by not attempting to maintain the original plant electrical output level. Upon partial loss of EP and/or EC, the PCDIS controls automatically reconfigure and stabilize plant operation at those reduced EP and EC levels supported by operationally limited components maintaining their initial operating levels, if possible.

The PSCS presents pertinent plant information and a recovery plan to the operator for assessing the off-normal conditions and determining a course of action. The PSCS accepts operator acknowledgements, dispositions, and permissives to proceed with automatic control sequences. Each NSSS and ECA is returned to its original EP and EC levels within the capabilities of limiting components following completion of diagnostic and corrective measures (collectively determined by the plant operators and the PCDIS automated diagnostics). The PSCS compensates for loss of energy production by reallocating EP and/or EC loads to available modules and T/Gs to the extent their operating margins and admissible load configurations allow for this without compromising investment protection and safety protection.

2.3.3.1.1 Off-Normal Energy Production Control (Goal 2, State 1)

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

Under abnormal conditions (e.g., reactor power greater than heat sink capability) a set of actions referred to as automatic load runback are performed. Commands are given automatically to the NSSSCS and ECAC to minimize temperature transients to the steam generator and reactor components. This is achieved by adjustments to reactor and turbine load, feedwater supply and helium circulation. The NSSSCS and ECAC controls are designed to mitigate the effects of transients which would otherwise load to a turbine trip and loss of power generation. If certain modules become constrained during these transients, then the maximum load change rate limits are lowered for constrained modules to avoid challenges to equipment and component protection.

Automatic load reallocation is executed if an imbalance occurs among any of the following:

1. total module steam production demanded
   and
   total feedwater supply available,

2. total module steam production demanded
   and
   total T/G steam admission capability,

3. total T/G steam admission demanded
   and total module steam production capability,

4. total T/G steam admission demanded
   and
   total feedwater supply available,

5. total feedwater supply demanded
   and
   total module steam production capability.

6. total feedwater supply demanded
   and
   total T/G steam admission capability.

Table I-1 in Appendix I summarizes the alternate load allocation strategies available to the PSCS to (re)configure and maneuver the plant in response to plant off-normal conditions.

2.3.3.1.2 Off-Normal Shutdown Control
(Goal 2, State 2)

[LATER]

2.3.3.1.3 Off-Normal Control During Refueling
(Goal 2, State 3)

[LATER]

2.3.3.1.4 Off-Normal Startup/Shutdown Control
(Goal 2, State 4)

Table 2-8 first lists the initial conditions and operational objectives and requirements for a shutdown operational sequence following detection of a leaking module feedwater valve. These are are followed by a tabulated list of the associated operational sequence activities (OSAs). Figure [TBD] provides the reference Piping and Instrumentation Diagram (P&ID) for this particular operational sequence.

2.3.3.2 System Response to Specific Plant Transient Events

This section describes the sequence of actions of the PSCS, NSSSCS, and ECAC in response to the following plant transient events:

[LATER - The next revision of this SDD will incorporate the FY87 MGCRS Transient Analysis results. A detailed description of plant controllability and performance based on the FY86 design is provided Reference 6.]

2.3.4 System Failure Modes and Effects

2.3.4.1 PSCS Failure Modes and Effects

The PSCS contains no devices or performs any functions, the failure or unavailability of which could lead to, or increase the probability of, radionuclide releases to the public or environment in excess of 10CFR100 limits. Safety-related systems, structures and components are functionally independent of the PSCS; the PSCS does not have any direct, physical interfaces with safety-related equipment. The PSCS equipment is physically separated from safety-related equipment. The PSCS indirectly interfaces with safety-related systems via the DMS to monitor safety system status. Thus, as shown in Figure 2-2, the DMS has physical interfaces with safety systems but these interfaces are only used for unidirectional data acquisition from the safety-related systems. The PSCS cannot prevent or inhibit any safety-related function from being performed. All failure modes of the PSCS leave intact the plant safety-related functions.

The effective forced outage hour (EFOH) allocation of the PSCS is 11.5 hours per year. The PSCS meets this requirement by contributing only [6.5] hours per year to the overall plant forced outage time. The PSCS reliability is [1.8×10^{-5}]. The reliability is the time-averaged probability in any hour over the 40-year plant life that the PSCS will fail in such a way as to require an entire plant shutdown. This corresponds to a mean time between failure (MTBF) of approximately [6.3] years.

Due to the non-safety function of the PSCS, the MCR facility is a non-safety category structure; there are no safety-related systems or components in the MCR. The operability requirements of the PSCS are such that the MCR is located in the Operations Center off, but adjacent to, the Nuclear Island. Damage or failure of the PSCS or the MCR cannot impact safety-related systems, structures or components. The MCR structural design is based on seismic and wind loading design criteria of ANSI A58.1-1982, Minimum Design Loads for Buildings and Other Structures. Operator and PSCS equipment exposure to dust, fume and other particle ingress is limited by the HVAC system for the MCR and by maintaining the MCR slightly pressurized.

The capability is provided outside the MCR for operators (control room or roving) to achieve depressurized shutdown conditions. Controls and instrumentation of other plant systems located outside the MCR are used to complete reactor shutdown, initiate and maintain cooling and bring the plant to a safe, cold shutdown condition. Their use is required under any combination of the following when limiting conditions for operation require a plant shutdown:

1. the MCR becomes uninhabitable,
2. the PSCS computers become unavailable,
3. the CROW becomes unavailable.

For item 1. above, the MCR operator initiates reactor shutdowns prior to evacuation of the MCR. Completion of a controlled plant shutdown is performed at the alternate shutdown facility. For item 2. above, a controlled plant shutdown is performed at the alternate shutdown facility upon a loss, or long-term anomalous status indication, of PSCS computers. For item 3. above, the PSCS computers are designed to coordinate a controlled plant shutdown upon long-term unavailability (estimate hours) of the CROW. Reliable operator response is ensured by the response time requirements (on the order of hours), and environmental, access and security control measures.

2.3.4.1.1 PSCS Computers

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

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

2.3.4.1.2 Control Room Operator Workstation

The plant is normally operated from the CROW in the MCR except under conditions that render the MCR uninhabitable and/or the PSCS unavailable. Should these conditions occur, control and monitoring of selected safety and non-safety systems can be performed at their respective equipment locations outside the control room. Normal access to these controls and instrumentation outside the MCR is also required during maintenance, prestartup, etc. since only PSCS equipment and some DMS equipment is located in the MCR.

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

2.3.4.2 NSSSCS Failure Modes and Effects

[LATER - Refer to the NSSSCS SSDD]

2.3.4.3 DMS Failure Modes and Effects

2.3.4.3.1 DMS Failure Modes

[LATER]

2.3.4.3.2 Effects of DMS Failures

Total loss of the DMS communication network would require a complete plant shutdown.

2.3.4.4 TOSS Failure Modes and Effects

2.3.4.4.1 TOSS Failure Modes

[LATER]

2.3.4.4.2 Effects of TOSS Failures

TOSS failures would result in loss of technical support workstation availability (i.e., loss of technical computations and information processing capability). Failure of any portion of the TOSS has no direct impact on any other plant structure, system or component.

2.4 System Arrangement

2.4.1 PSCS Arrangement

2.4.1.1 PSCS Computers

The PSCS computers embodying the supervisory control software (strategies and algorithms) are located in a secured area of the computer facility in the Operations Center. There is sufficient time, environmental control and security measures for the plant staff to access this and other PCDIS equipment outside the control room when control, monitoring or maintenance are required. In addition, test/calibration/diagnostic operations are automated and the devices for this accompany the equipment and/or the maintenance personnel outside the control room.

2.4.1.2 Operator Workstations

The single MHTGR main control room (MCR) within the Operations Center is the plant's operations mission management center. Plant operations are managed and coordinated under the integrated roles of the licensed operators and the PSCS. Included in the MCR are seated-operator arrangements of all plant control initiators and monitors required by the operators. These seated-operator arrangements are the workstation components of the PSCS referred to in previous sections. The operability requirements of other MHTGR plant systems and components are such that their respective controls and instrumentation are located outside the control room in the proximity of the system, component and/or process. The initiators and monitors embodied within the workstations collectively form what are referred to as the Control Room Operator Workstation (CROW) and the Control Room Assistant Workstation (CRAW). Figure 2-8 depicts the workstation arrangements within the main control room.

2.4.1.2.1 Control Room Operator Workstation (CROW)

The CROW is the control room operator's interface with the plant systems, processes and controls. The CROW contains all the control initiators and monitors required for the single licensed operator to start up, operate, and shut down the plant in conjunction with the PSCS. The CROW consists of CRT monitors with touch-activation screen display capabilities and touch-activated control panels. Figure 2-9 provides a conceptual illustration of the CROW.

2.4.1.2.2 Control Room Assistant Workstation (CRAW)

The CRAW contains display generation and printing equipment that can generate any display or print any information normally available to the operator at the CROW. It also provides the capability to access plant data bases maintained by the Data Management Subsystem. Plant systems, equipment and components cannot be controlled or operated from the CRAW.

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

2.4.1.2.3 Communication and Display Generation Equipment

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

Entrance to the control room is controlled by the shift supervisor when present; otherwise, the assistant operator is allocated this responsibility. For operator comfort and security, access to kitchen, lounge and lavatory facilities is provided. The MCR has low-pile, low-static carpeting to reduce noise levels and aid operator comfort. It is also slightly pressurized for minimizing dust and other particle ingress.

2.4.2 NSSSCS Arrangement

[LATER - Refer to NSSSCS SSDD]

2.4.3 DMS Arrangement

[LATER]

2.4.4 TOSS Arrangement

[LATER]

2.5 Instrumentation and Control

The PCDIS is a system of instrumentation and controls. Therefore, refer to all other sections of this document.

[Pages 2-30 through 2-59 intentionally left blank.]

TABLE 2-4

STARTUP OF TWO NSSS MODULES AND ONE ECA

Initial Conditions:

NSSS module 1	0% rated power	NSSS module 3	0% rated power
NSSS module 2	0% rated power	NSSS module 4	0% rated power
ECA module A (T/G A, FW Train A)	0% rated output	ECA module B (T/G B, FW Train B)	0% rated output

Sequence Initiator: None other than an operations decision to return units to service.

Top-Level Operational Requirement: Return units to service in a timely and efficient manner

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

Ordered Objectives:

1. Establish necessary conditions to facilitate startup of NSSS modules 1 & 2 and ECA module A.

2. Achieve necessary conditions for stable steam generator startup operation in NSSS module 1.

3. Generate steam sufficient for component (e.g., main steam header and T/G A) warm-up.

4. Complete a smooth transition from startup system flow paths to main steam and feedwater flow paths.

5. Synchronize and load T/G A.

6. Achieve stable operation and necessary conditions to facilitate startup of NSSS module 2 and bring NSSS module 2 onto the main steam header.

7. Allow T/G A to dictate its steam admission (e.g., maintaining a constant T/G load) while bringing NSSS module 2 onto the main steam header.

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
1.	Complete and verify valve lineups and other preoperational procedures	24-48 hrs
2.	Prestart checks ascertain that required auxiliaries are properly in service.	8 hrs
3.	Verify auxiliary boiler & steam subsystems are operating and supplying steam to flash tank and steam seal header of T/G A.	
4.	Establish T/G A turbine seals.	8-12 hrs
5.	Establish condenser vacuum.	for steps
6.	Establish condensate recirculation flow for chemistry limit check.	3 through 7
7.	Establish FW Train A feedwater flow to main feedwater header when chemistry is within limits for low power operation of NSSS module 1 steam generator.	
8.	Pressurize NSSS module 1 vessel to full helium inventory. Perform precritical checks.	5 hrs
9.	Verify NSSS module 1 status meets specifications for initiating rod withdrawal	0.5 hrs

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
16.	Increase secondary pressure to 1800 psia (20 psia/min).	0.5 hrs
17.	Increase feedwater temperature from 220 °F to 380 °F (1 °F per minute).	3 hrs
18.	Increase power to 7% (0.039%/min). Verify correct moisture monitor sample flow. Reset flow setpoint for power operation.	2 hrs
19.	* Operator acknowledges operational hold point for verifying that reactor module status meets specifications for increasing reactor power. *	0.1 hrs
20.	Continue control rod withdrawal per established sequence to increase reactor power to 16% (0.30%/min) and circulator speed to 30% (0.58%/min).	0.5 hrs
21.	Maintain He flow such that core temperature rise limits are not exceeded. Establish minimum required feedwater flow to steam generator. Maintain backpressure as module power increases heat input.	1 hr
22.	Establish boiling in the steam generator with flow directed to startup bypass.	0.5 hrs

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
10.	While monitoring subcritical multiplication on startup neutron monitoring, withdraw control rods per withdrawal sequence to predicted critical position.	1.5 hrs
11.	Bring NSSS module 1 reactor to critical (0.5% power). Ascertain criticality is established within allowable limits (otherwise reinsert control rods to shutdown).	1 hr
12.	Conduct rod worth and reactivity coefficient measurements as required (0.25 hrs per rod; 30 rods).	7.5 hrs
	Concurrently increase secondary pressure (startup bypass setpoint) to 1200 psia (17 psi/min).	0.5 hrs
13.	Complete T/G A pre-start checks and place turning gear in operation if not already in operation	0.5 hrs
14.	Increase feedwater flow to 15% (0.21%/min). Increase reactor power to 3% (0.053%/min). Increase circulator speed from 5% (min. value) to 12.5% (0.16%/min).	1 hr
15.	* Operator acknowledges operational hold point for maintaining approx. 400 ^{o}F steam generator secondary outlet temperature for feedwater cleanup as necessary. *	5 hrs

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
30.	* Operator provides permissive acknowledging stable NSSS and ECA parameters and designating continued automatic feedwater flow control without operational hold points. *	1 hr
31.	Close startup bypass valves to achieve full module steam flow to the main steam header.	0.1 hrs
32.	Close turbine bypass valves. When the turbine is warmed, roll turbine to synchronous speed, excite the generator, and synchronize and load the generator to low load conditions.	0.5 hrs
33.	Increase T/G A load to 12.5% at 1% per minute.	0.1 hrs
34.	Transfer housepower from the startup transformer to the unit auxiliary transformer.	n/a
35.	Concurrently increase NSSS module 1 load to 100% at 5% per minute and T/G A load to 50% at 2.5% per minute.	0.25 hrs
36.	REPEAT OPERATIONAL SEQUENCE ACTIVITIES 1 - 2 (in parallel with previous activities), 8 - 12 (16 hrs), 14 - 23 (8 hrs), and 25 - 28 (6 hrs) FOR STARTUP OF NSSS MODULE 2.	30 hrs
37.	Balance NSSS module 2 steam generator outlet pressure with the main steam header pressure.	0.1 hrs

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
23.	Decrease reactor power to 14.7% (0.011 % /min).	2 hrs
24.	* Operator acknowledges operational hold point for maintaining approx. 800 °F main steam temperature for secondary component warm-up. Warm main steam header by partially opening the steam generator outlet valve and the main stop valves above seat drains. *	4 hrs
25.	* Operator provides operational permissive for designating reactor power and circulator speed control via automatic main steam temperature control (setpoint at 826 °F). *	0.5 hrs
26.	When the main steam header is available, place the auxiliary boiler in a standby mode and close the steam generator startup bypass valves.	0.1 hrs
27.	Increase reactor module power to 25% (0.039% /min). Stabilize steam generator operation.	4.5 hrs
28.	Ramp main steam temperature setpoint to 1005 °F (2 °F per minute).	1.5 hrs
29.	* Operator acknowledges operational hold point for increasing secondary pressure setpoint to 2430 psia (11 psi/min). *	1 hr

TABLE 2 - 8

ORDERLY SHUTDOWN FOLLOWING A MODULE FEEDWATER VALVE LEAK

Initial Conditions:

NSSS module 1	100% rated power	NSSS module 3	100% rated power
NSSS module 2	80% rated power	NSSS module 4	50% rated power
ECA module A (T/G A, FW Train A)	100% rated output	ECA module B (T/G B, FW Train B)	65% rated output

Other: Magnitude of valve leak is such that there is no measurable disturbance to plant operation observed by the control room operators

Sequence Initiator: Roving operations crew discovers leaking module feedwater valve

Top-Level Operational Requirement: Limit the impact of the valve failure on plant availability.

TABLE 2-4
(continued)

STARTUP OF TWO NSSS MODULES AND ONE ECA

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
38.	* Operator acknowledges pressure balance conditions and the reset of NSSS module 1 load allocation from 100% to 75%. *	1 min
39.	Open NSSS module 2 steam generator outlet isolation valve.	1 min
40.	Concurrently close NSSS module 2 startup bypass valve and reduce NSSS module 1 load to 75%.	0.1 hrs

TABLE 2 - 8
(continued)

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
1.	Based on prognosis of roving operations crew, assess the potential of the problem to impact plant operation. Decide on courses of immediate planned actions (i.e., shut down NSSS modules 1 & 2 and ECA module A) and long-term planned actions (i.e., valve repair)	n/a
2.	Determine loading and system performance limitations.	0.25 hrs
3.	Determine and set the load reallocations that achieve balanced main steam header and feedwater header mass flow balance conditions required for isolation of NSSS modules 1 & 2 and ECA module A.	0.1 hrs
4.	Concurrently ramp T/G A output and FW Train A flow from 100% to 90% and T/G B output and FW Train B flow from 65% to 75% at 5% per minute such that plant electrical output does not change appreciably.	0.1 hrs
5.	Ascertain achievement of mass flow balance between main steam header and feedwater header a) request mass balance calculation, b) calculate mass balance, c) confirm satisfactory balance conditions.	0.1 hrs
6.	Initiate and complete the closure of FW Train A feedwater header division valve.	0.1 hrs
7.	Determine rates of NSSS module and ECA module load reductions.	0.1 hrs

TABLE 2 - 8
(continued)

ORDERLY SHUTDOWN FOLLOWING A MODULE FEEDWATER VALVE LEAK

Ordered Objectives:

1. Based on prognosis of roving operations crew, assess the potential of the problem to impact plant operation.
(Shift supervisor responsibility)

2. Decide on a course of immediate planned action (which is to shut down NSSS modules 1 & 2 and ECA module A) and a course of long-term planned action (which is to repair the valve).

3. Establish necessary plant conditions to facilitate immediate planned actions.

4. Maneuver NSSS modules 1 & 2 and ECA module A to shutdown conditions necessary for transition from HTS to SCS operation (excluding Feedwater Train A).

5. Achieve transition from HTS to SCS operation.

6. Shut down and depressurize Feedwater Train A while maintaining condensate recirculation flow.

7. Secure required auxiliaries, systems and components.

8. Undertake long-term planned actions.

TABLE 2 - 8
(continued)

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
16.	Reduce reactor power levels, steam generator outlet temperatures and feedwater inlet temperatures to meet conditions required for SG floodout and subsequent shutdown of NSSS module 1 & 2 helium circulators.	2 mins
17.	Shut down NSSS module 1 & 2 helium circulators.	0.1 hrs
18.	Transfer from "standby" to "core cooling" mode of shutdown cooling.	0.1 hrs
19.	Shut down feedwater pumps in FW Train A and depressurize while maintaining condensate recirculation flow.	0.5 hrs
20.	Isolate the module feedwater valve requiring maintenance.	0.1 hrs
21.	Secure required auxiliaries.	2 - 4 hrs
22.	Undertake long-term planned actions.	n/a

TABLE 2 - 8
(continued)

	OPERATIONAL SEQUENCE ACTIVITY	TOTAL EXECUTION TIME
8.	Concurrently ramp NSSS module 1 from 100% to 80% at 5% per minute and ECA module A from 90% to 80% at 2.5% per minute.	0.1 hrs
9.	Concurrently ramp NSSS modules 1 and 2 and ECA module A from 80% to 25% at 5% per minute.	0.2 hrs
10.	* Operator acknowledges minimum flow conditions and grants permissive to initiate taking T/G A off line. *	2 mins
11.	Electrically isolate T/G A from the grid while maintaining 25% flow conditions in FW Train A.	0.1 hrs
12.	* Operator initiates (and acknowledges completion of) sequential transition of NSSS module 1 & 2 operations from main steam and feedwater systems to startup and bypass systems. *	0.1 hrs
13.	Initiate and complete closure of associated main steam header division valve and steam generator isolation valves.	2 mins
14.	* Operator acknowledges completion of isolation. *	1 min
15.	Reduce NSSS module 1 & 2 parameters (i.e., reactor power, feedwater flow, He flow, etc.) to levels corresponding to minimum stable steam generator operation (from 25% to approx. 15%).	0.5 hrs

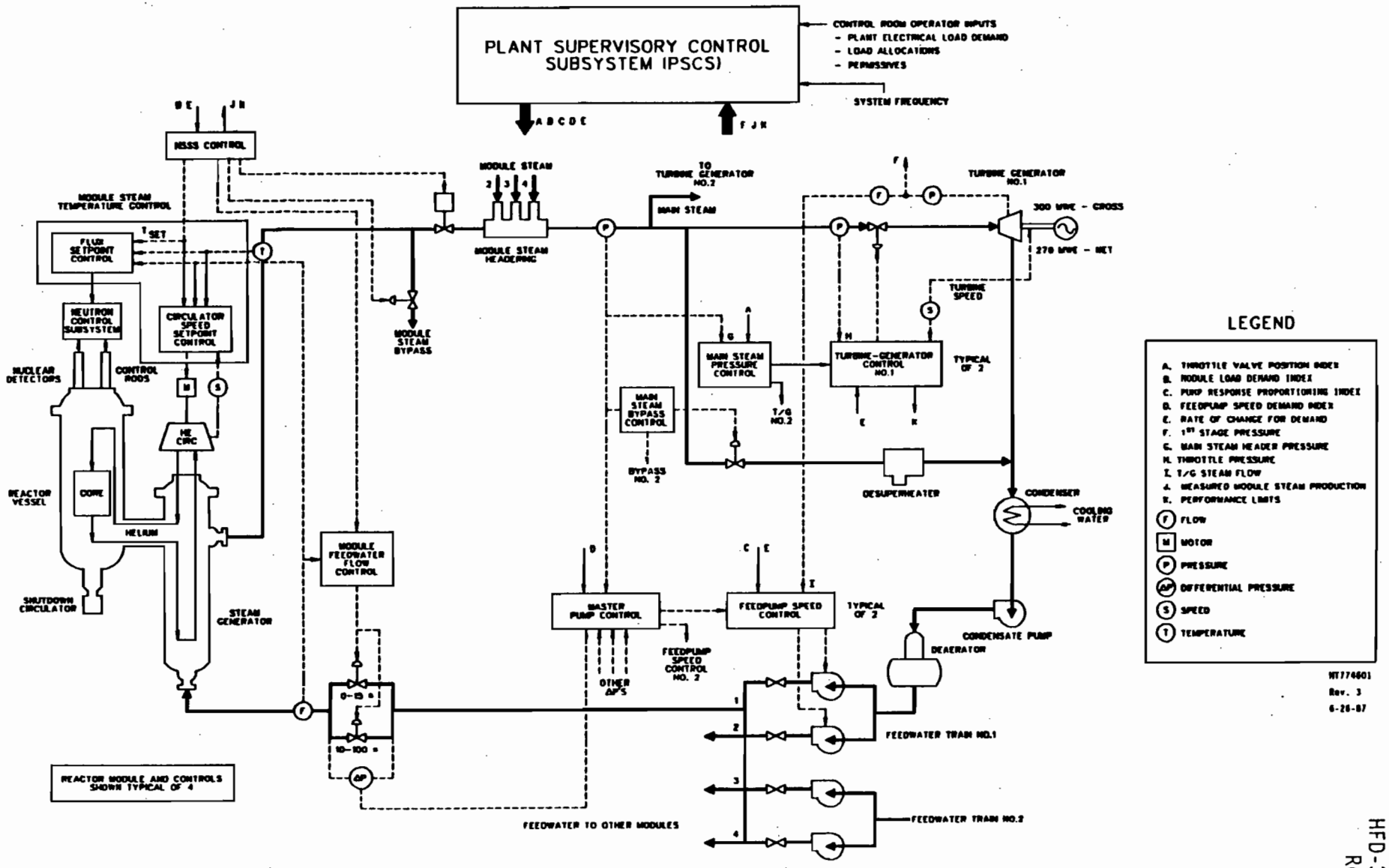


FIGURE 2-2 MHTGR INTEGRATED CONTROL AND INTERFACE SCHEME

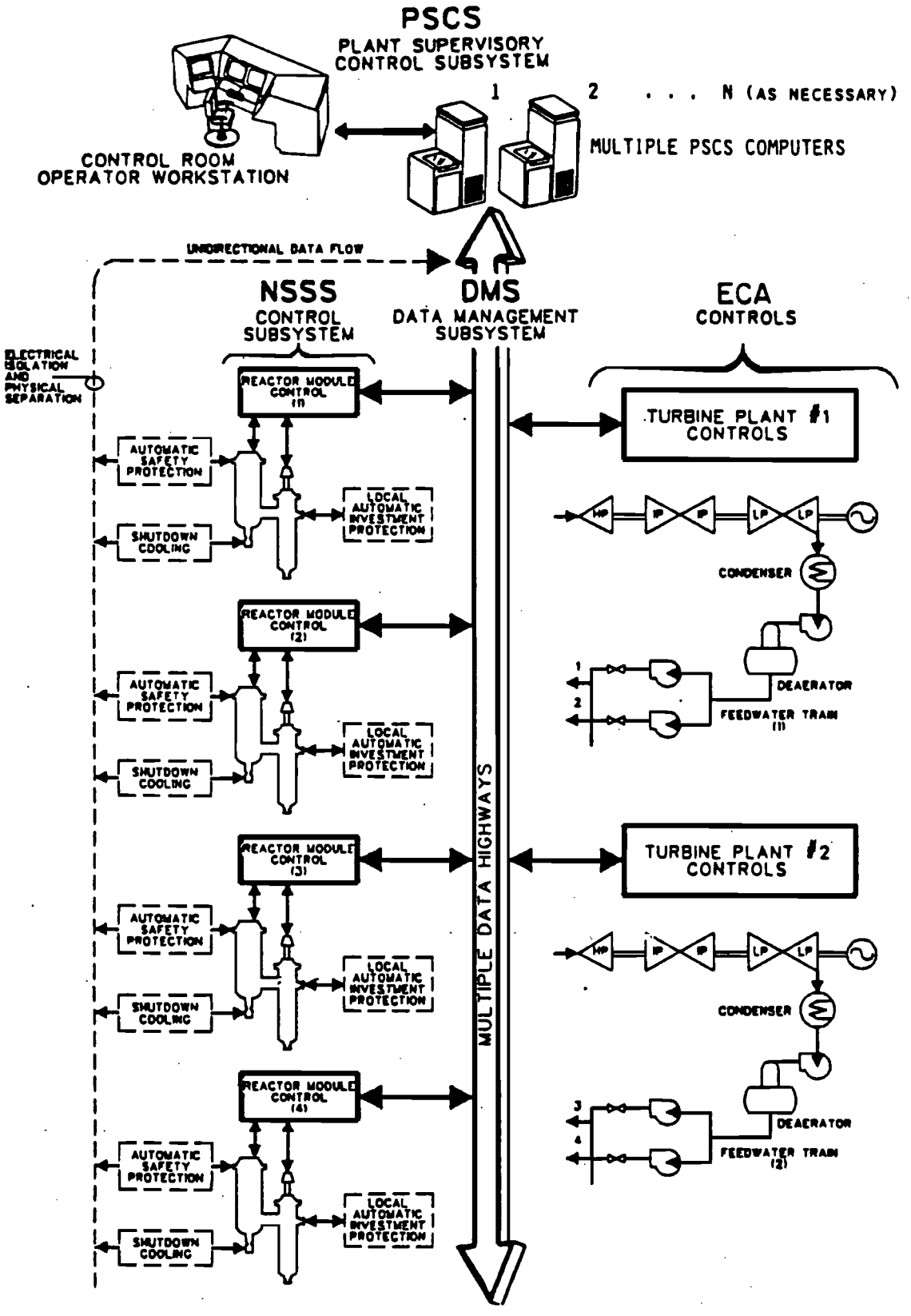


FIGURE 2-1 PCDIS INTEGRATED CONTROL OVERVIEW

LEGEND

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

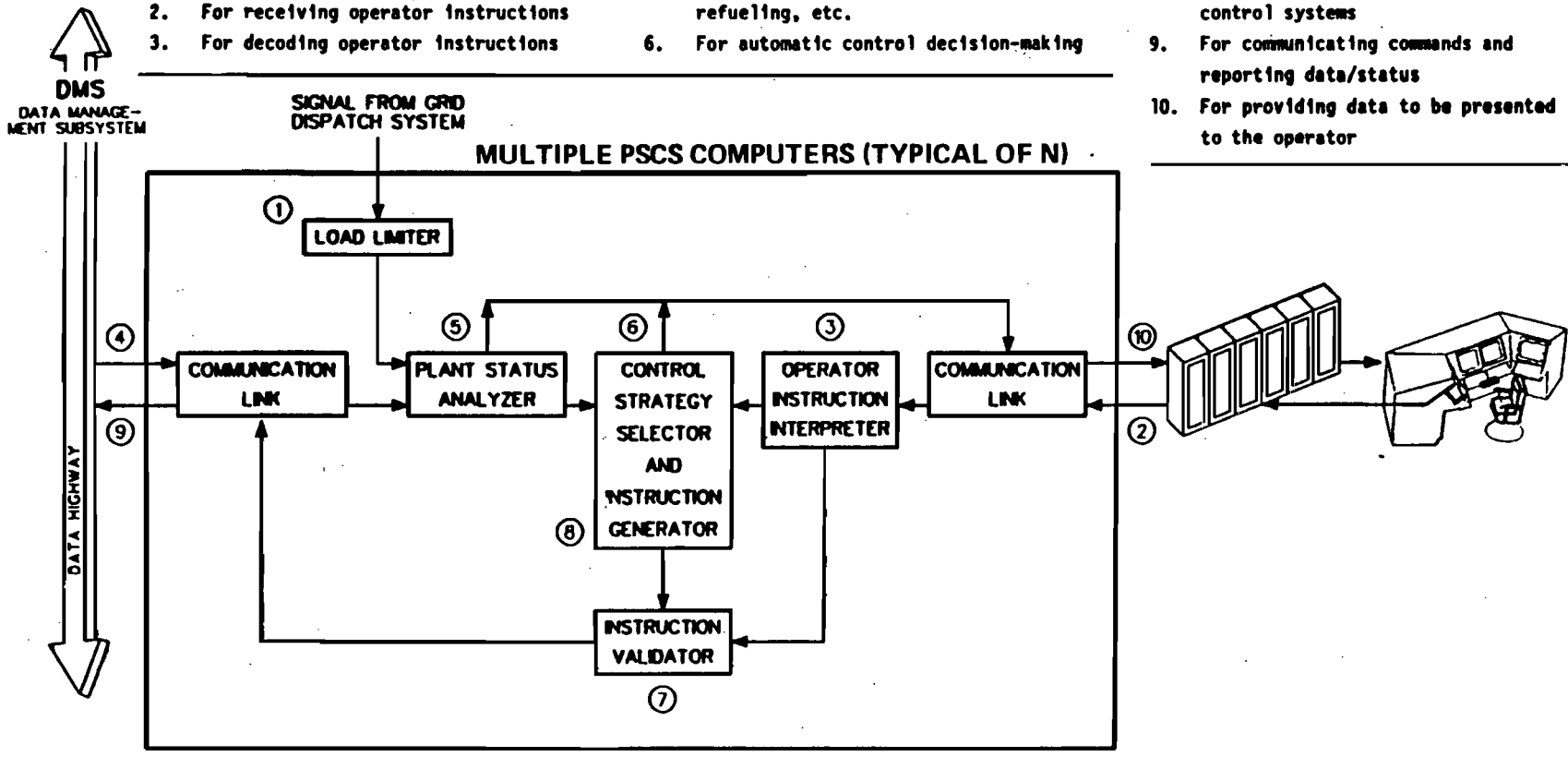


FIGURE 2-4 FUNCTIONAL CONFIGURATION OF PSCS COMPUTERS

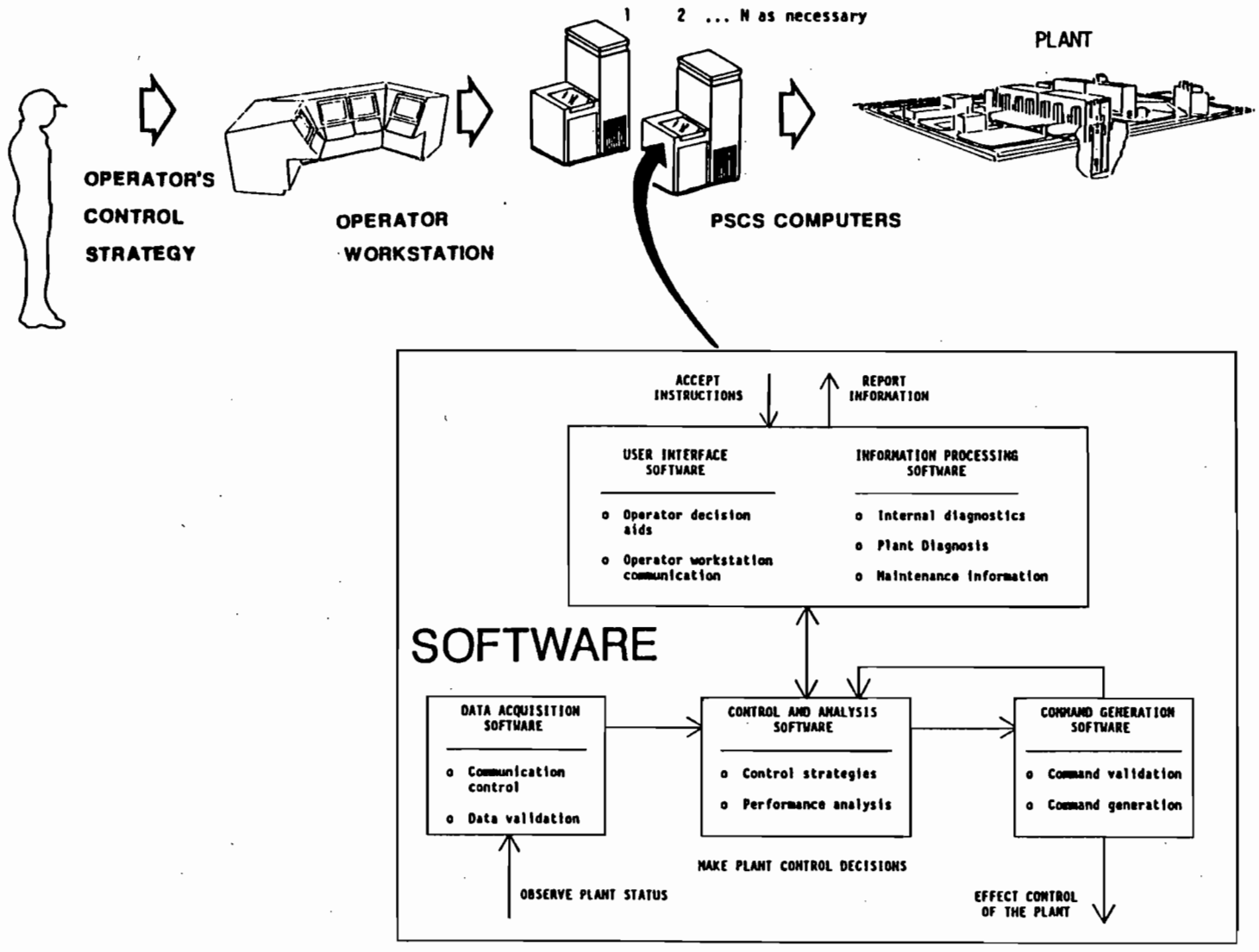


FIGURE 2-3 PSCS CONFIGURATION OVERVIEW

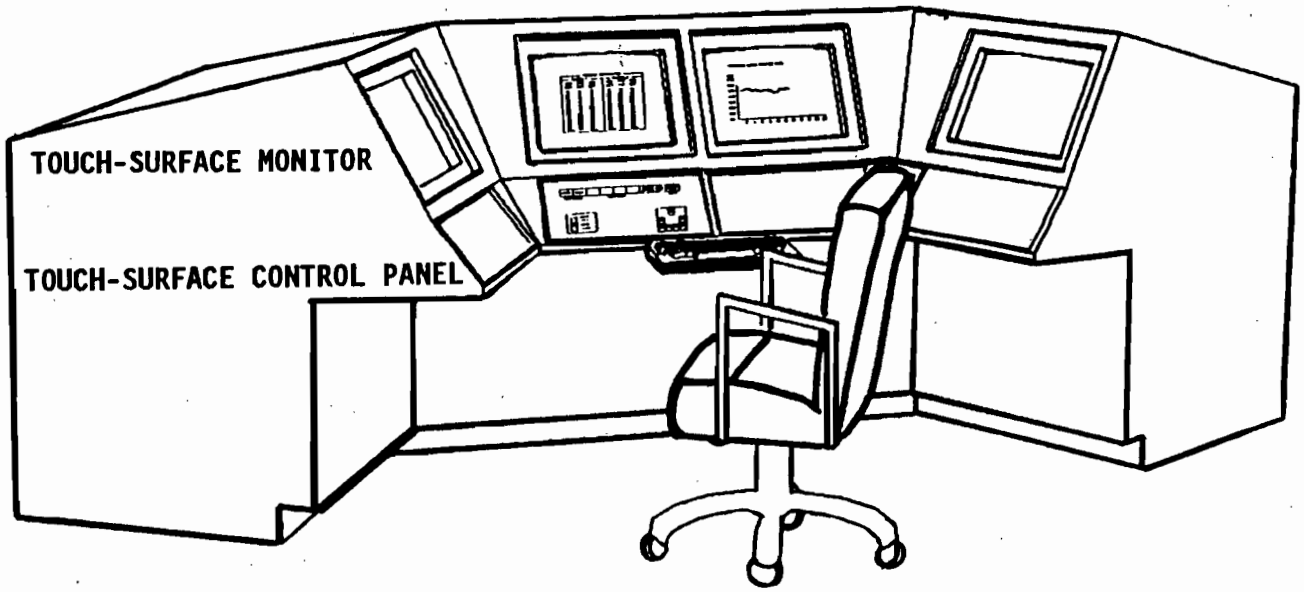


FIGURE 2-9 CONTROL ROOM OPERATOR WORKSTATION

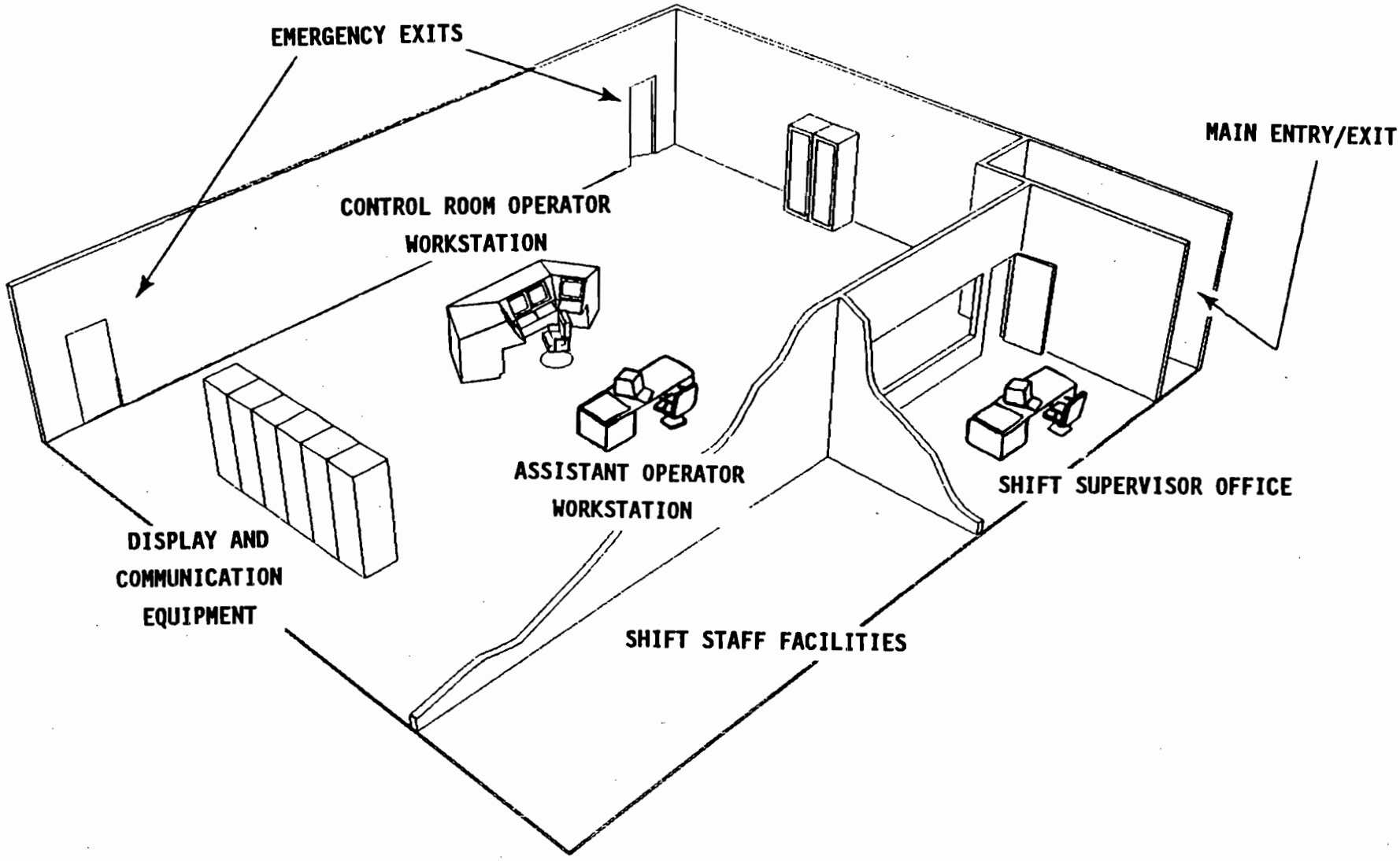


FIGURE 2-8 MHTGR SINGLE CONTROL ROOM ARRANGEMENT

SECTION 3

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

Per the Integrated Approach, five system-level functions are defined for overall plant control. The five functions, from which all subordinate PCDIS subfunctions are derived from, are the following:

- o Accept control direction
- o Observe plant status
- o Make control decisions
- o Effect control of the plant
- o Report information

Logical groupings are identified for the subfunctions of these five functions. The subfunctions are logically grouped according to one of the following functional categories:

- o Supervising and coordinating plant control and operation
- o Controlling energy production (nuclear steam supply)
- o Controlling energy conversion (turbine plant)
- o Managing plant data
- o Supporting plant technical operations

These logical groupings are the basis for the allocation of subfunctions to PCDIS subsystems (including controls for the energy conversion area) made in Appendix H and described in this section. Allocation of the subfunctions in each of the above categories is made to the following PCDIS subsystems

- o Plant Supervisory Control Subsystem (PSCS)
- o NSSS Control Subsystem (NSSSCS)
- o Data Management Subsystem (DMS)
- o Technical Operations Support Subsystem (TOSS)

and what is referred to as the Energy Conversion Area Controls (ECAC). The ECAC is the title used in this document to refer collectively to the controls for the balance of the plant (e.g., main steam, bypass and feedwater systems, turbine-generator control systems, etc.).

3.1 Subsystem Functions

3.1.1 Plant Supervisory Control Subsystem Functions

3.1.1.1 PSCS Computers

The functions of the PSCS computers are the following:

1. Accept plant control and operating directions, for example:

   a. operator-initiated reactor shutdown
   b. operator hold points and permissives during startups
   c. instructions from the operator workstation to provide information for display
   d. plant load requests from the grid dispatcher

2. Observe plant status, for example:

   a. main steam and feedwater conditions
   b. energy production and conversion load configuration
   c. major component performance and operational limits

3. Make plant-level control decisions, for example:

   a. determine how to partition and allocate the overall plant load to individual reactor modules and turbine-generators
   b. determine the rate of main steam and feedwater flow changes necessary to achieve optimum plant response to concurrent or unbalanced load maneuvers.

4. Effect control at the plant level, for example:

   a. communicating operator instructions for starting or stopping major equipment
   b. communicating automatic control instructions for changing load

5. Report plant information, for example:

   a. information required by the operator
   b. PSCS status information required for surveillance and maintenance

3.1.1.2 PSCS Operator Workstations

3.1.1.2.1 Control Room Operator Workstation

The functions of the control room operator workstation (CROW) are the following:

1. Accept plant operating directions, for example:

   a. instructions from the operator
   b. instructions from the PSCS computers regarding operator display generation

2. Observe plant operating status, for example:

   a. NSSS and ECA process and component conditions and performance
   b. safety system status
   c. proper operator acknowledgement of permissives, interlocks, bypasses, etc.

3. Make operator workstation decisions, for example:

   a. perform self-testing of key workstation functions
   b. detect (im)proper, (in)valid and (in)correct operator instructions regarding display generation or printing

4. Effect (generate) plant operating instructions, for example:

   a. interpret (decode) operator instructions
   b. communicate digitized operator instructions to PSCS computers

5. Report plant operations information, for example:

   a. display video images
   b. print data and graphics

3.1.1.2.2 Control Room Assistant Workstation

The functions of the control room assistant workstation (CRAW) are the following:

[LATER]

3.1.2 NSSS Control Subsystem Functions

The functions of the NSSSCS are the following:

1. Accept directions, for example:
   a. apportioned module load demands from the PSCS
   b. permissives (acknowledgement of operational hold points) from the operators during operational sequences such as startup

2. Observe NSSS-related status, for example:
   a. module steam conditions
   b. module feedwater flow

3. Make NSSS-related decisions, for example:
   a. determine what module feedwater demand is required to meet its allocated load demand and module steam conditions.
   b. determine circulator speed setpoints

4. Effect control of the NSSS, for example:
   a. analog and digital control signals to final control elements to bring module steam and reactor power to desired conditions
   b. module steam bypass valve positioning

5. Report NSSS information, for example:
   a. control rod positions
   b. module feedwater flows

The NSSSCS regulates reactor power and module steam conditions and the supply of steam to the main steam header. It accomplishes this through control of module feedwater flow, circulator speed, neutron flux and thermal power.

3.1.3 Data Management Subsystem Functions

[LATER]

3.1.4 Technical Operations Support Subsystem Functions

[LATER]

3.2 Subsystem Requirements

This section defines the PCDIS subsystem requirements. The subsystem requirements are those derived from analyses, trade studies and/or functional allocation on the plant-level and system-level requirements in Section 1. Each requirement is followed by its requirement traceability number used in Appendix A.

3.2.1 Plant Supervisory Control Subsystem (PSCS) Requirements

3.2.1.1 Subsystem Configuration and Essential Features Requirements

3.2.1.1.1 System Configuration Requirements

The PSCS shall be capable of coordinating plant control and operation for the performance and transient characteristics of the following reactor and turbine-generator combinations:

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

(3700.0321.020)

PSCS components whose failure would not have an immediate impact on plant output shall be located outside the control room with status indication provided to the control room.

(3700.0321.040)

The PSCS shall be designed for a Nuclear Island that includes four (4) standard reactor modules.

(3700.0321.042)

The PSCS shall be designed for an Energy Conversion Area that includes two (2) steam turbine-generators.

(3700.0321.044)

Human-machine interfaces and machine-machine communication interfaces shall be provided for PSCS equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.

(3700.0321.045)

Features of the PSCS (e.g., inter-system communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.

(3700.0321.050)

The PSCS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating de-energizing electronics or affecting the operation of other electronic equipment.

(3700.0321.055)

3.2.1.1.2 Essential Features Requirements

Human engineering techniques shall be employed in the design of the PSCS to enhance operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD].

(3700.0321.060)

PSCS features shall be included to facilitate operation of reactor modules and turbine-generators at different power levels.

(3700.0321.070)

Base the PSCS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.

(3700.0321.072)

3.2.1.2 Operational Requirements

3.2.1.2.1 Operational Staffing Requirements

The PSCS shall accommodate operation of the plant by two reactor operators in the control room.

(3700.0321.120)

3.2.1.2.2 Normal Operational Requirements

The PSCS shall facilitate the normal duty cycle events specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0102.128)

3.2.1.2.2.1 Operational Performance Requirements

The PSCS shall provide the capability to concurrently coordinate energy production, shutdown, refueling and startup/shutdown operations for different reactor modules and T/G's in a manner consistent with optimizing the economics of each.

(3700.0321.132)

3.2.1.2.2.2 Energy Production Requirements

The PSCS shall be designed to automatically accept, with concurrence by the operating staff, baseload and load following net electrical output load demands allocated to the plant by the utility grid dispatcher.

(3700.0321.135)

The PSCS shall include features to enable automatic control during plant operation.

(3700.0321.138)

3.2.1.2.2.3 Shutdown Requirements

The PSCS shall be designed to accommodate one or more reactor modules shutting down.

(3700.0321.139)

The PSCS shall include features to enable automatic control during orderly shutdowns.

(3700.0321.148)

3.2.1.2.2.4 Refueling Requirements

The PSCS shall accommodate removal of a reactor from service for refueling and its return to service with the remaining reactors and the turbine plant in operation.

(3700.0321.155)

3.2.1.2.2.5 Startup Requirements

The PSCS shall be designed to accommodate one or more reactor modules starting up.

(3700.0321.164)

The PSCS shall include features to enable automatic control during startups.

(3700.0321.168)

3.2.1.2.2.6 Main Control Room Operational Requirements

The control room operator workstation shall be human engineered to concurrently accept those inputs from a single operator required to control plant energy production, shutdown, refueling and startup/shutdown operations.

(3700.0321.170)

The control room operator workstation shall incorporate features necessary to facilitate startup, shutdown, monitoring and control and shall provide for the shutdown of major systems and components by the operator in order to limit investment risk and assure personnel protection.

(3700.0321.175)

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

(3700.0321.180)

The operator workstations to initiate and monitor all actions and information, respectively, requiring operator interaction from within the main control room shall be human-engineered and designed as a functional entity of the PSCS.

(3700.0321.185)

3.2.1.2.3 Off-Normal Operational Requirements

The PSCS shall be designed to operate the plant through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0321.190)

The PSCS shall be designed to sustain continuous plant operation at reduced electrical output through and following transients associated with the loss or failure of a major component, system or train, including an individual reactor or turbine-generator.

(3700.0321.195)

PSCS features shall be included to limit recovery time to resumption of reactor power operation when a protection trip occurs consistent with meeting the plant availability goal.

(3700.0321.200)

Features shall be included in the PSCS to facilitate continual plant operation through the transients of OPDS Table 2.1-1 (except for shutdown) and at reduced electrical output upon loss of function of major plant components where more than one is employed.

(3700.0321.205)

3.2.1.3 Structural Requirements

The PSCS shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0321.210)

3.2.1.3.1 Seismic Tolerance Requirements

Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE.

(3700.0321.212)

Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.

(3700.0321.215)

OBE seismic response spectrum load level specifications for the PSCS shall be based on the plant seismic response spectra provided in the FY86 MHTGR plant seismic assessment.

(3700.0321.217)

3.2.1.4 Environmental Requirements

3.2.1.4.1 Environmental Qualification Requirements

Environmental qualification requirements pertaining to PSCS operation and structural design shall be based upon relevant plant site characteristics as specified in OPDS Table 2.1-2.

(3700.0321.220)

3.2.1.5 Instrumentation and Control Requirements

The PSCS shall provide the controls, monitors and instrumentation for automatically coordinating energy production and conversion, startups and shutdowns, coordinating with refueling operations and maintaining shutdown of the plant or portions thereof.

(3700.0321.250)

3.2.1.5.1 Instrumentation Requirements

3.2.1.5.1.1 Monitoring Requirements

Malfunctions within the PSCS shall be alarmed in the main control room.

(3700.0321.252)

PSCS alarm points to the control room shall be restricted to those critical parameters which can lead to to initiation of protective action for major plant components or the loss of electrical production.

(3700.0321.255)

Provisions shall be made to automatically detect and document the sequence of significant events (e.g., control inputs, changes in operation of major systems and components, protective trips, etc.) that occur during plant operation.

(3700.0321.260)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the PSCS.

(3700.0321.265)

Provisions shall be made for monitoring plant and PSCS status, configuration and performance as a basis for decision-making.

(3700.0321.270)

The PSCS shall provide the capability to sense, process and analyze those variables, states, modes, limits, conditions, etc., required for the plant processes and subsystems to be observable.

(3700.0321.275)

Portions and/or derivations of those PSCS observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the operators.

(3700.0321.280)

The control room operator workstation shall be human engineered to provide the capability for a single operator to concurrently observe plant energy production, shutdown, refueling and startup/ shutdown status.

(3700.0321.285)

3.2.1.5.1.2 Analytic Requirements

The PSCS shall provide the capability to assist that energy production, shutdown and startup/shutdown decision making responsibility allocated to the operators.

(3700.0321.290)

The PSCS shall be capable of evaluating and determining the state of the plant and the corresponding plant-level control state maneuvers required for concurrent energy production, shutdown, refueling and startup/shutdown control of different modules and T/Gs.

(3700.0321.295)

3.2.1.5.2 Control Requirements

3.2.1.5.2.1 Plant Loading Requirements

The PSCS shall coordinate plant operational responses for the load change duty cycle events specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3. For plant load maneuvers, these are

5. Rapid Load Increase (+5%/min.)
6. Normal Load Increase (+0.5%/min.)
7. Rapid Load Decrease (-5%/min.)
8. Normal Load Decrease (-0.5%/min.)
9. Step Load Increase (+15%)
10. Step Load Decrease (-15%)

(3700.0321.320)

The PSCS shall be designed for base load plant operation and be capable of accommodating the weekly load cycle of OPDS Figure 2.1-1 over its design life.

(3700.0321.325)

3.2.1.5.2.2 Load Change Requirements

3.2.1.5.2.2.1 Ramp Load Change Requirements

The PSCS shall coordinate changes in reactor and plant output under automatic control at a rate up to and including 5% of rated output per minute of those reactors on-line.

(3700.0321.335)

The PSCS shall coordinate reloading at 5% of rated load per minute following:

a) load rejection from full generator output to house electrical load without a reactor trip, and
b) turbine trip (except on low condenser vacuum) from any load level without a reactor trip,

without the necessity for a mandatory hold except for those associated with the turbine-generators.

(3700.0321.340)

3.2.1.5.2.2.2 Step Load Change Requirements

The PSCS shall coordinate sustained and controlled plant operation for step changes of ±15% in plant output caused by utility electrical transmission grid upsets.

(3700.0321.345)

3.2.1.5.2.3 Control Transfer Requirements

The control room operator workstation shall be designed to accept direction from the operators to transfer control of auxiliary processes to a mode of operation that can be supervised at locations outside the control room during energy production, shutdown, refueling and startups/shutdowns.

(3700.0321.350)

3.2.1.5.2.4 Subsystem Coordination Control Requirements

The PSCS shall provide the capability to automatically allocate demands for individual energy production (module) and energy conversion (T-G's) sources. These demands shall be the energy production and coversion equivalents of baseload and load following plant net electrical output load demands from the utility grid dispatcher.

(3700.0321.365)

Load demands shall be distributed, during normal plant energy production, among the energy production (modules) and the energy conversion (turbine-generators) sources in operation consistent with plant economic and availability requirements.

(3700.0321.370)

The PSCS shall provide the capability to automatically determine and allocate equivalent rates of change in energy production and conversion required for a rate of change in net plant electrical output anywhere from a minimum of [TBD] %/minute to a maximum of ±5%/minute.

(3700.0321.375)

The PSCS shall acknowledge process and other plant subsystem variables, states, modes, performance limits, conditions, etc., in the energy production, shutdown, refueling and startup/shutdown analysis and decision making process

(3700.0321.380)

The PSCS shall provide startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] %/minute to a maximum of [+TBD] %/minute.

(3700.0321.385)

The PSCS shall provide shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD] %/minute to a maximum of [-TBD] %/minute.

(3700.0321.390)

The PSCS shall provide the capability to automatically allocate startup/shutdown demands for individual energy production (module) and energy conversion (T-G's) sources. These demands shall be equivalent rates of change in energy production and energy conversion of 1%/minute for startup and shutdown, respectively.

(3700.0321.395)

3.2.1.5.3 Electrical Requirements

[LATER]

3.2.1.5.4 Data Communication Requirements

The control room operator workstation shall provide the capability to communicate digital control and monitoring signals using non-hardwired, signal transmission techniques.

(3700.0321.400)

The control room operator workstation shall provide the capability for a single operator to initiate the concurrent communication of control state maneuvering commands for energy production, shutdown, refueling and startup/shutdown.

(3700.0321.405)

3.2.1.5.5 Software Requirements

[LATER]

3.2.1.5.6 Information Presentation Requirements

The control room operator workstation shall provide the capability to concurrently and automatically report information required for observation and use in the control room.

(3700.0321.600)

3.2.1.6 Surveillance and In-Service Inspection Requirements

[Refer to requirements 3700.0321.265 and 3700.0321.655]

3.2.1.7 Availability Assurance Requirements

3.2.1.7.1 Availability Requirements

The Effective Forced Outage Hour (EFOH) values specified for the PSCS in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. The PSCS shall be designed to meet a planned outage allocation of [TBD] hours.

(3700.0321.610)

3.2.1.7.1.1 Operating Life Requirements

The PSCS shall be designed for a plant operating life of forty calendar years.

(3700.0321.615)

3.2.1.7.2 Reliability Requirements

The PSCS shall be designed to meet its reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The PSCS shall be designed to meet an overall reliability allocation of [TBD].

(3700.0321.620)

3.2.1.8 Maintenance Requirements

The PSCS shall be configured to enable maintenance of PSCS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant lifetime as defined in OPDS Table 5.1-4.

(3700.0321.630)

Special PSCS maintenance and installation tools not commercially available shall be provided by the PSCS equipment vendor.

(3700.0321.635)

PSCS components shall be designed to facilitate hands-on maintenance.

(3700.0321.640)

3.2.1.8.1 On-Line Maintenance Requirements

The PSCS shall be designed and arranged with equipment and components located in the plant to facilitate on-line maintenance.

(3700.0321.645)

The PSCS design shall accommodate removal of a reactor from service for maintenance and its return to service with the remaining reactors and the turbine plant in operation.

(3700.0321.650)

3.2.1.8.2 Testing Requirements

The PSCS shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.

(3700.0321.655)

3.2.1.8.3 Diagnostics Requirements

Provisions shall be made for monitoring PSCS status, configuration and performance as a basis for maintenance diagnostics.

(3700.0321.660)

3.2.1.9 Safety and Licensing Requirements

3.2.1.9.1 Safety Requirements

[The PSCS is a not "safety-related". Therefore, it has no nuclear safety-related requirements.]

3.2.1.9.2 Licensing Requirements

The PSCS shall be functionally independent from major component and equipment monitoring and protective features.

(3700.0321.665)

The PSCS shall be designed to meet applicable top-level regulatory criteria.

(3700.0321.670)

3.2.1.10 Codes and Standards Requirements

PSCS design, analysis, fabrication and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justifed in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, QA Program Requirements for Nuclear Facilities
DOE NE F2-10, QA Program Requirements (Supplement to ANSI/ASME NQA-1)

(3700.0321.680)

3.2.1.11 Quality Assurance Requirements

3.2.1.11.1 Quality Assurance and Control Program

Items that are not "safety-related" 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 DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5).

(3700.0321.760)

3.2.1.11.2 Materials

PSCS components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory.

(3700.0321.785)

3.2.1.12 Construction Requirements

Shop, factory, or field fabricated, assembled and erected components shall be utilized as appropriate to reduce costs and enhance quality control.

(3700.0321.795)

The PSCS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.

(3700.0321.800)

3.2.1.13 Decommissioning Requirements

The PSCS shall include features that accommodate decommissioning or refurbishment of one reactor while maintaining others in operation.

(3700.0321.805)

3.2.2 NSSS Control Subsystem (NSSSCS) Requirements

3.2.2.1 System Configuration and Essential Features Requirements

3.2.2.1.1 System Configuration Requirements

The NSSSCS design shall accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations:

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

(3700.0322.010)

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

(3700.0322.020)

The NSSSCS shall be deisgned for a Nuclear Island that includes four (4) standard reactor modules.

(3700.0322.025)

Human-machine interfaces and machine-machine communication interfaces shall be provided for the NSSSCS equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.

(3700.0322.030)

Features of the NSSSCS (e.g., inter-system communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of equipment and device interfaces.

(3700.0322.040)

The NSSSCS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating de-energizing electronics or affecting the operation of other electronic equipment.

(3700.0322.050)

3.2.2.1.2 Essential Features Requirements

Human engineering techniques shall be employed in the design of the NSSSCS to enhance operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD].

(3700.0322.060)

NSSSCS features shall be included to facilitate operation of reactor modules at different power levels.

(3700.0322.080)

Base the NSSSCS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.

(3700.0322.090)

The design of structures, systems and components (SSCs) within the Nuclear Island shall be standardized.

(3700.0322.092)

3.2.2.2 Operational Requirements

The NSSSCS shall provide the capability for roving operators to control, under supervision from the control room, selected processes and subsystems during energy production, shutdown, refueling and startups/shutdowns not requiring direct control room operator interfacing and interaction. Communications and status information shall be made available at the locations involved in the operations outside the control room.

(3700.0322.110)

3.2.2.2.1 Operational Staffing Requirements

[LATER]

3.2.2.2.2 Normal Operational Requirements

3.2.2.2.2.1 Operational Performance Requirements

The system shall be designed to control the helium mass flow through the active steam generator bundle between 25% and 100% of rated feedwater flow for steady-state operation as specified in OPDS Table 5.12-2.

(3700.0322.115)

The NSSSCS shall be designed to measure and control the performance of the NSSS parameters at any point between 25% and 100% rated feedwater flow for steady-state operation as specified in OPDS Table 5.12-1.

(3700.0322.117)

The NSSSCS shall be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in OPDS Figures 5.1-1 through 5.1-5, Tables 5.1-1 and 5.1-2, and in the Thermal Performance Requirements Report.

(3700.0322.120)

3.2.2.2.2.2 Energy Production Requirements

The NSSSCS shall include features to enable automatic control during plant operation.

(3700.0322.125)

3.2.2.2.2.3 Shutdown Requirements

The NSSSCS shall be designed to accommodate one or more reactor modules shutting down.

(3700.0321.139)

Reactor module shutdown shall range between 25% and 0% rated feedwater flow rate on a per reactor module basis.

(3700.0322.130)

The NSSSCS shall include features to enable automatic control during orderly shutdowns.

(3700.0322.138)

3.2.2.2.2.4 Refueling Requirements

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

(3700.0322.140)

3.2.2.2.2.5 Startup Requirements

The NSSSCS shall be designed to accommodate one or more reactor modules starting up.

(3700.0322.145)

The NSSSCS shall include features to enable automatic control during startups.

(3700.0322.148)

Reactor module startup shall range between 0% and 25% rated feedwater flow rate on a per reactor module basis.

(3700.0322.150)

3.2.2.2.2.6 Main Control Room Operational Requirements

[LATER]

3.2.2.2.3 Off-Normal Operational Requirements

The NSSSCS shall be designed to operate through the design transients specified in the MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0322.160)

The NSSSCS shall be designed to sustain continuous operation of available reactor modules under reduced plant electrical output through and following transients associated with the loss or failure of a major component, system or train, including an individual reactor.

(3700.0322.170)

NSSSCS features shall be included as required to limit recovery time to resumption of reactor power operation when a protection trip occurs consistent with meeting the plant availability goal.

(3700.0322.180)

Features shall be included in the NSSSCS to facilitate continual NSSS operation through the transients of OPDS Table 2.1-1 (except for shutdown) and at reduced electrical output upon loss of function of major subsystem components where more than one is employed.

(3700.0322.190)

3.2.2.3 Structural Requirements

The NSSSCS shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0322.195)

3.2.2.3.1 Seismic Tolerance Requirements

Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE.

(3700.0322.197)

Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.

(3700.0322.200)

OBE seismic response spectrum load level specifications for the NSSSCS shall be based on the plant seismic response spectra provided in the FY86 MHTGR plant seismic assessment.

(3700.0322.205)

3.2.2.4 Environmental Requirements

3.2.2.4.1 Environmental Qualification Requirements

Environmental qualification requirements pertaining to NSSSCS operation and structural design shall be based upon relevant plant site characteristics as specified in OPDS Table 2.1-2.

(3700.0322.207)

3.2.2.5 Instrumentation and Control Requirements

3.2.2.5.1 Instrumentation Requirements

3.2.2.5.1.1 Monitoring Requirements

Malfunctions within major plant control and electric systems shall be alarmed in the main control room.

(3700.0322.215)

NSSSCS alarm points to the control room shall be restricted to those critical parameters which can lead to initiation of protective action for major plant components or the loss of electrical production.

(3700.0322.220)

Provisions shall be made to automatically detect and document the sequence of significant NSSS events (e.g., control inputs, changes in operation of major systems and components, protective trips, etc.) that occur during plant operation.

(3700.0322.225)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the NSSSCS.

(3700.0322.230)

Provisions shall be made for monitoring NSSS status, configuration and performance as a basis for decision making.

(3700.0322.240)

The NSSSCS shall provide the capability to sense, process and analyze those variables, states, modes, limits, conditions, etc., required for the NSSS to be observable.

(3700.0322.250)

Portions and/or derivations of NSSS observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.

(3700.0322.260)

3.2.2.5.1.2 Analytic Requirements

The NSSSCS shall be capable of evaluating and determining the state of the NSSS and the corresponding module-level control state maneuvers required for energy production, shutdown, refueling and startup/shutdown control.

(3700.0322.270)

3.2.2.5.2 Control Requirements

The NSSS shall provide the capability to automatically regulate conditions (e.g., pressure, flow, temperature, etc.) of the steam produced and delivered by each module.

(3700.0322.280)

The NSSSCS shall provide the capability to control and regulate the conditions of the nuclear steam supply so as to deliver 2400 psig, 1000 degree F steam to the high pressure turbine admission valves.

(3700.0322.285)

The NSSSCS shall provide the capability to control those actuators and devices required to effect a change in state in the NSSS during energy production, shutdown, refueling and startup/shutdown.

(3700.0322.290)

3.2.2.5.2.1 Plant Loading Requirements

The NSSSCS shall be designed for base load operation and be capable of accommodating the weekly load cycle of OPDS Figure 2.1-1 over its design life.

(3700.0322.300)

Each individual reactor module shall be capable of continuous operation under automatic control between 25 and 100% of nominal module feedwater flow.

(3700.0322.310)

3.2.2.5.2.2 Load Change Requirements

3.2.2.5.2.2.1 Ramp Load Change Requirements

The NSSSCS shall be capable of changing reactor output under automatic control at a rate up to and including 5% of rated output per minute.

(3700.0322.320)

The NSSSCS design shall permit for reloading at 5% of rated load per minute following:

a) load rejection from full generator output to house electrical load without a reactor trip, and
b) turbine trip (except on low condenser vacuum) from any load level without a reactor trip, without the necessity for a mandatory hold

except for those associated with the turbine-generators.

(3700.0322.330)

3.2.2.5.2.2.2 Step Load Change Requirements

The NSSSCS design shall provide sustained and controlled operation for step changes of ±15% in plant output caused by utility electrical transmission grid upsets.

(3700.0322.340)

3.2.2.5.2.2.3 Control Transfer Requirements

[LATER]

3.2.2.5.2.4 Subsystem Coordination Control Requirements

The NSSSCS shall be designed to accept directions corresponding to energy production load demand changes at rates anywhere from a minimum of [TBD % per minute] to a maximum of 5% per minute.

(3700.0322.350)

The NSSSCS shall be capable of accepting plant energy production, shutdown, refueling and startup/shutdown instructions from the control room operators and operator workstation.

(3700.0322.360)

The NSSSCS shall acknowledge process and other subsystem variables, states, modes, performance limits, conditions, etc., in the energy production, shutdown, refueling and startup/shutdown analysis and decision making process.

(3700.0322.370)

The NSSSCS shall be designed to accept startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] %/minute to a maximum of [+TBD] %/minute.

(3700.0322.380)

The NSSSCS shall be designed to accept shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD % per minute] to a maximum of [-TBD % per minute].

(3700.0322.390)

3.2.2.5.3 Electrical Requirements

[LATER]

3.2.2.5.4 Data Communication Requirements

The NSSSCS shall provide the capability to communicate digital control and monitoring signals using non-hardwired, signal transmission techniques.

(3700.0322.400)

3.2.2.5.5 Software Requirements

[LATER]

3.2.2.5.6 Information Presentation Requirements

[LATER]

3.2.2.6 Surveillance and In-Service Inspection Requirements

[Refer to requirements 3700.0322.230 and 3700.0322.470]

3.2.2.7 Availability Assurance Requirements

3.2.2.7.1 Availability Requirements

The Effective Forced Outage Hour (EFOH) values specified for the NSSSCS in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. The NSSSCS shall be designed to meet a planned outage allocation of [TBD] hours.

(3700.0322.410)

3.2.2.7.1.1 Operating Life Requirements

The NSSSCS shall be designed for a plant operating life of forty calendar years.

(3700.0322.420)

3.2.2.7.2 Reliability Requirements

The NSSSCS shall be designed to meet its reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The NSSSCS shall be designed to meet an overall reliability allocation of [TBD].

(3700.0322.430)

3.2.2.8 Maintenance Requirements

NSSSCS components shall be designed to facilitate hands-on maintenance.

(3700.0322.440)

The NSSSCS shall be configured to enable maintenance of NSSSCS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant lifetime as defined in OPDS Table 5.1-4.

(3700.0322.445)

Special NSSSCS maintenance and installation tools not commercially available shall be provided by the NSSSCS equipment vendor.

(3700.0322.447)

3.2.2.8.1 On-Line Maintenance Requirements

The NSSSCS shall be designed and arranged, and equipment and components located in the plant, to facilitate on-line maintenance.

(3700.0322.450)

The NSSSCS shall make provisions for removing a reactor from service, performing maintenance and returning it to service with the remaining reactors and the turbine plant in operation.

(3700.0322.460)

3.2.2.8.2 Testing Requirements

The NSSSCS shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.

(3700.0322.470)

3.2.2.8.3 Diagnostics Requirements

Provisions shall be made for monitoring NSSS status, configuration and performance as a basis for maintenance diagnostics.

(3700.0322.480)

3.2.2.9 Safety and Licensing Requirements

3.2.2.9.1 Safety Requirements

[The NSSSCS is not "safety-related". Therefore, it has no nuclear safety-related requirements.]

3.2.2.9.2 Licensing Requirements

The NSSSCS shall be functionally independent from major component and equipment monitoring and protective features.

(3700.0322.490)

The NSSSCS shall be designed to meet applicable top-level regulatory criteria.

(3700.0322.500)

3.2.2.10 Codes and Standards Requirements

NSSSCS design, analysis, fabrication and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justifed in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, QA Program Requirements for Nuclear Facilities
DOE NE F2-10, QA Program Requirements (Supplement to ANSI/ASME NQA-1)

(3700.0322.510)

3.2.2.11 Quality Assurance Requirements

3.2.2.11.1 Quality Assurance and Control Program

Items that are not "safety-related" 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 DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5).

(3700.0322.520)

3.2.2.11.2 Materials

NSSSCS components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory.

(3700.0322.530)

3.2.2.12 Construction Requirements

Shop, factory, or field fabricated, assembled and erected components and subsystems shall be utilized as appropriate to reduce costs and enhance quality control.

(3700.0322.540)

The NSSSCS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.

(3700.0322.550)

3.2.2.13 Decommissioning Requirements

The NSSSCS shall include features that accommodate decommissioning or refurbishment of one reactor while maintaining others in operation.

(3700.0322.560)

3.2.3 Data Management Subsystem (DMS) Requirements

3.2.3.1 System Configuration and Essential Features Requirements

3.2.3.1.1 System Configuration Requirements

The DMS shall accommodate changes in data communication network loading associated with the performance and transient characteristics of the following reactor/turbine-generator combinations:

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

(3700.0323.020)

Human-machine interfaces and machine-machine communication interfaces shall be provided for DMS equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.

(3700.0323.045)

The DMS configuration shall provide the capability to interface subsystem equipment distributed throughout the plant. Features of the DMS (e.g., intersystem communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.

(3700.0323.050)

The DMS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating deenergizing electronics or affecting the operation of other electronic equipment.

(3700.0323.055)

3.2.3.1.2 Essential Features Requirements

Human engineering techniques shall be employed in the DMS design to enhance operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD].

(3700.0323.060)

Base the DMS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.

(3700.0323.072)

3.2.3.2 Operational Requirements

3.2.3.2.1 Operational Staffing Requirements

[LATER]

3.2.3.2.2 Normal Operational Requirements

3.2.3.2.2.1 Operational Performance Requirements

[LATER]

3.2.3.2.2.2 Energy Production Requirements

The DMS shall include data communication features to enable automatic control during plant operation.

(3700.0323.138)

3.2.3.2.2.3 Shutdown Requirements

The DMS shall include data communication features to enable automatic control during orderly shutdowns.

(3700.0323.148)

3.2.3.2.2.4 Refueling Requirements

None.

3.2.3.2.2.5 Startup Requirements

The DMS shall be designed to accommodate the signal transmission and data communication required when one or more reactor modules are started up.

(3700.0323.164)

The DMS shall include data communication features to enable automatic control during startups.

(3700.0323.168)

3.2.3.2.3 Off-Normal Operational Requirements

The DMS shall sustain operation through design transients specified in the MHTGR Plant Design Basis Transient Analysis Report.

(3700.0323.190)

The DMS shall sustain continuous operation through and following plant transients associated with the loss or failure of a major component, system or train, including an individual reactor or turbine-generator.

(3700.0323.195)

Features shall be included in the DMS to facilitate continual plant operation through the transients of OPDS Table 2.1-1 (except for shutdown) and at reduced electrical output upon loss of function of major plant components where more than one is employed.

(3700.0323.205)

3.2.3.3 Structural Requirements

The DMS shall be designed to withstand the mechanical and thermal loads resulting from the design transients specified in MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.

(3700.0102.210)

3.2.3.3.1 Seismic Tolerance Requirements

Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE.

(3700.0102.212)

Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.

(3700.0323.215)

OBE seismic response spectrum load level specifications for the DMS shall be based on the plant seismic response spectra provided in the FY86 MHTGR plant seismic assessment.

(3700.0323.217)

3.2.3.4 Environmental Requirements

3.2.3.4.1 Environmental Qualification Requirements

Environmental qualification requirements pertaining to DMS operation and structural design shall be based upon relevant plant site characteristics as specified in OPDS Table 2.1-2.

(3700.0323.220)

3.2.3.5 Instrumentation and Control Requirements

3.2.3.5.1 Instrumentation Requirements

[LATER]

3.2.3.5.1.1 Monitoring Requirements

Malfunctions within the DMS shall be alarmed in the main control room.

(3700.0321.252)

DMS alarm points to the control room shall be restricted to those critical parameters which can lead to to initiation of protective action for major plant components or the loss of electrical production.

(3700.0323.255)

Provisions shall be made in the DMS to automatically detect and document the sequence of significant events (e.g., control inputs, changes in operation of major systems and components, protective trips, etc.) that occur during plant operation.

(3700.0323.260)

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the DMS.

(3700.0323.265)

Provisions shall be made for monitoring the DMS status, configuration and performance as a basis for decision-making.

(3700.0323.270)

The DMS shall provide the capability to communicate those variables, states, modes, limits, conditions, etc., required for the processes and subsystems to be observed.

(3700.0323.275)

Portions and/or derivations of those DMS observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.

(3700.0323.280)

3.2.3.5.1.2 Analytic Requirements

The DMS shall be capable of communicating the state of the plant and the corresponding plant-level control state maneuvers required for concurrent energy production, shutdown, refueling and startup/shutdown control of different modules and turbine-generators.

(3700.0323.295)

3.2.3.5.2 Control Requirements

None.

3.2.3.5.3 Electrical Requirements

[LATER]

3.2.3.5.4 Data Communication Requirements

The DMS shall provide the capability to communicate digital control and monitoring signals between plant subsystems and the control room operator workstation using non-hardwired, signal transmission techniques.

(3700.0323.400)

The DMS shall provide the capability to concurrently communicate control state maneuvering commands for energy production, shutdown, refueling and startup/shutdown.

(3700.0323.405)

3.2.3.5.5 Software Requirements

[LATER]

3.2.3.5.6 Information Presentation Requirements

[LATER]

3.2.3.6 Surveillance and In-Service Inspection Requirements

[Refer to requirements 3700.0323.265 and 3700.0323.655]

3.2.3.7 Availability Assurance Requirements

3.2.3.7.1 Availability Requirements

The Effective Forced Outage Hour (EFOH) values specified for the DMS in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. The DMS shall be designed to meet a planned outage allocation of [TBD] hours.

(3700.0323.610)

3.2.3.7.1.1 Operating Life Requirements

The DMS shall be designed for a plant operating life of forty calendar years.

(3700.0323.615)

3.2.3.7.2 Reliability Requirements

The DMS shall be designed to meet its reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The DMS shall be designed to meet an overall reliability allocation of [TBD].

(3700.0323.620)

3.2.3.8 Maintenance Requirements

The DMS shall be configured to enable maintenance of DMS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant lifetime as defined in OPDS Table 5.1-4.

(3700.0323.630)

Special DMS maintenance and installation tools not commercially available shall be provided by the DMS equipment vendor.

(3700.0323.635)

The DMS shall be designed to facilitate hands-on maintenance.

(3700.0323.640)

3.2.3.8.1 On-Line Maintenance Requirements

The DMS shall be designed and arranged with equipment and components located in the plant to facilitate on-line maintenance.

(3700.0323.645)

3.2.3.8.2 Testing Requirements

The DMS shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.

(3700.0323.655)

3.2.3.8.3 Diagnostics Requirements

Provisions shall be made for monitoring DMS status, configuration and performance as a basis for maintenance diagnostics.

(3700.0323.660)

3.2.3.9 Safety and Licensing Requirements

3.2.3.9.1 Safety Requirements

[The DMS is not "safety-related". Therefore, it has no nuclear safety-related requirements.]

3.2.3.9.2 Licensing Requirements

The DMS shall be functionally independent from major component and equipment monitoring and protective features.

(3700.0323.665)

DMS components shall be designed to meet applicable top-level regulatory criteria.

(3700.0323.670)

3.2.3.10 Codes and Standards Requirements

DMS design, analysis, fabrication and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justifed in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, QA Program Requirements for Nuclear Facilities
DOE NE F2-10, QA Program Requirements (Supplement to ANSI/ASME NQA-1)

(3700.0323.680)

3.2.3.11 Quality Assurance Requirements

3.2.3.11.1 Quality Assurance and Control Program

Items that are not "safety-related" 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 DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5).

(3700.0323.760)

3.2.3.11.2 Materials

DMS components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory.

(3700.0323.785)

3.2.3.12 Construction Requirements

Shop, factory, or field fabricated, assembled and erected components shall be utilized as appropriate to reduce costs and enhance quality control.

(3700.0323.795)

The DMS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.

(3700.0323.800)

3.2.3.13 Decommissioning Requirements

DMS features shall accommodate decommissioning or refurbishment of one reactor while others remain in operation.

(3700.0323.805)

3.2.4 Technical Operations Support Subsystem (TOSS) Requirements

3.2.4.1 System Configuration and Essential Features Requirements

3.2.4.1.1 System Configuration Requirements

TOSS components whose failure would not have an immediate impact on plant output shall be located outside the control room with status indication provided to the control room.

(3700.0324.040)

Human-machine interfaces and machine-machine communication interfaces shall be provided for the TOSS equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.

(3700.0324.045)

Features of the TOSS (e.g., intersystem communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.

(3700.0324.050)

The TOSS design shall permit the addition of new control and data communication interfaces, including signal input/output field wiring, without necessitating de-energizing electronics or affecting the operation of other electronic equipment.

(3700.0324.055)

3.2.4.1.2 Essential Features Requirements

Human engineering techniques shall be employed in the TOSS design to enhance operator response and reduce the probability of human error as specified in the Human Factors Engineering Plan [TBD].

(3700.0324.060)

Base the TOSS design on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.

(3700.0324.072)

3.2.4.2 Operational Requirements

[LATER]

3.2.4.2.1 Operational Staffing Requirements

[LATER]

3.2.4.2.2 Normal Operational Requirements

[LATER]

3.2.4.2.2.1 Operational Performance Requirements

[LATER]

3.2.4.2.2.2 Energy Production Requirements

None.

3.2.4.2.2.3 Shutdown Requirements

None.

3.2.4.2.2.4 Refueling Requirements

The TOSS shall provide technical support services for refueling with the remaining reactors and the turbine plant in operation.

(3700.0324.155)

3.2.4.2.2.5 Startup Requirements

The TOSS shall provide the technical support services required when one or more reactor modules are started up.

(3700.0324.164)

3.2.4.2.2.6 Main Control Room Operational Requirements

[LATER]

3.2.4.3 Structural Requirements

3.2.4.3.1 Seismic Tolerance Requirements

Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE.

(3700.0324.212)

Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.

(3700.0324.215)

OBE seismic response spectrum load level specifications for the TOSS shall be based on the plant seismic response spectra provided in the FY86 MHTGR plant seismic assessment.

(3700.0324.217)

3.2.4.4 Environmental Requirements

3.2.4.4.1 Environmental Qualification Requirements

Environmental qualification requirements pertaining to TOSS operation and structural design shall be based upon relevant plant site characteristics as specified in OPDS Table 2.1-2.

(3700.0324.220)

3.2.4.5 Instrumentation and Control Requirements

3.2.4.5.1 Instrumentation Requirements

3.2.4.5.1.1 Monitoring Requirements

Internal diagnostic monitoring to detect malfunctions shall be incorporated within the TOSS.

(3700.0324.265)

Provisions shall be made for monitoring TOSS status, configuration and performance as a basis for decision making.

(3700.0324.270)

The TOSS shall provide technical support services for processing and analyzing variables, states, modes, limits, conditions, etc., required for the plant processes and subsystems to be observable.

(3700.0324.275)

Portions and/or derivations of those TOSS observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.

(3700.0324.280)

3.2.4.5.1.2 Analytic Requirements

[LATER]

3.2.4.5.2 Control Requirements

None.

3.2.4.5.3 Electrical Requirements

[LATER]

3.2.4.5.4 Data Communication Requirements

TOSS equipment outside the control room shall be capable of communicating with equipment in the control room.

(3700.0324.360)

3.2.4.5.5 Software Requirements

[LATER]

3.2.4.5.6 Information Presentation Requirements

The TOSS shall provide the capability and the associated user workstations to report plant technical information.

(3700.0324.600)

3.2.4.6 Surveillance and In-Service Inspection Requirements

[Refer to requirements 3700.0324.265 and 3700.0324.655]

3.2.4.7 Availability Assurance Requirements

3.2.4.7.1 Availability Requirements

The Effective Forced Outage Hour (EFOH) values specified for the TOSS in Reliability Allocations for the Standard MHTGR shall not be exceeded when using a model employing equipment mean time to failure and mean time to repair data for like type or similar systems and/or components. The TOSS shall be designed to meet a planned outage allocation of [TBD] hours.

(3700.0324.610)

3.2.4.7.1.1 Operating Life Requirements

The TOSS shall be designed for a plant operating life of forty calendar years.

(3700.0324.615)

3.2.4.7.2 Reliability Requirements

The TOSS shall be designed to meet its reliability requirements specified in Reliability Allocations for the Standard MHTGR and the Investment Protection Performance Requirements for the Standard MHTGR. The TOSS shall be designed to meet an overall reliability allocation of [TBD].

(3700.0324.620)

3.2.4.8 Maintenance Requirements

The TOSS shall be configured to enable maintenance of TOSS equipment within a plant total scheduled outage time of less than 876 hours per year averaged over the plant lifetime as defined in OPDS Table 5.1-4.

(3700.0324.630)

Special TOSS maintenance and installation tools not commercially available shall be provided by the TOSS equipment vendor.

(3700.0324.635)

TOSS components shall be designed to facilitate hands-on maintenance.

(3700.0324.640)

3.2.4.8.1 On-Line Maintenance Requirements

The TOSS shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance.

(3700.0324.645)

3.2.4.8.2 Testing Requirements

The TOSS shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.

(3700.0324.655)

3.2.4.8.3 Diagnostics Requirements

Provisions shall be made for monitoring TOSS status, configuration and performance as a basis for maintenance diagnostics.

(3700.0324.660)

3.2.4.9 Safety and Licensing Requirements

3.2.4.9.1 Safety Requirements

[The TOSS is not "safety-related". Therefore, it has no nuclear safety-related requirements.]

3.2.4.9.2 Licensing Requirements

The TOSS shall be functionally independent from major component and equipment monitoring and protective features.

(3700.0324.665)

The TOSS components shall be designed to meet applicable top-level regulatory criteria.

(3700.0324.670)

3.2.4.10 Codes and Standards Requirements

TOSS design, analysis, fabrication and construction shall comply with applicable codes and standards that are needed to meet the four goals of the Integrated Approach. All such applicable codes and standards shall be identified and documented in system design descriptions and other appropriate documentation during the design effort. Applicable state and local government regulations, codes and standards shall be identified and documented subsequent to the time a specific site is identified. Use of all codes and standards shall be justifed in appropriate lower level design documents. The specific codes and standards that have been selected to date as being applicable to the overall plant are as follows:

ANSI/ASME NQA-1, QA Program Requirements for Nuclear Facilities
DOE NE F2-10, QA Program Requirements (Supplement to ANSI/ASME NQA-1)

(3700.0324.680)

3.2.4.11 Quality Assurance Requirements

3.2.4.11.1 Quality Assurance and Control Program

Items that are not "safety-related" 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 DOE NE F2-10 regarding Management Assessment (NE 02-4.3.0), Engineering Holds (NE 03-1.3.2), Design Reviews (NE 03-1.3.4), and Engineering Drawings Lists (NE 03-1.3.5).

(3700.0324.760)

3.2.4.11.2 Materials

TOSS components shall be classified to reduce the number of different types, sizes, and temperature and pressure ratings in order to reduce the cost of spare parts inventory.

(3700.0324.785)

3.2.4.12 Construction Requirements

Shop, factory, or field fabricated, assembled and erected components shall be utilized as appropriate to reduce costs and enhance quality control.

(3700.0324.795)

The TOSS design shall be based upon parallel construction of the complete plant; features shall be included that facilitate construction and startup in increments of two standard reactor modules and one turbine.

(3700.0324.800)

3.2.4.13 Decommissioning Requirements

TOSS technical support services shall accommodate decommissioning or refurbishment of one reactor while others remain in operation.

(3700.0324.805)

SECTION 4

SYSTEM AND SUBSYSTEM INTERFACES

4.1 Interface Requirements Imposed on Other Systems

The PCDIS imposes interface requirements on other plant systems in order to meet its requirements listed in Section 1 of this document. These interface requirements are listed in Table 4.1-1. More detailed, quantitative descriptions of each interface requirement are documented at the subsystem level which contains references to Interface Control Documents (ICDs).

There is a subset of interface requirements in addition to those in Table 4.1-1. These requirements are imposed on the ECA controls by the PCDIS. These requirements have been derived through analysis of Section 1 requirements. This subset of requirements has been purposely segregated from Table 4.1-1 because it belongs to a larger set of requirements associated with the design of fully integrated controls for the plant. Table 4.1-2 contains the subset of requirements imposed on the ECA controls.

4.2 Subsystem Boundary Definition

The physical boundaries of the PCDIS subsystems are inherently defined by the equipment within each subsystem. The equipment within each subsystem is listed in Appendix G of the respective SSDD. The functional role of each equipment item is also described in the SSDD.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
REACTOR SERVICE GROUP			
HFD-42001	Hot Service Facility System		None.
HFD-42002	Decontamination Services System		None.
HFD-42016	Reactor Service Equipment System		None.
HFD-42023	Helium Purification System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-42024 Helium Storage & Transfer System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-42025 Liquid Nitrogen System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-42047	Reactor Plant Cooling Water System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-42062	Liquid Radioactive Waste Management System		None.
HFD-42064	Gaseous Radioactive Waste Management System		None.
HFD-42065	Solid Radioactive Waste Management System		None.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
MISCELLANEOUS CONTROL AND INSTRUMENTATION GROUP			
HFD-43001	NSSS Analytical Instrumentation System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-43003	Radiation Monitoring System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-43004	Seismic Monitoring System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-43005 Meteorological Monitoring System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-43006 Fire Detection and Alarm System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
POWER CONVERSION GROUP			
HFD-45001 Turbine Generator & Auxiliaries System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45002 Feedwater and Condensate System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45004 Main & Bypass Steam System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45005 Extraction and Auxiliary Steam System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45006 Heater Drains and Condensate Returns System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45007 Condensate Polishing System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45008 Steam Vents and Drains System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS		NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45009	Turbine Plant Sampling System			
		Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
		Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45010	Chemical Feed System			None.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45011 Turbine Building Closed Cooling Water System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45012 Startup and Shutdown System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45013 Steam and Water Dump System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HEAT REJECTION GROUP			
HFD-45241 Circulating Water System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-45242 Circulating Water Makeup and Blowdown System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-45244 Service Water System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-35600 Reactor Cavity Cooling System			None.
BUILDINGS, STRUCTURES AND BUILDING SERVICE GROUP			
HFD-47001 Reactor Building			
	Provide space and structural support for PCDIS equipment	Controller cabinets, data highway cabling, etc.	Layout and dimensions for the equipment in Appendix G as specified by applicable drawings listed in Appendix B
HFD-47002 Reactor Service Building			
	Provide space and structural support for PCDIS equipment	Controller cabinets, data highway cabling, etc.	Layout and dimensions for the equipment in Appendix G as specified by applicable drawings listed in Appendix B
HFD-47003 Reactor Auxiliary Building			
	Provide space and structural support for PCDIS equipment	Controller cabinets, data highway cabling, etc.	Layout and dimensions for the equipment in Appendix G as specified by applicable drawings listed in Appendix B

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS		NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-47004	Operations Center			
		Provide space and structural support for PCDIS equipment	Operator workstations, Controller cabinets, data highway cabling, etc.	Layout and dimensions for the equipment in Appendix G as specified by applicable drawings listed in Appendix B
HFD-47005	Standby Power Building			None.
HFD-47006	Radioactive Waste Management Building			None.
HFD-47009	Personnel Service Building			None.
HFD-47010	Turbine Building			
		Provide space and structural support for PCDIS equipment	Controller cabinets, data highway cabling, etc.	Layout and dimensions for the equipment in Appendix G as specified by applicable drawings listed in Appendix B
HFD-47011	Fire Pump House			None.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-47012	Warehouse Buildings		None.
HFD-47013	Helium Storage Structure		None.
HFD-47014	Intake Pumphouse and Discharge Structure		None.
HFD-47016	Maintenance Building		None.
HFD-47018	Cooling Tower Basin and Circulating Water Pump Intake (Structure)		None.
HFD-47020	Makeup Water Treatment & Auxiliary Boiler Building		None.
PLANT SERVICE GROUP			
HFD-49001	Potable Water System		None.
HFD-49002	Storm Drainage System		None.
HFD-49003	Sanitary Drainage & Treatment System		None.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49004 Plant Fire Protection System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-49005 Waste Water Treatment System			None.
HFD-49006 Auxiliary Boiler System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS		NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49007	Raw Water Treatment System			
		Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-49008	Instrument & Service Air System			None.
HFD-49009	Central Hot Water Heating System			None.
HFD-49010	Plant Drains System			None.
HFD-49011	ECA HVAC System			
		Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
		Meet PCDIS equipment environment control requirements	N/A because the nature of this interface is functional	Heat loads, humidity and temperature control requirements as specified in the SSDDs

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49012 Demineralized Water Makeup System			None.
HFD-49013 NI HVAC System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Meet PCDIS equipment environment control requirements	N/A because the nature of this interface is functional	Heat loads, humidity and temperature control requirements as specified in the SSDDs
HFD-49014 Station Chilled Water System			None.

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
ELECTRICAL GROUP			
HFD-49201	Offsite and Main Generator Transmission System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-49202	AC Power Distribution System		
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Provide electrical power for PCDIS equipment	Controller cabinets, operator workstations, computers, peripherals, etc.	Power specifications defined in SSDDs

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49204 Uninterruptible Power Supply System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Provide electrical power for PCDIS equipment	Controller cabinets, operator workstations, computers, peripherals, etc.	Power specifications defined in SSDDs
HFD-49205 Essential Uninterruptible Power Supply System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-49206 Standby Power Generator System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49207 DC Power Distribution System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Provide electrical power for PCDIS equipment	Controller cabinets, operator workstations, computers, peripherals, etc.	Power specifications defined in SSDDs
HFD-49208 Essential DC Power System			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-49209 Communications System			
	Provide access to, and the equipment for, audio communication between PCDIS equipment locations and the the remainder of the plant, as required.	Operator and technical support workstations	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-49210 Lighting and Service Power System			
	Provide lighting for operations and maintenance activities at PCDIS equipment locations	N/A because the nature of this interface is functional	[Refer to PCDIS SSDDs]
HFD-49211 Plant Security System			None.
HFD-49212 Grounding, Lightning Protection, Heat Tracing and Cathodic Protection System			
	Provide grounding and electrical transient protection for PCDIS equipment	Operator workstations, controller cabinets, computers, peripherals, etc.	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS		NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-31000	REACTOR SYSTEM			
HFD-41012	Neutron Control Subsystem			
HFD-41017	Reactor Internals Subsystem			
HFD-41018	Reactor Core Subsystem			
		Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
		Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-31100	VESSEL SYSTEM			
HFD-41105	Pressure Relief Subsystem			
HFD-41106	Vessel & Ducts Subsystem			
HFD-41107	Vessel Support Subsystem			
		Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-32100 HEAT TRANSPORT SYSTEM HFD-42101 Main Circulator Subsystem HFD-42102 Steam Generator Subsystem			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
HFD-33200 PLANT PROTECTION AND INSTRUMENTATION SYSTEM HFD-43201 Investment Protection Subsystem HFD-43202 Safety Protection Subsystem HFD-43203 Special Nuclear Area Instrumentation Subsystem			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-33400 FUEL HANDLING AND STORAGE SYSTEM HFD-43413 Core Refueling Subsystem HFD-43414 Site Fuel Handling Subsystem HFD-43487 Spent Fuel Cooling Subsystem			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

TABLE 4.1-1

IDENTIFICATION OF INTERFACES FOR THE PCDIS

INTERFACING SYSTEMS	NATURE OF THE INTERFACE	INTERFACING COMPONENT	INTERFACE REQUIREMENT
HFD-35700 SHUTDOWN COOLING SYSTEM			
HFD-45701 Shutdown Cooling Circulator Subsystem			
HFD-45702 Shutdown Cooling Heat Exchanger Subsystem			
HFD-45703 Shutdown Cooling Heat Removal Control Subsystem			
HFD-45704 Shutdown Cooling Water Subsystem			
	Provide signals compatible with PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]
	Accept output signals from PCDIS data acquisition or serial communications interfaces	Signal termination/connector at PCDIS equipment cabinet or a serial communications cable terminated at the interfacing system equipment	[Refer to PCDIS SSDDs]

Table 4.1-2

INTERFACE REQUIREMENTS IMPOSED ON THE ECA CONTROLS

REQUIREMENT	TRACEABILITY NUMBER
Human-machine interfaces and machine-machine communication interfaces shall be provided for ECAC equipment outside the control room requiring human interaction during energy production, shutdown, refueling and startup/shutdown.	3700.0102.045
Features of the ECAC (e.g., inter-system communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.	3700.0102.050
The ECAC design shall permit the addition of new controland data communication interfaces, including signal input/output field wiring, without necessitating deenergizing electronics or affecting the operation of other electronic equipment.	3700.0102.055
The ECAC shall provide the capability for roving operators to control, under supervision from the control room, selected processes and control subsystems during energy production, shutdown, refueling and startups/shutdowns not requiring direct control room operator interfacing and interaction. Communications and status information shall be made available at the locations involved in the operations outside the control room.	3700.0102.095
ECAC equipment shall conform to the RFI protection rules as specified in the Federal Communications Commission (FCC) Rules, Part 14, Subpart J, Class B, Digital Equipment Radio Interference.	3700.0102.248
The ECAC shall provide the controls and instrumentation for automatically controlling energy conversion, ECA startups and shutdowns, and maintaining shutdown of the ECA or portions thereof.	3700.0102.250

Table 4.1-2

INTERFACE REQUIREMENTS IMPOSED ON THE ECA CONTROLS

REQUIREMENT	TRACEABILITY NUMBER
The ECAC shall provide the capability to sense, process and analyze those variables, states, modes, limits, conditions, etc., required for the ECA processes and subsystems to be observable.	3700.0102.275
Portions and/or derivations of those ECA observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.	3700.0102.280
The ECAC shall be capable of evaluating and determining the state of the ECA and the corresponding ECA-level control state maneuvers required for energy conversion, shutdown, and startup/shutdown control of an individual T/G and its associated feedwater train.	3700.0102.300
The ECAC shall provide the capability to automatically regulate the main steam admitted to the turbines and the feedwater supplied to the main feedwater header.	3700.0102.310
The ECAC shall provide the capability to control those actuators and devices required to effect a change in state in the energy conversion processes.	3700.0102.315
ECAC shall be designed to accept directions corresponding to energy conversion load demand changes at rates anywhere from a minimum of [TBD] %/minute to a maximum of ±5%/minute.	3700.0102.355
The ECAC located outside the control room shall be capable of accepting plant energy conversion, shutdown, and startup/shutdown instructions from the control room operators and operator workstation.	3700.0102.360
The ECAC shall acknowledge process and other plant subsystem variables, states, modes, performance limits, conditions, etc., in the energy conversion, shutdown, and startup/shutdown analysis and decision making process.	3700.0102.380

Table 4.1-2

INTERFACE REQUIREMENTS IMPOSED ON THE ECA CONTROLS

REQUIREMENT	TRACEABILITY NUMBER
ECAC shall be designed to accept startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] %/minute to a maximum of [-TBD] %/minute.	3700.0102.385
ECAC shall be designed to accept shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD] %/minute to a maximum of [-TBD] %/minute.	3700.0102.390
ECAC shall provide the capability to communicate digital control and monitoring signals using non-hardwired, signal transmission techniques.	3700.0102.400
ECAC shall provide self-test capabilities (i.e., monitoring, checking and diagnosing) for key functional components.	3700.0102.655

SECTION 5

SYSTEM CONSTRUCTION

5.1 Packaging and Shipping

[LATER]

5.2 Handling at Delivery

[LATER]

5.3 Receiving Inspection

[LATER]

5.4 Storage

[LATER]

5.5 Access

[LATER]

5.6 Installation and/or Field Fabrication

[LATER]

5.7 Construction Testing

[LATER]

5.8 As-Built Drawings

[LATER]

SECTION 6

SYSTEM OPERATION

6.0 System Operation

This section describes the operational aspects of the PCDIS with respect to the plant processes it controls and the role of the operations personnel and their interactions with the system. The scope of this section includes the following:

a) process control variable limits and setpoints
b) system functional limitations and operating precautions
c) preoperational (system readiness) functions and associated operator tasks
d) the functional role of the system to effect energy production and energy conversion startups and shutdowns and support refueling operations
e) the functional role of operations personnel in order for the PCDIS to complete execution of its functions
f) casualty events (not necessarily caused by the PCDIS) that can affect PCDIS operation
g) PCDIS design features and methods of recovery to mitigate consequences of casualty events and restore the PCDIS and its controlled processes to acceptable conditions.

6.1 System Limitations, Setpoints and Precautions

6.1.1 System Limitations and Setpoints

The controller portions of the PCDIS regulate the properties of the energy production and energy conversion processes according to setpoints associated with some (but not all) of the properties. These properties (e.g., main steam temperature and pressure, feedwater mass flow, etc.) are "control variables" with respect to the controllers. There is a prescribed range in control variable magnitude for a particular process operating mode associated with each control variable. The ranges are defined on the basis of component operating requirements and requirements associated with the thermodynamic characteristics of the energy production and energy conversion processes. PCDIS controllers regulate the control variables within specific tolerances of their setpoints. A setpoint is typically the median of the control variable range for the respective process operating mode.

Tables 6-1 through 6-4 provide consolidated lists of PCDIS subsystem control variables, control variable limits (range of magnitude) and control variable setpoints for steady state and startup operations, normal transitions during energy production (e.g., ramp load increase) and transient conditions.

6.2 Preoperational Checkout

[LATER]

6.3 Startup/Shutdown

6.3.1 Normal Operation During Startup/Shutdown (Goal 1, State 4)

6.3.1.1 PSCS Normal Operations During Startup/Shutdown

[LATER]

6.3.1.2 NSSSCS Normal Operations During Startup/Shutdown

[LATER - Refer to NSSSCS SSDD]

6.3.1.3 DMS Normal Operations During Startup/Shutdown

[LATER]

6.3.1.4 TOSS Normal Operations During Startup/Shutdown

[LATER]

6.4 Normal Operation

6.4.1 Normal Operation During Energy Production (Goal 1, State 1)

6.4.1.1 PSCS Normal Operations During Energy Production

During normal plant operations, the role of the assistant operator at the CRAW is to monitor startup, shutdown and refueling activities and auxiliary systems whose operations are not a direct function of the main energy production and energy conversion process. The operator at the CROW tends to the controls and monitors for the main energy production and energy conversion processes.

The PCDIS automatic control subsystems, particularly the PSCS, perform operational procedures that reduce the scope and number of manual operator tasks and assists operators in the performance of their tasks. Although the plant is expected to be in the energy production state most of the time, similar automatic functions are also performed in normal and off-normal shutdown, refueling and startup/shutdown states. These machine-allocated functions aid the operators (and maintainers) in their roles as supervisors during semi-automatic plant control and as verifiers/validators during full automatic plant control.

Most of the plant operating procedures are automated. Recalling predefined procedures or prompting/queueing to the operator is performed via menu-oriented instructions and associated video displays. It is not necessary for the operator at the CROW to use operating procedure manuals (documents); all procedures can be accessed via the video displays. Printed operating manuals are available in the control room to supplement reference to operating procedures.

PSCS control software operates on measurements of key energy production state variables, comparison of the measurements to expected (precharacterized) state variables and generation of control commands based on the automated operating and control procedures. The PSCS diagnoses whether or not an initial energy production state can be re-entered automatically in the event the initial state is exited (e.g., due to transients or operator intervention). The PSCS also initiates the appropriate control actions that would otherwise be carried out by operators manually according to written procedures. In addition, the PSCS requests certain component and equipment to cease operation if the plant status information indicates that operating limits have, or may be, exceeded; this will reduce the likelihood of inadvertant trips and potential equipment damage.

The control room operators are presented with information consisting of symptomatic variables describing the physical plant state conditions. Information presented indicates the automatic actions to be taken for successful mitigation of a transient condition even though the operator may not be required to intervene. The information also consists of graphically annunciated information pertaining to any remaining signals which are in a transient state.

6.4.1.2 NSSSCS Normal Operations During Energy Production

[LATER - Refer to NSSSCS SSDD]

6.4.1.3 DMS Normal Operations During Energy Production

[LATER]

6.4.1.4 TOSS Normal Operations During Energy Production

[LATER]

6.5 Refueling

6.5.1 Normal Operations During Refueling (Goal 1, State 3)

6.5.1.1 PSCS Normal Operations During Refueling

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

Refueling control is performed by the refueling operations crew using the core refueling subsystem of the Fuel Handling and Storage System. The refueling control and operations performed at the reactor module are monitored from the MCR by the assistant operator at the CRAW. The DMS provides the data communication interconnection between the fuel handling control stations and the CRAW for monitoring. The control room and refueling operators are provided with voice communication equipment at their respective workstations.

6.5.1.2 NSSSCS Normal Operations During Refueling

[LATER - Refer to NSSSCS SSDD]

6.5.1.3 DMS Normal Operations During Refueling

[LATER]

6.5.1.4 TOSS Normal Operations During Refueling

[LATER]

6.6 Shutdown

6.6.1 Normal Operation During Shutdown (Goal 1, State 2)

6.6.1.1 PSCS Normal Operations During Shutdown

With respect to that portion of the plant in a shutdown mode, the PSCS and the operators perform primarily monitoring functions. The status of reactor and vessel systems, components and equipment are monitored to ensure the reactor is being properly maintained in a shutdown condition [for cold shutdown, neutron multiplication factor k less than 0.99 at fuel temperatures of 23°C (73°F)], the necessary core geometry is established, neutron source range measurements are within specification, and sufficient decay heat and residual heat transfer is provided (15 percent helium and feedwater flow). Also, various checks are made to ascertain that startup and shutdown instrumentation is operating, reactivity shutdown margins are verified, and that the necessary auxiliary and bypass systems and process loops are configured (e.g., for shutdown with condenser or deaerator unavailable).

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

6.6.1.2 NSSSCS Normal Operations During Shutdown

[LATER - Refer to NSSSCS SSDD]

6.6.1.3 DMS Normal Operations During Shutdown

[LATER]

6.6.1.4 TOSS Normal Operations During Shutdown

[LATER]

6.7 Abnormal Operation

6.7.1 Abnormal Operation During Energy Production (Goal 2, State 1)

6.7.1.1 PSCS Abnormal Operations During Energy Production

During abnormal plant conditions, the assistant operator monitors the remainder of the plant while the operator at the CROW tends to the controls for the affected portion of the plant. The assistant operator monitors the affected portion of the plant once it is restored to normal operating conditions or removed from service while the operator at the CROW resumes normal operating tasks.

From an operational standpoint, there are no requirements for the operator at the CROW to perform manual trips or post-trip cooling and shutdown initiation under accident conditions. However, direct communications interfaces are established when operator intervention or interrogation of the PSCS is desired or required. Means are provided for discretionary operator intervention under automatic control when intervention is judged by the operator to be appropriate for protecting plant investment.

Operator interactions are long-term measures taken, for example, to ensure extended post-trip cooling and shutdown but not under accident conditions. During off-normal operations, these discretionary operator actions can be taken to avoid potential challenges to investment protection but they are verified and validated by the automatic controls.

6.7.1.2 NSSSCS Abnormal Operations During Energy Production

[LATER - Refer to NSSSCS SSDD]

6.7.1.3 DMS Abnormal Operations During Energy Production

[LATER]

6.7.1.4 TOSS Abnormal Operations During Energy Production

[LATER]

6.7.2 Abnormal Operation During Shutdown (Goal 2, State 2)

6.7.2.1 PSCS Abnormal Operations During Shutdown

The capability is provided for the licensed operating staff to access shutdown initiators and monitors required to achieve reactor shutdown, initiate and maintain cooling and bring the plant to a safe, cold shutdown condition in the event a) the main control room becomes uninhabitable or inaccessible for any reason during plant operation, or the PSCS becomes unavailable (extremely remote probability). For the latter case, selected plant systems are designed to trip the modules upon long-term anomalous indication or loss of a PSCS status monitoring signal. The requirements (environmental, accessibility, time response, interlocks, security, etc.) are such that the licensed operating staff can perform the necessary actions in a safe, timely and effective manner from the alternate shutdown facility.

6.7.2.2 NSSSCS Abnormal Operations During Shutdown

[LATER - Refer to NSSSCS SSDD]

6.7.2.3 DMS Abnormal Operations During Shutdown

[LATER]

6.7.2.4 TOSS Abnormal Operations During Shutdown

[LATER]

6.7.3 Abnormal Operation During Refueling (Goal 2, State 3)

6.7.3.1 PSCS Abnormal Operations During Refueling

[LATER]

6.7.3.2 NSSSCS Abnormal Operations During Refueling

[LATER - Refer to NSSSCS SSDD]

6.7.3.3 DMS Abnormal Operations During Refueling

[LATER]

6.7.3.4 TOSS Abnormal Operations During Refueling

[LATER]

6.7.4 Abnormal Operation During Startup/Shutdown (Goal 2, State 4)

6.7.4.1 PSCS Abnormal Operations During Startup/Shutdown

[LATER]

6.7.4.2 NSSSCS Abnormal Operations During Startup/Shutdown

[LATER - Refer to NSSSCS SSDD]

6.7.4.3 DMS Abnormal Operations During Startup/Shutdown

[LATER]

6.7.4.4 TOSS Abnormal Operations During Startup/Shutdown

[LATER]

6.8 Casualty Events and Recovery Procedures

6.8.1 Casualty Events

[LATER]

6.8.2 Design Features to Mitigate Effects of Casualty Events

[LATER]

6.8.3 Recovery Procedures

[LATER]

TABLE 6-1

PCDIS PARAMETRIC CONTROL VARIABLE LIMITS AND SETPOINTS
STEADY STATE

Subsystem	Process Operating Mode	Parametric Control Variable	Control Variable Limits with respect to the Process Operating Mode	Control Variable Setpoints
PSCS	25 - 100% Reactor Module Feedwater Supply	Module Load Index (% Feedwater Flow)	0.25 - 1.00	varies within the range depending on allocated load demand
PSCS	25 - 100% Turbine Steam Admission	Turbine Load Index (% Main Steam Admission)	0.25 - 1.00	varies within the range depending on allocated load demand
NSSS	25 - 100% Reactor Module Steam Supply	Module Steam Temperature at the Steam Generator outlet	[TBD]	1005°F
NSSS	25 - 100% Reactor Module Steam Supply	Vent Valve Pressure at the Steam Generator outlet	[TBD]	2700 psia
NSSS	25 - 100% Reactor Module Steam Supply	Safety Relief Valve Pressure at the Steam Generator outlet	[TBD]	2750 psia
BOP Controls	[TBD] - 100% Turbine Load	Main Steam Header Pressure	[TBD]	2415 psia
BOP Controls	[TBD] - 100% Turbine Load	Main Bypass Valve Pressure	[TBD]	2475 psia
BOP Controls	[TBD] - 100% Module Feedwater Flow	Minimum Pressure Drop Across Feedwater Flow Control Valve	[TBD]	100 psi

TABLE 6-2

PCDIS PARAMETRIC CONTROL VARIABLE LIMITS AND SETPOINTS
STARTUP

Subsystem	Process Operating Mode	Parametric Control Variable	Control Variable Limits with respect to the Process Operating Mode	Control Variable Setpoints
PSCS	0 - 10 % Reactor Module Feedwater Supply	Module Load Index (% Feedwater Flow)	0.00 - 0.25	varies within the range depending on allocated load demand
PSCS	0 - 10 % Turbine Steam Admission	Turbine Load Index (% Main Steam Admission)	0.00 - 0.25	varies within the range depending on allocated load demand
PSCS	0 - 10 % Reactor Module Feedwater Supply	Module Load Change Rate (Rate of change in feedwater flow)	[TBD] - 5.0%/min.	varies within the range depending on load response capabilities and plant load demand
PSCS	0 - 10 % Turbine Steam Admission	Turbine Load Change Rate (Rate of change in main steam admission)	[TBD] - 5.0%/min.	varies within the range depending on load response capabilities and plant load demand
PSCS	0 - 10 % Turbine Steam Admission	Turbine Load Index (% Main Steam Admission)	0.00 - 0.25	varies within the range depending on allocated load demand
NSSS	25 - 100% Reactor Module Steam Supply	Startup Bypass Valve Pressure	[TBD]	2475 psia

TABLE 6-3

PCDIS PARAMETRIC CONTROL VARIABLE LIMITS AND SETPOINTS
NORMAL TRANSITIONS

Subsystem	Process Operating Mode	Parametric Control Variable	Control Variable Limits with respect to the Process Operating Mode	Control Variable Setpoints

[LATER]

TABLE 6-4

PCDIS PARAMETRIC CONTROL VARIABLE LIMITS AND SETPOINTS
TRANSIENT CONDITIONS

Subsystem	Process Operating Mode	Parametric Control Variable	Control Variable Limits with respect to the Process Operating Mode	Control Variable Setpoints

[LATER]

SECTION 7

SYSTEM MAINTENANCE

This section defines an approach, a procedural outline, and types and forms of maintenance for the Plant Control, Data and Instrumentation System (PCDIS). This section also describes special design features that enhance the maintainability of the PCDIS. Specific maintenance requirements are identified when appropriate. Interfaces with other systems required to support PCDIS maintenance operations are also identified.

This section provides the basis for PCDIS subsystem maintenance requirements and procedures. More detailed maintenance requirements, activities and procedures are described in the Subsystem Design Descriptions (SSDDs) and O&M manuals. However, this section describes system-level maintenance activities not addressed by these lower tier documents. The system operating procedures of Section 6 provide the instructions for preparing portions of the system for maintenance.

7.1 Maintenance Approach

PCDIS maintenance is based on principles of modularity and redundancy permitting maintenance of a component (software or hardware) without compromising system availability. System availability and component reliability permit on-line maintenance or maintenance during scheduled outages thus limiting PCDIS contributions to forced outage time due to unplanned maintenance. The maintenance approach for software is functionally similar to the approach for hardware maintenance. Software is designed and structured so that software maintenance can be performed without requiring system downtime.

The PCDIS maintenance approach is designed to limit the frequency of personnel exposure to hazardous environments. Anticipated exposures to radionuclides are derived from estimated dose rates for individual locations where the PCDIS components reside. They are also based on the total time required for access, preparation, repair, removal, handling and replacement that takes place during maintenance.

Figure 7-1 outlines the PCDIS system-level maintenance approach. Figure 7-1 designates the scope of each type of maintenance and the typical sequence of maintenance operations.

7.1.1 Order of Preference

The basis for the PCDIS maintenance approach is high system availability (and thus plant availability) and limiting personnel exposure to hazardous environments or conditions during maintenance activities. The following order of preference is consistent with the maintenance approach and serves as a guide for determining the proper maintenance approach for the various components of the PCDIS.

a) Adjust or repair in-place

b) Repair components by hands-on (contact) maintenance to the extent permissible and consistent with personnel exposure and safety needs

c) Replace component with a spare unit; have failed component repaired and requalified as applicable

d) Remove component by hands-on (contact) maintenance for repair and replace the same component (see note)

e) Perform remote replacement of failed components

f) Repair components in-place by remote maintenance

NOTE: It is not within the scope of this section to account for repair of components after removal and subsequent replacement. Reference is made to O&M manuals.

7.1.2 Types of Maintenance

The PCDIS maintenance approach involves only two types of maintenance which account for all required maintenance operations. These types of maintenance are preventive maintenance and corrective maintenance.

Preventive maintenance is used, in part, to meet PCDIS reliability, availability and maintainability requirements. Preventive maintenance operations can be performed during scheduled outages but most operations are performed during normal plant operation with the PCDIS subsystems in service.

Corrective maintenance procedures are employed only in the event that preventive maintenance operations determine the need for it or that a major failure causes system unavailability. Corrective maintenance is used to locate and repair failed components and return the components to service if they are not replaced.

7.2 Corrective Maintenance

Corrective maintenance involves three basic activities with varying degrees of automation. These activities are

a) troubleshooting,
b) repair (see Section 7.1.1), and
c) restoring to normal servive conditions

Corrective maintenance is performed, in some cases, on an unscheduled basis and consists of identifying the cause of a failure and restoring the system to normal service conditions. In most cases, a failure (e.g., loss of a data communication cable or computer) can be tolerated such that corrective maintenance can be performed during the next scheduled outage or during a period of plant operation when the component can be removed from the system and repaired or replaced. Redundant PCDIS components (e.g., multiple data highways, processors and spares) and fault isolation features enable the system to tolerate various types of failure that would otherwise cause system unavailability. The nature of failures or casualty events (see Sections 2.3.4 and 6.8) is such that corrective maintenance does not have to be initiated immediately in most cases.

7.2.1 Troubleshooting

Troubleshooting is necessary for the majority of the PCDIS components to determine the cause of component failures if self-tests are not sufficient and the causes are not conclusively diagnosed. Failures are typically software and timing errors, incorrect electrical grounds, defective wiring, degradation from atmospheric conditions or contamination, failed power supplies or discrete component failures (e.g., integrated circuits). Troubleshooting, from a system standpoint, is essentially identical to the approach for component troubleshooting.

The following outlines the general approach for troubleshooting failures in the PCDIS:

a) Validate the operating parameter that appears to be inconsistent with the respective priority, address, set point, limitation or operation as listed in Section 6.1.

b) Verify if the above parameter actually is in violation of technical specification. This can usually be accomplished through one of the following:

   1. Self-test checks
   2. System process or component specification comparisons
   3. Cross channel comparisons
   4. System or component logistics
   5. Operating performance data (trends)

c) Have the affected portion of the system prepared for maintenance.

d) Verify, to the smallest replaceable component level, which component has failed. Troubleshooting inherently involves specific tests for this determination. O&M manuals must be consulted during this phase of maintenance.

7.2.2 Repair

Repair of components is performed on a basis of the results of troubleshooting. This maintenance work is accomplished according to the order of preference given in Section 7.1.1. Most PCDIS components are designed for quick, easy removal and replacement (i.e., modular). Therefore, although the maintenance approach considers an order of preference, various conditions govern the actual approach taken at the time of repair. These will evolve from time constraints, interfacing systems requirements or failure to locate faulty components by troubleshooting, for example.

The primary method for corrective maintenance on modular components is replacement of the defective component. Bench testing or off-site maintenance is not within the scope of this section. Other components that could fail such as communications controllers, isolation devices, keyboards, modems, power supplies and portions of display equipment can be temporarily replaced with spare components maintained for that purpose.

7.2.3 Restoring to Normal Service Conditions

Corrective maintenance also includes activities for restoring the components of the PCDIS to their normal service conditions. Section 6 provides the procedures for returning portions of the system to normal service conditions. The activities performed during this phase of corrective maintenance are inspection, self-tests, calibration with calibration verification and functional checks. These are typically carried out in the order given.

7.3 Preventive Maintenance

Preventive maintenance activities are performed on a specific schedule and provide a means of monitoring system or component performance. These activities maintain individual components in a specified operating condition such that the overall system performance meets or exceeds both design and plant operating requirements. Preventive maintenance is also used as a basis for early detection and prevention of incipient failures.

Preventive maintenance is composed of two forms of scheduled maintenance activities. These are referred to as routine maintenance and periodic maintenance. The frequency at which these activities are performed is based upon (1) past plant experience with similar components and operating conditions, (2) failure modes and effects analysis of the PCDIS, (3) engineering judgement, (4) consistency with other plant system maintenance activities based on location of components, and (5) plant operating approach and technical specifications.

7.3.1 Routine Maintenance

Routine maintenance for the PCDIS is a form of preventive maintenance. It is performed on the basis of reported automatic diagnostics and daily observations of system operating performance. In-service inspection and surveillance are performed as part of the routine maintenance activities. Inspection of the PCDIS is primarily a manual activity pertaining to equipment conditions and mountings, wiring, mode settings, etc. Surveillance accounts for functional checks of the instrumentation and controls (e.g., multiplexer performance verification, diagnostic and alarm checks and communication network operation).

7.3.2 Periodic Maintenance

Periodic maintenance is a form of preventive maintenance. It is performed according to individual schedules specified for various hardware and software of the PCDIS. Periodic maintenance is predominantly automated self-testing with manual verification of these tests. Hardware components such as multiplexers, processors, power supplies and instrumentation are subjected to adjustments, corrections, comparisons and resets as applicable during self-testing. Periodic maintenance also includes special test activities which, in general, are described in O&M manuals.

Automated self-testing with manual verification of components is carried out in conjunction with O&M manuals and the PCDIS technical specifications. It is initiated upon repair or replacement of a the PCDIS component, failure to meet the criteria of functional checks or on a specific periodic basis. Qualified component replacements are tested prior to installation. Once installed, the component functionally self-checked. This assures that additional components which may be faulty or out of specification will be detected as such.

7.4 In-Service Inspection

Unlike mechanical components and structures, in-service inspection is one phase of routine preventive maintenance for instrumentation and control systems. Refer to Section 7.3 for a description of PCDIS in-service inspection activities.

7.5 Surveillance

Unlike mechanical components and structures, surveillance is one phase of routine preventive maintenance for instrumentation and control systems. Refer to Section 7.3 for a description of PCDIS surveillance activities.

FIGURE 7-1

PCDIS MAINTENANCE APPROACH

TYPE	FORM	PHASE	METHOD
Preventive	Routine	Inspection	1. Inspection a. computers, cabinet equipment and peripherals b. field located equipment c. terminations, cabling, wiring & ventilation d. user interfaces (e.g., panel mounted displays)
		Surveillance	2. Functional Checks a. data processing equipment b. data communication equipment c. user interfaces d. calibration verification e. alarm & setpoint logic
	Periodic		3. Calibration a. I/O components and peripherals b. data communications equipment c. channels and networks
Corrective			4. Troubleshooting a. on-line fault detection, diagnosis and isolation b. off-line fault detection, diagnosis and isolation
			5. Repair or Replace a. according to order of preference
			6. Return to Service a. inspection b. calibration with calibration verification c. functional checks

SECTION 8

SYSTEM DECOMMISSIONING

[LATER]

SECTION 9

REFERENCES

1. MHTGR Program Procedure HP-10402, Rev. 0, Design Description Document Preparation.

2. Overall Plant Design Specification (OPDS), 4x350 MW(t) MHTGR, HTGR-86-004, Rev. 4, May 1987.

3. Quality Assurance Requirements, HP-20801, Rev. 1, dated September 21, 1984.

4. HTGR-86-002, Rev. 1, Functional Analysis Report, Standard MHTGR, September 1986.

5. Not used.

6. "An Overall Plant Control/Transient Study of the MHTGR"; attachment to GE letter XL-848-860184, J.E. Quinn to J.K. Hartman (DOE-SAN); GE SLPP Milestone 5102.02.06, "Overall Plant Control/Transient Analysis Input to the PSID", dated June 27, 1986.

7. "Reliability Allocations for the Standard MHTGR", HTGR-85-008, dated February 1987.

8. "Control of a Multi-Module HTGR Plant", HTGR-85-172, dated February 1986.

9. Zizzo, D.M., Preliminary Study of System Architectures and Distributed Control Requirements for the PCAPS Data Handling and Transmission System 91 (DHTS), May 30, 1984. GE letter XL-897-840151, S.M. Davies to R.D. Larson, et al., "WBS 240.6.3, DHTS Milestone 240.3b", dated June 5, 1984.

10. "Final O&M Assessment Report", GE letter XL-848-850319, J.E. Quinn to L. Lanni (DOE), "Fulfillment of FY85 SLPP Milestone 5100.06.09, same subject", dated September 30, 1985.

11. SWEC letter SWEC/GCRA-0518, W.C. Craig to L.D. Mears (GCRA), "Heat Balance Diagram and Power Generation Cycle - MHTGR Plant", dated April 26, 1985.

12. "Interim Automation Assessment", WBS 5237.01(05), GE letter XL-848-870104, J.E. Quinn to W. Craig (SWEC), A. Neylan (GAT) and L. Mears (GCRA), same subject, dated May 5, 1987.

13. "Plant Control Design Report", GE letter XL-848-860261, J.E. Quinn to J.K. Hartman (DOE), same subject, SLPP Milestone 5237.01.04, dated September 30, 1986.

REFERENCES
(continued)

14. "Cable Reduction Optimization Study - Final Report", General Electric and Burns & Roe, Inc., Large Developmental Plant (LDP) program Cable Reduction Optimization Study, B&R letter BR-BE-350, C.S. Ehrman to LDP Distribution, dated September 30, 1982.

15. DOE letter, A.C. Millunzi to L.D. Mears (GCRA), "Agreement Reached on Utility/User Requirement 3.3.1-2", dated June 10, 1987.

16. PDCO letter PDCO-275-87, D.V. Graf to Distribution, "Quality Assurance Requirements Section for Design Descriptions", dated June 15, 1987.

17. PDCO letter PDCO-282-87, D.V. Graf to J.E. Quinn, "PDCO Review of PCDIS SDD Prior to Finalization", dated June 22, 1987.

18. GE letter XL-848-870079, J.E. Quinn to A.C. Millunzi (DOE), "Regulatory Guide Assessment for the MHTGR PCDIS", dated April 6, 1987.

19. GE Teleconference Call Record XP-270C-870044, Phone discussion between L.P. Walker (SWEC/GCRA), J. Lewis (GAT) and GE, dated June 3, 1987.

20. GAT letter GA/DOE-161-87, G.C. Bramblett to A.C. Millunzi (DOE), "Section 5 of the OPDS (Rev. 4)", dated June 23, 1987.

APPENDIX A

PCDIS TRACEABILITY OF REQUIREMENTS

REQUIREMENTS TRACEABILITY

Tables A-1 and A-2 of this appendix provide traceability of the PCDIS requirements. These requirements are

1. program-level requirements applicable, as judged by the system designer, to the PCDIS. These are Utility/User and institutional requirements from OPDS Section 2 (Ref. 2); they are not derived. These requirements are identified by those having traceability numbers with the following format: 0100.02xx.yyy

2. derived plant-level requirements passed down from OPDS Section 5. These requirements are identified by those having traceability numbers with the following format: 0100.05xx.yyy

3. system-level requirements from Section 3 which were derived from analyses and/or trade studies on the program-level requirements and the plant-level requirements in Section 1.

Table A-1 provides traceability for Items 1. and 2. above. Columns 1 through 4 in Table A-1 include, in order, the following:

- requirement traceability number (whose use and coding scheme is prescribed in Ref. 1),
- a summary statement of the requirement (for simplicity of indexing),
- a referenced source of the requirement, and
- a source descriptive (comments or reference details).

Table A-2 provides traceability for Item 3. above.

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.020	Accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations: 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. Four (4) reactor modules operating in parallel supplying steam to two turbine-generators.	2 17	0100.0501.012 Attachment 1, Comment #1
3700.0102.040	Supporting controls and instrumentation shall be located outside the control room.	2	0100.0501.056
3700.0102.042	The PCDIS shall be designed for a Nuclear Island that includes four standard reactor modules.	2	0100.0501.004
3700.0102.044	The PCDIS shall be designed for an ECA that includes two steam T/Gs. standard reactor modules.	2	0100.0501.005
3700.0102.045	Human-machine interfaces and machine-machine communication interfaces shall be provided for PCDIS subsystem equipment outside the control room requiring human interaction.	8	Sections 1.2.2.1 and 2.5.2.3
3700.0102.050	Features of the PCDIS (e.g., inter-system communication performance or data highway cable configuration) shall not impose limiting or restrictive requirements on the physical location of subsystem equipment and device interfaces.	9	Section 2.1.2.1
3700.0102.055	Permit the addition of new control and data communication interfaces, without necessitating deenergizing electronics or affecting the operation of other electronic equipment.	9	Section 2.1.2.1

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.060	Human-engineering techniques shall be employed in the design.	2	0100.0501.055
3700.0102.065	Design modifications and improvements shall be considered if a one percentage increase in the total capital investment produces, at a minimum, a seven tenths percentage improvement in the equivalent plant availability factor.	2	0100.0501.075
3700.0102.070	Facilitate operation of reactor modules and turbine-generators at different power levels.	2	0100.0512.002
3700.0102.072	Base subsystem designs on proven technology or on new technology expected to be demonstrated in time to support the construction licensing process.	10	Page 11, 6th item
3700.0102.092	The design of structures, systems and components within the Nuclear Island shall be standardized.	2	0100.0501.002
3700.0102.095	Provide the capability for roving operators to control selected not requiring direct control room operator interfacing and interaction.	12	Sections 3.2.1 and 3.2.2
3700.0102.100	Concurrently coordinate energy production, shutdown, refueling and startup/shutdown operations of different reactor modules and T/G's in a manner consistent with optimizing the economics of each.	8	Sections 5 & 6
3700.0102.105	Design the PCDIS to support meeting the plant permanent operating staff goal of 50 full-time personnel maximum.	2	0100.0201.006

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.110	The PCDIS design basis shall include an evaluation of required operator response for each anticipated operating staff position.	2	0100.0201.708
3700.0102.115	At least one of the licensed control room operators per shift shall be a senior licensed operator.	8	Sections 1.2.1.5, 6.0 and 7.4.1
3700.0102.120	As a design goal the plant shall be designed to be operated by a maximum shift staff of: 1. One senior licensed supervisor. 2. Two licensed reactor operators in the control room. 3. Four roving operators.	2	0100.0201.007
3700.0102.128	The PCDIS controls shall facilitate the normal startup and shutdown duty cycle events.	2	0100.0501.017
3700.0102.130	Be designed to operate from 25% to 100% feedwater flow for the performance parameters specified in OPDS Figures 5.1-1 through 5.1-5, Tables 5.1-1 and 5.1-2, and in the NSSS Thermal Performance Requirements Report.	2	0100.0501.016
3700.0102.135	Automatically accept baseload and load following net electrical output load demands allocated to the plant by the grid dispatcher.	8	Section 5
3700.0102.138	Automatic control during plant operation.	2	0100.0204.003
3700.0102.139	Accommodate one or more reactor modules shutting down.	2	0100.0512.018

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.145	Reactor module shutdown shall range between 25% and 0% rated feedwater flow rate on a per reactor module basis.	2	0100.0512.019
3700.0102.148	Automatic control during orderly shutdown.	2	0100.0204.003
3700.0102.155	Provisions shall be made to remove a reactor from service, perform refueling and return it to service with the remaining reactors and the turbine plant in operation.	2	0100.0501.018
3700.0102.160	Reactor module startup shall range between 0% and 25% rated feedwater flow rate on a per reactor module basis.	2	0100.0512.017
3700.0102.164	Accommodate one or more reactor modules starting up.	2	0100.0512.016
3700.0102.168	Automatic control during startup.	2	0100.0204.003
3700.0102.170	The control room operator workstation shall be human engineered to concurrently accept those inputs from a single operator required to control plant energy production, shutdown, refueling and startup/shutdown operations.	8	Sections 2.5 and 6.6
3700.0102.175	The control room shall incorporate features necessary to facilitate startup, shutdown, monitoring and control and shall provide for the shutdown of major systems and components by the operator.	2 15	0100.0201.222 DOE direction
3700.0102.180	The plant shall be normally operated from a single control room except during postulated events that would render the control room uninhabitable or the controls inoperable.	2	0100.0501.051

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.185	Operator workstations requiring operator interaction from within the main control room shall be human-engineered and designed as a functional entity of one PCDIS subsystem.	8	Secs. 1.2.1.5, 2.5.2.3, 6.0 and 7.4.1
3700.0102.190	The PCDIS shall be designed to operate through specified design transients.	2	0100.0501.017
3700.0102.195	Sustain continuous operation through and following transients associated with the loss or failure of a major component, system, or train, including an individual reactor or turbine-generator.	2	0100.0501.015
3700.0102.200	Features as required to limit recovery time to resumption of reactor power operation when a protection trip occurs consistent with meeting the plant availability goal.	2	0100.0201.003
3700.0102.205	Facilitate continual plant operation through the transients of OPDS Table 2.1-1 (except for shutdown) and at a reduced electrical output upon loss of function of major plant components where more than one is employed.	2	0100.0201.214
3700.0102.210	Be designed to withstand the mechanical and thermal loads resulting from the design transients specified in MHTGR Plant Design Basis Transient Analysis Report for the number of cycles specified in OPDS Table 5.1-3.	2	0100.0501.032
3700.0102.212	Failure of SSCs that are not "safety-related" shall not cause failure of "safety-related" SSCs during an SSE.	2	0100.0501.037 (# changed per Ref. 20)

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.215	Non-safety related systems shall be designed for ANSI A58.1 seismic load requirements, as a minimum.	2	0100.0501.034
3700.0102.217	OBE seismic response spectrum load level specifications shall be based on the plant seismic response spectra.	2	0100.0501.035
3700.0102.220	Environmental qualification requirements pertaining to operation and structural design shall be based on relevant plant site characteristics as specified in OPDS Table 2.1-2.	2	0100.0501.013 and 0100.0501.033
3700.0102.250	The PCDIS shall provide the controls, monitors and instrumentation for automatically controlling energy production and conversion, startups and shutdowns, coordinating with refueling operations and maintaining shutdown of the plant or portions thereof.	8	Section 4.5
3700.0102.252	Malfunctions alarmed in the control room.	2	0100.0501.054
3700.0102.255	Fixed audible alarm annunciator points in the control room shall be restricted to parameters which can lead to initiation of protective actions or the loss of electrical production.	2	0100.0512.004
3700.0102.260	Automatically detect and document the sequence of significant events that occur during plant operation.	2	0100.0512.005
3700.0102.265	Internal diagnostic monitoring shall be incorporated within major plant control and electric systems.	2	0100.0501.053

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.270	Provisions made for monitoring plant status, configuration and performance as a basis for decision making.	2	0100.0201.241
3700.0102.275	PCDIS subsystems shall provide the capability to sense, process and analyze those variables, states, modes, limits, conditions, etc., required for the processes and subsystems to be observable.	13	Sec. 3.1.4.2 & Appendix B
3700.0102.280	Portions and/or derivations of those observations required for controlling energy production, shutdown, refueling and startup/shutdown from a single control room shall be made available for use by the PSCS and the operators.	8 12	Sections 4 and 6 and Sections 3.2.1 and 3.2.2
3700.0102.285	The control room operator workstation shall be human engineered to provide the capability for a single operator to concurrently observe plant energy production, shutdown, refueling and startup/shutdown status.	8	Sections 4 and 6
3700.0102.290	Provide the capability to assist that energy production, shutdown and startup/shutdown decision making responsibility allocated to the operators.	8 13	Section 4.5.1 and Section 3.1.4.2 and Appendix B
3700.0102.295	Evaluate and determine the state of the plant and plant-level control state maneuvers.	13	Section 3.1.4.2 and Appendix B
3700.0102.300	Evaluate and determine the state of the NSSS and the ECA and the corresponding control state maneuvers.	13	Section 3.1.4.2 and Appendix B

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.302	Control and regulate the conditions of the nuclear steam supply so as to deliver 2400 psig, 1000°F steam to the high pressure turbine admission valves.	11	
3700.0102.306	Measure and control the performance of the steam and feedwater parameters at any point between 25% and 100% rated feedwater flow for steady-state operation.	2	0100.0512.014
3700.0102.308	Control the helium mass flow through the active steam generator bundle between 25% and 100% of rated feedwater flow for steady-state operation.	2	0100.0512.015
3700.0102.310	Automatically regulate conditions of main steam supplied to the T/Gs, feedwater supplied to each module, and the steam produced and delivered by each module.	8	Section 5
3700.0102.315	Control those actuators and devices required to effect a change in state in the energy production and conversion processes.	8	Section 5
3700.0102.320	PCDIS controls shall facilitate the normal, rapid and step load change duty cycle events.	2	0100.0501.017
3700.0102.325	The system shall be designed for base-load operation and accommodating the weekly load cycle of OPDS Figure 2.1-1 over its design life.	2	0100.0201.212
3700.0102.330	Continuous operation under automatic control between 25% and 100% of nominal module feedwater flow.	2	0100.0512.011

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.335	Changing reactor and plant output under automatic control at a rate up to and including 5% of rated output per minute of those reactors on line.	2	0100.0512.013
3700.0102.340	Permit reloading the plant at 5% of rated load per minute without the necessity for a mandatory hold except for those associated with the turbine-generators.	2	0100.0512.012
3700.0102.345	The PCDIS design shall provide sustained and controlled operation for load rejection, turbine trip (except on low condenser vacuum), and step changes of ±15% in plant output.	2	0100.0501.014
3700.0102.350	The control room operator workstation shall be designed to accept direction from the operators to transfer control of auxiliary processes to a mode of operation that can be supervised at locations outside the control room.	12	Section 3.2.2 (e.g., refueling)
3700.0102.355	Accept directions corresponding to energy production and conversion load demand changes at rates anywhere from a minimum of ± [TBD] %/minute to a maximum of ± 5%/minute.	8	Section 5
3700.0102.360	Roving operators and subsystems located outside the control room shall be capable of accepting instructions from the control room operators and operator workstation, respectively.	8	Section 2.5
3700.0102.365	Automatically allocate demands for individual energy production (module) and energy conversion (T-G's) sources.	13	Section 3.2

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.370	Load demands shall be distributed, during normal plant energy production, among the energy production (modules) and the energy conversion (turbine-generators) sources in operation consistent with plant economic and availability requirements.	13	Section 3.2
3700.0102.375	Automatically determine and allocate equivalent rates of change in energy production and conversion required for a rate of change in net plant electrical output anywhere from a minimum of ± [TBD] %/minute to a maximum of ± 5%/minute.	8 13	Section 2.5 Section 3.2
3700.0102.380	Acknowledge process and other plant subsystem variables, states, modes, performance limits, conditions, etc., in the analysis and decision-making process.	13	Secs. 3.1.4.2.1, 3.1.4.2.3, B.2.3.1, and B.2.3.2
3700.0102.385	Accept startup directions corresponding to rated load demand changes at rates anywhere from a minimum of [+TBD] %/minute to a maximum of [+TBD] %/minute.	8	Section 5.2.2
3700.0102.390	Accept shutdown directions corresponding to rated load demand changes at rates anywhere from a minimum of [-TBD] %/minute to a maximum of [-TBD] %/minute.	8	Section 5.2.3
3700.0102.395	Automatically allocate startup/shutdown demands for individual energy production (module) and energy conversion (T-G's) sources.	8	Section 5.2.2
3700.0102.400	Communicate digital control and monitoring signals using non-hardwired signal transmission techniques.	8 14	Secs. 2.5.2 and 7.0, and Secs. 2.1.1 and 3.1

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.600	The PCDIS shall provide the capability and the associated operator workstations to concurrently and automatically report information where required.	8 13	Section 4.5.1 Sections B.2.1.5 B.2.2.4 and B.2.3.4
3700.0102.610	Meet a planned outage allocation of [49.5 hours].	2	0100.0501.072
3700.0102.615	Design for a plant operating life of 40 calendar years.	2	0100.0501.011
3700.0102.620	Meet an overall reliability allocation of [TBD].	2	0100.0501.074
3700.0102.630	Enable maintenance within the average yearly plant scheduled outage time.	2	0100.0501.081
3700.0102.635	Special maintenance and installation tools shall be provided by the equipment vendor.	2	0100.0501.083 and 0100.0501.122
3700.0102.640	Facilitate hands-on maintenance.	2	0100.0201.026
3700.0102.645	The PCDIS shall be designed and arranged, and equipment and components located, to facilitate on-line maintenance.	2	0100.0201.027
3700.0102.650	Provisions shall be made to remove a reactor from service, perform maintenance and return it to service with the remaining reactors and the turbine plant in operation.	2	0100.0501.018
3700.0102.655	Provide self-test capabilities for key functional components.	13	Section B.2.4
3700.0102.660	Provisions made for monitoring plant status, configuration and as a basis for maintenance diagnostics.	2	0100.0201.241

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.665	The plant process controls shall be functionally independent from major component and equipment monitoring and protective features.	2	0100.0512.001
3700.0102.670	Meet applicable top-level regulatory criteria.	2	0100.0201.121 and 0100.0202.001
3700.0102.680	Design, analysis, fabrication and construction shall comply with codes and standards required to meet the four goals of the Integrated Approach. These include ANSI/ASME NQA-1 and DOE NE F2-10.	2	0100.0501.101
3700.0102.700	Regulatory Guides applicable to the PCDIS design.	18 & 19	
3700.0102.710	RDT F1-2T.	2	0100.0204.005
3700.0102.760	Items that are not "safety-related" shall come under a quality assurance program which complies with selected basic requirements and appropriate supplements of ANSI/ASME NQA-1 and supplements 02-4.3.0, 03-1.3.2, 03-1.3.4 and 03-1.3.5 from DOE NE F2-10.	2 16	0100.0501.111 Attachment 1
3700.0102.785	PCDIS components shall be classified to reduce ratings and the cost of spare parts inventory.	2	0100.0201.029
3700.0102.795	Shop, factory, or field fabricated, assembled and erected components and subsystems shall be utilized as appropriate.	2	0100.0201.041

TABLE A-1

PCDIS REQUIREMENTS TRACEABILITY INDEX

HFD-33700 TRACEABILITY NUMBER	SUMMARY REQUIREMENT DESCRIPTION	SOURCE REFERENCE (see Sec. 9)	SOURCE DESCRIPTIVE
3700.0102.800	Design systems based upon parallel construction of the complete plant; facilitate construction and startup in increments of two standard reactor modules and one turbine.	2	0100.0501.121
3700.0102.805	Incorporate features that facilitate decommissioning or refurbishment of one reactor while maintaining others in operation.	2	0100.0501.133

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

SECTION 3 REQUIREMENT TRACEABILITY NUMBERS				TRACEABLE SOURCE
PSCS	NSSSCS	DMS	TOSS	(i.e., Section 1 requirement numbers)
3700.0321.020	3700.0322.010	3700.0323.020		3700.0102.020
3700.0321.040	3700.0322.020		3700.0324.040	3700.0102.040
3700.0321.042	3700.0322.025			3700.0102.042
3700.0321.044				3700.0102.044
3700.0321.045	3700.0322.030	3700.0323.045	3700.0324.045	3700.0102.045
3700.0321.050	3700.0322.040	3700.0323.050	3700.0324.050	3700.0102.050
3700.0321.055	3700.0322.050	3700.0323.055	3700.0324.055	3700.0102.055
3700.0321.060	3700.0322.060	3700.0323.060	3700.0324.060	3700.0102.060
3700.0321.070	3700.0322.080			3700.0102.070
3700.0321.072	3700.0322.090		3700.0324.072	3700.0102.072
	3700.0322.092			3700.0102.092
3700.0321.095	3700.0322.110			3700.0102.095
				3700.0102.105
				3700.0102.110
				3700.0102.115

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

PSCS	SECTION 3 REQUIREMENT TRACEABILITY NUMBERS NSSSCS	DMS	TOSS	TRACEABLE SOURCE (i.e., Section 1 requirement numbers)
3700.0321.120				3700.0102.120
3700.0321.128	3700.0322.160			3700.0102.128
	3700.0322.120			3700.0102.130
3700.0321.132				3700.0102.132
3700.0321.135				3700.0102.135
3700.0321.138	3700.0322.125	3700.0323.138		3700.0102.138
3700.0321.139	3700.0322.129			3700.0102.139
	3700.0322.130			3700.0102.145
3700.0321.148	3700.0322.138	3700.0323.148		3700.0102.148
3700.0321.155	3700.0322.140		3700.0324.155	3700.0102.155
	3700.0322.150			3700.0102.160
3700.0321.164	3700.0322.145	3700.0323.164	3700.0324.164	3700.0102.164
3700.0321.168	3700.0322.148	3700.0323.168		3700.0102.168
3700.0321.170				3700.0102.170
3700.0321.175				3700.0102.175
3700.0321.180				3700.0102.180

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

PSCS	SECTION 3 REQUIREMENT TRACEABILITY NUMBERS NSSSCS	DMS	TOSS	TRACEABLE SOURCE (i.e., Section 1 requirement numbers)
3700.0321.185				3700.0102.185
3700.0321.190	3700.0322.160	3700.0323.190		3700.0102.190
3700.0321.195	3700.0322.170	3700.0323.195		3700.0102.195
3700.0321.200	3700.0322.180			3700.0102.200
3700.0321.205	3700.0322.190	3700.0323.205		3700.0102.205
3700.0321.210	3700.0322.195	3700.0323.210		3700.0102.210
3700.0321.212	3700.0322.197	3700.0323.212	3700.0324.212	3700.0102.212
3700.0321.215	3700.0322.200	3700.0323.215	3700.0324.215	3700.0102.215
3700.0321.217	3700.0322.205	3700.0323.217	3700.0324.217	3700.0102.217
3700.0321.220	3700.0322.207	3700.0323.220	3700.0324.220	3700.0102.220
3700.0321.250				3700.0102.250
3700.0321.252	3700.0322.215	3700.0323.252		3700.0102.252
3700.0321.255	3700.0322.255	3700.0323.255		3700.0102.255
3700.0321.260	3700.0322.225	3700.0323.260		3700.0102.260
3700.0321.265	3700.0322.230	3700.0323.265	3700.0324.265	3700.0102.265
3700.0321.270	3700.0322.240	3700.0323.270	3700.0324.270	3700.0102.270

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

SECTION 3 REQUIREMENT TRACEABILITY NUMBERS				TRACEABLE SOURCE
PSCS	NSSSCS	DMS	TOSS	(i.e., Section 1 requirement numbers)
3700.0321.275	3700.0322.250	3700.0323.275	3700.0324.275	3700.0102.275
3700.0321.280	3700.0322.260	3700.0323.280	3700.0324.280	3700.0102.280
3700.0321.285				3700.0102.285
3700.0321.290	3700.0322.290			3700.0102.290
3700.0321.295	3700.0322.295	3700.0322.295		3700.0102.295
	3700.0322.270			3700.0102.300
	3700.0322.285			3700.0102.302
	3700.0322.117			3700.0102.306
	3700.0322.115			3700.0102.308
	3700.0322.280			3700.0102.310
	3700.0322.290			3700.0102.315
3700.0321.320	3700.0322.160			3700.0102.320
3700.0321.325	3700.0322.300			3700.0102.325
	3700.0322.310			3700.0102.330
3700.0321.335	3700.0322.320			3700.0102.335

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

PSCS	SECTION 3 REQUIREMENT TRACEABILITY NUMBERS NSSSCS	DMS	TOSS	TRACEABLE SOURCE (i.e., Section 1 requirement numbers)
3700.0321.340	3700.0322.330			3700.0102.340
3700.0321.345	3700.0322.340			3700.0102.345
3700.0321.350				3700.0102.350
	3700.0322.350			3700.0102.355
3700.0321.360			3700.0324.360	3700.0102.360
3700.0321.365				3700.0102.365
3700.0321.370				3700.0102.370
3700.0321.375				3700.0102.375
3700.0321.380	3700.0322.370			3700.0102.380
3700.0321.385	3700.0322.380			3700.0102.385
3700.0321.390	3700.0322.390			3700.0102.390
3700.0321.395				3700.0102.395
3700.0321.400	3700.0322.400	3700.0323.400		3700.0102.400
3700.0321.600			3700.0324.600	3700.0102.600
3700.0321.610	3700.0322.410	3700.0323.610	3700.0324.610	3700.0102.610
3700.0321.615	3700.0322.420	3700.0323.615	3700.0324.615	3700.0102.615

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

SECTION 3 REQUIREMENT TRACEABILITY NUMBERS				TRACEABLE SOURCE
PSCS	NSSSCS	DMS	TOSS	(i.e., Section 1 requirement numbers)
3700.0321.620	3700.0322.430	3700.0323.620	3700.0324.620	3700.0102.620
3700.0321.630	3700.0322.445	3700.0323.630	3700.0324.630	3700.0102.630
3700.0321.635	3700.0322.447	3700.0323.635	3700.0324.635	3700.0102.635
3700.0321.640	3700.0322.440	3700.0323.640	3700.0324.640	3700.0102.640
3700.0321.645	3700.0322.450	3700.0323.645	3700.0324.645	3700.0102.645
3700.0321.650	3700.0322.460			3700.0102.650
3700.0321.655	3700.0322.470	3700.0323.655	3700.0324.655	3700.0102.655
3700.0321.660	3700.0322.480	3700.0323.660	3700.0324.660	3700.0102.660
3700.0321.665	3700.0322.490	3700.0323.665	3700.0324.665	3700.0102.665
3700.0321.670	3700.0322.500	3700.0323.670	3700.0324.670	3700.0102.670
3700.0321.680	3700.0322.510	3700.0323.680	3700.0324.680	3700.0102.680
				3700.0102.700
				3700.0102.710
3700.0321.760	3700.0322.520	3700.0323.760	3700.0324.760	3700.0102.760

TABLE A-2

PCDIS SUBSYSTEM REQUIREMENTS TRACEABILITY INDEX

SECTION 3 REQUIREMENT TRACEABILITY NUMBERS				TRACEABLE SOURCE
PSCS	NSSSCS	DMS	TOSS	(i.e., Section 1 requirement numbers)
3700.0321.785	3700.0322.530	3700.0323.785	3700.0324.785	3700.0102.785
3700.0321.795	3700.0322.540	3700.0323.795	3700.0324.795	3700.0102.795
3700.0321.800	3700.0322.550	3700.0323.800	3700.0324.800	3700.0102.800
3700.0321.805	3700.0322.560	3700.0323.805	3700.0324.805	3700.0102.805

APPENDIX B

DRAWINGS LIST

[LATER]

APPENDIX C

TRANSIENTS

[LATER]

APPENDIX D

DESIGN BASIS SEISMIC INPUTS

[LATER]

APPENDIX E

PARAMETER LISTS

[LATER]

APPENDIX F

PROPRIETARY CLAIMS

[NONE]

APPENDIX G

EQUIPMENT AND FACILITIES

PCDIS EQUIPMENT AND FACILITIES

Subsystem	Equipment	Facility Location
PSCS	Control room operator workstation	MCR of the Operations Center
	Assistant operator workstation	MCR of the Operations Center
	Supervisory control computers	Computer facility in the Operations Center
NSSSCS	[Refer to NSSSCS SSDD]	
DMS	General purpose computers	Computer facility in the Operations Center
	Data communication network	N/A
	Data communication computers	Computer facility in the Operations Center
	Shift supervisor workstation	MCR of the Operations Center
TOSS	Operations support workstations	TOSS facility
	Technical support workstations	TOSS facility

APPENDIX H

ALLOCATION OF FUNCTIONS TO PCDIS SUBSYSTEMS AND THE ENERGY CONVERSION AREA CONTROLS

Table H-1 lists the functions within the functional "tree" developed from Functional Analysis (Reference 4) as part of the Integrated Approach to the PCDIS design(footnote). The allocation of these functions to the various PCDIS subsystems and the ECA controls is identified by the function identification number associated with each function. The format of the function identification numbers for plant control functions (i.e., PCDIS functions) is the following:

M.N.8.X.Y.(a.b.c...)

where

M = an integer from 1 to 4 corresponding to one of four goals of the Integrated Approach to the MHTGR plant design

N = an integer from 1 to 4 corresponding to one of four operational states defined for the MHTGR plant

X = an integer from 1 to 5 corresponding to one of five generic functions of plant control systems

Y = an integer from 1 to 5 corresponding to one of the four PCDIS subsystems or the ECA controls

a, b, c, etc. = integers corresponding to subfunctions at lower levels in the functional "tree"

The allocation of functions to PCDIS subsystems and the ECA controls is as follows:

M.N.8.X.1.(a.b.c...) = NSSSCS
M.N.8.X.2.(a.b.c...) = ECA controls
M.N.8.X.3.(a.b.c...) = PSCS
M.N.8.X.4.(a.b.c...) = DMS
M.N.8.X.5.(a.b.c...) = TOSS

Footnote: The PSCS, DMS and TOSS function titles in Table H-1 reflect the most recent revision of similar function titles in the Reference 4 report. The next revision of the Reference 4 report will include the function titles of Table H-1.

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.1.8	Coordinate Plant Energy Production Control
1.1.8.1	Accept Plant Energy Production Direction
1.1.8.1.1	Accept Energy Production Direction
1.1.8.1.1.1	Accept Energy Production Control Commands
1.1.8.1.1.2	Accept Energy Production Information Commands
1.1.8.1.1.3	Accept Energy Production Information
1.1.8.1.2	Accept Energy Conversion Direction
1.1.8.1.3	Accept Supervisory Energy Production Directions
1.1.8.1.4	Accept Plant Data Management Direction
1.1.8.1.5	Accept Energy Production Operations Support Direction
1.1.8.2	Observe Plant Energy Production Status
1.1.8.2.1	Observe Energy Production Status
1.1.8.2.1.1	Acquire Energy Production Information
1.1.8.2.1.2	Convert Energy Production Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.1.8.2.1.3	Retain Energy Production Information
1.1.8.2.2	Observe Energy Conversion Status
1.1.8.2.3	Observe Plant Energy Production Coordination Status
1.1.8.2.4	Observe Plant Data Management Status
1.1.8.2.5	Observe Energy Production Operations Support Status
1.1.8.3	Make Plant Energy Production Decisions
1.1.8.3.1	Make Energy Production Decisions
1.1.8.3.1.1	Select Retained Energy Production Information
1.1.8.3.1.2	Process Energy Production Data
1.1.8.3.1.3	Retain Processed Energy Production Information
1.1.8.3.1.4	Communicate Energy Production Information
1.1.8.3.2	Make Energy Conversion Decisions
1.1.8.3.3	Make Supervisory Energy Production Decisions
1.1.8.3.4	Make Plant Data Management Decisions

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.1.8.3.5	Make Energy Production Operations Support Decisions
1.1.8.4	Effect Plant Energy Production Coordination
1.1.8.4.1	Effect Energy Production Control
1.1.8.4.1.1	Output Energy Production Control Signals
1.1.8.4.1.2	Output Energy Production Override Signals
1.1.8.4.2	Effect Energy Conversion Control
1.1.8.4.3	Effect Supervisory Energy Production Control
1.1.8.4.4	Effect Management of Plant Data
1.1.8.4.5	Effect Support of Energy Production Operations
1.1.8.5	Report Plant Energy Production Information
1.1.8.5.1	Report Energy Production Information
1.1.8.5.1.1	Annunciate Energy Production Conditions
1.1.8.5.1.2	Display Energy Production Information
1.1.8.5.1.3	Create Energy Production Hardcopy

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.1.8.5.2	Report Energy Conversion Information
1.1.8.5.3	Report Energy Production Coordination Information
1.1.8.5.4	Report Plant Data Management Information
1.1.8.5.5	Report Energy Production Operations Support Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.2.8	Coordinate Plant Shutdown Control
1.2.8.1	Accept Plant Shutdown Direction
1.2.8.1.1	Accept Energy Production Shutdown Direction
1.2.8.1.1.1	Accept Energy Production Control Shutdown Commands
1.2.8.1.1.2	Accept Energy Production Shutdown Information Commands
1.2.8.1.1.3	Accept Energy Production Shutdown Information
1.2.8.1.2	Accept Energy Conversion Shutdown Direction
1.2.8.1.3	Accept Supervisory Shutdown Directions
1.2.8.1.4	Accept Shutdown Communications
1.2.8.1.5	Accept Shutdown Operations Support Direction
1.2.8.2	Observe Plant Shutdown Status
1.2.8.2.1	Observe Energy Production Shutdown Status
1.2.8.2.1.1	Acquire Energy Production Shutdown Information
1.2.8.2.1.2	Convert Energy Production Shutdown Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.2.8.2.1.3	Retain Energy Production Shutdown Information
1.2.8.2.2	Observe Energy Conversion Shutdown Status
1.2.8.2.3	Observe Shutdown Coordination Status
1.2.8.2.4	Observe Shutdown Data Management Status
1.2.8.2.5	Observe Shutdown Operations Support Status
1.2.8.3	Make Plant Shutdown Decisions
1.2.8.3.1	Make Energy Production Shutdown Decisions
1.2.8.3.1.1	Select Retained Energy Production Shutdown Information
1.2.8.3.1.2	Process Energy Production Shutdown Data
1.2.8.3.1.3	Retain Processed Energy Production Shutdown Information
1.2.8.3.1.4	Communicate Energy Production Shutdown Information
1.2.8.3.2	Make Energy Conversion Shutdown Decisions
1.2.8.3.3	Make Supervisory Shutdown Decisions
1.2.8.3.4	Make Shutdown Data Management Decisions

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.2.8.3.5	Make Shutdown Operations Support Decisions
1.2.8.4	Effect Plant Shutdown Coordination
1.2.8.4.1	Effect Energy Production Shutdown Control
1.2.8.4.1.1	Output Energy Production Shutdown Control Signals
1.2.8.4.1.2	Output Energy Production Shutdown Override Signals
1.2.8.4.2	Effect Energy Conversion Shutdown Control
1.2.8.4.3	Effect Supervisory Shutdown Control
1.2.8.4.4	Effect Management of Plant Shutdown Data
1.2.8.4.5	Effect Support of Shutdown Operations
1.2.8.5	Report Plant Shutdown Information
1.2.8.5.1	Report Energy Production Shutdown Information
1.2.8.5.1.1	Annunciate Energy Production Shutdown Conditions
1.2.8.5.1.2	Display Energy Production Shutdown Information
1.2.8.5.1.3	Create Energy Production Shutdown Hardcopy

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.2.8.5.2	Report Energy Conversion Shutdown Information
1.2.8.5.3	Report Shutdown Coordination Information
1.2.8.5.4	Report Shutdown Data Management Information
1.2.8.5.5	Report Shutdown Operations Support Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.3.8	Coordinate Plant Control During Refueling
1.3.8.1	Accept Plant Direction During Refueling
1.3.8.1.1	Accept Module Direction During Refueling
1.3.8.1.1.1	Accept Module Control Commands During Refueling
1.3.8.1.1.2	Accept Module Information Commands During Refueling
1.3.8.1.1.3	Accept Module Information During Refueling
1.3.8.1.2	Accept Energy Conversion Direction During Refueling
1.3.8.1.3	Accept Refueling Coordination Directions
1.3.8.1.4	Accept Refueling Communications
1.3.8.1.5	Accept Refueling Operations Support Direction
1.3.8.2	Observe Plant Refueling Status
1.3.8.2.1	Observe Module Status During Refueling
1.3.8.2.1.1	Acquire Module Information During Refueling
1.3.8.2.1.2	Convert Module Information During Refueling

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.3.8.2.1.3	Retain Module Information During Refueling
1.3.8.2.2	Observe Energy Conversion Status During Refueling
1.3.8.2.3	Observe Refueling Coordination Status
1.3.8.2.4	Observe Refueling Data Management Status
1.3.8.2.5	Observe Refueling Operations Support Status
1.3.8.3	Make Coordination Decisions for Refueling
1.3.8.3.1	Make Module Decisions During Refueling
1.3.8.3.1.1	Select Retained Module Information During Refueling
1.3.8.3.1.2	Process Module Data During Refueling
1.3.8.3.1.3	Retain Processed Module Information During Refueling
1.3.8.3.1.4	Communicate Module Information During Refueling
1.3.8.3.2	Make Energy Conversion Decisions During Refueling
1.3.8.3.3	Make Refueling Coordination Decisions
1.3.8.3.4	Make Refueling Data Management Decisions

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.3.8.3.5	Make Refueling Operations Support Decisions
1.3.8.4	Effect Plant Coordination with Refueling
1.3.8.4.1	Effect Module Control During Refueling
1.3.8.4.1.1	Output Module Control Signals During Refueling
1.3.8.4.1.2	Output Module Override Signals During Refueling
1.3.8.4.2	Effect Energy Conversion Control During Refueling
1.3.8.4.3	Effect Supervisory Control During Refueling
1.3.8.4.4	Effect Management of Plant Refueling Data
1.3.8.4.5	Effect Support of Refueling Operations
1.3.8.5	Report Plant Refueling Information
1.3.8.5.1	Report Module Information During Refueling
1.3.8.5.1.1	Annunciate Module Conditions During Refueling
1.3.8.5.1.2	Display Module Information During Refueling
1.3.8.5.1.3	Create Module Hardcopy During Refueling

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.3.8.5.2	Report Energy Conversion Information During Refueling
1.3.8.5.3	Report Refueling Coordination Information
1.3.8.5.4	Report Refueling Data Management Information
1.3.8.5.5	Report Refueling Operations Support Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.4.8	Coordinate Plant Startup/Shutdown Control
1.4.8.1	Accept Plant Startup/Shutdown Direction
1.4.8.1.1	Accept Energy Production Startup/Shutdown Direction
1.4.8.1.1.1	Accept Energy Production Control Startup/Shutdown Commands
1.4.8.1.1.2	Accept Energy Production Startup/Shutdown Information Commands
1.4.8.1.1.3	Accept Energy Production Startup/Shutdown Information
1.4.8.1.2	Accept Energy Conversion Startup/Shutdown Direction
1.4.8.1.3	Accept Supervisory Startup/Shutdown Directions
1.4.8.1.4	Accept Startup/Shutdown Communications
1.4.8.1.5	Accept Startup/Shutdown Operations Support Direction
1.4.8.2	Observe Plant Startup/Shutdown Status
1.4.8.2.1	Observe Energy Production Startup/Shutdown Status
1.4.8.2.1.1	Acquire Energy Production Startup/Shutdown Information
1.4.8.2.1.2	Convert Energy Production Startup/Shutdown Information

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.4.8.2.1.3	Retain Energy Production Startup/Shutdown Information
1.4.8.2.2	Observe Energy Conversion Startup/Shutdown Status
1.4.8.2.3	Observe Startup/Shutdown Coordination Status
1.4.8.2.4	Observe Startup/Shutdown Data Management Status
1.4.8.2.5	Observe Startup/Shutdown Operations Support Status
1.4.8.3	Make Plant Startup/Shutdown Decisions
1.4.8.3.1	Make Energy Production Startup/Shutdown Decisions
1.4.8.3.1.1	Select Retained Energy Production Startup/Shutdown Information
1.4.8.3.1.2	Process Energy Production Startup/Shutdown Data
1.4.8.3.1.3	Retain Processed Energy Production Startup/Shutdown Information
1.4.8.3.1.4	Communicate Energy Production Startup/Shutdown Information
1.4.8.3.2	Make Energy Conversion Startup/Shutdown Decisions
1.4.8.3.3	Make Supervisory Startup/Shutdown Decisions
1.4.8.3.4	Make Startup/Shutdown Data Management Decisions

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.4.8.3.5	Make Startup/Shutdown Operations Support Decisions
1.4.8.4	Effect Plant Startup/Shutdown Coordination
1.4.8.4.1	Effect Energy Production Startup/Shutdown Control
1.4.8.4.1.1	Output Energy Production Startup/Shutdown Control Signals
1.4.8.4.1.2	Output Energy Production Startup/Shutdown Override Signals
1.4.8.4.2	Effect Energy Conversion Startup/Shutdown Control
1.4.8.4.3	Effect Supervisory Startup/Shutdown Control
1.4.8.4.4	Effect Management of Plant Startup/Shutdown Data
1.4.8.4.5	Effect Support of Startup/Shutdown Operations
1.4.8.5	Report Plant Startup/Shutdown Information
1.4.8.5.1	Report Energy Production Startup/Shutdown Information
1.4.8.5.1.1	Annunciate Energy Production Startup/Shutdown Conditions
1.4.8.5.1.2	Display Energy Production Startup/Shutdown Information
1.4.8.5.1.3	Create Energy Production Startup/Shutdown Hardcopy

TABLE H-1
FUNCTIONS OF THE PLANT CONTROL, DATA AND INSTRUMENTATION SYSTEM

Functional Analysis Function Number	Function Title
1.4.8.5.2	Report Energy Conversion Startup/Shutdown Information
1.4.8.5.3	Report Startup/Shutdown Coordination Information
1.4.8.5.4	Report Startup/Shutdown Data Management Information
1.4.8.5.5	Report Startup/Shutdown Operations Support Information

APPENDIX I

ALTERNATE LOAD ALLOCATION STRATEGIES

TABLE I-1
ALTERNATE LOAD ALLOCATION STRATEGIES

Change in plant electrical output required ?	Unit(s) become unavailable or limited ?	Initial unit load allocation configuration	Load allocation strategy	LOAD ALLOCATION STRATEGY #
NO	NO	EQUALIZED	REMAIN EQUALIZED	1
NO	NO	EQUALIZED	DON'T EQUALIZE UNITS	2
NO	NO	UNEQUAL	EQUALIZE ALL UNITS	3
NO	NO	UNEQUAL	REMAIN UNEQUAL	4
NO	LIMITED	UNEQUAL	EQUALIZE NON-LIMITED UNITS	5
NO	LIMITED	UNEQUAL	DO NOT EQUALIZE NON-LIMITED UNITS	6
YES	NO	EQUALIZED	EQUALIZE ALL UNITS	7
YES	NO	EQUALIZED	DON'T EQUALIZE UNITS	8
YES	LIMITED	EQUALIZED	EQUALIZE NON-LIMITED UNITS	9
YES	LIMITED	EQUALIZED	DO NOT EQUALIZE NON-LIMITED UNITS	10
YES	NO	UNEQUAL	EQUALIZE ALL UNITS	11
YES	NO	UNEQUAL	DON'T EQUALIZE UNITS	12
YES	LIMITED	UNEQUAL	EQUALIZE NON-LIMITED UNITS	13
YES	LIMITED	UNEQUAL	DO NOT EQUALIZE NON-LIMITED UNITS	14
NO	UNAVAILABLE	EQUALIZED	EQUALIZE AVAILABLE UNITS	15
NO	UNAVAILABLE	EQUALIZED	DO NOT EQUALIZE AVAILABLE UNITS	16
NO	UNAVAILABLE	UNEQUAL	EQUALIZE AVAILABLE UNITS	17
NO	UNAVAILABLE	UNEQUAL	DO NOT EQUALIZE AVAILABLE UNITS	18

Equal load allocation = Strategies 1, 3, 7, 11, 15 and 17
Unequal load allocation = All other strategies

Strategies #1 and #7

Following refueling or shutdown, a reactor module is transitioned from startup to the energy production state with one or more other units already in the energy production state.

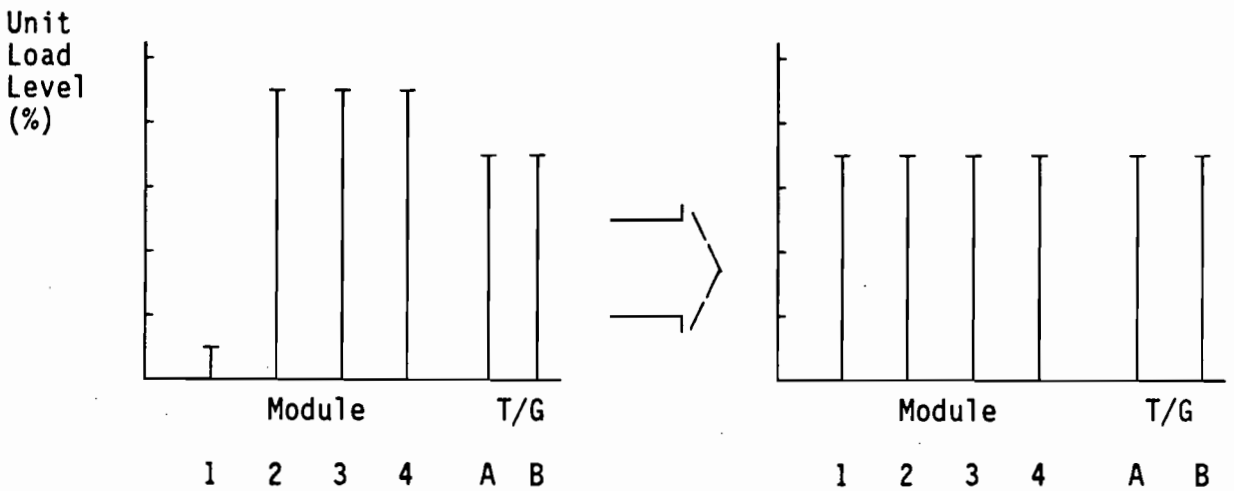
[Plant electrical output changes for Strategy #7 but not for Strategy #1.]

Basis for equal load allocation:

Section 1	Requirements:	.132	.155	.370
Section 2.3	Performance :	c)	h)	i)

Assumptions:
1) Units currently in operation are not scheduled to be shutdown.
2) Constant plant output to the grid is desirable for Strategy #1.

Graphical illustration of load maneuvering:



Strategies #3 and #11

Units are maneuvered from an unequal load configuration to an equal load configuration.

[Plant electrical output changes for Strategy #11 but not for Strategy #3.]

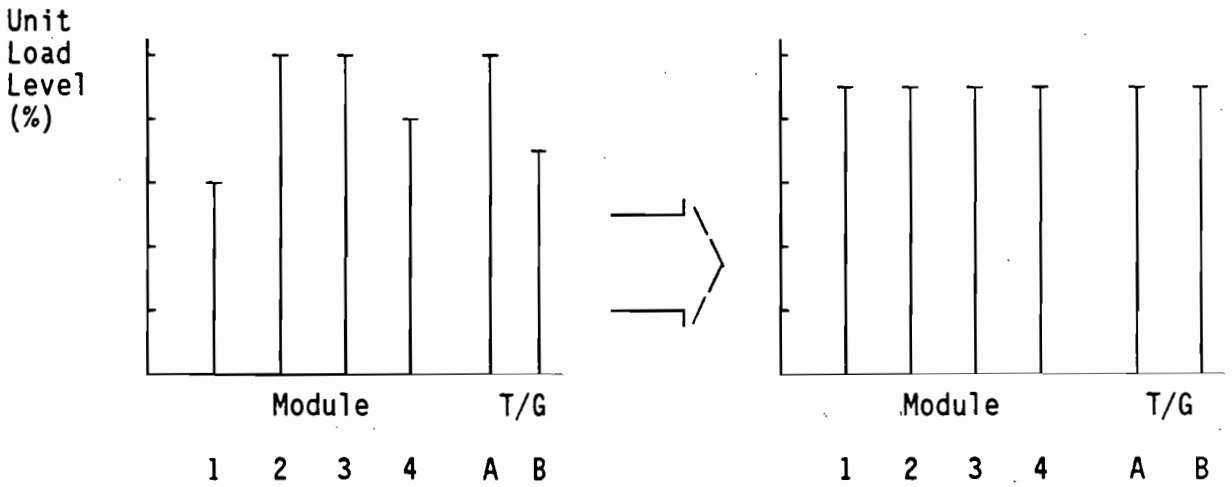
Basis for equal load allocation:

Section 1	Requirements:	.132	.325	.370	
Section 2.3	Performance :	a)	b)	c)	h)

Assumptions:

1) The initial conditions of the plant are such that units are operating at different load levels.
2) A balanced load configuration is preferred (i.e., there are no disincentives to do so)

Graphical illustration of load maneuvering:



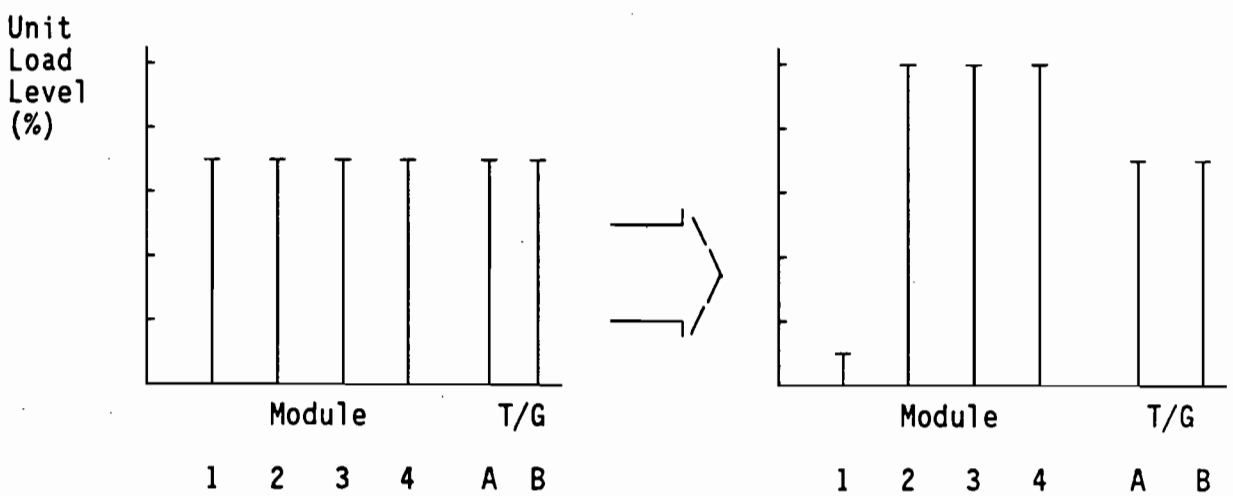
Strategy #15

A reactor module is transitioned from the energy production state to a shutdown or refueling state with one or more other units already in the energy production state.

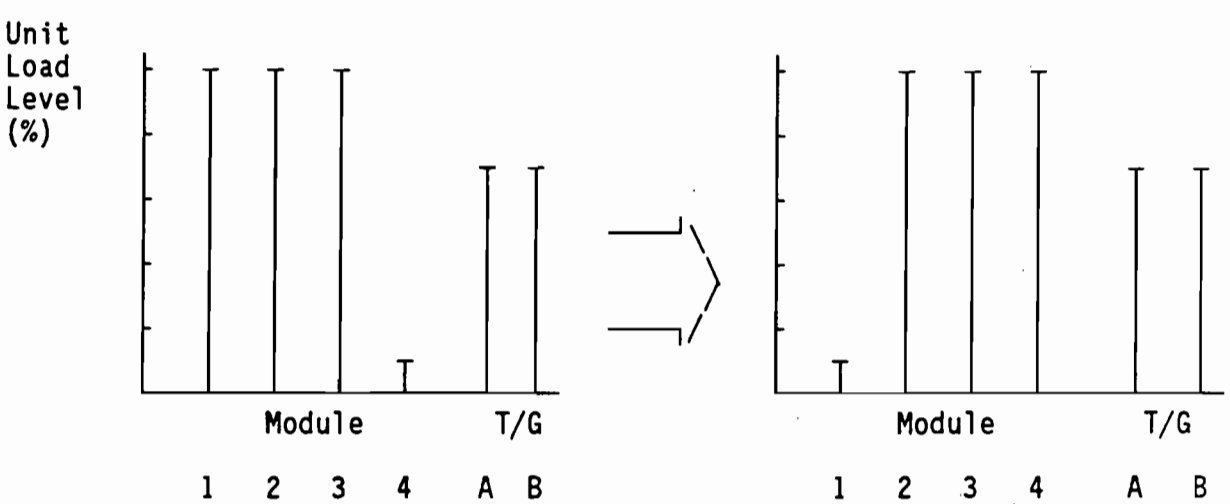
Basis for equal load allocation:

Section 1	Requirements:	.132	.155	.195	.295
Section 2.3	Performance :	b)	c)		

Assumptions:
1) There is no grid dispatcher request for a change in plant output.
2) Constant plant output to the grid is desirable.



Another version of Strategy #15 is the following:



Strategy #17

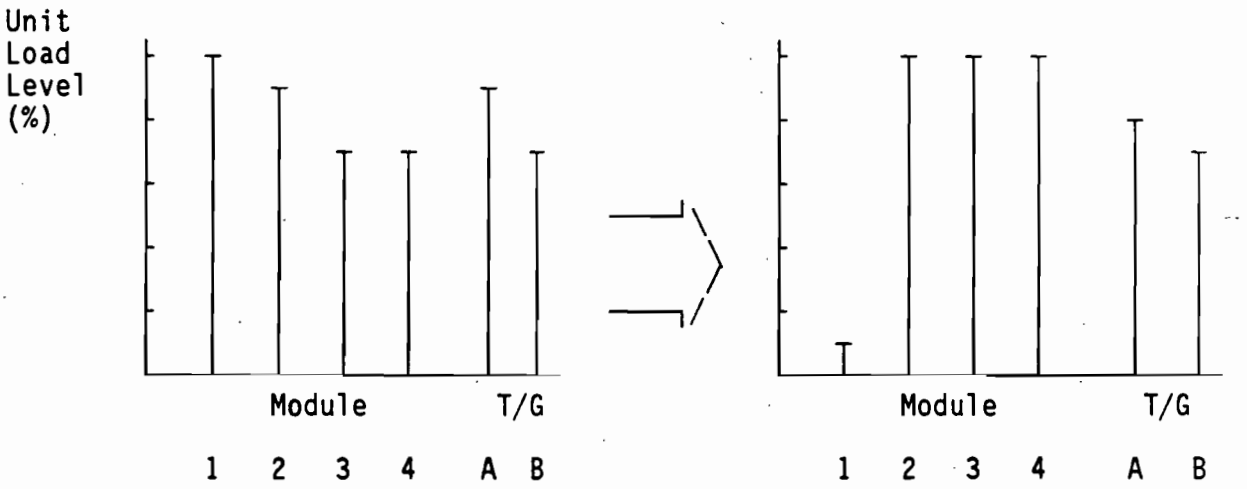
A reactor module is transitioned from the energy production state to a shutdown or refueling state with one or more other units already in the energy production state.

Basis for equal load allocation:

Section 1	Requirements:	.070	.132	.155	.295
Section 2.3	Performance :	a)	b)	c)	h) i)

Assumptions:
1) There is no grid dispatcher request for a change in plant output.
2) Constant plant output to the grid is desirable.

Graphical illustration of load maneuvering:



Strategies #2 and #8

Units are transitioned from an equalized load configuration to an unequal load configuration.

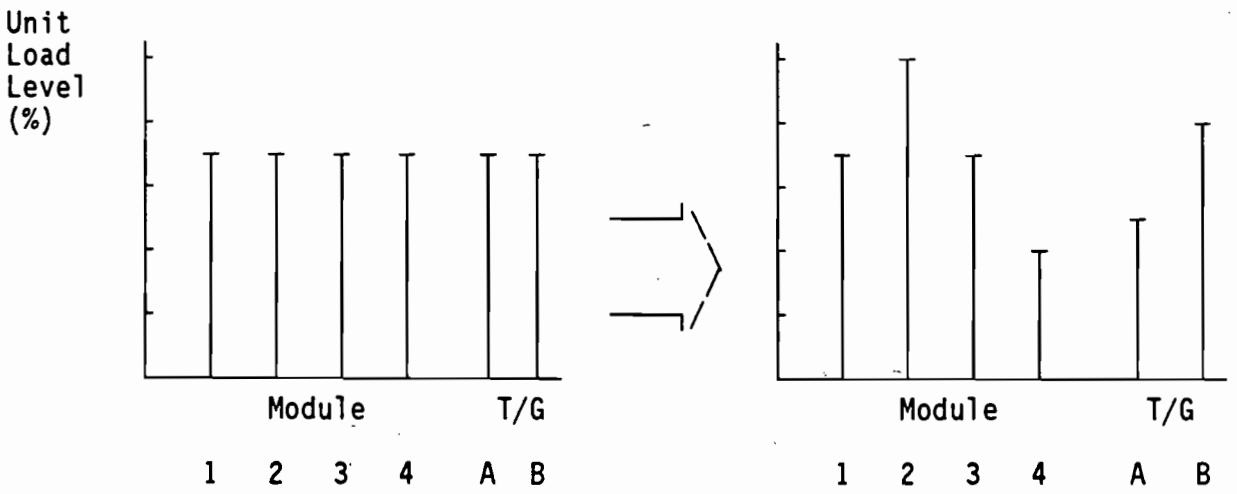
[Plant electrical output changes for Strategy #8 but not for Strategy #2.]

Basis for unequal load allocation:

Section 1	Requirements:	.070	.370
Section 2.3	Performance :	d)	f)

Assumptions:

1) Overall plant thermodynamics, efficiencies and integrated effects of operational duty cycling are not consistent among units.
2) Consistency can be achieved with units operating at different load levels.
3) Constant plant output to the grid is desirable for Strategy #2.



Strategy #9

A change in plant output is necessary at a time when a unit is operationally constrained (e.g., due to poor performance attributes, above-average integrated thermal stresses, on-line testing, redundant component trip or failure, reactor module core geometry or power distribution factors, partial loss of T/G stator cooling, etc.) yet not precluded from contributing to the change in plant output.

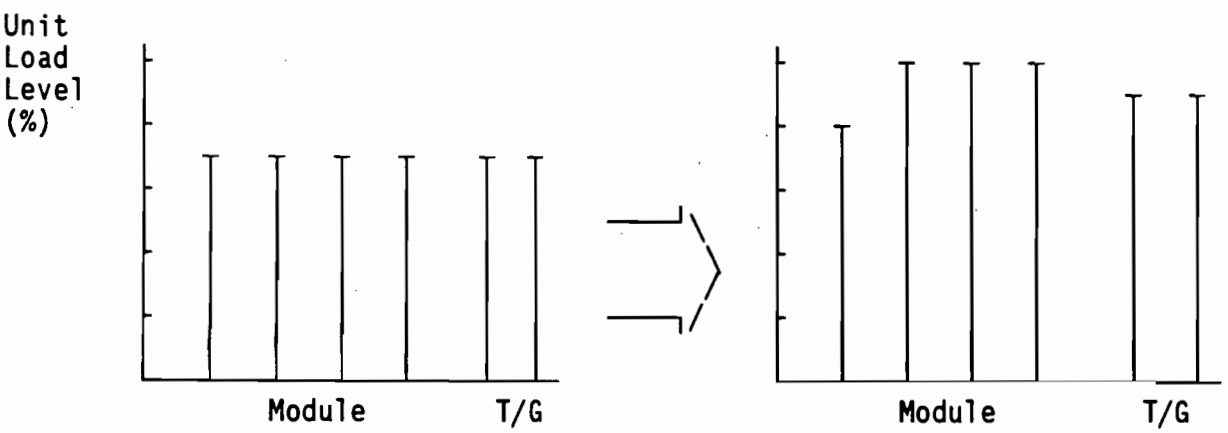
Basis for unequal load allocation:

Section 1	Requirements:	.070	.370	.380
Section 2.3	Performance :	b)	h)	

Assumptions:

1) Total plant load demand cannot be met without the contribution from the constrained unit.
2) Maneuvering the constrained unit does not challenge safety or investment protection.

The form of load allocation used for Strategy #5 is also used for those situations described in Strategy #9. The allocation of loads is represented by the following numerical and graphical example of Strategy #9.



	1	2	3	4	A	B
Initial load level:	70	70	70	70	70	70

	1	2	3	4	A	B
Final load level:	80	100	100	100	95	95

Module 1 is constrained to an 80% load limit.

Strategies #4 and #12

Units are maneuvered from one unequal load configuration to another unequal load configuration.

[Plant electrical output changes for Strategy #12 but not for Strategy #4.]

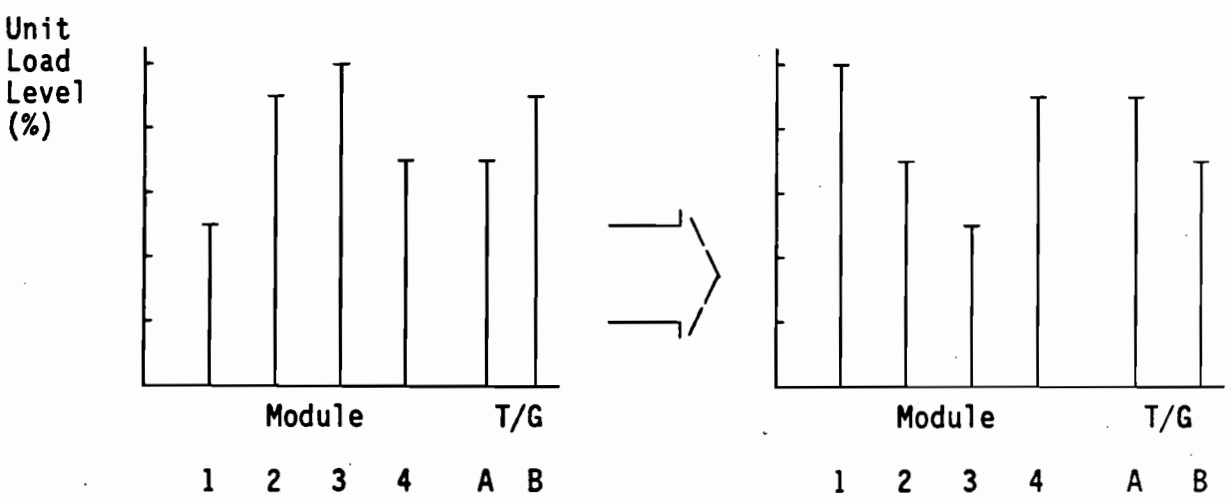
Basis for unequal load allocation:

Section 1	Requirements:	.070	.370	.380
Section 2.3	Performance :	d)	e)	f)

Assumptions:

1) Overall plant thermodynamics, efficiencies and integrated effects of operational duty cycling are not consistent among units.
2) Consistency can be achieved with units operating at different load levels.

Graphical illustration of load maneuvering:



Strategies #5 and #13

Non-limited units are maneuvered to similar load levels.

[Plant electrical output changes for Strategy #13 but not for Strategy #5.]

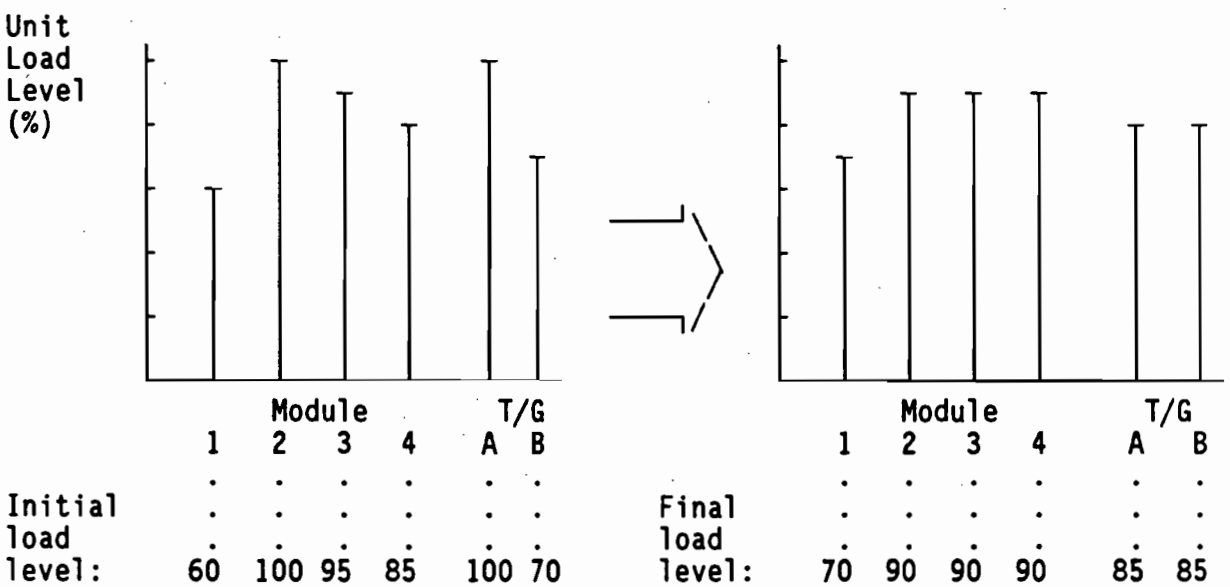
Basis for unequal load allocation:

Section 1	Requirements:	.070	.325	.370	.380	
Section 2.3	Performance :	a)	b)	c)	f)	h) i)

Assumptions:

1) The initial conditions of the plant are such that units are operating at different load levels.
2) At least one unit is constrained to a known load limit.

The load allocation used in Strategy #5 is the most common form of unequal load allocation. It achieves equal final load levels among unconstrained units. This is represented by the following numerical, graphical example of Strategy #5.



Module 1 constrained to 70% load.

Strategies #6 and #14

Units are transitioned and operated at different load levels during partial plant load demand periods.

[Plant electrical output changes for Strategy #14 but not for Strategy #6.]

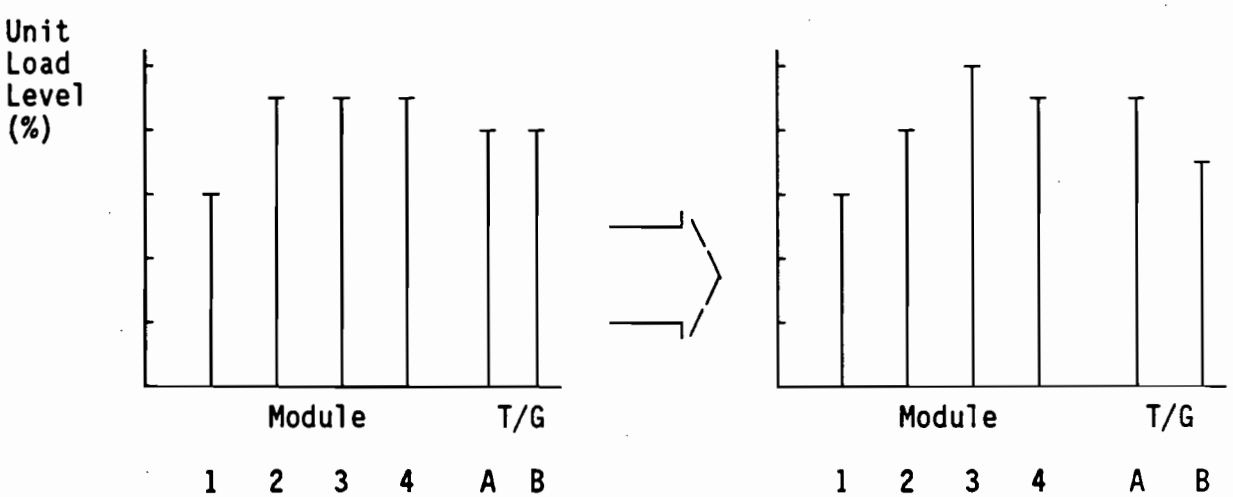
Basis for unequal load allocation:

Section 1	Requirements:	.070	.370	.380
Section 2.3	Performance :	d)	e)	

Assumptions:

1) Accelerated or deaccelerated fuel burnup is acceptable, and sometimes necessary, to meet predicted (planned) refueling and maintenance schedules.
2) Balancing integrated operational duty cycling effects will require unequal load allocation.
3) At least one unit is constrained to a known load limit.

Graphical illustration of load maneuvering:



Module 1 is constrained
Module 3 under accelerated burnup schedule

Strategy #10

Units are transitioned and operated at different load levels during partial plant load demand periods.

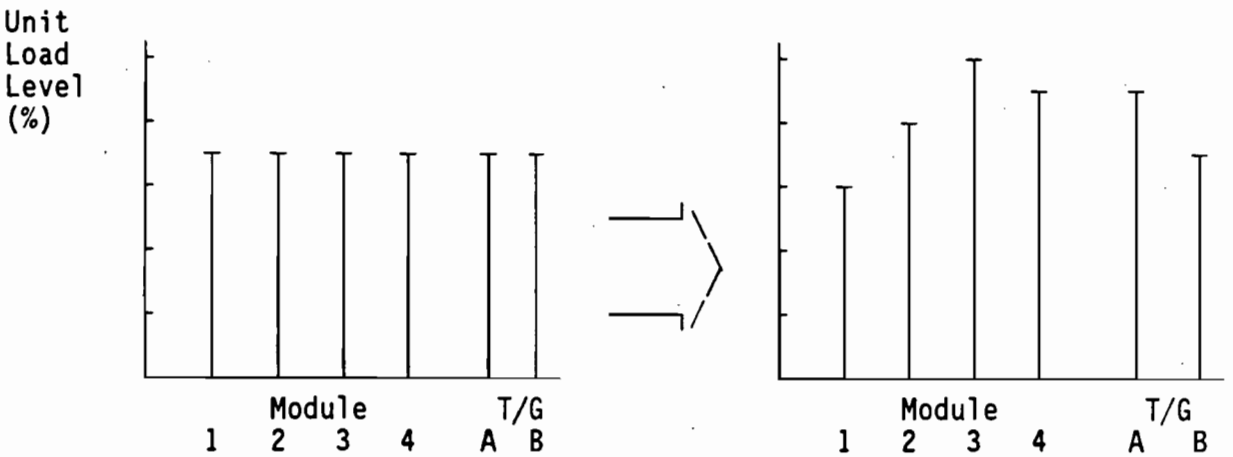
Basis for unequal load allocation:

Section 1	Requirements:	.070	.370	.380
Section 2.3	Performance :	d)	e)	

Assumptions:

1) Accelerated or deaccelerated fuel burnup is acceptable, and sometimes necessary, to meet predicted (planned) refueling and maintenance schedules.
2) Balancing integrated operational duty cycling effects will require unequal load allocation.
3) At least one unit is constrained to a known load limit.
4) When plant electrical load demand is sufficiently less than plant electrical power generating capability, load levels of constrained units are maintained approximately 10% below their respective load limits provided stable unit operation can be maintained (e.g., above 25% rated load). This control strategy permits a higher rate of response to a plant load increase than the rate allowable (i.e., 5/4% per minute times the number of non-limited units in operation) if limited unit(s) were at its(their) upper load limits.

Graphical illustration of load maneuvering:

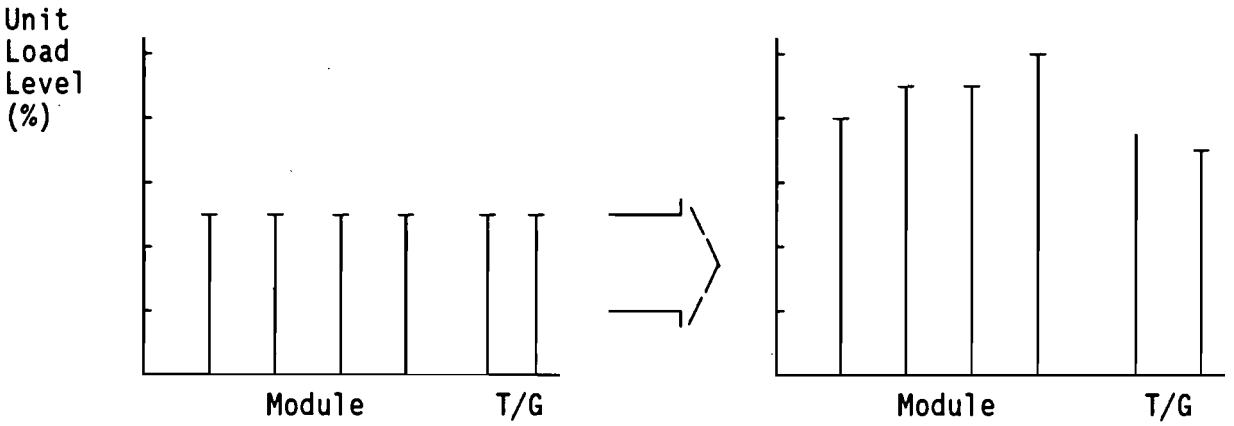


Module 1 is constrained
Module 3 under accelerated burnup schedule

An additional example on the following page illustrates Assumption 4 above.

Strategy #10 (continued)

Suppose a plant increase from 50% to 90% rated output is required yet one module is load limited and another module is rate limited. The following illustrates the allocation of loads based on Assumption 4.



	1	2	3	4	A	B
Initial load level	50	50	50	50	50	50

	1	2	3	4	A	B
Final load level:	80	90	90	100	90	90

Module 1 is constrained to an 80% load limit
Module 4 is rate limited but not load limited

Note that Strategy #9 would have resulted in the following final module load levels:

Module	1	2	3	4
	80.0	93.3	93.3	93.3

However, Modules 2 and 3 are reduced slightly to 90% (with Module 4 load increased to compensate for this) in order to permit equal load <u>changes</u> and maximum rates of change if additional plant output is demanded.

Strategy #16

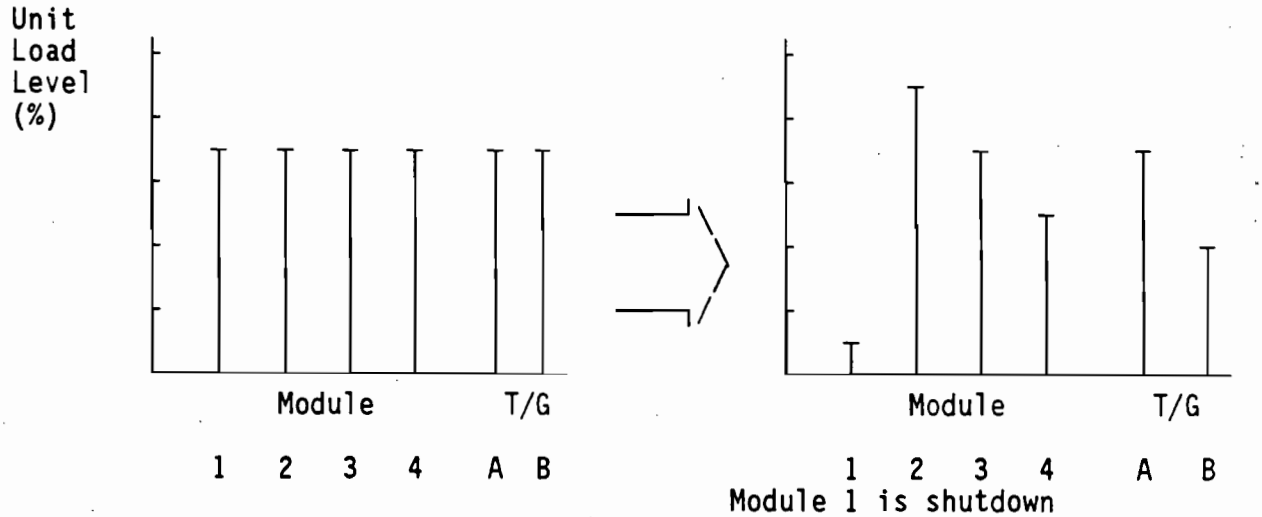
An equalized load configuration is changed to an unequal load configuration following shutdown (unavailability) of a reactor module.

Basis for unequal load allocation:

Section 1	Requirements:	.070	.132	.155	.195	.295	.300
Section 2.3	Performance :	(none identified)					

Assumptions:

1) There is no grid dispatcher request for a change in plant output.
2) Constant plant output to the grid is desirable.



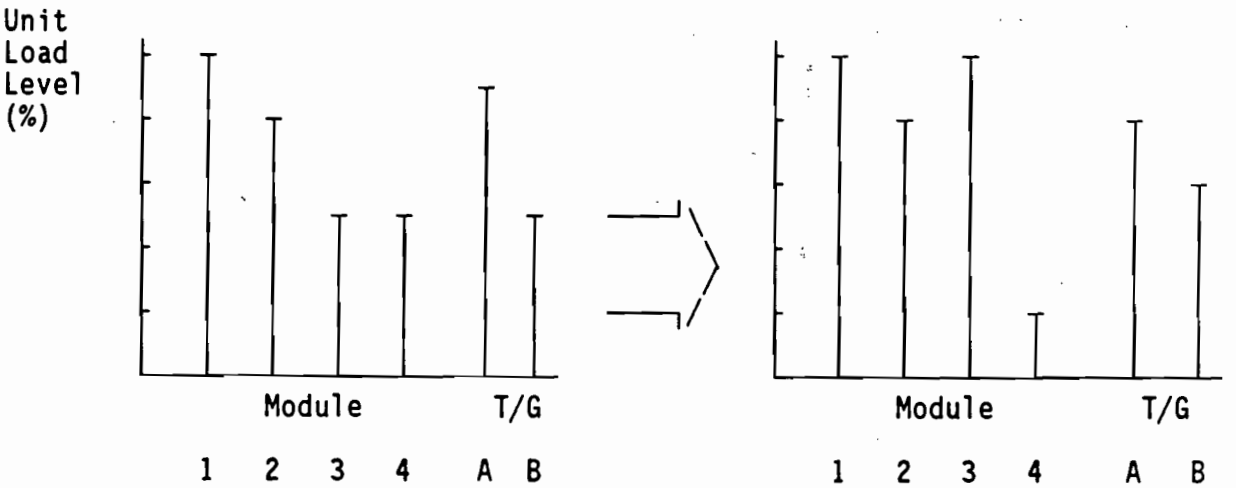
Strategy #18

An unequal load configuration is maintained following shutdown of a reactor module.

Basis for unequal load allocation:

Section 1	Requirements:	.070	.132	.155	.205	.370	.380
Section 2.3	Performance :	c)	i)				

Assumptions:
1) There is no grid dispatcher request for a change in plant output.
2) Constant plant output to the grid is desirable.



Module 4 is shutdown.

HTGR-86-052

HTGR

NSSS ANALYTICAL INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION

[redacted]

A[redacted]ent 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.

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 the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HTGR–86–052
908504/1

NSSS ANALYTICAL INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION

[redacted]

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

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

SEPTEMBER 1986

[redacted]

ROLL 2084

GA 1485 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY

TITLE				
NSSS Analytical Instrumentation Subsystem Design Description	☐ R & D ☐ DV & S ☒ DESIGN	APPROVAL LEVEL 5		

DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO.	ISSUE NO./LTR.
0	30 01	SSDD	6300	908504	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	JUL 11 1986	L. Weaver L.Weaver	C.Rodriguez F.Silady Interface Assurance R. Phelps	G.P.Connors	G.C.Bramblett		Initial Issue (HFD-43001) 6352.300.102

CONTINUE ON GA FORM 1485-1

Cover Sheets	= 2 (Unnumbered	A-1 through A-9	= 9
Issue summary 1,1a	= 2		
ii through xvii	=16	Total	69
1-1 through 1-17	=17		
2-1 through 2-7	= 7		
3-1	= 1		
4-1 through 4-6	= 6		
5-1	= 1		
6-1 through 6-4	= 4		
7-1 through 7-2	= 2		
8-1	= 1		
9-1	= 1		

[redacted]

NEXT INDENTURED DOCUMENTS

908446 (HFD-33000)

REV	1		0	↔		0																					
SH	1a		57	THRU		69																					
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

(LGLASNAPP.SDD4x350) SR-6899

ROLL 2084/rev. 1

GA 1485-1 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY CONTINUATION SHEET

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
NSSS Analytical Instrumentation Subsystem Design Description	908504	1

INFO 1

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: FUNDING PROJECT	APPROVAL: APPLICABLE PROJECT	ISSUE DESCRIPTION/ CWBS NO.
1	SEP 09 1986	L. Weaver	C.Rodriguez F. Silady Interface Assurance	G.P.Connors	G.C.Bramblett		HTGR cover added HTGR-86-052/0 (HFD-43001,Rev. 1) Class II Change 6301998201

LIST OF EFFECTIVE PAGES

SECTION	PAGE(S)	REV.
--	Cover	0
--	ii through xvii	
1	1-1 through 1-17	
2	2-1 through 2-7	
3	3-1	
4	4-1 through 4-6	
5	5-1	
6	6-1 through 6-4	
7	7-1 through 7-2	
8	8-1	
9	9-1	
Appendix A	A-1 through A-9	

TABLE OF CONTENTS

	PAGE
LIST OF EFFECTIVE PAGES	ii
LIST OF APPENDICES	vii
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS AND ACRONYMS	x
DEFINITIONS	xi
PREFACE	xv
SUMMARY	xvii
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-2
1.2.3 Structural Requirements	1-3
1.2.4 Environmental Requirements	1-5
1.2.5 Instrumentation and Control Requirements	1-7
1.2.6 Surveillance and In-Service Inspection Requirements	1-9
1.2.7 Availability Assurance Requirements	1-9
1.2.8 Maintenance Requirements	1-10
1.2.9 Safety Requirements	1-11
1.2.10 Codes and Standards Requirements	1-11
1.2.11 Quality Assurance Requirements	1-16
1.2.12 Construction Requirements	1-16
1.2.13 Decommissioning Requirements	1-17

TABLE OF CONTENTS (Continued)

	PAGE
2. DESIGN DESCRIPTION	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-1
2.3 Subsystem Performance Characteristics	2-5
2.3.1 Subsystem Operating Modes	2-5
2.3.2 Subsystem Steady-State Performance	2-6
2.3.3 Subsystem Response to Plant Transients	2-6
2.3.4 Subsystem Failure Modes and Effects	2-6
2.4 Subsystem Arrangement	2-7
2.5 Instrumentation and Control	2-7
3. COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS	3-1
4. SUBSYSTEM AND COMPONENT INTERFACES	4-1
4.1 Subsystem Interface Requirements	4-1
4.1.1 Interface Requirements Imposed on Other Systems and Subsystems Within Other Systems	4-1
4.1.2 Interface Requirements Imposed on Subsystems Within the Miscellaneous Control and Instrumentation Group	4-1

TABLE OF CONTENTS (Continued)

PAGE

4.2 Component Boundary Definition 4-1

4.2.1 Sensors 4-1
4.2.2 Electrical Transmission Boundaries 4-2

5. SUBSYSTEM CONSTRUCTION 5-1

6. SUBSYSTEM OPERATION 6-1

6.1 Subsystem Limitations, Setpoints, and Precautions 6-1

6.1.1 Subsystem Limitations and Setpoints 6-1
6.1.2 Precautions 6-2

6.2 Preoperation Checkout 6-2

6.3 Startup/Shutdown 6-2

6.3.1 Startup to 25% Steam Flow 6-2
6.3.2 Shutdown from 25%Steam Flow 6-2

6.4 Normal Operation 6-3

6.5 Refueling 6-3

6.6 Shutdown 6-3

6.7 Abnormal Operation 6-3

TABLE OF CONTENTS (Continued)

PAGE

6.8 Casualty Events and Recovery Procedures 6-3

6.8.1 Casualty Events 6-3

6.8.2 Design Features to Mitigate Effects of Casualty Events 6-4

6.8.3 Recovery Procedures 6-4

7. SUBSYSTEM MAINTENANCE 7-1

7.1 Maintenance Approach 7-1

7.2 Corrective Maintenance 7-1

7.3 Preventive Maintenance 7-1

7.4 In-Service Inspection 7-1

7.5 Surveillance 7-2

8. SUBSYSTEM DECOMMISSIONING 8-1

9. REFERENCES 9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability of Requirements	A-1

LIST OF ILLUSTRATIONS

		PAGE
2.2-1	Analytical Instrumentation System	2-2

LIST OF TABLES

		PAGE
1.2-1	Environmental Requirements for Portions of Analytical Instrumentation System Exposed to High Pressure Coolant	1-6
1.2-2	Surveillance Requirements	1-12
1.2-3	Analytical Instrumentation System Allocation of Annual Man-Rem Exposure from Plateout	1-13
1.2-4	Preventive Maintenance Requirements for Circuit Analysis	1-14
1.2-5	Industrial Codes and Standards Applicable to the Analytical Instrumentation Subsystem	1-15
4-1	Analytical Instrumentation Subsystem Interface Requirements Imposed on Other Systems and Subsystems With Other Systems	4-3
4-2	Interface Requirements Imposed on Other Subsystems Within the Miscellaneous Control and Instrumentation Group	4-6

LIST OF ABBREVIATIONS AND ACRONYMS

AIS	Analytical Instrumentation Subsystem
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrences
ASME	American Society of Mechanical Engineers
HVAC	Heating, Ventilating and Air Conditioning
IEEE	Institute of Electrical and Electronic Engineers
ISA	Instrument Society of America
ISI	In-service Inspection
MHTGR	Modular High Temperature Gas Cooled Reactor
NE	Nuclear Energy
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NNS	Nonnuclear Safety
NSSS	Nuclear Steam Supply System
OBE	Operating Basis Earthquake
OPDS	Overall Plant Design Specification
SSE	Safe Shutdown Earthquake

DEFINITIONS

Availability: The status of a major piece of equipment (or module) such that it is capable of service, whether or not it is actually in service.

Equivalent Full Power Hours: Module Operating Hours times Module Output (MW) divided by Module Rated Output (MW).

Condensible Vapors: For the purpose of this document, the radionuclides iodine, cesium, strontium, and silver which do condense on surfaces under reactor conditions.

Corrective Maintenance: Nonscheduled repair activity which requires that the component or system, and possibly the total NSSS, be taken out of service in order to restore the component or system to satisfactory conditions.

Function: A statement of what is to be achieved.

Goal: An endpoint or accomplishment towards which an effort is directed.

Grab Sample: A small quantity of primary coolant collected in a high pressure gas cylinder for later analysis in a radiological laboratory.

Group: Systems which have different requirements but collectively have a common function.

Interface Requirement: A requirement imposed by a system, subsystem or component on another system, subsystem, or component, which must be accomplished to facilitate satisfaction of a function(s) of the imposing system, subsystem or component.

Noble Gases: For the purpose of this document, the radionuclides argon, krypton, and xenon.

DEFINITIONS (Continued)

Noncondensible Gases: Gases which do not condense under reactor conditions. For the purpose of this document, the chemical impurities carbon monoxide, carbon dioxide, methane, nitrogen, hydrogen, oxygen, water; the noble gas radionuclides argon, krypton, and xenon; and the radionuclide tritium. Note that water may be present in the primary coolant as a vapor or liquid.

Non-Class 1E: All electrical equipment and sytems associated with the nuclear facility that are not class 1E.

Operating Basis Earthquake (OBE): The earthquake which could reasonably be expected to affect the plant site during the operating life of the plant and for which the normal operating systems of the power plant are designed to remain functional.

Outage: A major piece of equipment (or module) that is out of service.

Planned Outage: The removal of equipment (or a module) from service for inspection or overhaul which scheduled well in advance.

Plant Protection and Instrumentation System: System which monitors and protects plant systems and equipment to protect plant investment and to protect public health and safety.

Plateout: The depositing of condensible vapors from the primary coolant on surfaces within the vessel system.

Plateout Probe: A device for collecting condensible vapors on a surface for later analysis in a radiological laboratory.

DEFINITIONS (Continued)

Preventive Maintenance: The systematic servicing or replacement of parts plus inspection to assess and correct deterioration. Also includes performance testing to verify functional adequacy by periodic operational testing off-line.

Primary coolant Impurities: For the purpose of this document, noncondensible gases and condensible vapors.

Radionuclide: A radioactive nuclide.

Safe Shutdown Earthquake (SSE): That earthquake for which those structures, systems and components are designed to ensure:

1. The integrity of the reactor coolant pressure boundary.

2. The capability to shutdown the reactor and maintain it in a safe shutdown condition.

3. Continued reactor core decay heat removal.

Safety Class 1E: Electrical equipment and systems that are essential to an emergency reactor shutdown, confinement isolation, reactor core cooling and confinement and reactor heat removal or otherwise are essential in preventing significant release of radioactive material to the environment.

Seismic Category I: Those structures, systems and components that are designed to remain safely functional during and after an earthquake, as designated in Regulatory Guide (RG) 1.29.

Surveillance: Continuing, periodic examination of specimens or components to ensure adequacy.

DEFINITIONS (Continued)

System: A collection of electrical, mechanical and/or structural components and associated software and human actions treated as a unit for technical, administrative or contractural purposes.

Tritium: A radioactive isotope of hydrogen with two neutrons and one proton in the nucleus.

PREFACE

The objective of the MHTGR plant project 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 MHTGR plant (Ref. 1.1). 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

This document contains the Subsystem Design Description for the NSSS Analytical Instrumentation System (AIS), a subsystem of the Miscellaneous Control and Instrumentation Group. The subsystem consists of a depressurization rack and an analytical instrument module. The depressurization rack reduces the pressure of the incoming gas samples to the required operating pressure of the analytical instruments. The analytical instrument module contains the analytical instruments, signal conditioning and interfacing electronics.

The function of the Analytical Instrumentation System is to monitor circulating primary coolant impurities and circulating/plateout radioactivity.

The Analytical Instrumentationn System fulfills this function by providing analytical instrumentationn and radiation monitoring equipment to detect, identify and measure important primary coolant impurities which include both stable and radioactive impurities in the Vessel System, Helium Purification Subsystem and Gaseous Radioactive Waste Subsystem. The AIS also provides gamma and airborne activity measurements in the vicinity of and within the AIS to provide operator protection from radiological exposure. Included within the AIS are the associated piping and controls needed for gas sampling and sample conditioning, as well as primary coolant impurity detection, identification and measurement.

The monitored primary coolant impurities include noncondensible gases (gases which do not condense under reactor conditions) and condensible vapors. The noncondensible gases consist of the stable impurities carbon monoxide (CO), carbon dioxide (CO_2), hydrogen (H_2), methane (CH_4), nitrogen (N_2), oxygen (O_2), water (H_2O); the noble gas radionuclides argon (Ar), krypton (Kr) and xenon (Xe); and the radionuclide tritium. Also, water may be present in the primary coolant as a vapor or liquid. The important condensible vapors are the radionuclides iodine (I_2), cesium (Cs), strontium (Sr), and silver (Ag).

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SUBSYSTEM FUNCTIONS

The function of the NSSS Analytical Instrumentation System (AIS) is to monitor primary coolant impurities in Goals 1 and 2 and monitor primary coolant circulating and plateout radioactivity in Goals 1, 2, and 3.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

The AIS shall include two major features. One is the sample depressurization, performed in the depressurization rack. It shall contain pressure regulators and a piping distribution manifold for reducing primary coolant to a pressure low enough to be piped into the gas analysis instruments. (3001.0102.001)

The other is the measurement function, performed by the analytical instrument module. It shall contain instruments for the detection of primary coolant impurities. The analytical instrument module is fed primary coolant from the depressurization rack. (3001.0102.002)

After analysis, the primary coolant shall be discharged into the plant Gaseous Radioactive Waste System. (3001.0102.003)

Grab sample points shall be located in the analytical instrument module for obtaining samples for laboratory analysis. (3001.0102.004)

1.2.2 Operation Requirements

The AIS shall perform the functions and provide for the equipment and the operation of the AIS as follows:

1. Measure the following primary coolant impurities in the reactor circulating primary coolant automatically with on-line instruments: carbon monoxide (CO), carbon dioxide (CO_2), hydrogen (H_2), methane (CH_4), nitrogen (N_2), oxygen (O_2), water (H_2O), and the radionuclides iodine (I_2), argon (Ar), krypton (Kr), xenon (Xe), and tritium. (3001.0102.010)

2. Measure the same primary coolant impurities in the reactor circulating primary coolant automatically when requested by a preprogrammed command signal from a human operator. (3001.0102.011)

3. Provide the capability to measure condensible vapor plateout in the thermally hot circulating reactor primary coolant. (3001.0102.012)

4. Provide real time electronic output information regarding the overall primary coolant impurity status. (3001.0102.013)

5. Provide on-line calibration and maintenance capabilities during reactor power operation. (3001.0102.014)

6. Primary coolant impurity measurement accuracy and sensitivity as specified in paragraph 1.2.5, Instrumentation and Control Requirements. (3001.0102.015)

7. Provide grab sample points for obtaining bulk samples of primary coolant for analysis in either the AIS or in the radiological laboratory. (3001.0102.016)

8. Depressurization of primary coolant samples from reactor pressure to a low enough level to be measured by analytical instruments. This shall be done in a way that provides maximum safety to the human operator from both pressure and radiation in both the analytical instrument mode and depressurization rack. (3001.0102.017)

9. Automatically and continuously monitor primary coolant sensing lines to detect primary coolant leaks. (3001.0102.018)

10. Immediately and automatically isolate primary coolant sensing lines when a leak is detected. (3001.0102.019)

11. Protect human operators from radiation exposure. (3001.0102.020)

The AIS shall be designed for a 40-year service lifetime. (3001.0102.021)

The design of the AIS shall incorporate human factors engineering. The integration of plant operators and mechanical and electronic components shall be optimized to effectively achieve the objective of economical, safe production of steam and electrical power. (3001.0102.022)

1.2.3 Structural Requirements

1.2.3.1 Mechanical

The AIS shall be designed for a 40-year life. The structure for the analytical instrument mode and the depressurization rack shall be fabricated of welded steel. It shall have provisions for welding and bolting to the floor and walls. (3001.0102.030)

1.2.3.2 Seismic

The depressurization rack and all passive and active components within the depressurization rack that contain primary coolant or could contain primary coolant during any reactor operational phase, including shutdown, startup, refueling, and any standby condition, shall be seismic category Non CAT I. (3001.0102.040)

Electrical control signals to and feedback signals from all components shall be non-class 1E but shall be powered from a highly reliable power supply. (3001.0102.041)

The depressurization rack portion of the AIS shall be designed to operate through and after the operating basis earthquake (OBE). (3001.0102.042)

Piping, valves, instruments and passive engineered piping specialities that are primary coolant pressure boundaries shall continue to maintain their pressure boundary function during and after the OBE. (3001.0102.043)

Valves, instruments, and other active devices shall also continue to perform their function during and after the OBE. (3001.0102.044)

The response spectra for the OBE where the depressurization rack is located is shown in Fig. [Later]. The maximum ground acceleration for the OBE is [Later].

Piping valves, instruments, and passive engineered piping specialities that are primary coolant pressure boundaries shall continue to maintain their pressure boundary function during and after the safe shutdown earthquake (SSE). (3001.0102.045)

The response spectra for the SSE where the depressurization rack is located is shown in Fig. [Later]. The maximum ground acceleration for the SSE is [Later]. Valves, instruments, and other active devices that are not pressure boundaries are not required to function during or after the SSE. (3001.0102.046)

1.2.3.3 Material

[Later]

1.2.4 Environmental Requirements

Portions of the AIS exposed to primary coolant from the reactor to the primary side of the pressure regulation system shall be designed for the chemical impurities shown in Table 1.2-1. (3001.0102.060)

Portions of the AIS exposed to the reactor confinement building environment shall be designed for the following environmental conditions: (3001.0102.061)

Condition	Normal	Abnormal
Temperature, max °C (°F)	[Later]	[Later]
Temperature, min °C (°F)		
Relative humidity, max %		
Relative humidity, min %		
Pressure, psig		5
Nuclear irradiation	Negligible	Negligible

Table 1.2-1

ENVIRONMENTAL REQUIREMENTS FOR PORTIONS OF ANALYTICAL INSTRUMENTATION SYSTEM EXPOSED TO HIGH PRESSURE COOLANT

Chemical Impurities in Primary Coolant	Design Conditions At Rated Power	Maximum Allowable Value	
		Below 530°C (1000°F)	Above 538°C (1000°F)
Nonradioactive	[Later]	[Later]	[Later]
Carbon monoxide, CO			
Carbon dioxide, CO_2			
Chlorine compounds			
Hydrogen, H_2			
Methane, CH_4			
Nitrogen, N_2			
Oxygen, O_2			
Sulfur compounds			
Water, H_2O (moisture)			
Radioactive			
Iodine, I_2			
Argon, Ar			
Krypton, Kr			
Xenon, Xe			
Tritium			
Dust			

The remainder of the AIS consists of electronic equipment located in the [Later]. It shall be designed for the following environmental conditions: (3001.0102.062)

Condition	Normal	Abnormal
Temperature, max °C (°F)	[Later]	[Later]
Temperature, min °C (°F)		
Relative humidity, max %		
Relative humidity, min %		
Pressure, psig		
Nuclear irradiation	Negligible	Negligible

1.2.5 Instrumentation and Control Requirements

The AIS design shall minimize radiation exposure to plant personnel by locating all components in very low radiation areas. Shielding shall be used to the maximum extent possible to minimize personnel exposure to radiation. (3001.0102.070)

Area radiation monitoring shall be provided in the AIS area to detect and alarm radiation leaks from the primary coolant. (3001.0102.071)

Instrument sample ports shall be provided to sample circulating primary coolant and purified helium from the Helium Purification System. (3001.0102.072)

A penetration and handling means shall be provided in the hot circulating primary coolant for inserting and withdrawing an instrument to measure plateout. (3001.0102.073)

A depressurization rack shall be provided to decrease the pressure of the primary coolant samples from reactor pressure to that usable by the analytical instruments in the AIS. (3001.0102.074)

An analytical instrument module shall be provided containing instruments to detect CO, CO_2, CH_4, N_2, H_2, O_2, H_2O, and the radionuclides iodine, argon, krypton, xenon, and tritium. Monitoring shall be on-line and shall be done automatically as determined by a microprocessor-based sequencer. A human operator will program the sequence. (3001.0102.075)

The AIS shall also have the capability for a human operator to take manual grab sample and request trend information "on demand." Instrument range and accuracy is listed below for each measurement. (3001.0102.076)

Primary Coolant

Impurity Measurement	Range	Accuracy
Nonradioactive	{1.0 ppmv* - 10,000 ppmv}**	{±10%} of reading
Carbon monoxide, CO	[Later]	[Later]
Carbon dioxide, CO_2		
Hydrogen, H_2		
Methane, CH_4		
Nitrogen, N_2		
Oxygen, O_2		
Water, H_2O (moisture)		
Radioactive		
Iodine, I_2		
Argon, Ar		
Krypton, Kr		
Xenon, Xe		
Tritium		
Area radiation		

*ppmv = parts per million by volume.
**Numbers in {braces} are approximate values and subject to change.

1.2.5.2 Special Nuclear Area Instrumentation Subsystem

The AIS shall provide preprocessed primary coolant impurity status information to the Special Nuclear Area Instrumentation Subsystem of the Plant Protection and Instrumentation System. (3001.0102.077)

1.2.5.3 Bypasses

The AIS has no operating or maintenance bypasses.

1.2.6 Surveillance and In-Service Inspection Requirements

This subsystem does not perform a safety-related function and therefore no safety-related surveillance and/or in-service inspection is required.

Requirements in this category needed to satisfy the Integrated Approach Goals 1, 2, and 3 are covered under "Maintenance Requirements" in Section 1.2.8.

1.2.7 Availability Assurance Requirements

Planned outage is defined as that required for equipment inspection, surveillance, and preventive maintenance. The AIS shall not contribute to the planned outage of a single reactor module by more than [later] h/yr. (3001.0102.100)

The AIS shall not contribute to the average unplanned reactor module outage by more than [later] h/yr. (3001.0102.101)

Features shall be included in the AIS design to minimize recovery time to resumption of normal operation if an outage does occur. (3001.0102.102)

AIS 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. (3001.0102.103)

The equivalent full power hours lost per year due to the failure of the AIS to detect CO and H_2O to the required accuracy shall be less than [later] h/yr. (3001.0102.104)

The equivalent full power hours lost per year due to the failure of the AIS to detect CO_2, CH_4, N_2, H_2, and O_2 shall be less than [later] h/yr. (3001.0102.105)

The average equivalent full power hours lost per year due to the failure of the AIS to measure the radionuclides iodine argon, krypton, xenon, and tritium shall be less than [later] h/yr.

Sufficient reliability shall be provided to assure that the probability of exceeding the protective action guidelines limits is less than 5×10^{-7} per plan year (user). (3001.0102.106)

Sufficient reliability shall be provided to assure that the probability of exceeding the 10CFR100 limits is less than 1×10^{-4} per plant year (reg.). (3001.0102.107)

1.2.8 Maintenance Requirements

The AIS shall be designed, arranged, and equipment and components located in the plant to facilitate on-line maintenance. (3001.0102.120)

Portions of the AIS located at the primary coolant pressure boundaries shall be designed to function continuously without requiring maintenance except during a planned maintenance period. (3001.0102.121)

The AIS shall be designed to permit installation, maintenance, testing, removal, and replacement of all components during on-line operation excepting only the primary coolant double root valves in the primary coolant sample lines. (3001.0102.122)

The AIS shall be designed to permit surveillance to detect leakage, structural distress, and corrosion of the instrument sample lines. Table 1.2-2 lists the requirements for this examination. (3001.0102.123)

The AIS shall be designed to accommodate preventive maintenance, while limiting personnel radiation exposure within the level listed in Table 1.2-3. (3001.0102.124)

1.2.8.1 Preventive Maintenance

Preventive maintenance shall be done on the AIS to predict failures of mechanical and electrical components early enough to avoid unnecessary shutdowns. Table 1.2-4 lists the PM requirements. (3001.0102.125)

1.2.8.2 Corrective Maintenance

Preventive maintenance shall be identified and planned with emphasis on eliminating unplanned maintenance shutdowns. (3001.0102.126)

1.2.9 Safety Requirements

The design of the AIS shall satisfy the licensing methodology for the MHTGR. Under this methodology, this system is not safety-related. (3001.0102.127)

1.2.10 Codes and Standards Requirements

The AIS shall meet the other industrial standards as shown in Table 1.2-5. (3001.0102.140)

Table 1.2-2

SURVEILLANCE REQUIREMENTS

Method	Visual, surface.
Frequency	First inspection after 5 years. Thereafter, every 10 years.
Approach	On-line visual inspection of supports. Off-line surface inspection of integrally welded supports and piping welds after purging and verifying radiation levels and shielding requirements.
Access	Manual
Layout	Lines are run shielded in raceways or individually.
Complexity	Moderate (because of potential radiation complexity; otherwise, very easy).
Equipment/Tools	Dye penetrant, bright light, mirror, magnifying lens, ultrasonic inspection device.
Radiation Level	High. Must be monitored before and during test.
Human Factors	Must have direct (hands-on) access to all welds.
Other	Acceptance standard is no evidence of leakage, structural distress, or corrosion.

Table 1.2-3

ANALYTICAL INSTRUMENTATION SYSTEM
ALLOCATION OF ANNUAL MAN-REM EXPOSURE
FROM PLATEOUT

Activity	Man-rem/yr
Surveillance	[Later]
Planned maintenance	
Corrective maintenance	

Table 1.2-4

PREVENTIVE MAINTENANCE REQUIREMENTS FOR CIRCUIT ANALYSIS

Method	Computer based automatic signal analysis.
Frequency	Every 12 hours for signal pattern recognition, and yearly for calibration check.
Approach	Every 12 hours, surveillance computers automatically analyze signal trends and noise. Every year, a hands-on calibration check is performed on every measurement channel.
Access	Job is performed mainly via computer-depressurization rackiven graphic displays and hard copies. Hands-on calibration is via quick disconnect ports and data entry terminals.
Layout	Two independent surveillance computers to monitor measurement channels and cross-check each other.
Complexity	Moderate. Most of the work is done automatically by computers.
Equipment/Tools	Calibration sources, portable scope and access to signatures in surveillance data base.
Radiation Level	Low to high in about 50% of this surveillance effort, mainly in connection with primary coolant related measurements.
Human Factors	Quick disconnect calibration ports. Graphic displays. Administrative control of data entry.
Other	Acceptance standard is to minimize the number of failures in data channels and displays so as to meet plant availability.

Table 1.2-5

INDUSTRIAL CODES AND STANDARDS APPLICABLE TO THE ANALYTICAL INSTRUMENTATION SUBSYSTEM

A. IEEE Standards, Institute of Electrical and Electronic Engineers

IEEE-61, National Electric Safety Code

B. ANSI Standards, American National Standards Institute

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities

ANSI/ASME B31.1, Power Piping

C. NEMA Standards, National Electrical Manufacturers Association

NEMA-1CS1-78, General Standards for Industrial Control & Systems

D. National Electric Code, National Fire Protection Association

NFPA 70 National Electrical Code

E. ISA Standards, Instrument Society of America

ISA S12-11 Electrical Instruments in Hazardous Dust Locatiobns

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. System-level documents are assigned the QAL classification that corresponds to the highest QAL of any item in the system. Therefore, this SDD is classified as QAL II. (3001.0102.160)

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. (3001.0102.161)

1.2.12 Construction Requirements

The AIS equipment and arrangement features shall facilitate manufacture, installation, and removal of equipment on a modular basis. (3001.0102.170)

The design of the AIS shall incorporate materials, processes, and parts for civil, structural, mechanical, electrical, and instrumentation systems and their components as required to meet all transportation, handling, storage, construction, and operational functions. Appropriate specifications, codes, and code class and design categories shall be identified and used in order to meet the safety, economic, and reliability goals identified for the MHTGR design. As appropriate, materials specifications shall be in accordance with the applicable portions of the "Nuclear Systems Materials Handbook" (Ref. 1.2). (3001.0102.171)

1.2.13 Decommissioning Requirements

The AIS design shall include materials, configurations, and features that minimize the volume of activated and contaminated materials, radiation levels, radiation exposure and the time and cost of decommissioning. (3001.0102.190)

Until more specific criteria and/or rules are developed, NUREG-0586, Ref. 1.3, shall be used as guidance for the AIS design. (3001.0102.191)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The Analytical Instrumentation System (AIS) provides analytical instrumentation and radiation monitoring equipment to detect, identify and measure important primary coolant impurities which include both stable and radioactive impurities in the Vessel System, Helium Purification Subsystem, and Gaseous Radioactive Waste Subsystem. The AIS also provides gamma and airborne activity measurements in the vicinity of and within the AIS to provide operator protection from radiological exposure. Included within the AIS are the associated piping and controls needed for gas sampling and sample conditioning as well as primary coolant impurity detection, identification and measurement.

The monitored primary coolant impurities include noncondensible gases, (gases which do not condense under reactor conditions) and condensible vapors. The noncondensible gases consist of the stable impurities carbon monoxide (CO), carbon dioxide (CO_2), methane (CH_4), nitrogen (N_2), hydrogen (H_2), oxygen (O_2), water (H_2O); the noble gas radionuclides argon (Ar), krypton (Kr), and xenon (Xe); and the radionuclide tritium. Also, water may be present in the primary coolant as a vapor or liquid. The important condensible vapors are the radionuclides iodine (I_2), cesium (Cs), strontium (Sr), and silver (Ag.)

2.2 SUBSYSTEM CONFIGURATION

The AIS automatically extracts samples of circulating primary coolant from the Vessel, Helium Purification, and Gaseous Waste Systems, Fig. 2.2-1. It detects, identifies, and measures the presence and quantity of primary coolant noncondensible gases as well as iodine and provides this data to

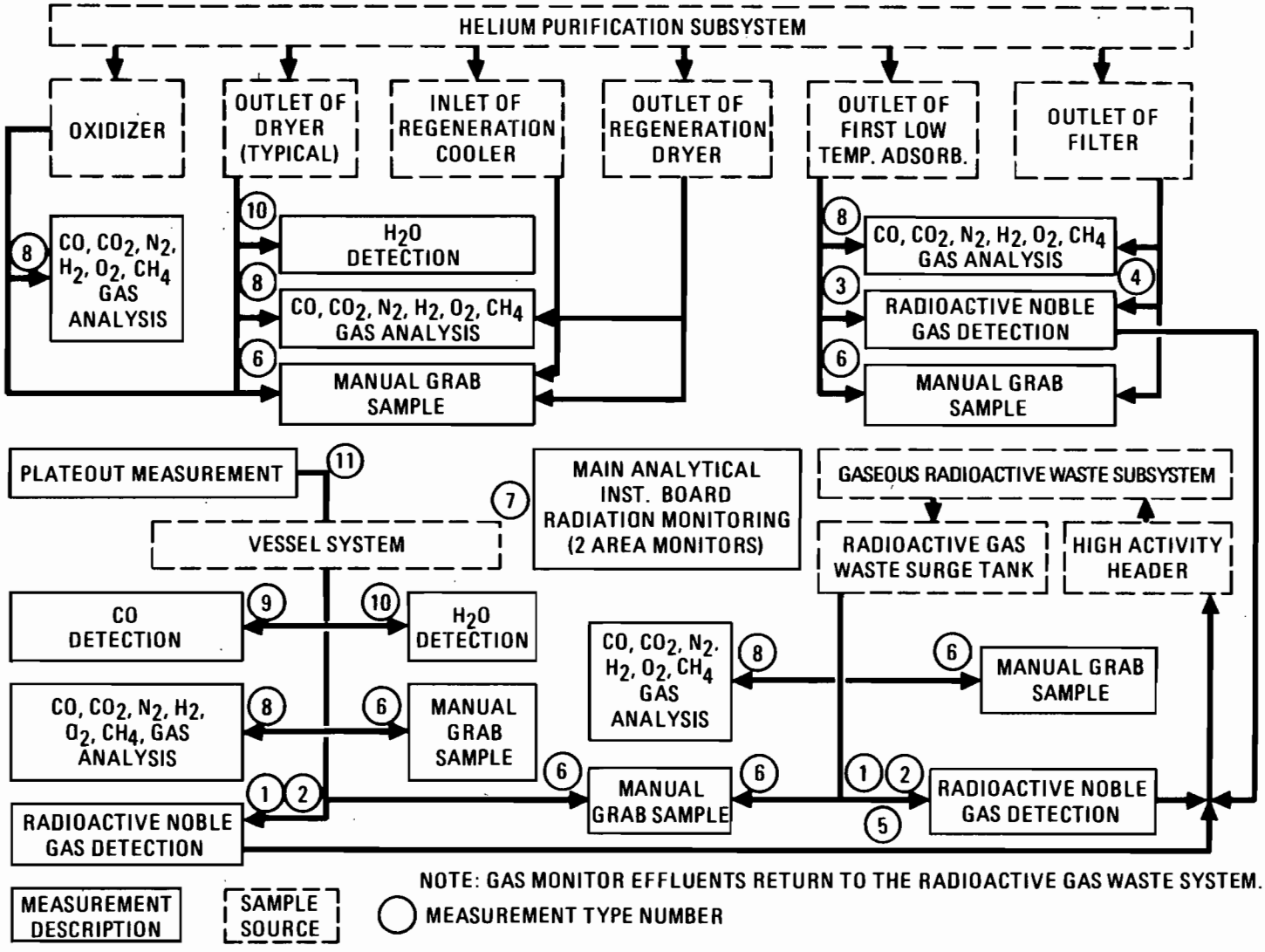


FIGURE 2.2-1 ANALYTICAL INSTRUMENTATION SUBSYSTEM.

plant personnel to confirm primary coolant quality and satisfactory operation of the Helium Purification System.

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

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

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

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

The sample piping and valves are sized to minimize flow rates. Means are included for measuring sample pressures, flow rates, and for detecting low flows.

Eleven types of measurements are needed for process radiation and primary coolant impurity monitoring. Each type monitors a process activity or

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

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

Measurement Type Number	Description
1.	Continuous monitoring of gross radioactivity to detect changes in primary coolant noble gas concentration to provide process control checks.
2.	Provision for sampling of primary coolant for tritium analysis.
3.	Detection of noble gas breakthrough from first low temperature adsorber in the Helium Purification Subsystem.*
4.	Measures noble gas activity in outlet of filter downstream of Helium Purification System second low temperature adsorber to provide process control.
5.	Measurement of noble gas activities in the Radioactive Gaseous Waste Subsystem surge tanks.

*Types 3 and 4 use the same radiation monitor.

Measurement Type Number	Description
6.	Provision for manual grab sampling of primary coolant for tritium analysis or other radionuclides.
7.	Measurement of gamma airborne activity changes in enclosed area of analytical instrument module. Two monitors are used.
8.	Chemical impurity monitoring of primary coolant.
9.	On-line monitoring for carbon monoxide in primary coolant.
10.	On-line monitoring of primary coolant for water in Vessel and Helium Purification Systems.
11.	Manually removable probe to detect primary coolant condensible vapor plateout.

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

2.3.1 Subsystem Operating Modes

The system is normally operated in the automatic mode. A human operator programs a programmable controller to automatically take samples of primary coolant and insert them into either a process chromatograph for primary coolant impurity analysis or radiation monitors for analysis of tritium, iodine and noble gases. A separate monitor continuously monitors carbon monoxide in the Vessel System.

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

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

2.3.2 Subsystem Steady-State Performance

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

2.3.3 Subsystem Response to Plant Transients

Except for a loss of electrical power in AOO-1, plant transients have no effect on the operation of the AIS. A loss of electrical power will not result in any failures or release of radioactive gases. When power is restored, the AIS will return to steady state operation as described in 2.3.2.

2.3.4 Subsystem Failure Modes and Effects

The AIS has two failure modes. The first is if the annalytical instruments fail or provide an incorrect analyses of primary coolant impurities. If this happens, the failure would not affect short term reactor operation. Even though failed, the system will record diagnostic graphic data in the control room to help determine the cause of the failure by manual analyses.

The second failure is a radioactive gas leak in the sample piping and valves from the Vessel System, Gaseous Radioactive Waste Subsystem, Helium Purification Subsystem, or internal to the AIS. If this happens, airborne activity monitors would alarm this condition and automatically isolate the system.

2.4 SUBSYSTEM ARRANGEMENT

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

2.5 INSTRUMENTATION AND CONTROL

Since the AIS is an instrument system, it does not require any additional instruments or controls.

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

[Later]

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

4.1.1 Interface Requirements Imposed on Other Systems and Subsystems Within Other Systems

Interface requirements at the system level are presented in tabular form in Table 4-1 for each system and subsystem on which requirements are imposed. The tabulation includes brief descriptive statements of the nature of the interface, identification of the interfacing components and interfrace requirements.

4.1.2 Interface Requirements Imposed on Subsystems Within the Miscellaneous Control and Instrumentation Group

Interface requirements, at the subsystem level, are presented in tabular form in Table 4-2 for the subsystems within the Miscellaneous Control and Instrumentation Group on which requirements are imposed.

4.2 COMPONENT BOUNDARY DEFINITION

4.2.1 Sensors

The boundary for each sensor that monitors or controls process conditions is the point at which the sensor penetrates the process pipe or vessel. (3001.0401.130)

For temperature or other measurements requiring thermowells, the thermowells may be specified and supplied with the NSSS. Or, they may be specified by the NSSS supplier and supplied by others. For sensors not requiring thermowells and for instruments requiring flanges or other appurtenances, the boundary shall be the point at which they touch the pipe or vessel wall. (3001.0401.131)

These type of instruments are supplied by the NSSS supplier. Flanges may be supplied by others as long as they are specified by the NSSS supplier.

4.2.2 Electrical Transmission Boundaries

There are two types of electrical boundaries. One is a multiplexing panel connected to one of the redundant data buses in the plant. In this case, the boundary is the electrical screen or crimp terminal strip at the multiplexer where the electrical wires from the field sensors are connected. (3001.0401.140)

For instrumentation with special requirements (e.g., temporary or hardwired) that is not connected to the multiplex bus, the boundary is the electrical terminal strip where the sensor or final control element is attached. This may be in a field control panel or on an instrument rack. For remotely actuated process valves, the terminal strip is on the valve actuator. (3001.0401.141)

TABLE 4-1

ANALYTICAL INSTRUMENTATION SUBSYSTEM INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interfacing Systems (with Subsystem Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Vessel System (1100)			
(Vessel and Ducts Subsystem) (1106)	Provides primary coolant samples.	Reactor vessel top head penetration for connection of AIS sample line.	Quantity: [TBD] m^3/s (scfm) flow of primary coolant. (3001.0401.001)
	Provides access to primary coolant.	Steam generator vessel bottom head penetration for plateout probe insertion.	Expose plateout probe to primary coolant. (3001.0401.002)
Reactor Services Group (2000)			
(Helium Purification Subsystem) (2023)	Provide helium samples.	Penetrations for connection of AIS sample lines.	Quantity: [TBD] m^3/s (scfm) flow of sample helium from [TBD] penetrations. (3001.0401.010)
(Liquid Nitrogen Subsystem) (2025)	Provide liquid nitrogen for portable dewars used in sample treatment.	Connection to AIS.	Quantity: [TBD] kg/day (lb/day) of liquid nitrogen. (3001.0401.011)
Gaseous Radioactive Waste Subsystem (2064)	Provides helium samples.	Penetration for connection of AIS sample line.	Quantity: [TBD] m^3/s (scfm) flow of sample helium. (3001.0401.012)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem Identification)	Nature of Interface	Interfacing Component	Interface Requirements
	Receives gaseous waste from AIS.	Connection of AIS gaseous waste lines.	Quantity: [TBD] m^3/s (scfm) flow of gaseous waste (3001.0401.013)
Plant Protection and Instrumentation System (3200)			
(Special Nuclear Area Instrumentation Subsystem) (3203)	Receives AIS status signals.	Connections to AIS.	Quantity: Digital signals. (3001.0401.030)
Plant Control Data and Instrumentation System (3700)			
(NSSS Control Subsystem) (3701)	Receives AIS status signals.	Connections to AIS.	Quantity: Digital signals. (3001.0401.040)
Heat Rejection Group (5200)			
Circulating Water Subsystem (5241)	Provide cooling water.	Connections to AIS.	Quantity: [TBD] m^3/s (gpm) flow of [TBD]°F cooling water. (3001.0401.050)
Building Structures and Building Service Group (7000)			
(Reactor Building Subsystem) (7001)	Structural support.	Concrete floor.	Quantity: [TBD] m^2 (ft^2) of floor space. (3001.0401.060)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Mechanical Services Group (9000)			
(HVAC Subsystem) (9011)	Provide room cooling for equipment.	Connections to AIS.	Quantity: [TBD] m^3/s (scfm) flow of [TBD] °C (°F) cooled air. (3001.0401.070)
Electrical Group (9200)			
(Non-class 1E AC Distribution Subsystem) (9202)	Power to equipment.	Electrical connections to AIS.	Quantity: The electrical power requirements are:

Voltage	Phase	Power
120 Vac	1 Ø	29.4 kW
120 Vac	1 Ø	74.6 kW (100 hp)

Table 4-2

INTERFACE REQUIREMENTS IMPOSED ON OTHER SUBSYSTEMS
WITHIN THE MISCELLANEOUS CONTROL AND INSTRUMENTATION GROUP

Interfacing Subsystems (with Subsystem Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Misc. Control and Instrumentation Group (3000)			
(Radiation Monitoring Subsystem) (3003)	Receives AIS output signals.	Connections to AIS.	Quantity: Digital signals. (3001.0401.100)

SECTION 5

SUBSYSTEM CONSTRUCTION

[Later]

SECTION 6

SUBSYSTEM OPERATION

6.1 SUBSYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

6.1.1 Subsystem Limitations and Setpoints

There are no limitations on operation of the AIS except to ensure that any radioactive gas leakage is detected, contained, and the source isolated.

Alarm set points for detection of primary coolant impurities are as follows:

Impurity	Range	Alarm Setpoint
Nonradioactive	[Later]	[Later]
Carbon monoxide, CO		
Carbon dioxide, CO_2		
Hydrogen, H_2		
Methane, CH_4		
Nitrogen, N_2		
Oxygen, O_2		
Water, H_2O (Moisture)		
Radioactive		
Iodine, I_2		
Argon, Ar		
Krypton, Kr		
Xenon, Xe		
Tritium		
Area radiation		

6.1.2 Precautions

When human operators are working at the analytical instrument mode control panel, precaution must be taken against exposure from radiation in the primary coolant, gases radioactive waste, and purified helium gas samples. This is especially true when grab samples are being taken.

6.2 PREOPERATIONAL CHECKOUT

Prior to flowing any sample gas into the AIS, the depressurization rack and analytical instrument mode must be pressurized and helium leak tested. The depressurization rack must be leak tested at full reactor test pressure to ensure that a leak will not develop in the depressurization rack if primary coolant pressure increases to the reactor relief valve pressure.

After the leak test, electrical power and cooling water (if used) must be connected to the analytical instrument mode. The depressurization rack requires only electrical power. A complete functional test including calibration shall then be performed.

6.3 STARTUP/SHUTDOWN

6.3.1 Startup to 25% Steam Flow

Operation is as during normal operation except that a pump is used when sample source pressure is inadequate.

6.3.2 Shutdown from 25% Steam Flow

Operation is as durinhg normal operation except that a pump is used when sample source pressure is inadequate.

6.4 NORMAL OPERATION

During normal plant operation the AIS automatically samples primary coolant from the Vessel System, the Helium Purification Subsystem, and Gaseous Radioactive Waste Subsystem, maintains a data base of information and actuates alarms when Primary coolant impurities are excessive. A human operator preprograms the AIS to sample in a certain sequence and at a certain rate and starts the programmable controller. The rest is done automatically.

6.5 REFUELING

Operation is as during normal operation except that a pump is used when sample source pressure is inadequate.

6.6 SHUTDOWN

Operation is as during normal operation except that a pump is used when sample source pressure is inadequate.

6.7 ABNORMAL OPERATION

Operation is as during normal operation except that a pump is used when sample source pressure is inadequate.

6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES

6.8.1 Casualty Events

Radioactive gas leaks are the only casualty events that could occur in this system.

6.8.2 Design Features to Mitigate Effects of Casuality Events

The design must incorporate automatic detection of radioactive gas leaks and automatic isolation of the source(s) of those leaks. It must also provide biological shielding to protect human operators during grab sample taking.

6.8.3 Recovery Procedures

Recovery from radiation dispersion due to a radioactive pressure boundary rupture is to decontaminate the area and replace the leaking component. If the component is a root valve on a vessel or pipe containing primary coolant, the system or reactor must first be shut down.

SECTION 7

SUBSYSTEM MAINTENANCE

7.1 MAINTENANCE APPROACH

By performing preventive maintenance based on the manufacturer's recommended replacement interval, corrective maintenance will only be minimal. Visual and surface inspection will be used to inspect pipes, valves, and engineered piping specialties. On-line surveillance computer techniques will be used to detect early failure trends in electrical and electronic equipment.

7.2 CORRECTIVE MAINTENANCE

It is not expected that corrective maintenance will be necessary since failure will be detected early by the preventive maintenance program. If corrective maintenance is required, the affected component will be isolated and repaired without affecting reactor operation.

7.3 PREVENTIVE MAINTENANCE

The preventive maintenance program will utilize equipment supplier's recommended replacement interval data to predict early failures. Components will be replaced prior to their predicted failure time to avoid unscheduled downtime.

7.4 IN-SERVICE INSPECTION

Not required because the AIS does not perform a safety related function.

7.5 SURVEILLANCE

Surveillance will be performed on electrical and electronic equipment automatically by the plant surveillance computers. Manual surveillance of pipes, valves, and engineered piping specialties will be performed by visual and surface inspection techniques. Refer to Tables 1.2-1, 1.2-2 and 1.2-3.

SECTION 8

SUBSYSTEM DECOMMISSIONING

[Later]

SECTION 9

REFERENCES

1.1. "Overall Plant Design Specification, Modular High Temperature Gas Cooled Reactor," HTGR-86-004, Rev. 1, (HFS-20100, Rev. 1) (908397/2), February 18, 1986.

1.2. Nuclear Systems Materials Handbook [TBD].

1.3 Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities, NUREG-0586, January 1981.

APPENDIX A

TRACEABILITY OF REQUIREMENTS

1. INTRODUCTION

This appendix provides traceability of requirements to sources within the OPDS and to sources in external documents. The requirement traceability summary (Table A-1) identifies the requirement as outlined below, provides a summary description, and identifies the source. Table A-2 is a list of the references which are identified as sources in Table A-1.

Each requirement is given a traceability number which is composed of three groups of digits. The first group identifies the system (e.g., 01 is used for multi-systems and for the OPDS); the second group identifies the section and subsection numbers of this document where the requirement is located (e.g., 0202 for OPDS Section 2, Subsection 2); and the third group identifies the sequential requirement number (e.g., 001 for Requirement 1).

Table A-1

ANALYTICAL INSTRUMENTATION SUBSYSTEM TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0102.001	Depressurization rack shall contain primary coolant pressure reducing manifold.	1	5.11
3001.0102.002	AIM shall contain analytical instruments to detect primary coolant impurities.	1	5.11
3001.0102.003	After analysis, primary coolant shall be discharged to gas waste system.		
3001.0102.004	Grab sample points shall be located in AIM.		
3001.0102.010	With on-line instruments, measure CO_2, CO, H_2O, CH_4, N_2, H_2, O_2, and radionuclides I_2, Ar, Kr, Xe and tritium.		
3001.0102.011	Measure the same impurities (as in 3001.0102.010) on demand with a programmed command signal from human operator.		
3001.0102.012	Provide capability to measure condensible vapor plateout in thermally hot circulating primary coolant.		
3001.0102.013	Provide real time electronic output information regarding overall primary coolant impurity status.		
3001.0102.014	Provide on-line calibration and maintenance during power operation.		
3001.0102.015	Primary coolant impurity measurement accuracy and sensitivity per Para. 1.2.5.		
3001.0102.016	Provide bulk grab sample points for analysis in AIS or radiological laboratory.		
3001.0102.017	Protect human operator from pressure and radiation while reducing primary coolant pressure for monitoring.		

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0102.018	Automatically monitor primary coolant lines to detect leaks.		
3001.0102.019	Automatically isolate primary coolant lines when leak detected.	1	5.11
3001.0102.020	Protect human operators from radiation exposure.	1	5.11
3001.0102.021	Design AIS for 40-year lifetime.	1	5.1.1
3001.0102.022	Design of AIS shall include human factors engineering.	1	5.10.1
3001.0102.030	AIS structure shall be welded steel and shall be boltable and weldable to the walls and floor.	1	5.1.1
3001.0102.040	All components containing primary coolant shall be seismic category 1.		
3001.0102.041	Electrical control and feedback signals shall be non-class 1E but powered from a highly reliable power supply.		
3001.0102.042	Depressurization rack shall be designed to operate through and after the OBE.		
3001.0102.043	Components that are primary coolant pressure boundaries shall maintain their function during and after the OBE.		
3001.0102.044	Valves, instruments, and other active devices shall continue to perform their function during and after the OBE.		
3001.0102.045	Components that are primary coolant pressure boundaries shall maintain their function during and after the SSE.		
3001.0102.046	Valves, instruments, and active devices that are not pressure boundaries are not required to function during or after the SSE.		

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0102.060	AIS components exposed to primary coolant shall be designed for chemical impurities listed in Table 1.2-1.		
3001.0102.061	AIS in reactor confinement building shall be designed to stated environmental conditions.	1	5.11.1
3001.0102.062	AIS electronic equipment located elsewhere shall be designed to stated environmental conditions.	1	5.10.1
3001.0102.070	AIS shall minimize radiation exposure to plant personnel and shielding shall be used.	1	5.11.1
3001.0102.071	Area radiation monitoring shall be provided in the AIS area.	1	5.16.2
3001.0102.072	Primary coolant and purified helium sample ports shall be provided.	1	5.16.2
3001.0102.073	Plateout instrument shall be provided.	1	5.11.1
3001.0102.074	A depressurization rack shall be provided.	1	5.1.1
3001.0102.075	An analytical instrument module shall be provided.	1	
3001.0102.076	Manual grab sample and on demand trend data shall be provided.	1	
3001.0102.077	AIS shall provide impurity status data to the PPS.	1	5.9.1
3001.0102.100	Average planned outage of a reactor module ≤[THD] h/yr.	1	5.1.1
3001.0102.101	Average unplanned outage of a reactor module ≤[TBD] h/yr.		
3001.0102.102	AIS design shall minimize recovery time from an outage.		

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0102.103	Operating availability shall be accomplished by reliability, redundancy, maintenance, human factors, spare parts, material, and manpower.	1	5.1.1
3001.0102.104	Average yearly loss due to failure to detect CO and H_2O accurately shall be <[TBD].		
3001.0102.105	Average yearly loss due to failure to detect CO_2, CH_4, N_2, H_2, and O_2 shall be <[TBD].		
3001.0102.106	Reliability shall preclude exceeding PAG limit of $<5 \times 10^{-7}$/yr.		
3001.0102.107	Reliability shall preclude exceeding 10CFR10 limits of $<1 \times 10^{-4}$/yr.		
3001.0102.120	AIS design shall facilitate maintenance.		5.1.3
3001.0102.121	AIS pressure boundary components shall require maintenance during a planned shutdown period.		5.2.1
3001.0102.122	All AIS components shall be replaceable on-line except primary coolant root valves.		
3001.0102.123	Table 1.2-1 lists surveillance requirements for instrument sample lines.	1	5.1.3
3001.0102.124	AIS design shall accommodate preventive maintenance but limit personnel exposure.		
3001.0102.125	AIS preventive maintenance requirements are listed in Table 1.2-3 and for faulty sensors and components of control loops in Table 1.2-4.		
3001.0102.126	Preventive maintenance shall emphasize eliminating unplanned maintenance shutdowns.		

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0102.127	AIS design shall satisfy licensing methodology for the MHTGR.		5.1.1
3001.0102.140	AIS shall meet industrial standards in Table 1.2-4.	1	5.1.1
3001.0102.160	AIS components are QAL II or III and shall come under a quality assurance program which complies with NQA-1.	2	
3001.0102.161	AIS SDD is classified as QAL II	2	
3001.0102.170	AIS equipment and arrangement shall facilitate manufacture, installation, and removal on a modular basis.	1	5.1.1
3001.0102.171	AIS design shall meet all transportation, handling, storage, construction, and operational functions. In addition, safety economic, and reliability goals shall be met.	1	5.11.1
3001.0102.190	AIS design shall minimize volume of activated and contaminated materials, radiation levels, exposure, and time and cost of decommissioning.		
3001.0102.191	AIS design shall use "Draft Generic Environmental Statement on Decommissioning of Nuclear Facilities" as a guide.		
3001.0401.001	Vessels and Ducts Subystem to provide primary coolant samples.		
3001.0401.002	Vessels and Ducts Subystem to provide access to primary coolant.		
3001.0401.010	Helium Purification Subsystem to provide helium samples.		
3001.0401.011	Liquid Nitrogen Subsystem to provide liquid nitrogen for portable dewars used in sample treatment.		
3001.0401.012	Gaseous Radioactive Waste Subsystem provides helium samples.		

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3001.0401.013	Gaseous Radioactive Waste Subsystem receives gaseous radioactive waste from AIS.		
3001.0401.030	Special Nuclear Area Instrumentation Subsystem receives AIS status signals.	1	5.11.2
3001.0401.040	NSSS Control Subsystem reveives AIS status signals.		
3001.0401.050	Circulating Water Subsystem provides cooling water.		
3001.0401.060	Reactor Building Subsystem provides structural support.		
3001.0401.070	HVAC Subsystem provides room cooling for equipment.		
3001.0401.080	Mon-Class 1E AC Distribution Subsystem provides electrical power to AIS equipment.		
3001.0401.100	Radiation monitoring subsystem receives AIS output signals.		
3001.0401.130	Boundary for sensors that monitor or control process conditions shall be the point at which the sensor penetrates the process pipe or vessel.		
3001.0401.131	Boundary for sensors not requiring thermowells and for instruments requiring flanges or other appurtenances shall be the point at which they touch the pipe or vessel wall.		
3001.0401.140	For field sensors, the electrical boundary is the electrical screen or crimp terminal strip at the multiplexer where the wires are connected.		
3001.0401.141	For instrumentation with special requirements (e.g., temporary or hardwired) that is not connected to the multiplex bus, the boundary is the electrical terminal strip where the sensor or final control element is attached.		

Table A-2

TRACEABILITY SUMMARY REFERENCE LIST

1. "Overall Plant Design Specification (OPDS), Modular High Temperature Gas Cooled Reactor," HTGR-86-004, Rev. 1, (HFS-20100, Rev. 1) (980397/2), February 18, 1986.

2. "Quality Assurance Requirements," HP-20801, Rev. 1 (PC-000190/0), September 21, 1984.

DOE-HTGR-86-047
Revision 1

HTGR

PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

[redacted]Y

An[redacted]cument
or[redacted]esenting
Fo[redacted]Com-
par[redacted]ns of
U.S[redacted]or, HTR
Develop[redacted]ergy.

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

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

JULY 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

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

PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION

[redacted]

Any Further Distribution by any Holder of this Document o[redacted]ing Forei[redacted] Interests, Foreign Governments, Foreign Companies [redacted]ns of U.S[redacted]or, HTR Develop[redacted].

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

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

JULY 1987

[redacted]

[redacted]

ROLL 20:4-rev 0

GA 1485 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY

NUCLEAR SAFETY-RELATED

TITLE			
PLANT PROTECTION AND INSTRUMENTATION SYSTEM DESIGN DESCRIPTION	☐ R & D ☐ DV & S ☒ DESIGN	APPROVAL LEVEL 5	

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

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

INFO

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 F.A.Silady Interface Assurance	G.P.Connors	G.C.Bramblett		Initial issue (HFD-33200 Rev. 0) 6352320103

[redacted] Any Further Distribution by any Holder of this Document [redacted] enting [redacted] Com- panies [redacted] S. [redacted] HTR Development [redacted] of Energy.

CONTINUE ON GA FORM 1485-1

*See List of Effective Pages

NEXT INDENTURED DOCUMENTS

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

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

ROLL 2084/ rev. 1 & 2

GA 1485-1 (REV. 10/82)

GA Technologies Inc.

ISSUE SUMMARY
CONTINUATION SHEET

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

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

INFO 1

INFO 1

LIST OF EFFECTIVE PAGES

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

TABLE OF CONTENTS

	PAGE
LIST OF EFFECTIVE PAGES	ii
LIST OF APPENDICES	viii
LIST OF ILLUSTRATIONS	ix
LIST OF TABLES	x
LIST OF ABBREVIATIONS AND ACRONYMS	xiii
DEFINITIONS	xiv
PREFACE	xviii
SUMMARY	xx
1 SYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 SYSTEM FUNCTIONS	1-1
1.2 SYSTEM DESIGN REQUIREMENTS	1-1
1.2.1 System Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-3
1.2.3 Structural Requirements	1-16
1.2.4 Environmental Requirements	1-16
1.2.5 Instrumentation and Control Requirements	1-17
1.2.6 Surveillance and In-Service Inspection Requirements	1-18
1.2.7 Availability Assurance Requirements	1-18
1.2.8 Maintenance Requirements	1-19
1.2.9 Safety Requirements	1-19
1.2.10 Industry Codes and Standards	1-27
1.2.11 Quality Assurance Requirements	1-27
1.2.12 Construction Requirements	1-29
1.2.13 Decommissioning Requirements	1-29

2 DESIGN DESCRIPTION 2-1
2.1 SUMMARY DESCRIPTION 2-1
2.2 SYSTEM CONFIGURATION 2-3
2.2.1 Investment Protection Subsystem 2-5
2.2.2 Safety Protection Subsystem 2-13
2.2.3 Special Nuclear Area Instrumentation Subsystem . . 2-22
2.3 SYSTEM PERFORMANCE CHARACTERISTICS 2-27
2.3.1 System Operating Modes 2-27
2.3.2 System Steady State Performance 2-36
2.3.3 System Response to Plant Transients 2-36
2.3.4 System Failure Modes and Effects 2-56
2.4 SYSTEM ARRANGEMENT 2-57
2.5 INSTRUMENTATION AND CONTROL 2-76
3 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS 3-1
3.1 SUBSYSTEM FUNCTIONS 3-1
3.1.1 Investment Protection Subsystem Functions 3-1
3.1.2 Safety Protection Subsystem Functions 3-1
3.1.3 Special Nuclear Area Subsystem Functions 3-1
3.2 SUBSYSTEM DESIGN REQUIREMENTS 3-2
3.2.1 Investment Protection Subsystem Design Requirements 3-2
3.2.2 Safety Protection Subsystem 3-14
3.2.3 Special Nuclear Area Instrumentation Subsystem . . 3-29
4 SYSTEM AND SUBSYSTEM INTERFACES 4-1
4.1 INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS 4-1
4.2 SUBSYSTEM BOUNDARY DEFINITION 4-1
5 SYSTEM CONSTRUCTION 5-1
5.1 PACKAGING AND SHIPPING 5-1
5.2 HANDLING AT DELIVERY 5-1
5.3 RECEIVING INSPECTION 5-2
5.4 STORAGE 5-2
5.5 ACCESS 5-2
5.6 INSTALLATION AND/OR FIELD FABRICATION 5-2

5.7 CONSTRUCTION TESTING 5-3
5.8 AS-BUILT DRAWINGS 5-3
6 SYSTEM OPERATION 6-1
6.1 SYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS 6-1
6.1.1 System Limitations and Setpoints 6-1
6.1.2 Precautions 6-1
6.2 PREOPERATIONAL CHECKOUT 6-6
6.2.1 Initial Preoperational Checkout 6-6
6.2.2 Routine Preoperational Checkout 6-7
6.3 STARTUP/SHUTDOWN 6-9
6.3.1 Startup to 25% Steam Flow 6-9
6.3.2 Shutdown from 25% Steam Flow 6-10
6.4 NORMAL OPERATION 6-10
6.5 REFUELING 6-10
6.6 SHUTDOWN 6-11
6.6.1 Automatic Plant Shutdowns 6-11
6.6.2 Plant Protection and Instrumentation System Shutdown 6-12
6.7 ABNORMAL OPERATION 6-12
6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES 6-13
6.8.1 Casualty Events 6-13
6.8.2 Design Features to Mitigate Effects of Casualty Events 6-15
6.8.3 Recovery Procedures 6-18
7 SYSTEM MAINTENANCE 7-1
7.1 MAINTENANCE APPROACH 7-1
7.2 CORRECTIVE MAINTENANCE 7-2
7.3 PREVENTIVE MAINTENANCE 7-3
7.4 IN-SERVICE INSPECTION 7-3
7.5 SURVEILLANCE 7-4
7.5.1 Instrument Checks 7-4
7.5.2 Functional Tests 7-4
7.5.3 Calibration Verification Tests 7-5
7.5.4 Response Time Verification Tests 7-5

8 SYSTEM DECOMMISSIONING 8-1
9 REFERENCES 9-1

LIST OF APPENDICES

A TRACEABILITY OF REQUIREMENTS A-1
B DRAWINGS LIST B-1
C TRANSIENTS C-1
D DESIGN BASIS SEISMIC INPUTS D-1
E PLANT PROTECTION AND INSTRUMENTAION SYSTEM PARAMETERS AND MAJOR FEATURES E-1
F PROPRIETARY CLAIMS F-1

LIST OF ILLUSTRATIONS

FIGURE	TITLE	PAGE
1-1	Part Load Operating Conditions at the Steam Generator - Four Modules Operating at Equal Loads	1-5
1-2	Plant Heat Balance Diagram at 100% (Rated) Feedwater Flow	1-6
1-3	NSSS Heat Balance Diagram at 100% (Rated) Feedwater Flow	1-7
1-4	Plant Heat Balance Diagram at 25% Feedwater Flow	1-8
1-5	NSSS Heat Balance Diagram at 25% Feedwater Flow	1-9
2-1	Protection System Data Busses	2-4
2-2	Investment Protection Subsystem Functional Overview	2-6
2-3	Simplified Block Diagram, Reactor Trip - Inner Control Rods	2-8
2-4	Simplified Block Diagram, Steam Generator Isolation and Dump	2-9
2-5	Simplified Block Diagram, Primary Coolant Pumpdown	2-11
2-6	Simplified Block Diagram, Shutdown Cooling System Initiation	2-12
2-7	Simplified Block Diagram, Shutdown Cooling Heat Exchanger Isolation	2-14
2-8	Safety Protection Subsystem Functional Overview	2-15
2-9	Simplified Block Diagram, Reactor Trip - Outer Control Rods	2-17
2-10	Simplified Block Diagram, Reactor Trip - Reserve Shutdown Control Equipment	2-19
2-11	Simplified Block Diagram, Main Loop Shutdown and Main Steam Isolation	2-23
2-12	Plant Protection and Instrumentation System Equipment Arrangement	2-77
6-1	Relationship Between Setpoints and Component Damage Limits	6-2

LIST OF TABLES

TABLE	TITLE	PAGE
1-1	Design Point NSSS Performance at Rated (100%) Feedwater Flow	1-10
1-2	Nominal NSSS Performance at 25% Feedwater Flow	1-11
1-3	Design Duty Cycle Events	1-12
1-4	Plant Equipment Damage Limits for Use in Designing the Plant Protection and Instrumentation System	1-14
1-5	Reliability Allocations to Plant Protection and Instrumentation System	1-20
1-6	Scheduled Outage Allocations to Plant Protection and Instrumentation System	1-21
1-7	Radionuclide Release Limits	1-23
1-8	Equipment Classification	1-24
1-9	Safety-Related Design Conditions	1-26
1-10	Industry Codes and Standards Applicable to the Plant Protection and Instrumentation System Design	1-28
2-1	Allocation Within the Plant Protection and Instrumentation System	2-2
2-2	Plant Protection and Instrumentation System Protective Actions	2-28
2-3	Plant Protection and Instrumentation System Sensor Channel Parameters	2-30
2-4	Plant Protection and Instrumentation System Actuated Equipment	2-34
2-5	Plant Protection and Instrumentation System Operating Mode Versus Plant Condition	2-37
2-6	Plant Protection and Instrumentation Trip Parameters	2-38
2-7	Failure Modes and Efforts - Investment Protection Subsystem	2-58
2-8	Failure Modes and Efforts - Safety Protection Subsystem	2-69

LIST OF TABLES (Continued)

2-9 General Location of Plant Protection and Instrumentation System Equipment 2-78
3-1 External Environmental Conditions (Normal) 3-6
3-2 External Environmental Conditions (Abnormal) 3-7
3-3 External Environmental Conditions (Design Basis Event) . . . 3-8
3-4 Reliability Allocations to Investment Protection Subsystem 3-10
3-5 Scheduled Outage Allocation to Investment Protection Subsystem 3-11
3-6 Industry Codes and Standards Applicable to the Investment Protection Subsystem Design 3-13
3-7 External Environmental Conditions (Normal) 3-19
3-8 External Environmental Conditions (Abnormal) 3-20
3-9 External Environmental Conditions (Design Basis Event) . . . 3-21
3-10 Reliability Allocations to Safety Protection Subsystem . . . 3-23
3-11 Scheduled Outage Allocation to Safety Protection Subsystem 3-24
3-12 Safety-Related Design Conditions 3-26
3-13 Industry Codes and Standards Applicable to the Safety Protection Subsystem Design 3-28
3-14 External Environmental Conditions (Normal) 3-32
3-15 External Environmental Conditions (Abnormal) 3-33
3-16 External Environmental Conditions (Design Basis Event) . . . 3-34
3-17 Reliability Allocations to the Special Nuclear Area Instrumentation 3-37
3-18 Scheduled Outage Allocation to Special Nuclear Area Instrumentation Subsystem 3-38
3-19 Industry Codes and Standards Applicable to the Special Nuclear Area Instrumentation Subsystem Design 3-39
4-1 Plant Protection and Instrumentation System Interface Requirements Imposed on Other Systems 4-2
6-1 Operating Limits and Setpoints for the Plant Protection and Instrumentation System 6-3

LIST OF ABBREVIATIONS AND ACRONYMS

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

LIST OF ABBREVIATIONS AND ACRONYMS (Continued)

TBD	To Be Determined
USNRC	United States Nuclear Regulatory Commission

DEFINITIONS*

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

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

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

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

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

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

---

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

DEFINITIONS (Continued)

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

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

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

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

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

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

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

DEFINITIONS (Continued)

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

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

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

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

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

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

DEFINITIONS (Continued)

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

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

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

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

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

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

PREFACE

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

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

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

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

4. Maintain Emergency Preparedness

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

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

SUMMARY

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

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

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

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

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

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

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

SECTION 1
SYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SYSTEM FUNCTIONS

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

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

1.2 SYSTEM DESIGN REQUIREMENTS

1.2.1 System Configuration and Essential Features Requirements

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

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

*Requirements traceability number.

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

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

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

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

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

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

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

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

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

1.2.2 Operational Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

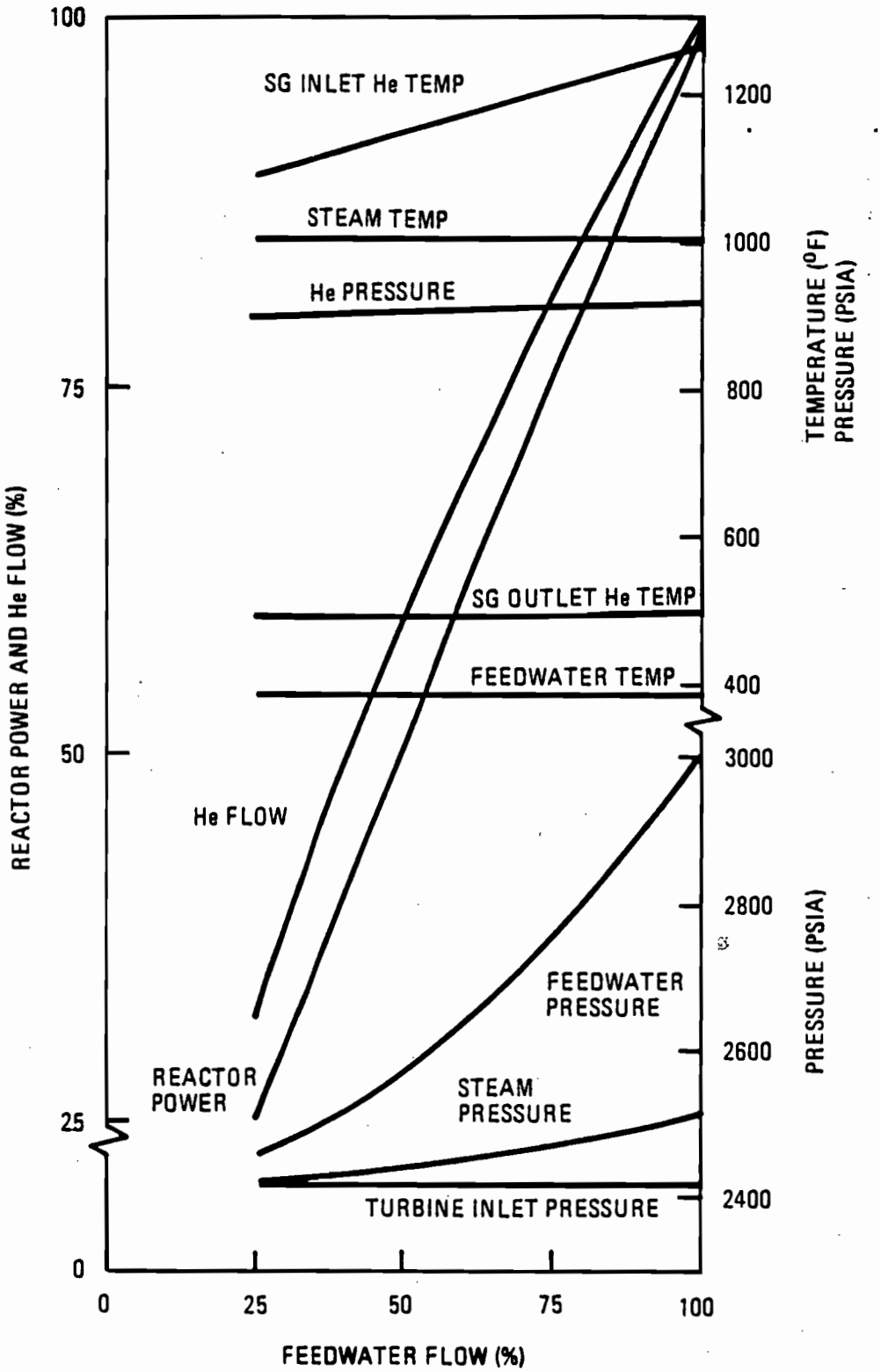
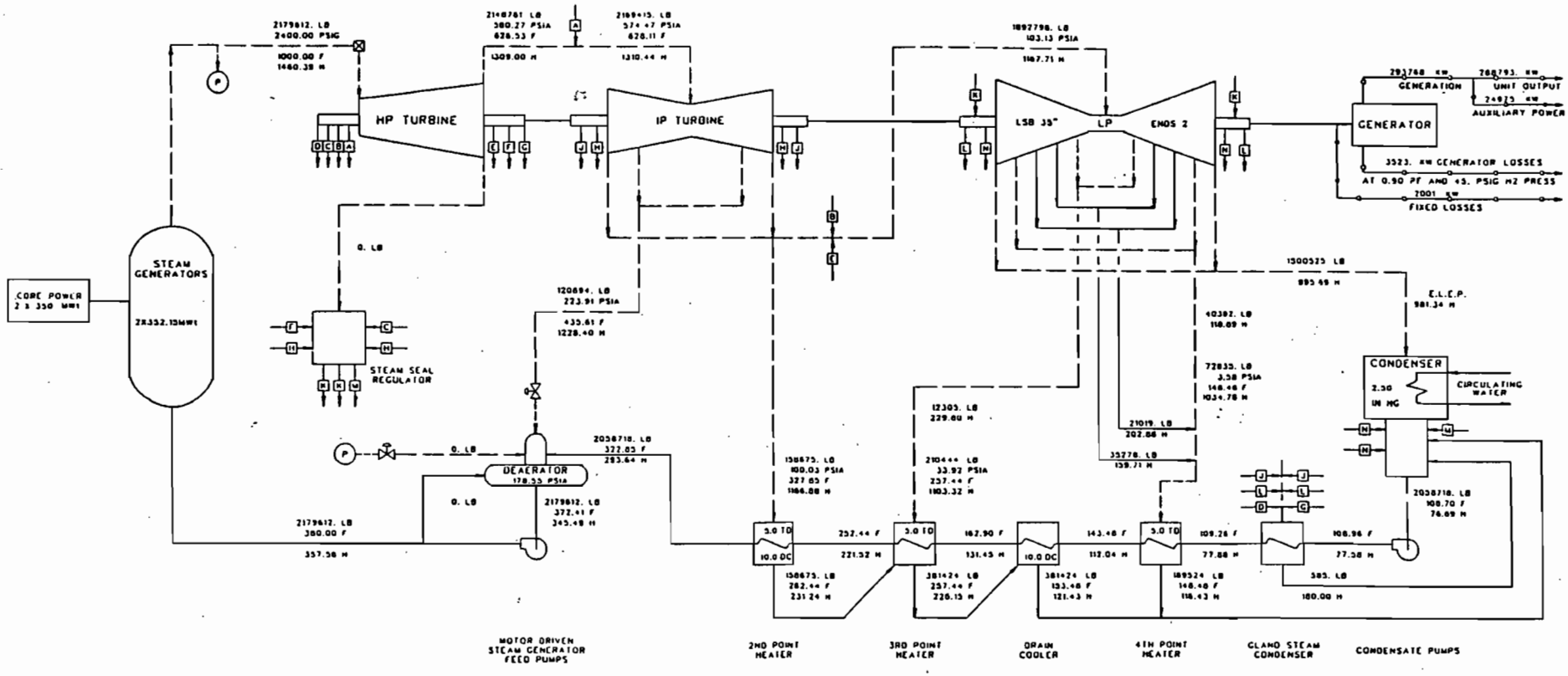


Figure 1-1
PART LOAD OPERATING CONDITIONS AT THE STEAM GENERATOR - FOUR MODULES OPERATING AT EQUAL LOADS



BASIS

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

STEAM GENERATOR FEED PUMP AND CONDENSATE PUMP EFFICIENCIES 83%

PRESSURE DROP IN EXTRACTION LINES 3%

	1X300 MWe UNIT	2X300 MWe UNIT TOTAL PLANT
CORE POWER, MWt	700.	1400.
HEAT INPUT, BTU/HR	2403746419.	4807492838.
SGFP POWER, KW	8371	16741.
AUXILIARY POWER, KW	24975.	49950.
GENERATION, KW	293768.	587536.
UNIT OUTPUT, KW	268793.	537588.

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

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

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

LEAKAGES

	FLOW	ENTHALPY
A	20654. LB	1480.39 H
B	3387. LB	1480.39 H
C	1405. LB	1480.39 H
D	38. LB	1480.39 H
E	4042. LB	1309.00 H
F	1295. LB	1309.00 H
G	35. LB	1309.00 H
H	2135. LB	1166.88 H
J	101. LB	1166.88 H
K	873. LB	1252.45 H
L	153. LB	1252.45 H
M	5824. LB	1252.45 H
N	518. LB	1252.45 H

LEGEND

STEAM
WATER
POWER

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

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

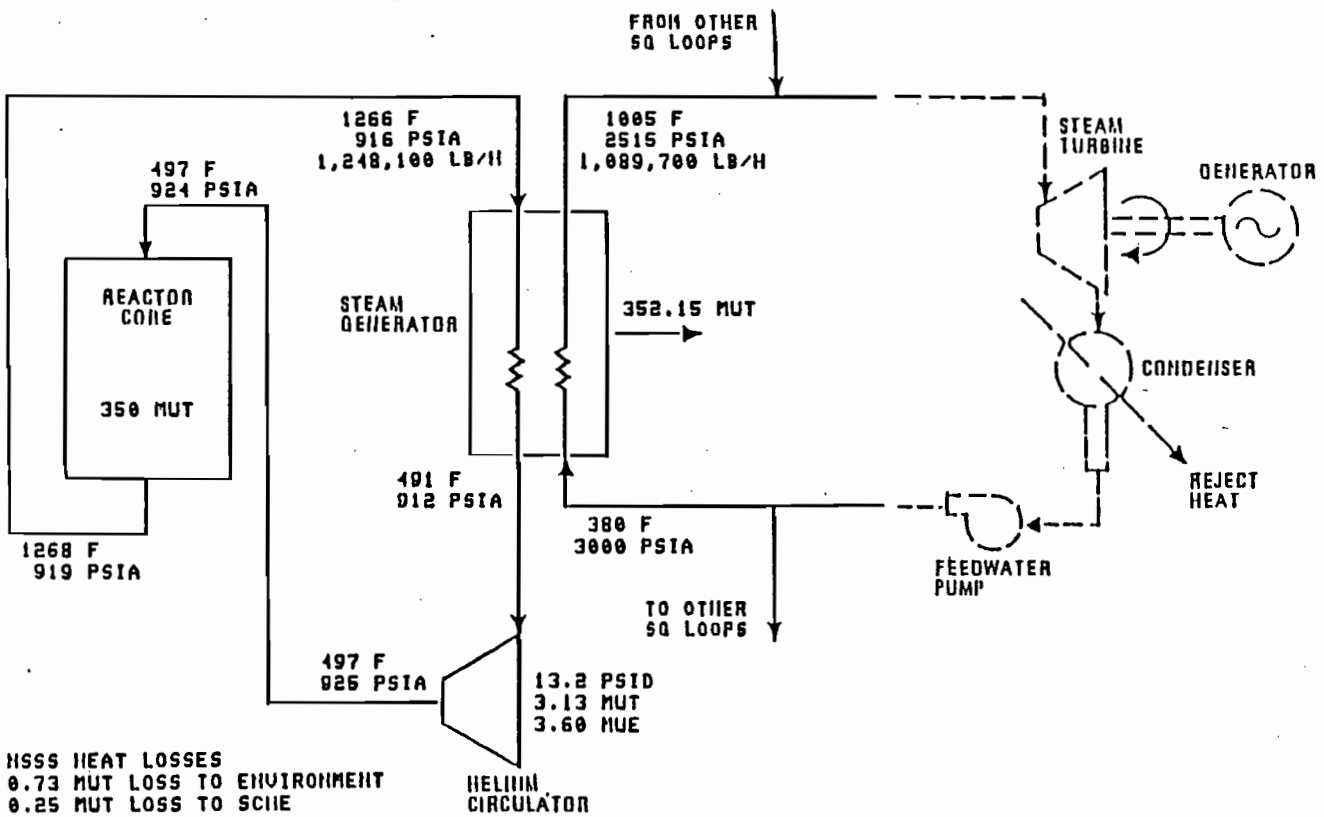
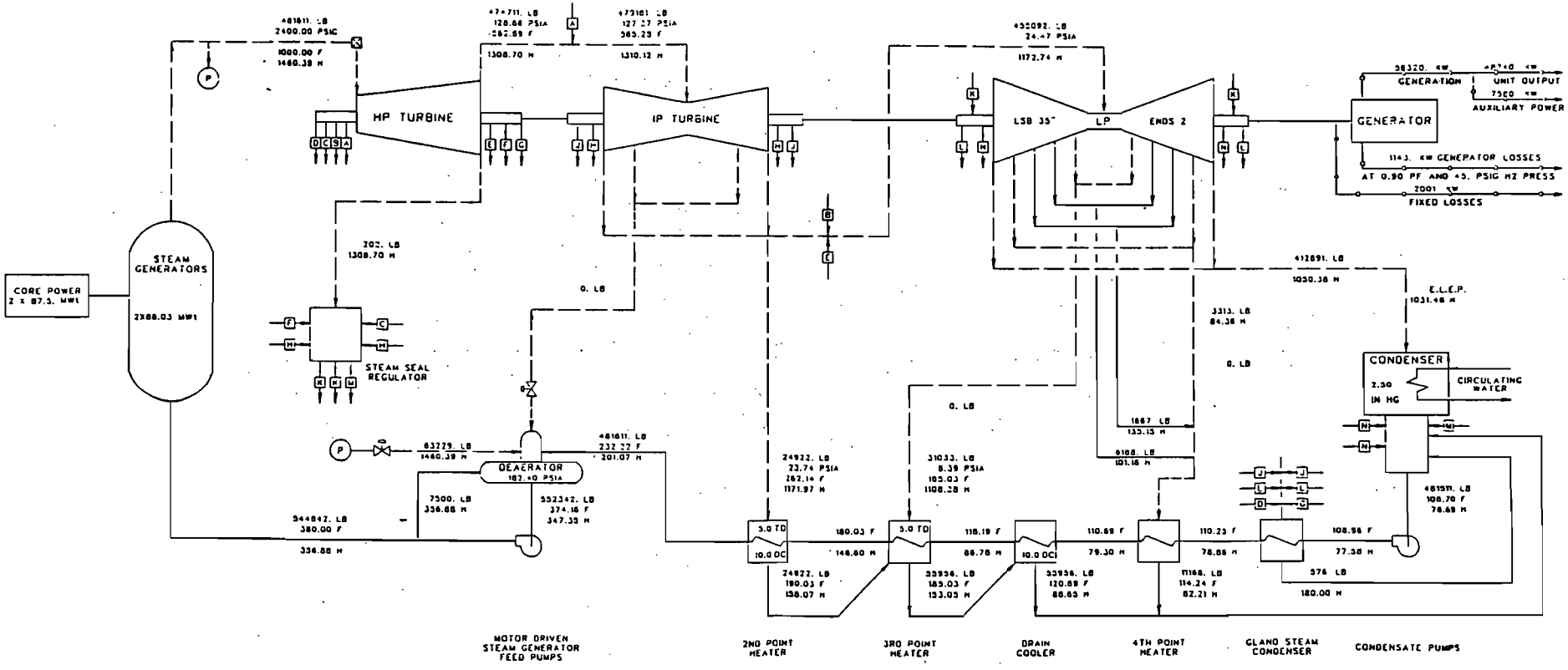


Figure 1-3 NSSS HEAT BALANCE DIAGRAM AT 100% (RATED) FEEDWATER FLOW



BASIS

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

STEAM GENERATOR FEED PUMP AND CONDENSATE PUMP EFFICIENCIES 83%

PRESSURE DROP IN EXTRACTION LINES 3%

	1X300 MWe UNIT	2X300 MWe UNIT TOTAL PLANT
CORE POWER, MWt	175.	350.
HEAT INPUT, BTU/HR	601241727.	1202483453.
SGFP POWER, KW	1674.	3348.
AUXILIARY POWER, KW	7580.	15160.
GENERATION, KW	56320.	112640.
UNIT OUTPUT, KW	48740.	97480.

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

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

UNIT HEAT RATE = CORE POWER / UNIT OUTPUT = 12231. BTU/KW-HR

LEAKAGES

	FLOW	ENTHALPY
A	4470. LB	1460.39 H
B	779. LB	1460.39 H
C	237. LB	1460.39 H
D	38. LB	1460.39 H
E	820. LB	1308.70 H
F	219. LB	1308.70 H
G	35. LB	1308.70 H
H	334. LB	1171.97 H
J	99. LB	1171.97 H
K	663. LB	1266.93 H
L	152. LB	1266.93 H
M	0. LB	1266.93 H
N	311. LB	1266.93 H

LEGEND

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

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

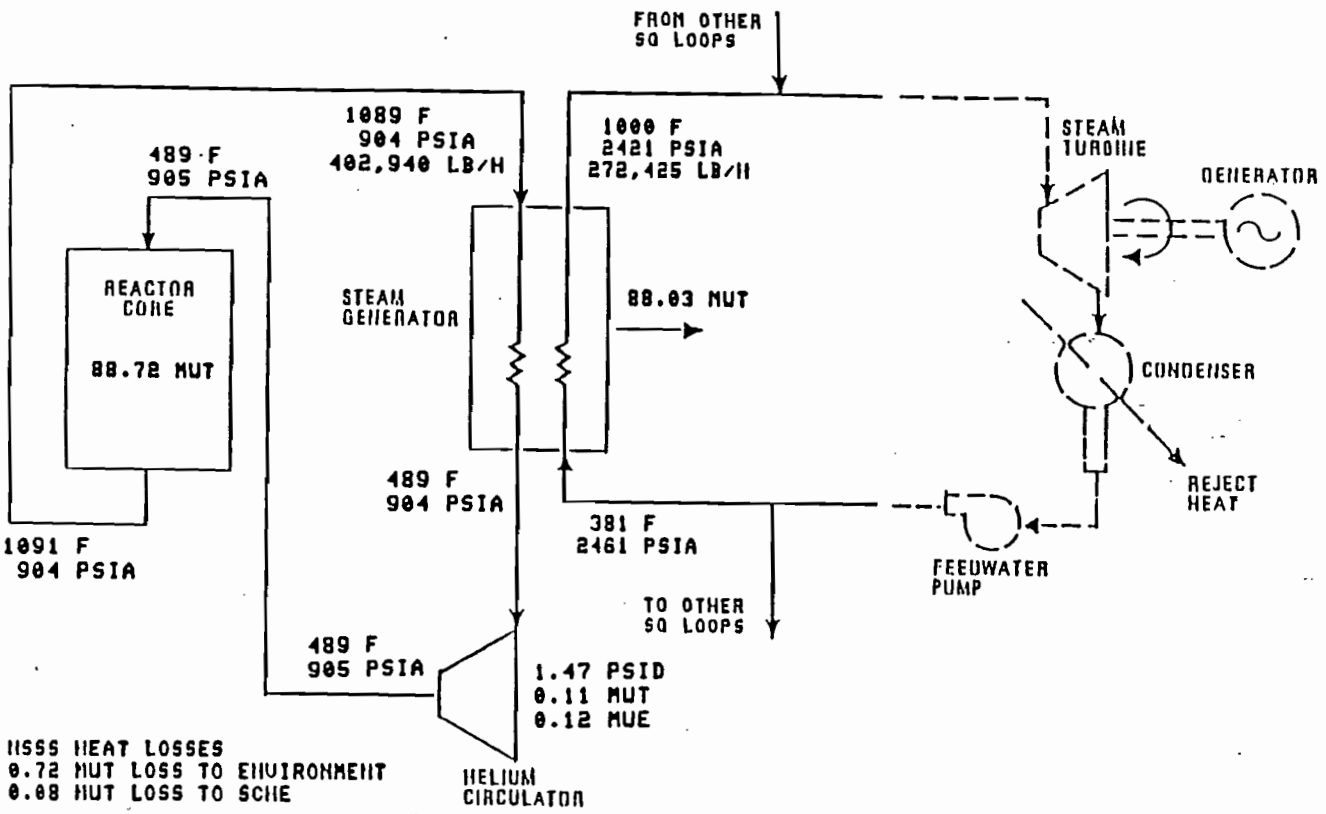


Figure 1-5 NSSS HEAT BALANCE DIAGRAM AT 25% FEEDWATER FLOW

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

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

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

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

Table 1-3 DESIGN DUTY CYCLE EVENTS

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

Table 1-3 (Continued)

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

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

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

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

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

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

Table 1-4 (Continued)

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

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

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

(3200.0102.040)

1.2.3 Structural Requirements

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

(3200.0102.400)

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

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

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

1.2.4 Environmental Requirements

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

(3200.0102.450)

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

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

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

1.2.5 Instrumentation and Control Requirements

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

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

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

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

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

1.2.6 Surveillance and In-Service Inspection Requirements

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

1.2.7 Availability Assurance Requirements

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

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

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

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

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

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

1.2.8 Maintenance Requirements

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

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

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

1.2.9 Safety Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1-7 RADIONUCLIDE RELEASE LIMITS

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

Table 1-8 EQUIPMENT CLASSIFICATION

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

Table 1-8 (Continued)

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

Table 1-9
SAFETY-RELATED DESIGN CONDITIONS

Pressurized Conduction Cooldown
(SRDC No. 1)

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

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

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

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

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

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

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

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

1.2.10 Industry Codes and Standards

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

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

1.2.11 Quality Assurance Requirements

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

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

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

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

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

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

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

1.2.12 Construction Requirements

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

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

1.2.13 Decommissioning Requirements

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

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

SECTION 2
DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

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

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

The Investment Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate protective actions required to protect the plant investment. The Investment Protection Subsystem's prime purpose is to protect major plant equipment and is, therefore, investment risk oriented. The investment protection provides an integrated response to various plant upsets and events to ensure equipment damage limits are not exceeded. The subsystem uses redundancy and other system characteristics to meet the plant investment and availability goals. Each reactor module has a separate and independent Investment Protection Subsystem.

The Safety Protection Subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate protective actions required to mitigate the consequences of design basis events, protecting the public health and safety. Each reactor module has a separate and independent Safety Protection Subsystem.

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

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

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

2.2 SYSTEM CONFIGURATION

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

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

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

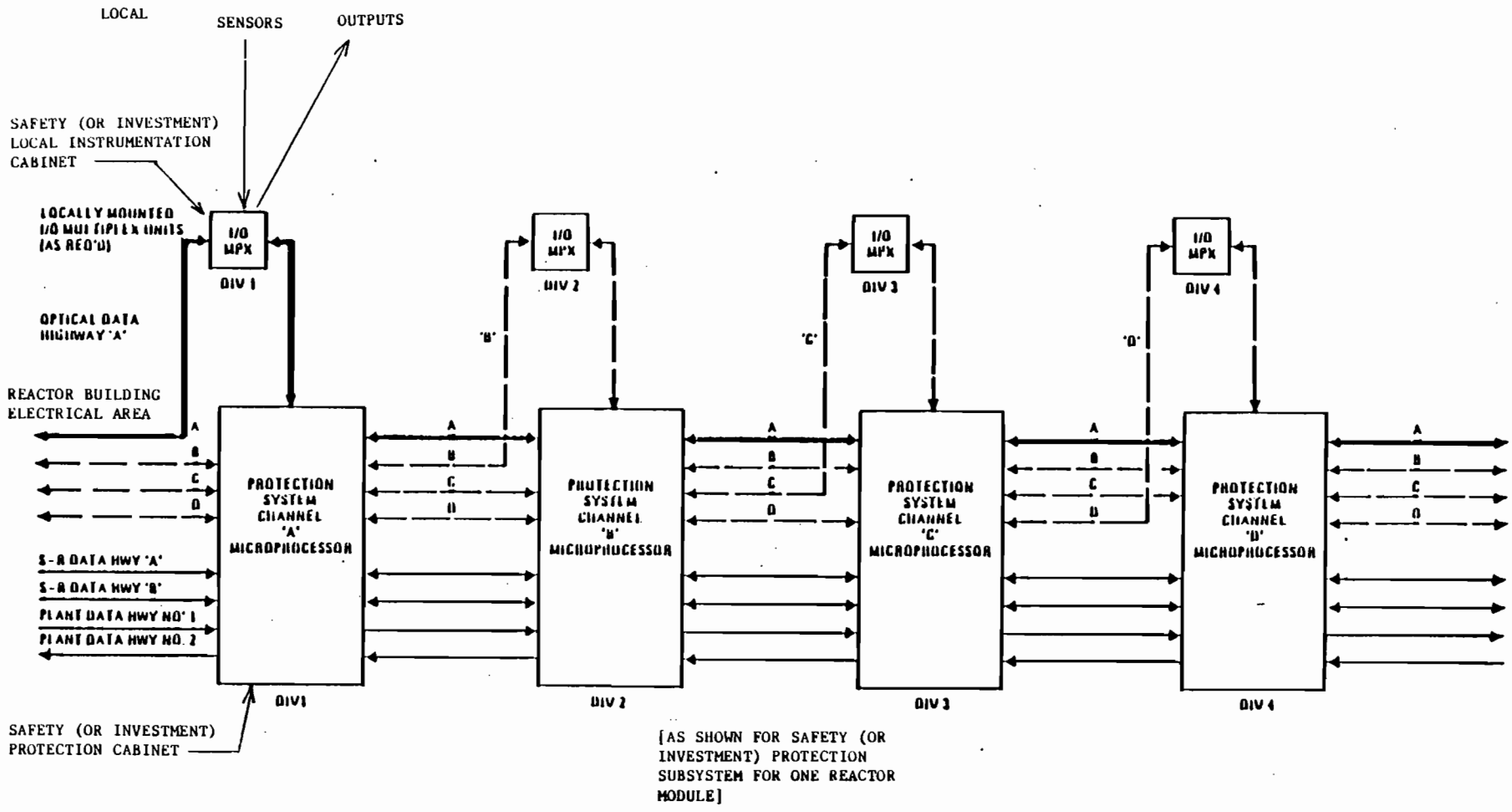


Figure 2-1 PROTECTION SYSTEM DATA BUSSES

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

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

2.2.1 Investment Protection Subsystem

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

Each Investment Protection Subsystem consists of the supporting trip subsystems as shown in Figure 2-2. Each trip subsystem consists of four separate (redundant) instrument channels and redundant two-out-of-four coincidence solid-state logic to command initiation of a protective action. Each instrument channel includes the field mounted process variable sensors, electronic signal conditioning equipment, and electronic trip setpoint comparator to provide a trip signal when the process variable value reaches the trip setpoint. The two-out-of-four coincidence logic circuitry provides a protective action initiation signal when any two or more separate instrument channels reach the trip setpoint. The protective action initiation signal is sent to separate and redundant actuation devices. The boundaries of the Investment Protection Subsystem are generally from, and including, the sensors to the input of the actuation devices. The Investment Protection Subsystem components may under some circumstances become associated circuits.

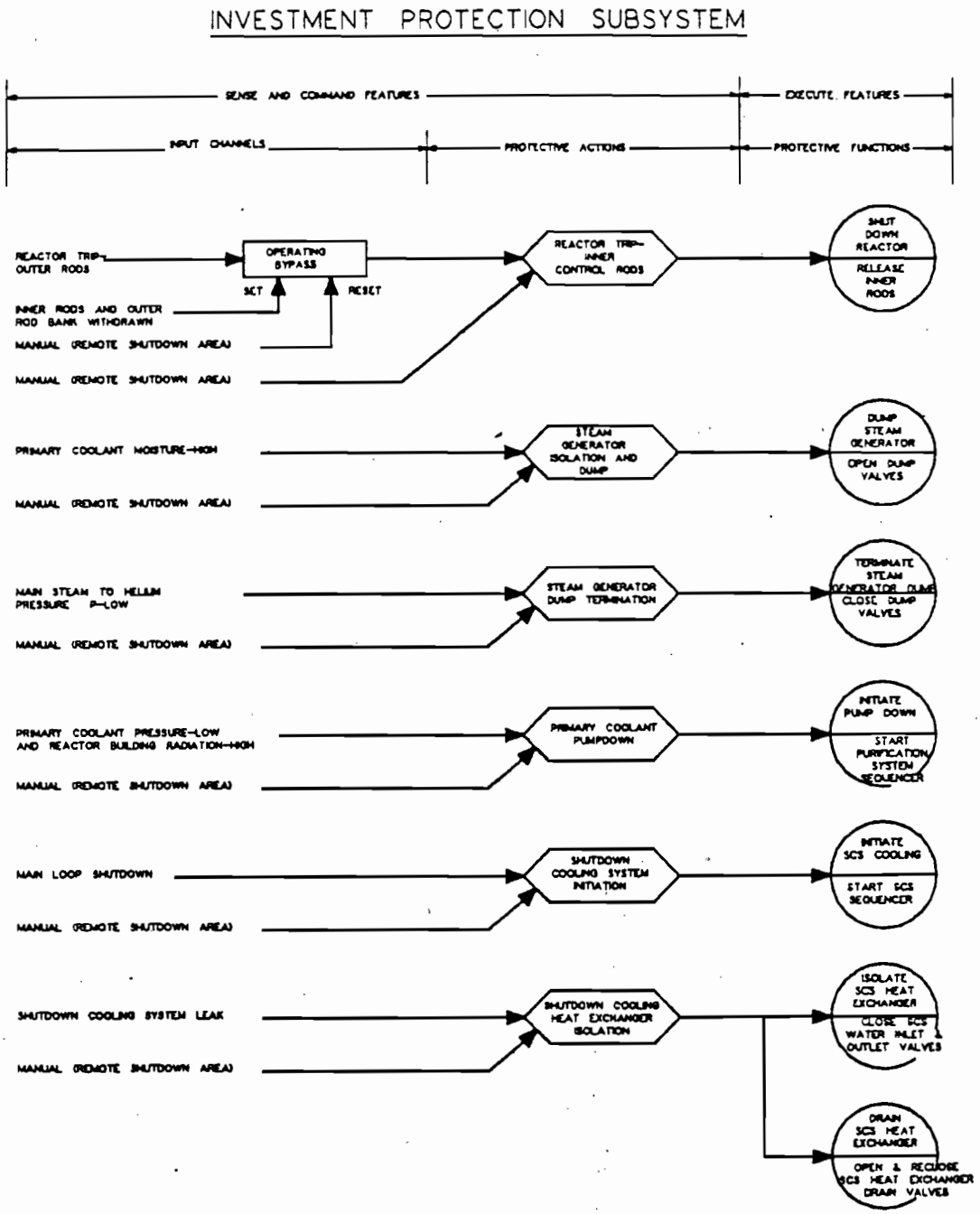


Figure 2-2 INVESTMENT PROTECTION SUBSYSTEM FUNCTIONAL OVERVIEW

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

2.2.1.1 Reactor Trip Using Inner Control Rods

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

2.2.1.2 Steam Generator Isolation and Dump

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

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

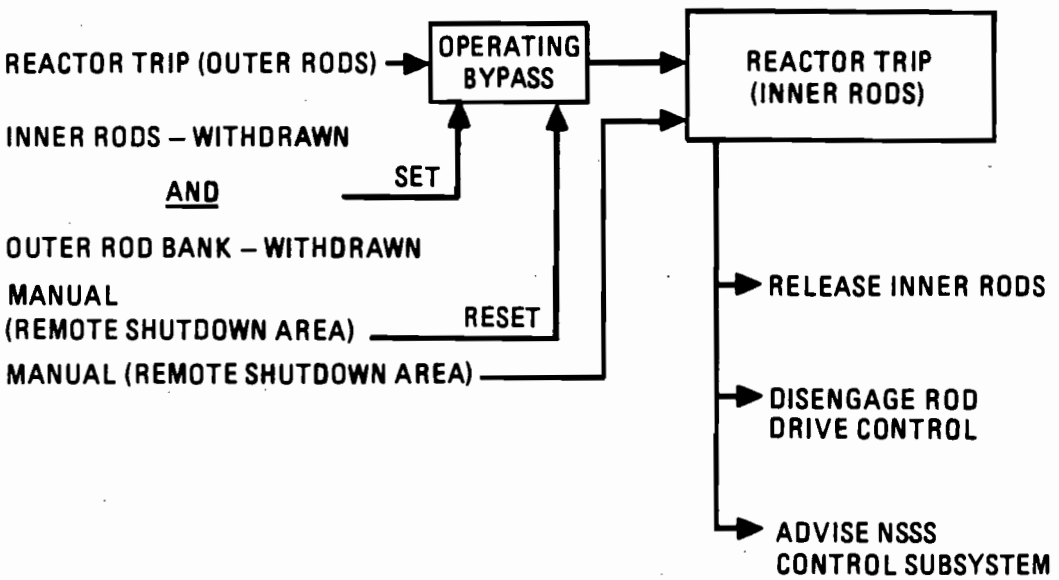


Figure 2-3 SIMPLIFIED BLOCK DIAGRAM REACTOR TRIP - INNER CONTROL RODS

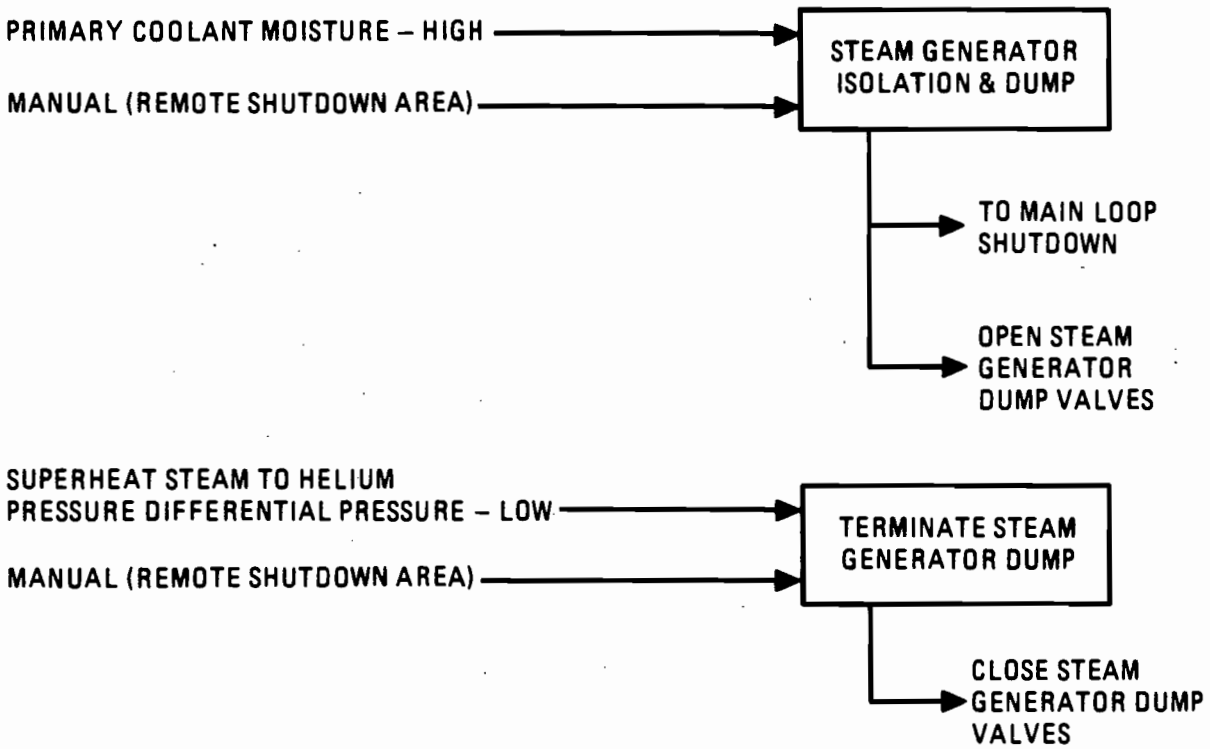


Figure 2-4
SIMPLIFIED BLOCK DIAGRAM, STEAM GENERATOR ISOLATION AND DUMP

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

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

2.2.1.3 Primary Coolant Pumpdown

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

2.2.1.4 Shutdown Cooling System Initiation

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

2.2.1.5 Shutdown Cooling Heat Exchanger Isolation

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

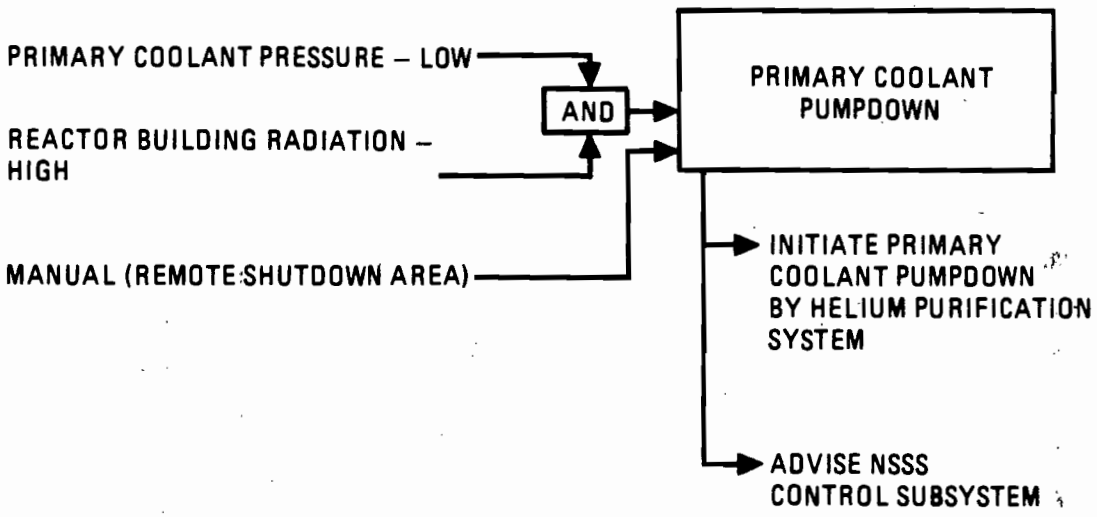


Figure 2-5 SIMPLIFIED BLOCK DIAGRAM, PRIMARY COOLANT PUMPDOWN

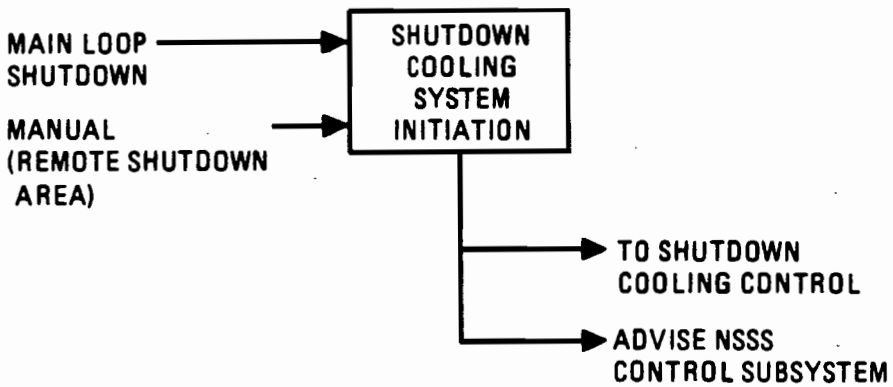


Figure 2-6
SIMPLIFIED BLOCK DIAGRAM, SHUTDOWN COOLING SYSTEM INITIATION

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

2.2.2 Safety Protection Subsystem

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

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

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

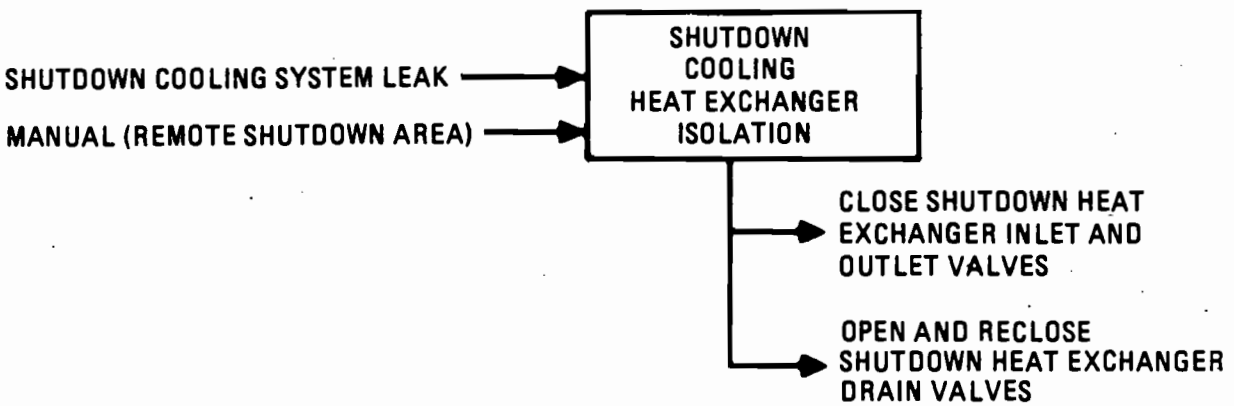


Figure 2-7
SIMPLIFIED BLOCK DIAGRAM, SHUTDOWN COOLING HEAT EXCHANGER ISOLATION

SAFETY PROTECTION SUBSYSTEM

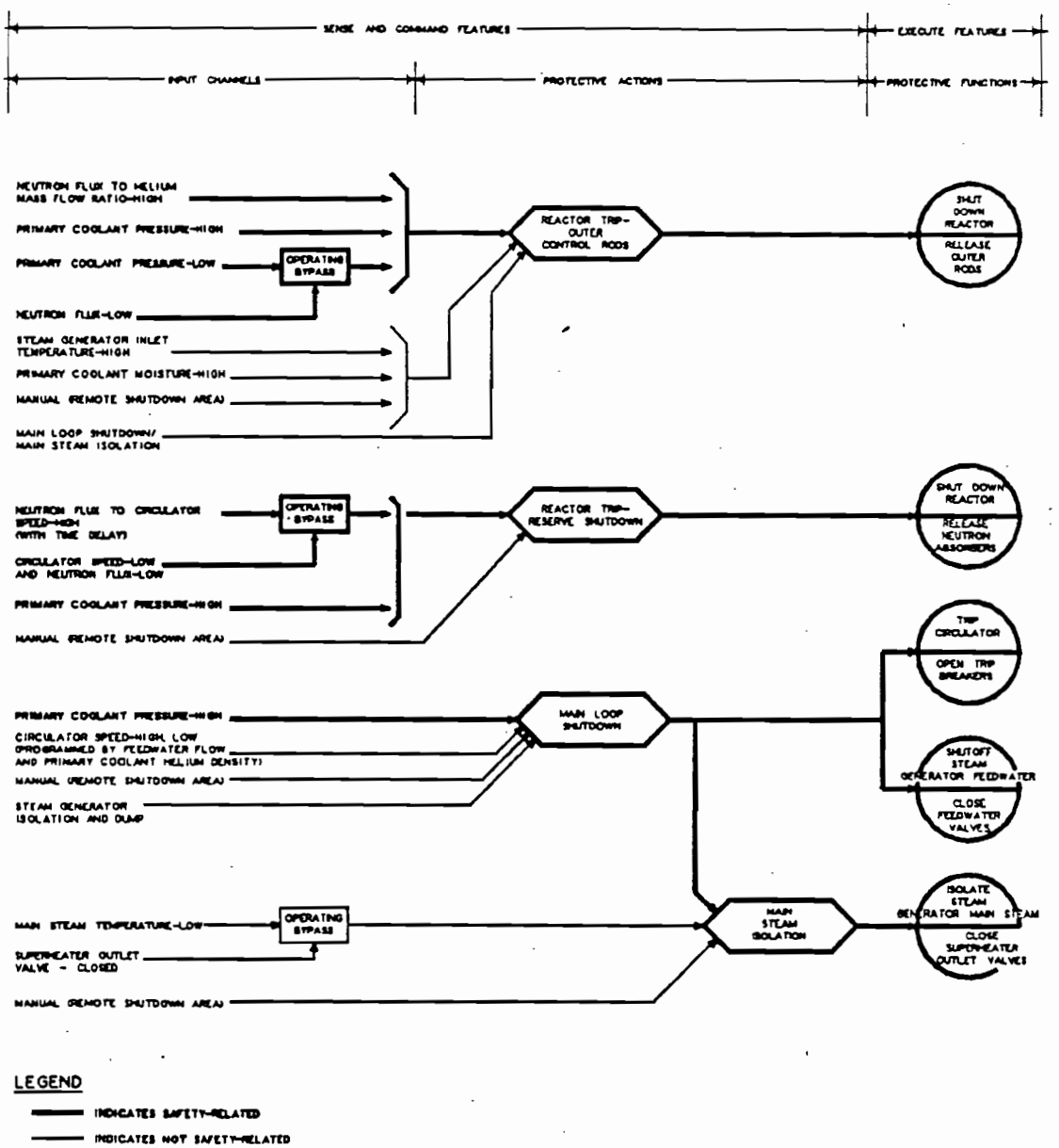


Figure 2-8 SAFETY PROTECTION SUBSYSTEM FUNCTIONAL OVERVIEW

2.2.2.1 Reactor Trip Using Outer Control Rods

This "safety-related" trip subsystem initiates a rapid reduction in reactor power following excessive reactivity increases, loss of adequate core cooling, water ingress events, or breach of the primary coolant barrier, by initiating the automatic insertion of all outer control rods, including any that may be in the process of being withdrawn. A simplified one channel block diagram is shown in Figure 2-9.

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

1. Neutron Flux to helium mass flow ratio high.

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

3. Primary coolant pressure high.

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

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

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

7. Manual initiation (not required for safety).

The reactor trip subsystem actuated equipment are the outer control rods and their release mechanisms. Upon initiation of the reactor trip signal all outer control rods are released and fully inserted in the core. On occurrence of a reactor trip, the reactor trip subsystem sends signals to

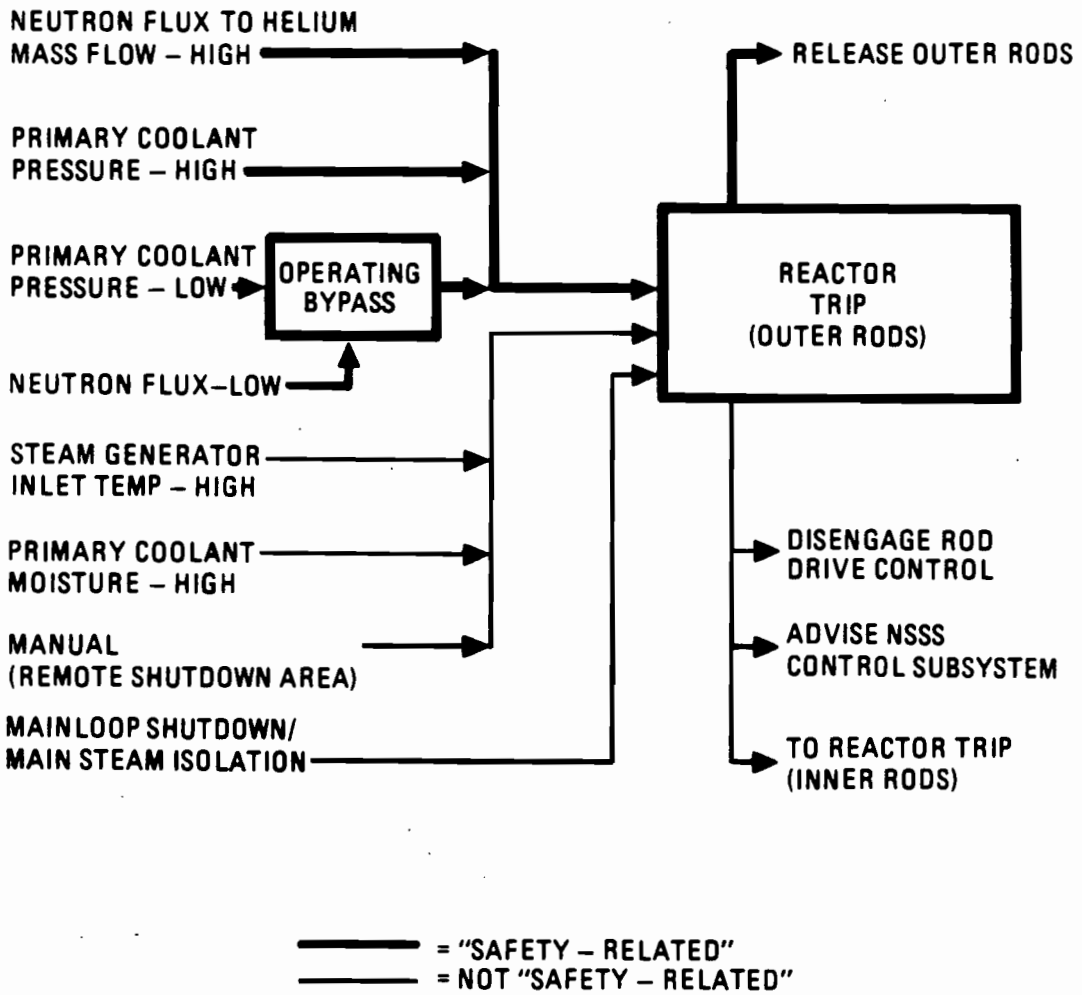


Figure 2-9
SIMPLIFIED BLOCK DIAGRAM REACTOR TRIP - OUTER CONTROL RODS

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

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

2.2.2.2 Reactor Trip Using Reserve Shutdown Control Equipment

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

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

The actuated equipment for this reactor trip subsystem are the reserve shutdown control equipment fusible links. Upon actuation the fusible links are energized, they open, causing the reserve shutdown hoppers to release the reserve shutdown material into receiver channels in fuel columns adjacent to the inner reflector. The protective action is completed when the reserve shutdown hoppers empty and the resulting negative reactivity in the reactor core shuts down the reactor. Upon initiation of a reactor trip

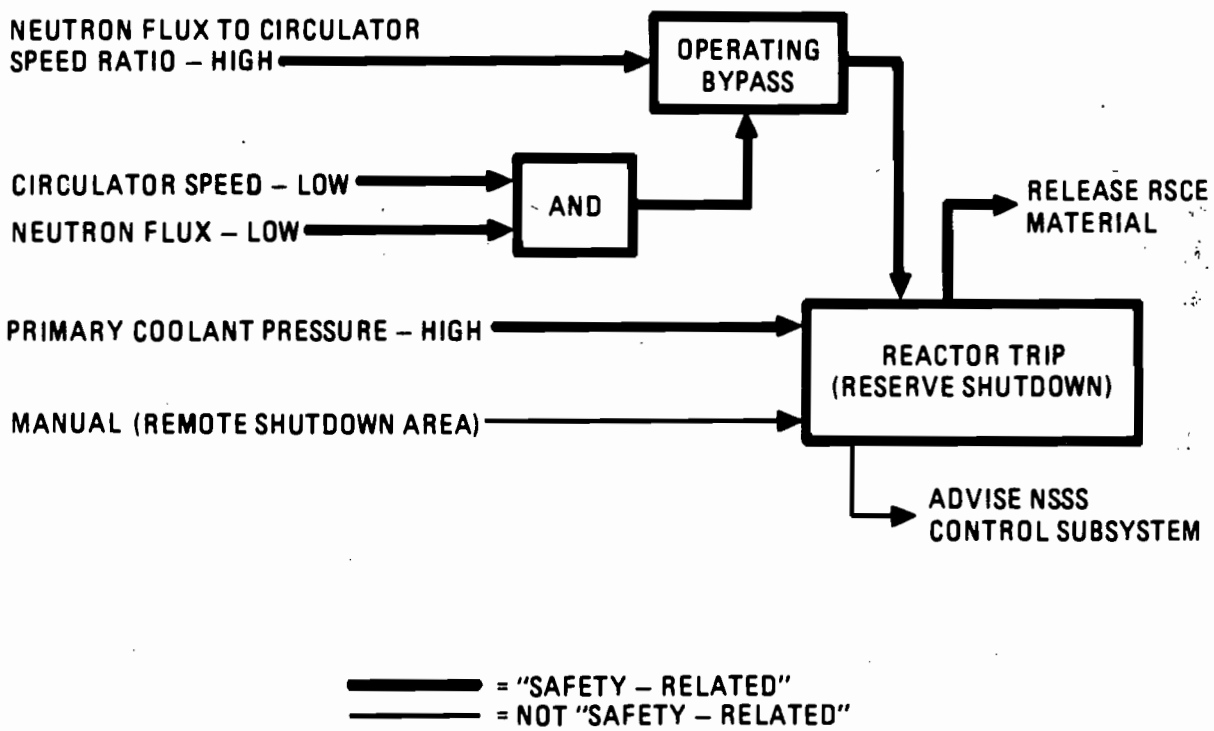


Figure 2-10
SIMPLIFIED BLOCK DIAGRAM, REACTOR TRIP - RESERVE SHUTDOWN CONTROL EQUIPMENT

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

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

2.2.2.3 Main Loop Shutdown and Main Steam Isolation

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

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

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

1. Primary coolant pressure high.

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

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

4. Manual initiation (not required for safety).

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

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

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

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

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

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

2.2.3 Special Nuclear Area Instrumentation Subsystem

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

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

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

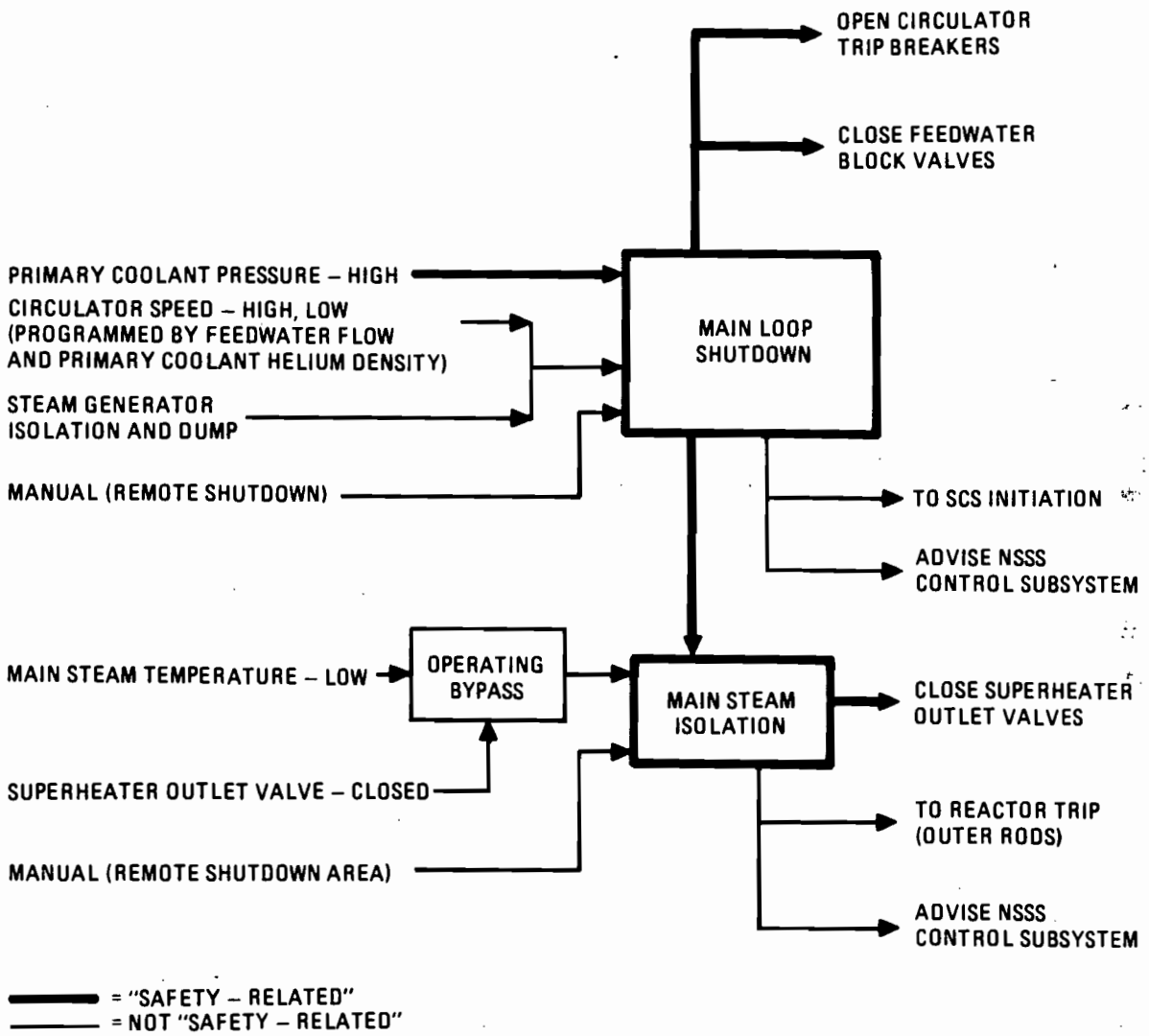


Figure 2-11
SIMPLIFIED BLOCK DIAGRAM, MAIN LOOP SHUTDOWN AND MAIN STEAM ISOLATION

The post-accident monitoring (PAM) instrumentation indicates plant information which is required by the operating personnel during accident situations to (1) provide information required to permit the operator to assess that the reactor is safely shut down and is being cooled; (2) determine whether reactor trip and other "safety-related" systems are performing their intended functions; and (3) provide information to the operators that will enable them to determine status of radioactivity barriers. In addition to the above, the post accident monitoring instrumentation processes data that provides information on the operation of plant "safety-related" systems and other systems that are required by the operating personnel during and accident to (1) furnish data regarding the operation of plant systems so the operator can make appropriate decisions as to their use, and to (2) provide information regarding the release of radioactive materials.

2.2.3.1 Vessel System Pressure Relief Block Valve Closure Interlock

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

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

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

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

2.2.3.2 Safety Protection Information Displays

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

1. Safety protection channel readouts.

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

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

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

2.2.3.3 Investment Protection Information Displays

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

1. Investment protection channel readouts.

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

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

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

2.2.3.5 Post-Accident Monitoring Instrumentation

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

2.3 SYSTEM PERFORMANCE CHARACTERISTICS

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

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

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

2.3.1 System Operating Modes

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

Table 2-2 PLANT PROTECTION AND INSTRUMENTATION SYSTEM PROTECTIVE ACTIONS

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

Table 2-2 (Continued)

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

[a]Numbers in { } estimated.

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

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

Table 2-3 (Continued)

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

Table 2-3 (Continued)

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

Table 2-3 (Continued)

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

(a){ } = numbers are estimated.

908444/2

Table 2-4
PLANT PROTECTION AND INSTRUMENTATION SYSTEM ACTUATED EQUIPMENT

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

Table 2-4 (Continued)

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

(a) { } = numbers are estimated.

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

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

2.3.2 System Steady State Performance

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

2.3.3 System Response to Plant Transients

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

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

2.3.3.1 System Response to Anticipated Operational Occurrences (AOOs)

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

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

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

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

Table 2-6 PLANT PROTECTION AND INSTRUMENTATION TRIP PARAMETERS

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

* [ ] = Number Tentative

Table 2-6 (Continued)

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

*[ ] = Number Tentative

Table 2-6 (Continued)

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

Table 2-6 (Continued)

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

*[ ] = Number Tentative

Table 2-6 (Continued)

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

*[ ] = Number Tentative

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.3.2 System Response to Design Basis Events (DBEs)

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

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

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

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

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

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

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

<u>DBE No. 2 HTS Transient Without Control Rod Trip</u>. The initiating event for DBE No. 2 is main loop cooling rampdown with a failure of reactor trip using the outer control rods to take place. Trouble with the main cooling

loop is detected as a circulator speed to feedwater flow mismatch and the PPIS commands a main loop shutdown. Main loop shutdown and high neutron flux to circulator speed ratio commands a reactor trip using the outer control rods. For this DBE, the outer control rods fail to trip. This situation is detected as a high neutron flux to circulator speed ratio measurement. If after a time delay the reactor trip using the outer control rods has not executed protective action, reactor trip using the reserve shutdown control equipment is commanded. Main loop shutdown also signals for Shutdown Cooling System initiation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.3.3 System Performance Under Safety-Related Design Conditions

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

SRDC No. 1 Pressurized Conduction Cooldown. SRDC No. 1 includes loss of offsite power and trip of both turbines. A loss of offsite power and turbine trip causes a loss of all primary ac power supplies. This causes the main loop helium circulator to coast down due to loss of power. This loss of primary coolant flow is detected by the PPIS as a high neutron flux to helium mass flow measurement and the PPIS commands a reactor trip using the outer control rods. The Safety Protection Subsystem takes no further action for this SRDC. If primary ac power is not restored and standby ac power is not available, the Safety Protection Subsystem loses battery backup power after approximately one hour. At this time the Safety Protection Subsystem fails "as is" since it has no further "safety-related" function to perform. Environmental conditions or other plant service conditions experienced during SRDC No. 1 have no effect on the ability of the Safety Protection Subsystem to perform its function.

SRDC No. 2 Pressurized Conduction Cooldown Without Control Rod Trip. SRDC No. 2 includes main loop cooling rampdown with a failure of reactor trip using the outer control rods to take place. This situation is detected by the PPIS as a high neutron flux to circulator speed ratio measurement. If after a time delay, the reactor trip using the outer control rods has not executed protective action, the PPIS commands a reactor trip using the reserve shutdown control equipment. Environmental conditions or other plant service conditions experienced during SRDC No. 2 have no effect on the ability of the Safety Protection Subsystem to perform its function.

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.4 System Failure Modes and Effects

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

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

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

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

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

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

2.4 SYSTEM ARRANGEMENT

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

The Special Nuclear Area Instrumentation Subsystem is arranged into modular electronic components. Each of the four MHTGR reactor modules has separate Special Nuclear Area Instrumentation associated with that reactor module. The Special Nuclear Area Instrumentation equipment includes its own operator interface equipment, operator interface equipment for the Safety Protection Subsystem, and operator interface equipment for the Investment Protection Subsystem. This operator interface equipment is located in the Reactor Building Electrical area and remote shutdown area (located in the

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

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

Table 2-7 (Continued)

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

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

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

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

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

Table 2-8 (Continued)

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

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

908444/2

Table 2-8 (Continued)

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

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

Table 2-8 (Continued)

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

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

Table 2-8 (Continued)

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

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

Table 2-8 (Continued)

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

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

Table 2-8 (Continued)

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

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

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

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

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

2.5 INSTRUMENTATION AND CONTROL

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

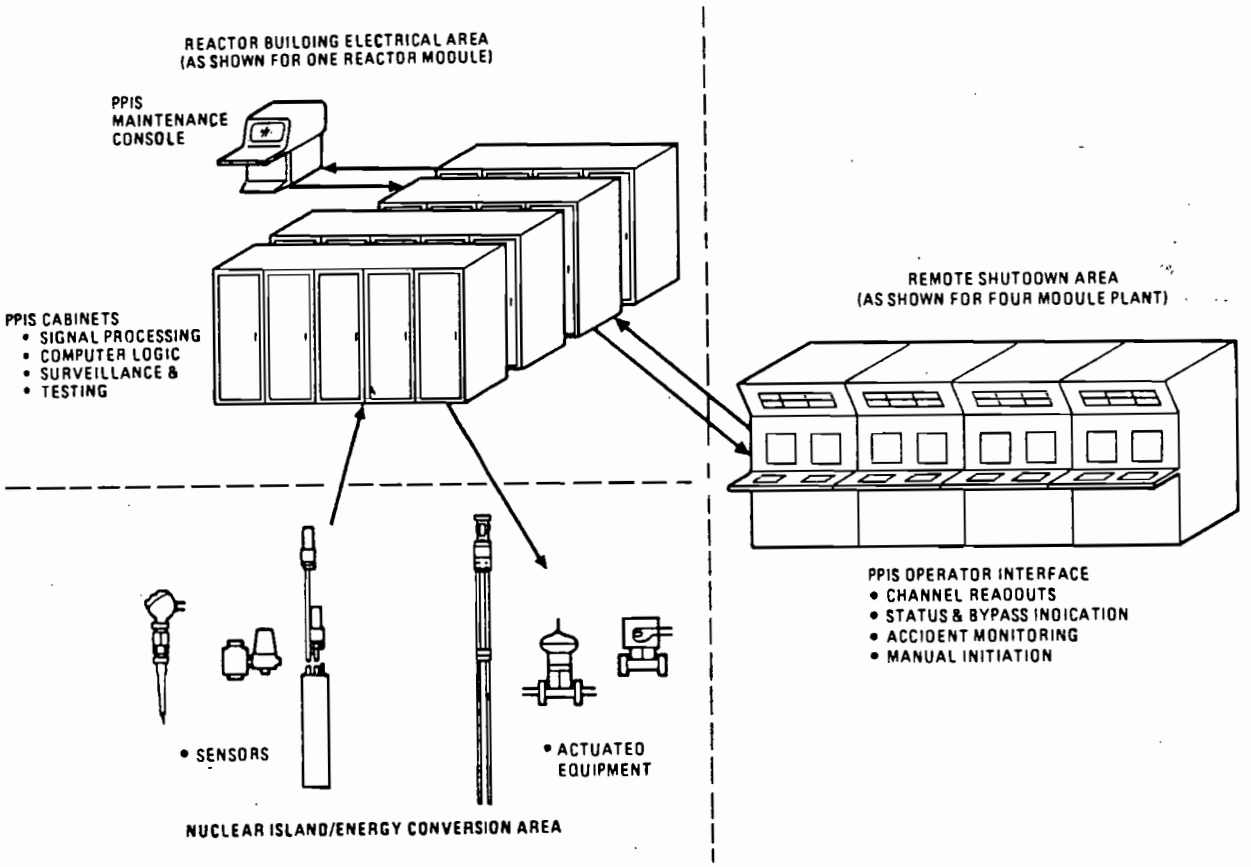


Figure 2-12
PLANT PROTECTION AND INSTRUMENTATION SYSTEM EQUIPMENT ARRANGEMENT

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

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

Table 2-9 (Continued)

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

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

SECTION 3
SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

3.1 SUBSYSTEM FUNCTIONS

3.1.1 Investment Protection Subsystem Functions

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

3.1.2 Safety Protection Subsystem Functions

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

3.1.3 Special Nuclear Area Subsystem Functions

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

3.2 SUBSYSTEM DESIGN REQUIREMENTS

3.2.1 Investment Protection Subsystem Design Requirements

3.2.1.1 Subsystem Configuration and Essential Features Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2.1.2 Operational Requirements

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

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

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

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

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

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

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

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

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

3.2.1.3 Structural Requirements

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

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

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

3.2.1.4 Environmental Requirements

The Investment Protection Subsystem shall be capable of performing its functions before, during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions shown in Tables 3-1, 3-2, and 3-3. (3200.0302.120)

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

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

3.2.1.5 Instrumentation and Control Requirements

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

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

Table 3-1
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

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

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

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

Table 3-2
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

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

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

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

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

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

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

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

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

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

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

3.2.1.6 Surveillance and In-Service Inspection Requirements

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

3.2.1.7 Availability Assurance Requirements

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

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

3.2.1.8 Maintenance Requirements

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

Table 3-4 RELIABILITY ALLOCATIONS TO INVESTMENT PROTECTION SUBSYSTEM

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

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

Table 3-5
SCHEDULED OUTAGE ALLOCATION TO INVESTMENT PROTECTION SUBSYSTEM

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

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

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

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

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

3.2.1.9 Safety Requirements

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

3.2.1.10 Industry Codes and Standards Requirements

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

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

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

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

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

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

3.2.1.11 Quality Assurance Requirements

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

3.2.1.12 Construction Requirements

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

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

3.2.1.13 Decommissioning Requirements

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

3.2.2 <u>Safety Protection Subsystem</u>

3.2.2.1 Subsystem Configuration and Essential Features Requirements

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

(3200.0302.301)

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

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

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

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

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

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

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

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

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

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

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

3.2.2.2 Operational Requirements

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

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

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

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

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

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

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

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

3.2.2.3 Structural Requirements

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

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

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

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

3.2.2.4 Environmental Requirements

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

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

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

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

3.2.2.5 Instrumentation and Control Requirements

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

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

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

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

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

Table 3-7
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

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

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

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

Table 3-8
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

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

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

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

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

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

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

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

3.2.2.6 Surveillance and In-Service Inspection Requirements

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

3.2.2.7 Availability Assurance Requirements

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

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

3.2.2.8 Maintenance Requirements

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

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

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

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

Table 3-10 RELIABILITY ALLOCATIONS TO SAFETY PROTECTION SUBSYSTEM

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

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

Table 3-11
SCHEDULED OUTAGE ALLOCATION TO SAFETY PROTECTION SUBSYSTEM

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

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

3.2.2.9 Safety Requirements

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

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

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

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

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

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

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

Table 3-12 SAFETY-RELATED DESIGN CONDITIONS

Pressurized Conduction Cooldown
(SRDC No. 1)

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

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

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

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

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

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

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

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

3.2.2.10 Industry Codes and Standards Requirements

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

3.2.2.11 Quality Assurance Requirements

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

3.2.2.12 Construction Requirements

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

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

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

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

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

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

3.2.2.13 Decommissioning Requirements

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

3.2.3 Special Nuclear Area Instrumentation Subsystem

3.2.3.1 Subsystem Configuration and Essential Features Requirements

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

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

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

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

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

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

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

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

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

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

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

3.2.3.2 Operational Requirements

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

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

3.2.3.3 Structural Requirements

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

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

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

3.2.3.4 Environmental Requirements

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

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

Table 3-14
EXTERNAL ENVIRONMENTAL CONDITIONS
(Normal)

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

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

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

Table 3-15
EXTERNAL ENVIRONMENTAL CONDITIONS
(Abnormal)

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

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

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

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

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

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

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

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

3.2.3.5 Instrumentation and Control Requirements

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

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

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

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

3.2.3.6 Surveillance and In-Service Inspection Requirements

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

3.2.3.7 Availability Assurance Requirements

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

3.2.3.8 Maintenance Requirements

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

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

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

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

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

3.2.3.9 Safety Requirements

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

3.2.3.10 Codes and Standards Requirements

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

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

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

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

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

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

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

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

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

3.2.3.11 Quality Assurance Requirements

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

3.2.3.12 Construction Requirements

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

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

3.2.3.13 Decommissioning Requirements

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

SECTION 4
SYSTEM AND SUBSYSTEM INTERFACES

4.1 INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

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

4.2 SUBSYSTEM BOUNDARY DEFINITION

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

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

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

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

4.1.1 Identification of Interfaces Between Systems

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

Table 4-1 (Continued)

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

Table 4-1 (Continued)

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

Table 4-1 (Continued)

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

Table 4-1 (Continued)

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

908444/2

SECTION 5
SYSTEM CONSTRUCTION

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

5.1 PACKAGING AND SHIPPING

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

5.2 HANDLING AT DELIVERY

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

5.3 RECEIVING INSPECTION

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

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

5.4 STORAGE

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

5.5 ACCESS

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

5.6 INSTALLATION AND/OR FIELD FABRICATION

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

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

5.7 CONSTRUCTION TESTING

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

5.8 AS-BUILT DRAWINGS

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

SECTION 6
SYSTEM OPERATION

6.1 SYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

6.1.1 System Limitations and Setpoints

Trip setpoints are conservatively established to assure that component damage limits are not reached. Figure 6-1 illustrates the relationship between trip setpoints and damage limits. The limiting protection system settings (allowable values) conservatively bound component damage thresholds so that if the limiting protection system setting is reached, automatic protective action corrects the abnormal situation before the damage threshold is exceeded. The limiting protection system setting takes into consideration sensor calibration errors, instrument accuracy, and transient overshoot. The actual protection system settings (trip setpoints), are conservatively bounded by the limiting protection system settings with allowance for instrument and setpoint drift. The lower setpoint limit is specified to prevent unnecessary system trips during normal operation transients. The SRDC and DBE transient analysis is performed at the "analysis trip level."

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

6.1.2 Precautions

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

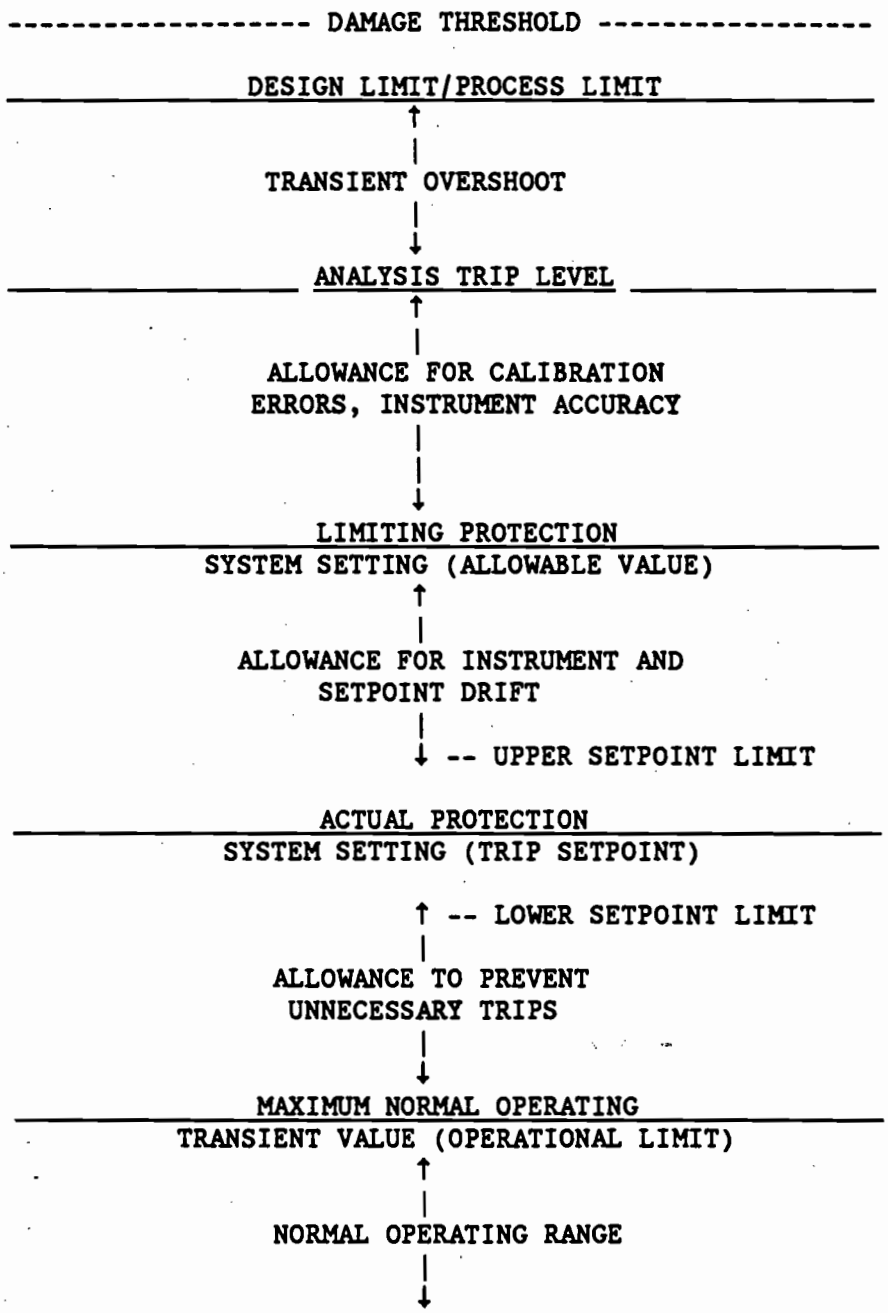


Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS AND COMPONENT DAMAGE LIMITS

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

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

Table 6-1 (Continued)

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

Table 6-1 (Continued)

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

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

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

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

6.2 PREOPERATIONAL CHECKOUT

6.2.1 Initial Preoperational Checkout

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

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

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

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

6.2.2 Routine Preoperational Checkout

The following prerequisites are required for routine preoperational checkout:

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

Checkout Procedure

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

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

2. Energize system, reset trips.

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

4. Calibrate readout instruments.

5. Confirm input channel operability.

6. Confirm channel trip operability, reset trip.

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

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

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

10. Monitor outputs to actuators.

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

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

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

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

6.3 STARTUP/SHUTDOWN

6.3.1 Startup to 25% Steam Flow

6.3.1.1 Prerequisites

The following prerequisites are required for plant startup:

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

6.3.1.2 Procedure

The startup procedure includes:

1. Reset Reactor Trip circuitry.

2. Reset any First-In Trip Annunciators.

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

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

6.3.2 Shutdown from 25% Steam Flow

The shutdown procedure includes:

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

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

6.4 NORMAL OPERATION

The procedures for normal operation are as follows:

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

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

6.5 REFUELING

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

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

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

6.6 SHUTDOWN

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

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

6.6.1 Automatic Plant Shutdowns

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

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

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

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

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

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

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

6.6.2 Plant Protection and Instrumentation System Shutdown

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

6.7 ABNORMAL OPERATION

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

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

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

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

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

6.8 CASUALTY EVENTS AND RECOVERY PROCEDURES

6.8.1 Casualty Events

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

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

2. Failure of a sensor.

3. Failure of component/module.

4. Failure of test units.

5. Electrical overload or loss of electrical power.

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

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

6.8.1.1 Logic or Output Channel Failures

Logic or output actuating channel failures include:

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

2. Failure of a component/module.

3. Failure of test units.

4. Electrical overload or loss of electrical power.

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

6.8.1.2 System Failures

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

1. Spurious trips resulting in unwanted protection actions.

2. Failure of the system to perform upon command.

6.8.2 Design Features to Mitigate Effects of Casualty Events

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

6.8.2.1 Input Sensing Channels

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

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

Loss of electrical power is alarmed.

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

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

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

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

6.8.2.2 Logic and Output Channels

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

Loss of electrical power is alarmed.

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

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

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

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

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

6.8.2.3 System Considerations

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

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

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

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

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

6.8.3 Recovery Procedures

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

6.8.3.1 Recovery from Sensor Channel Failures

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

6.8.3.2 Recovery from Logic and Output Channel Failures

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

6.8.3.3 Recovery from System Failures

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

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

SECTION 7
SYSTEM MAINTENANCE

7.1 MAINTENANCE APPROACH

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

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

1. Adjust in place.

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

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

7.2 CORRECTIVE MAINTENANCE

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

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

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

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

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

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

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

7. Proceed with the repair/maintenance.

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

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

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

7.3 PREVENTIVE MAINTENANCE

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

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

7.4 IN-SERVICE INSPECTION

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

7.5 SURVEILLANCE

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

7.5.1 Instrument Checks

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

7.5.2 Functional Tests

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

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

2. Manual control of electrically operated valves.

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

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

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

6. Testing of protection system status and bypass indications.

7.5.3 Calibration Verification Tests

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

7.5.4 Response Time Verification Tests

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

SECTION 8
SYSTEM DECOMMISSIONING

[TBD]

SECTION 9
REFERENCES

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

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

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

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

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

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

APPENDIX A
TRACEABILITY OF REQUIREMENTS

1. INTRODUCTION

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

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

TABLE A-1
TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-1 (Continued)

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

TABLE A-2

TRACEABILITY SUMMARY REFERENCE LIST

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

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

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

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

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

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

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

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

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

10. "NSSS Control Subsystem Design Description," HTGR-86-051, Rev. 1, (HFD-43701, Rev. 2) (908468, Rev. 2).

11. "Reactor Cavity Cooling System Design Description," HTGR-(later), Rev. 0, (HFD-35600, Rev. 1) (908442, Rev. 1).

12. "Main and Bypass Steam System Description," HTGR-(later) (HFD-45004, Rev. 1) (908516, Rev. 1).

13. "Core Refueling Subsystem Design Description," HTGR-86-097, Rev. 1, (HFD-43413, Rev. 2) (908500, Rev. 2).

APPENDIX B

DRAWINGS LIST

Ref. No.	Drawing No.	Title
1	GA Drawing 029950	IB Diagram - MHTGR Investment Protection Subsystem (GA Proprietary Information)
2	GA Drawing 029951	IB Diagram - MHTGR Safety Protection Subsystem (GA Proprietary Information)
3	GA Drawing 030055	IB Diagram - MHTGR Plant Protection and Instrumentation Systems Equipment and Locations

APPENDIX C
TRANSIENTS

Plant transients do not directly affect the performance of the Plant Protection and Instrumentation System. The PPIS is environmentally qualified to assure performance of its functions during all plant transients. The performance of the PPIS affects the outcome of various plant transients. The results of these plant transients are shown in DOE-HTGR-86-121, Revision 1 (908754/1), "Modular High Temperature Gas-Cooled Reactor Plant Design Basis Transients Analysis," April 1987.

Unprotected transients that contribute to the designs of the PPIS are given in "Unprotected Transients for PPIS Designs," Document 908940/0.

APPENDIX D
DESIGN BASIS SEISMIC INPUTS

[LATER]

APPENDIX E

PLANT PROTECTION AND INSTRUMENTATION SYSTEM PARAMETERS AND MAJOR FEATURES

A. GENERAL

Number of subsystems = Three
Input logic = Two out of four

Equipment location = Local, reactor building equipment room, reserve shutdown area

Subsystems and classification

Investment Protection Subsystem - not "safety-related"
Safety Protection Subsystem - "safety-related"
Special nuclear area instrumentation - not "safety-related"

Applicable Industry Standards

Safety Protection Subsystem - IEEE-603

B. INVESTMENT PROTECTION SUBSYSTEM

Reactor Trip - Inner control rods

Trip Parameters:

1. Primary coolant moisture-high.
2. Manual initiation.

Actuated Equipment:

1. Release mechanisms - inner control rods.

Steam Generator Isolation and Dump

Trip Parameters:

1. Primary coolant moisture-high.
2. Manual initiation.

Actuated Equipment:

1. Steam generator dump valves (4).
2. Signal to main loop shutdown and main steam isolation.

Primary Coolant Pressure Pumpdown.

Trip Parameters:

1. Primary coolant pressure low and reactor building radiation high.

2. Manual initiation.

Actuated Equipment:

1. Purification system pumpdown sequencer.

Shutdown Cooling System Initiation

Trip Parameters:

1. Main loop shutdown (to start the Shutdown Cooling System).

2. Manual initiation.

Actuated Equipment:

1. Shutdown Cooling System start circuitry.

Shutdown Cooling Heat Exchanger Isolation.

Trip Parameters:

1. Shutdown cooling system helium leak.
2. Manual initiation.

Actuated Equipment:

1. Inlet water block valves (2).
2. Outlet water block valves (2).
3. Heat exchanger drain valves (2).

C. SAFETY PROTECTION SUBSYSTEM ("SAFETY-RELATED")

Reactor Trip - Outer Control Rods.

Trip Parameters:

1. Neutron flux to helium mass flow ratio high.

2. Primary coolant pressure low.

3. Primary coolant pressure high.

4. Primary coolant moisture concentration high (not required for safety).

5. Main loop shutdown and main steam isolation trip signal (not required for safety).

6. Steam generator inlet helium temperature high (not required for safety).

7. Manual initiation (not required for safety).

Actuated Equipment:

1. Release mechanisms - outer control rods.

Reactor Trip - Reserve Shutdown.

Trip Parameters:

1. Reactor neutron flux to main helium circulator speed ratio - high.

2. Primary coolant pressure high.

3. Manual initiation (not required for safety).

Actuated Equipment:

1. Release mechanisms - reserve shutdown material.

Main Loop Shutdown and Main Steam Isolation.

Trip Parameters:

1. Primary coolant pressure high.

2. Circulator speed high or low (programmed by feedwater flow and helium density) (not required for safety).

3. Main steam temperature low (not required for safety).

4. Steam generator dump and isolation signal (not required for safety).

5. Manual initiation (not required for safety).

Actuated Equipment:

1. Feedwater block valves (2).
2. Superheater outlet valves (2).
3. Circulator motor trip contactors (2).

D. SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM

Vessel Pressure Relief Block Valve Closure Interlock.

Inputs: Block valve limit switches.

Outputs: Interlocks to prevent block valve closing.

Logic: 1 of 2

Safety and Investment Protection Information Displays.

Readouts:

1. All protection system input sensors and channels.

2. All protection subsystem status indications including status indications for actuation devices, actuated equipment, and auxiliary supporting features.

3. All protection system bypass indications including bypass indications for actuation devices, actuated equipment, and auxiliary supporting features.

4. Post accident monitoring.

Integrated Display System Requirements

Number of Inputs	
Internal to protection system	[100]*
External - analog	[50]
External - digital	[50]
Frequency to Poll Parameters	[Once per 10 s]
Number of Displays (Overviews, Safety, and Investment Protection Subsystems' Status, Status of Bypasses, Plant Status, Accident Monitoring, etc.)	
Displays	Color CRTs
Historical Trending	
Time history of variables available for trending	[30 minutes]
Number of variables for trending	[100]
Recording Capability	Magnetic Tape
Interfacing Protocol	RS-232

*Value of brackets [ ] is tentative.

APPENDIX F
PROPRIETARY CLAIMS

[NONE]

HTGR-86-049

HTGR

INVESTMENT PROTECTION SUBSYSTEM DESIGN DESCRIPTION

[redacted]

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

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 the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HTGR–86–049
908497/1

INVESTMENT PROTECTION SUBSYSTEM

DESIGN DESCRIPTION

[redacted]

An[redacted]ument
or [redacted] Data Herein to Third Parties Representing
For[redacted]ign Com-
pa[redacted]bsidiaries or Foreign Divisions of
[redacted], HTR
[redacted] Department of Energy.

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 Technologies Inc.

GA 1485 (REV. 10/82)

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 [redacted]	G.C.Bramblett		Initial issue (HFD-43201 Rev. 0) 6352-320-103

[redacted] ment [redacted] ther Data Therein to Third Parties Representing Foreign [redacted] Com- [redacted] U.S. Companies Shall Be Approved by the Director, HTR Develop[redacted] of Energy.

CONTINUE ON GA FORM 1485-1

Cover Sheets = 2 (Unnumbered)

Issue Summary 1,1a	2		
ii through xvii	13	A-1 through A-8	8
1-1 through 1-29	29	B-1	1
2-1 through 2-25	25	C-1	1
3-1	1	D-1	1
4-1 through 4-5	5	E-1	1
5-1 through 5-3	3	F-1	1
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

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
INVESTMENT PROTECTION SUBSYSTEM DESIGN DESCRIPTION	908497	1

INFO 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 J. Bauer	C.Rodriguez F.A.Silady Interface Assurance	G.P.Connors	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

	PAGE
LIST OF EFFECTIVE PAGES	ii
LIST OF APPENDICES	vii
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS AND ACRONYMS	x
DEFINITIONS	xi
PREFACE	xv
SUMMARY	xvii
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Integrated Approach Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-3
1.2.3 Structural Requirements	1-10
1.2.4 Environmental Requirements	1-15
1.2.5 Instrumentation and Control Requirements	1-15
1.2.6 Surveillance and In-Service Inspection Requirements	1-15
1.2.7 Availability Assurance Requirements	1-15
1.2.8 Maintenance Requirements	1-20
1.2.9 Safety Requirements	1-22
1.2.10 Codes and Standards Requirements	1-22
1.2.11 Quality Assurance Requirements	1-25
1.2.12 Construction Requirements	1-25
1.2.13 Decommissioning Requirements	1-29

CONTENTS (Continued)

		PAGE
2.	DESIGN DESCRIPTION	2-1
	2.1 Summary Description	2-1
	2.2 Subsystem Configuration	2-1
	2.2.1 Investment Protection Subsystem	2-2
	2.3 Subsystem Performance	2-6
	2.3.1 Subsystem Operating Modes	2-8
	2.3.2 Subsystem Steady-State Performance	2-8
	2.3.3 Subsystem Response to Plant Transients	2-8
	2.3.4 Subsystem Failure Modes and Effects	2-21
	2.4 Subsystem Arrangement	2-23
	2.5 Instrumentation and Control	2-23
3.	COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS	3-1
	3.1 Component Functions	3-1
	3.2 Component Design Requirements	
4.	SUBSYSTEM AND COMPONENT INTERFACES	4-1
	4.1 Subsystem Interface Requirements	4-1
	4.2 Component Boundary Definition	4-1

CONTENTS (continued)

		PAGE
5.	SUBSYSTEM CONSTRUCTION	5-1
5.1	Packaging and Shipping	5-1
5.2	Handling at Delivery	5-1
5.3	Receiving Inspection	5-2
5.4	Storage	5-2
5.5	Access	5-2
5.6	Installation and/or Field Fabrication	5-2
5.7	Construction Testing	5-3
5.8	As-Built Drawings	5-3
6.	SUBSYSTEM OPERATION	6-1
6.1	Subsystem Limitations, Setpoints, and Precautions	6-1
6.1.1	Operating Limits and Setpoints	6-1
6.1.2	Precautions	6-5
6.2	Preoperational Checkout	
6.2.1	Initial Preoperational Checkout	6-4
6.2.2	Routine Preoperational Checkout	6-5
6.3	Startup/Shutdown	6-7
6.3.1	Startup to 25% Steam Flow	6-7
6.3.2	Shutdown from 25% Steam Flow	6-8
6.4	Normal Operation	6-8

CONTENTS (continued)

		PAGE
6.5	Refueling	6-9
6.6	Shutdown	6-9
6.6.1	Automatic Plant Shutdowns	6-9
6.6.2	Plant Protection and Instrumentation System Shutdown	6-10
6.7	Abnormal Operation	6-10
6.8	Casualty Events and Recovery Procedures	6-11
6.8.1	Casualty Events	6-13
6.8.2	Design Features to Mitigate Effects of Casualty Events	6-14
6.8.3	Recovery Procedures	6-17
7.	SUBSYSTEM MAINTENANCE	7-1
8.	SUBSYSTEM DECOMMISSIONING	8-1
9.	REFERENCES	9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability of Requirements	A-1
B	Drawings	B-1
C	Transients	C-1
D	Design Basis Seismic Inputs	D-1
E	Parameter Lists	E-1
F	Proprietary Claims	F-1

LIST OF ILLUSTRATIONS

FIGURE		PAGE
1-1	Weekly Load Cycle	1-6
2-1	Protection System Data Busses	2-3
2-2	Arrangement of PPIS Equipment	2-2
6-1	Relationship Between Protection Setpoints and Component Damage Limits	6-2

LIST OF TABLES

TABLE		PAGE
1-1	Investment Protection Sensor Channel Parameters	1-4
1-2	Design Duty Cycle Events	1-7
1-3	HTGR Plant Transients	1-11
1-4	Plant Equipment Damage Limits for Use in Designing the Safety Protection Subsystem	1-12
1-5	External Environmental Conditions, Normal	1-16
1-6	External Environmental Conditions, Abnormal	1-13
1-7	External Environmental Conditions, Design Basis Event	1-18
1-8	Unavailability/Reliability Allocations	1-19
1-9	Equipment Classification	1-23
1-10	Industrial Codes and Standards Applicable to the Investment Protection Subsystem Design	1-24
1-11	Industrial Codes and Standards for Consideration in Investment Protection Subsystem Design	1-26
2-1	Plant Damage Limits for Use in Designing the Investment Protection Subsystem	2-7
2-2	Investment Protection Subsystem Protective Actions	2-9
2-3	Investment Protection Subsystem Actuated Equipment	2-10
2-4	Investment Protection Subsystem Operating Mode Versus Plant Condition	2-11
2-5	Investment Protection Subsystem Analysis Parameters	2-13
2-6	Failure Modes of Investment Protection Subsystem	2-22
2-7	Investment Protection Subsystem Equipment	2-25
4-1	Interface Requirements Imposed on Other Systems	4-2
6-1	Operating Limits and Setpoints for the Investment Protection Subsystem	6-3

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}

*Numbers in { } are estimated and subject to change.

Table 1-1 (Continued)

Monitored Variable → Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Sensor Channel Parameters: Minimum Accuracy	Sensor Channel Parameters: 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]

Fig. 1-1 Weekly Load Following Cycle

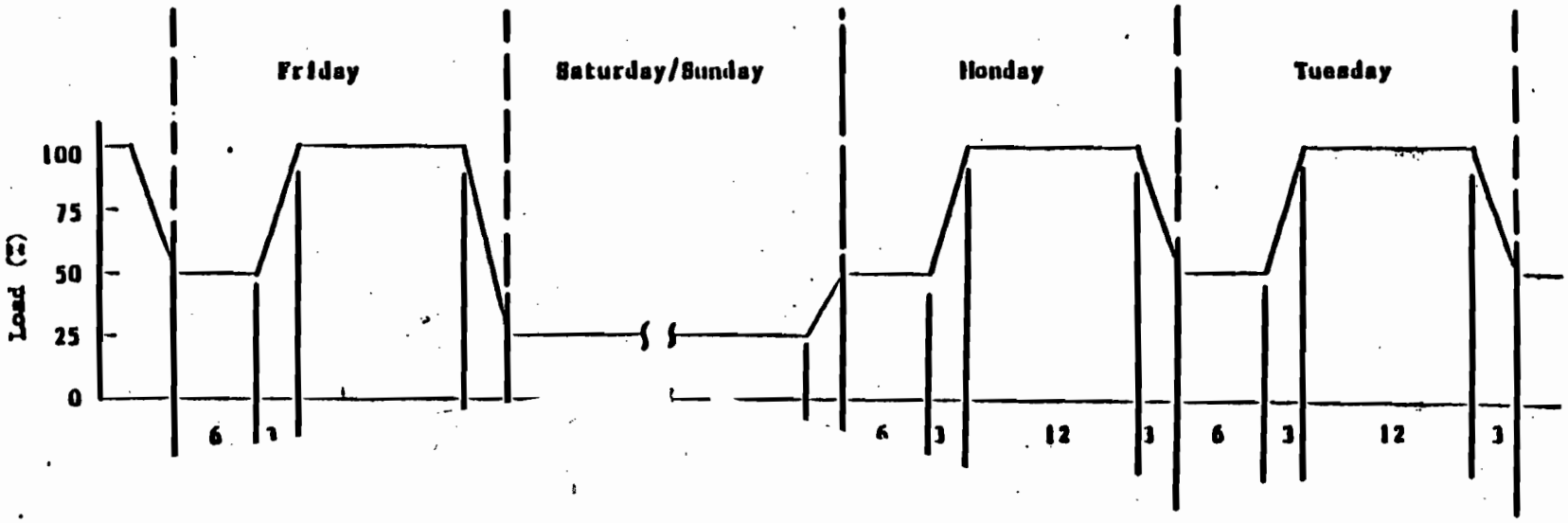


Table 1-2

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.

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)

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.

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.

908497/0

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

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.

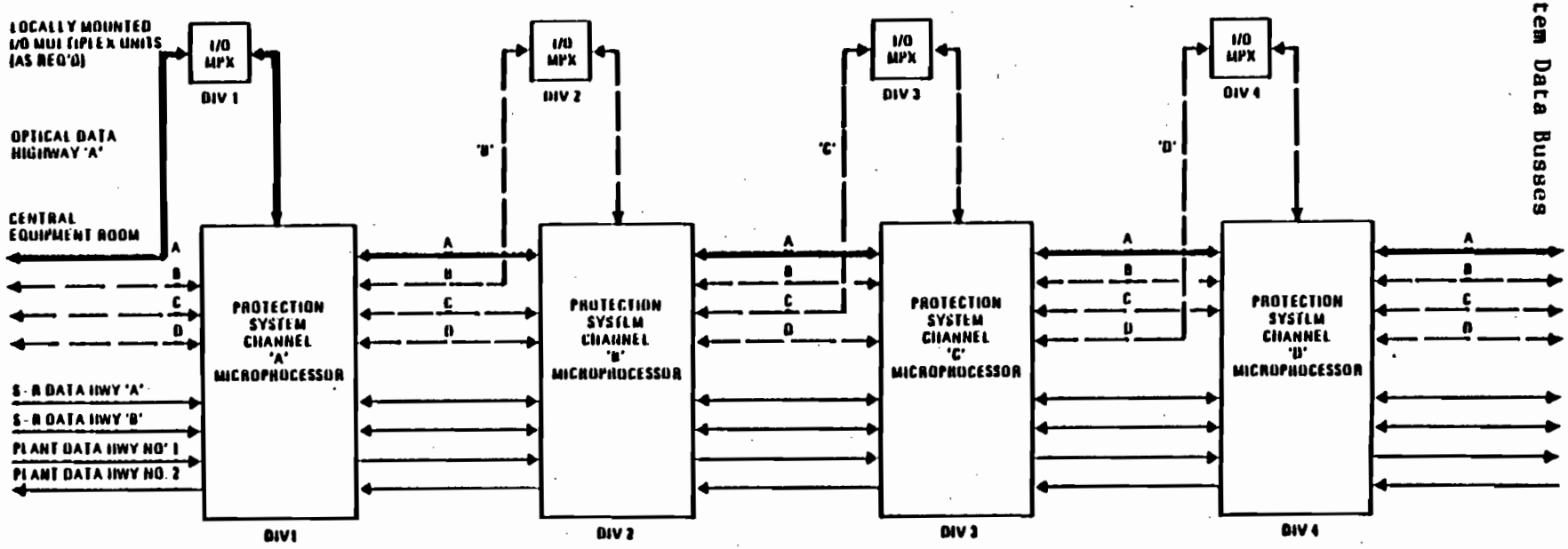
The design parameters of the Investment Protection Subsystem are based on the results of transient analysis, and are discussed in greater detail in Section 2.3.

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



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 not 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.

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	

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 main steam temperature not low	[625] psia and ≥[725]°F	[640] psia and ≥[740]°F	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s			Helium pressure measurement from reactor trip pressure measurement
					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

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
Steam generator isolation and dump	No	Primary coolant moisture concentration high	1200 ppmv	1000 ppmv	Moisture concentration (M)	[20] s	[5]* s	0 s	1 s	Main loop shutdown	(See main loop shutdown)	
										Steam generator dump valves	[5] s to open	
Steam generator dump terminate	No	Main steam pressure to primary coolant pressure ΔP low	[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 low and reactor building radiation high	[800] psia	[810] psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s	Helium purification system	[TBD] s	
			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

9084970

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 SRDC Performance

The Investment Protection Subsystem is not classified as safety-related; therefore, this section is not applicable.

2.3.4 Failure Modes and Effects

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

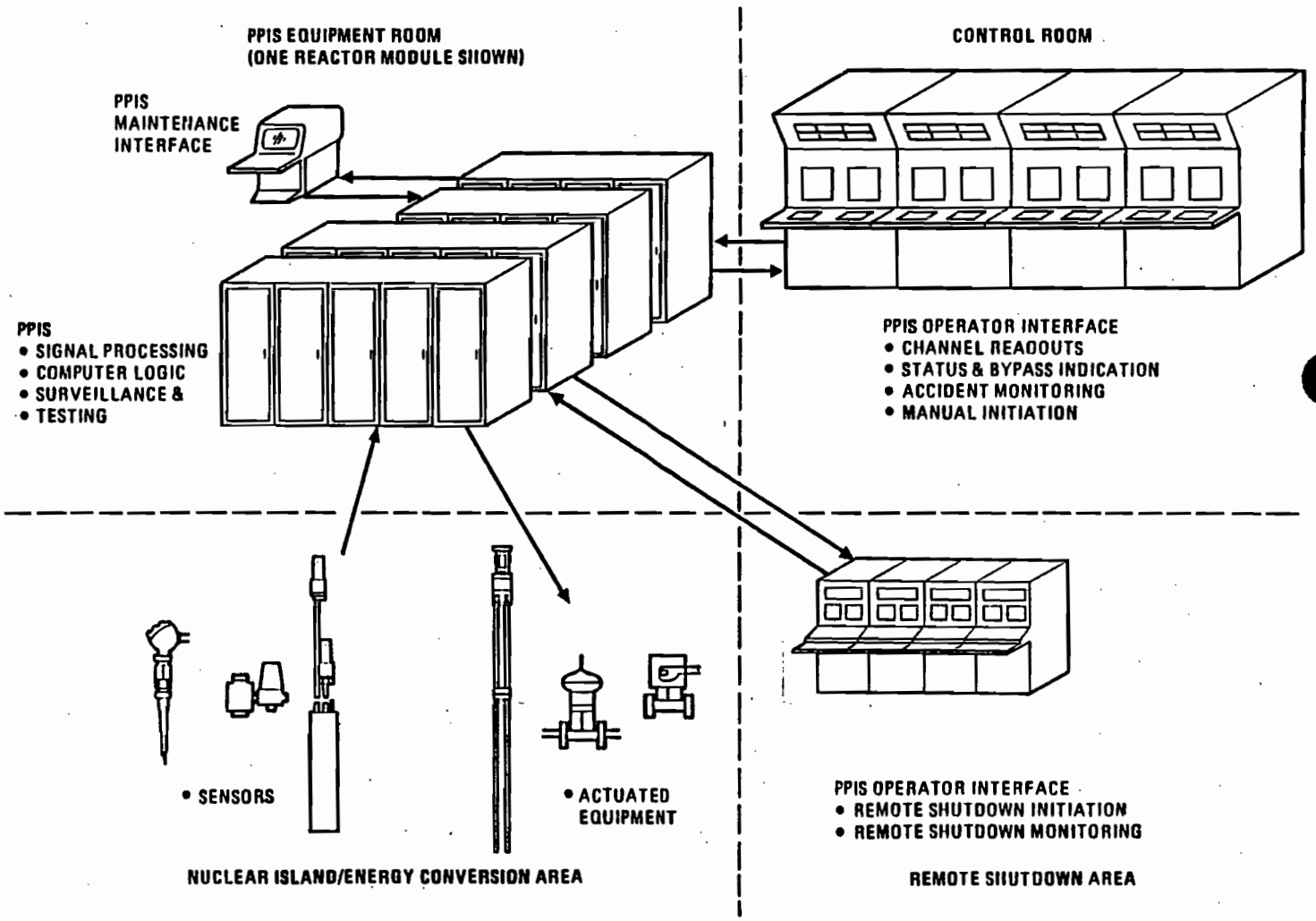


Table 2-7

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)

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.	Quantity: Four steam generator inlet thermowell access penetrations. (3201.0401.026)
4.1.1.3 Miscellaneous Control and Instrumentation Group (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.	Quantity: Four separate signals. (3201.0401.030)
4.1.1.4 Plant Protection and Instrumentation System (3200)			
Special Nuclear Area Instrumentation Subsystem (3203)	Provide monitoring of input channels and system status.	Isolated output electrical signals.	Quantity: Each input, each bypass, and output. (3201.0401.040)
4.1.1.5 Plant Control, Data, and Instrumentation System (3700)			
NSSS Control Subsystem (3701)	Adjust control system settings following investment protection trips.	Electrical signals.	Quantity: Five (reactor trip inner rods, main loop shutdown, SG isolation and dump, SCS initiation, and primary pressure pumpdown). (3201.0401.050)

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)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.7 Building, Structures, and Building Service Group (7000)			
Reactor Building (7001)	Provide building space and structural support to accommodate Investment Protection Subsystem	Floor mounting, piping, and electrcal.	Quantity: Nine cabinets, one hygrometer module, one compressor assembly, and one accumulator tank assembly. (3201.0401.090)
4.1.1.8 Mechanical Service Group (9000)			
HVAC (9011)	Provide HVAC to support the proper operation of the Investment Protection Subsystem.	None.	Quantity: Two. (3201.0401.100)
4.1.1.9 Electrical Group (9200)			
Non-Class 1E AC Distribution (9202)	Provide low-voltage ac distribution for the moisture monitor compressors.	Electric feeders.	Quantity: 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.	Quantity: Four separate Class 1E sources. (3201.0401.112)

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

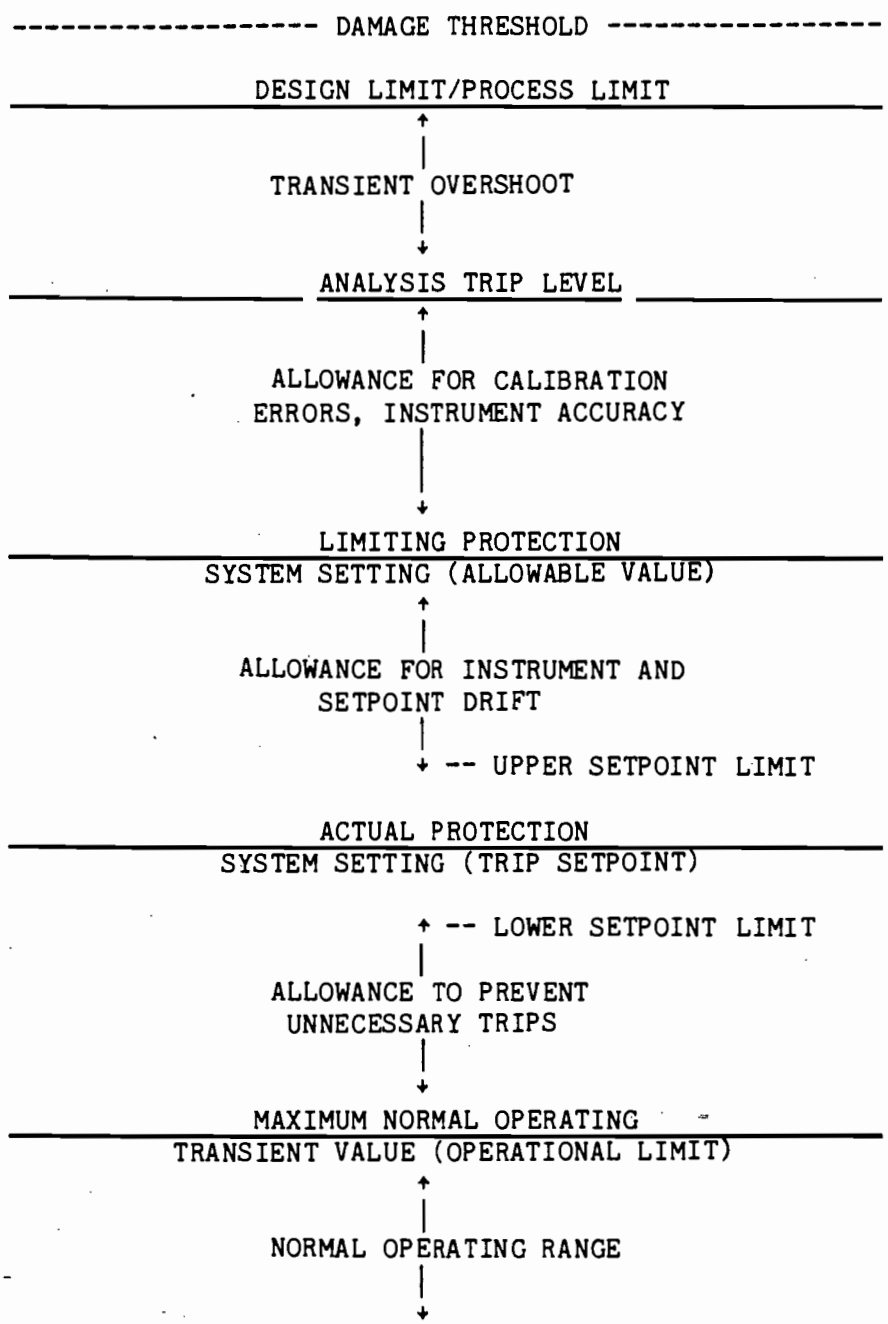


Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS AND COMPONENT DAMAGE LIMITS

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 Description/Reference Ref.	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 Description/Reference Ref.	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 Description/Reference Ref.	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

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

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	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]

HTGR-86-048

HTGR

SAFETY PROTECTION SUBSYSTEM DESIGN DESCRIPTION

[redacted]

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

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 the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HTGR–86–048
908498/1

SAFETY PROTECTION SUBSYSTEM

DESIGN DESCRIPTION

[redacted]

A[redacted]ent
or [redacted]g
Fo[redacted]
par[redacted]
U.S. [redacted]R
Development Division, U.S. Department of Energy.

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

NUCLEAR SAFETY-RELATED

TITLE					
SAFETY PROTECTION SUBSYSTEM DESIGN DESCRIPTION				☐ R&D ☐ DV&S ☒ DESIGN	APPROVAL LEVEL 5
DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO	ISSUE NO./LTR.
0	32 02	SSDD	6300	908498	1
QUALITY ASSURANCE LEVEL	SAFETY CLASSIFICATION	SEISMIC CATEGORY	ELECTRICAL CLASSIFICATION		
QAL I	SC 2	CAT I	1E		

INFO 11

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: FUNDING PROJECT	APPROVAL: APPLICABLE PROJECT	ISSUE DESCRIPTION/ CWBS NO.
0	JUN 27 1988	J.Zgliczynski J.Bauer	C.Rodriguez Interface Assurance [redacted] F.A.Silady	G.P.Connors [redacted]	G.Bramblett [redacted]	[redacted]	Initial issue (HFD-43202 Rev. 0) 6352-320-103

CONTINUE ON GA FORM 1485-1

Cover Sheets = 2 (Unnumbered

Issue Summary 1,1a	2		
ii through xvii	15	A-1 through A-7	7
1-1 through 1-31	31	B-1	1
2-1 through 2-26	26	C-1	1
3-1	1	D-1	1
4-1 through 4-4	4	E-1	1
5-1 through 5-3	3	F-1	1
6-1 through 6-11	11		
7-1	1	Total	111
8-1	1		
9-1	1		

NEXT INDENTURED DOCUMENTS

908444

(HFD-33200)

REV	1		0	←		→	0																			
SH	1a		57	THRU			111																			
REV	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

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
SAFETY PROTECTION SUBSYSTEM DESIGN DESCRIPTION	908498	1

INFO

ISSUE	DATE	PREPARED BY	APPROVAL: ENGINEERING	APPROVAL: QA	APPROVAL: FUNDING PROJECT	APPROVAL: APPLICABLE PROJECT	ISSUE DESCRIPTION/ CWBS NO.
1	SEP 09 1986	J.Zgliczynski for J.Zgliczynski J.Bauer	C.Rodriguez F.A.Silady Interface Assurance	G.P.Connors	G.Bramblett		HTGR cover added HTGR-86-048/0 (HFD-43202,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 1-31	0	6/30/86
2	2-1 through 2-26	0	6/30/86
3	3-1	0	6/30/86
4	4-1 through 4-4	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-7	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

	PAGE
LIST OF EFFECTIVE PAGES	ii
LIST OF APPENDICES	vii
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS AND ACRONYMS	x
DEFINITIONS	xi
PREFACE	xv
SUMMARY	xvii
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Integrated Approach Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-3
1.2.3 Structural Requirements	1-11
1.2.4 Environmental Requirements	1-14
1.2.5 Instrumentation and Control Requirements	1-18
1.2.6 Surveillance and In-Service Inspection Requirements	1-18
1.2.7 Availability Assurance Requirements	1-19
1.2.8 Maintenance Requirements	1-19
1.2.9 Safety Requirements	1-22
1.2.10 Codes and Standards Requirements	1-24
1.2.11 Quality Assurance Requirements	1-30
1.2.12 Construction Requirements	1-30
1.2.13 Decommissioning Requirements	1-31

CONTENTS (Continued)

		PAGE
2.	DESIGN DESCRIPTION	2-1
2.1	Summary Description	2-1
2.2	Subsystem Configuration	2-3
2.3	Subsystem Performance	2-6
2.3.1	Subsystem Operating Modes	2-10
2.3.2	Subsystem Steady-State Performance	2-10
2.3.3	Subsystem Response to Plant Transients	2-10
2.3.4	Subsystem Failure Modes and Effects	2-21
2.4	Subsystem Arrangement	2-22
2.5	Instrumentation and Control	2-26
3.	COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS	3-1
3.1	Component Functions	3-1
3.2	Component Design Requirements	3-1

CONTENTS (continued)

		PAGE
4.	SUBSYSTEM AND COMPONENT INTERFACES	4-1
	4.1 Subsystem Interface Requirements	4-1
	4.2 Component Boundary Definition	4-1
5.	SUBSYSTEM CONSTRUCTION	5-1
	5.1 Packaging and Shipping	5-1
	5.2 Handling at Delivery	5-1
	5.3 Receiving Inspection	5-2
	5.4 Storage	5-2
	5.5 Access	5-2
	5.6 Installation and/or Field Fabrication	5-2
	5.7 Construction Testing	5-3
	5.8 As-Built Drawings	5-3
6.	SUBSYSTEM OPERATION	6-1
	6.1 Subsystem Limitations, Setpoints, and Precautions	6-1
	6.1.1 Operating Limits and Setpoints	6-1
	6.1.2 Precautions	6-4
	6.2 Preoperational Checkout	6-4
	6.2.1 Initial Preoperational Checkout	6-4
	6.2.2 Routine Preoperational Checkout	6-5

CONTENTS (continued)

	PAGE
6.3 Startup/Shutdown	6-6
6.3.1 Startup to 25% Steam Flow	6-6
6.3.2 Shutdown from 25% Steam Flow	6-8
6.4 Normal Operation	6-8
6.5 Refueling	6-8
6.6 Shutdown	6-9
6.6.1 Automatic Plant Shutdowns	6-9
6.6.2 Plant Protection and Instrumentation System Shutdown	6-10
6.7 Abnormal Operation	6-10
6.8 Casualty Events and Recovery Procedures	6-11
7. SUBSYSTEM MAINTENANCE	7-1
8. SUBSYSTEM DECOMMISSIONING	8-1
9. REFERENCES	9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability of Requirements	A-1
B	Drawings	B-1
C	Transients	C-1
D	Design Basis Seismic Inputs	D-1
E	Parameter Lists	E-1
F	Proprietary Claims	F-1

LIST OF ILLUSTRATIONS

FIGURE		PAGE
1-1	Weekly Load Cycle	1-7
2-1	Protection System Data Busses	2-2
2-2	Arrangement of PPIS Equipment	2-24
6-1	Relationship Between Protection Setpoints and Component Damage Limits	6-2

LIST OF TABLES

TABLE		PAGE
1-1	Safety Protection Sensor Parameters	1-4
1-2	Design Duty Cycle Events	1-8
1-3	HTGR Plant Transients	1-12
1-4	Plant Equipment Damage Limits for Use in Designing the Safety Protection Subsystem	1-13
1-5	External Environmental Conditions, Normal	1-15
1-6	External Environmental Conditions, Abnormal	1-16
1-7	External Environmental Conditions, Design Basis Event	1-17
1-8	Unavailability/Reliability Allocations	1-20
1-9	Equipment Classification	1-23
1-10	Code of Federal Regulations (10CFR) Applicability to Safety Protection Subsystem Design	1-25
1-11	Industrial Codes and Standards Applicable to the Safety Protection Subsystem Design	1-26
1-12	Industrial Codes and Standards for Consideration in Safety Protection Subsystem Design	1-27
2-1	Plant Damage Limits for Use in Designing the Safety Protection Subsystem	2-7
2-2	Safety Protection Subsystem Protective Actions	2-8
2-3	Safety Protection Subsystem Actuated Equipment	2-9
2-4	Safety Protection Subsystem Operating Mode Versus Plant Condition	2-11
2-5	Safety Protection Subsystem Analysis Parameters	2-12
2-6	Failure Modes of Safety Protection Subsystem	2-23
2-7	Safety Protection Subsystem Equipment	2-25
4-1	Interface Requirements Imposed on Other Systems	4-2
6-1	Operating Limits and Setpoints for the Safety Protection Subsystem	6-3

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 Safety 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 Safety Protection Subsystem monitors and protects plant systems to protect public health and safety. The system monitors selected system process variables, compares the sensed values to preselected levels and, as required, commands and initiates predetermined plant corrective actions. The scope of the system starts with and includes the process sensors to the input of the actuated equipment.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 INTEGRATED APPROACH SUBSYSTEM FUNCTIONS

The function of the Safety Protection Subsystem is to monitor and protect plant systems and equipment to protect public health and safety. This is accomplished by sensing process variables to detect abnormal plant conditions, and actuating equipment to maintain plant parameters within acceptable limits established for design basis events, thereby maintaining an acceptable level of public safety risk.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Formal utility/user reviews of the Safety 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. (3202.0102.001)*

The Safety Protection Subsystem shall be compatible with a configuration whereby reactor modules are located within a Nuclear Island that is physically separated from the remaining portions of the plant.

(3202.0102.002)

The Safety 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.

(3202.0102.003)

---

*Requirements traceability number.

The plant control system and major equipment monitoring and protective systems of the Safety Protection Subsystem shall be functionally independent. (3202.0102.004)

The Safety Protection Subsystem shall consist of two supporting trip subsystems: (3202.0102.005)

1. Reactor Trip - Outer Rods.
2. Reactor Trip - Reserve Shutdown.

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. (3202.0102.006)

Each safety channel shall include the field mounted process variable sensor (e.g., resistance thermometers, flow transmitters, 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. (3202.0102.007)

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. (3202.0102.008)

The protective action initiation signal shall be sent to separate and redundant actuation devices. (3202.0102.009)

The boundaries of the Safety Protection Subsystem shall be from, and including, the sensors to the input terminals of the safety system actuation devices. (3202.0102.010)

The Safety 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.)
(3202.0102.011)

Sensor channel parameters shall be as given in Table 1-1. (3202.0102.012)

1.2.2 Operational Requirements

The design, development, fabrication/construction, and installation of the Safety Protection Subsystem shall accommodate a mid-1990s start-of-operation date. (3202.0102.020)

The Safety 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. (3202.0102.021)

The Safety Protection Subsystem shall be designed to accommodate the transients resulting from the duty cycle events in Table 1-2.
(3202.0102.022)

The Safety Protection Subsystem shall accommodate the performance and transient characteristics of the following reactor/turbine-generator combinations: (3202.0102.023)

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).

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.
(3202.0102.024)

Table 1-1

SAFETY PROTECTION SENSOR CHANNEL PARAMETERS

Monitored Variable - Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Sensor Channel Parameters: Minimum Accuracy	Sensor Channel Parameters: Minimum Range
Primary Coolant Pressure (Safety-Related) Receptive Subsystems: Reactor Trip using outer control rods	{2 s}*	{±1%} of span	(600-1100 psia)}
Differential Pressure Across Reactor Core (Safety-Related) Receptive Subsystems: Reactor trip using outer control rods	{2 s}	{±1%} of span	{0-100 psid}
Primary Coolant High Moisture Concentration Receptive Subsystems: Reactor Trip using outer control rods	{40 s} (constant at all loads and includes 25 s sample transit time and 5 s sensor time constant)	{±140 ppmv}	Not Applicable
Steam Generator Inlet Helium Temperature Receptive Subsystem: Reactor Trip using outer control rods	{20.0 s} time constant at 100% power	{±30°F}	{[350-2200°F}

*{ } = Numbers are estimated and subject to change.

Table 1-1 (Continued)

Monitored Variable - Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Sensor Channel Parameters: Minimum Accuracy	Sensor Channel Parameters: Minimum Range
Reactor Neutron Flux (Primary) (Safety-Related)	{10.0 ms}	{±1%} of span	{2-200%} of rated power
Receptive Subsystem: Reactor Trip Using Outer Control Rods			
Reactor Neutron Flux (Diverse) (Safety-Related)			
Receptive Subsystem: Reactor Trip using Reserve Shutdown System	{10.0 ms}	{±1%} of span	{2-200%} of rated power
Reactor Neutron Flux-to-Helium Mass Flow Ratio (Safety-Related)	{2.0 s}	±[TBD] at full power	{0-2}
Receptive Subsystem: Reactor Trip using outer control rods			
This ratio is continuously calculated by dividing the Reactor Neutron Flux by the Helium Mass Flow Rate			
Reactor Helium Mass Flow Rate (Safety-Related)	{2.0 s}	±[TBD] @ 100% flow	{8-120%} (pressurized)
Receptive Subsystems: Reactor Trip using outer control rods		±[TBD] @ 10% flow	

Table 1-1 (Continued)

Monitored Variable - Sensor Parameters	Sensor Channel Parameters: Maximum Response Time	Minimum Accuracy	Minimum Range
This parameter is continuously calculated from: Reactor core differential pressure (ΔP) psi, main circulator outlet helium temperature (T) °F, primary coolant pressure (P) psia, and a constant, C.			
Mass flow rate = $C \sqrt{\Delta P \; P/T}$			
Circulator Speed (Safety-Related)	{10 ms}	{±1%} of span	{0-3600} rpm
Receptive Subsystems: Reactor trip using outer control rods			
Reactor Neutron Flux-to-Circulator Speed Ratio (Safety-Related)			
Receptive Subsystem: Reactor trip using Reserve Shutdown System	{2.0 s}	±[TBD] at full power	{0-3 s}
Main Circulator Outlet Helium Temperature (Core Inlet Temp.) (Safety-Related)	{20.0 s} (time constant)	{+9°F}	{300-850°F}
Receptive Subsystems: Reactor trip using outer control rods			
Sensors at the outlet of the circulator. This measurement is also used in the helium mass flow rate calculation above.			

0/867498

Fig. 1-1 Weekly Load Following Cycle

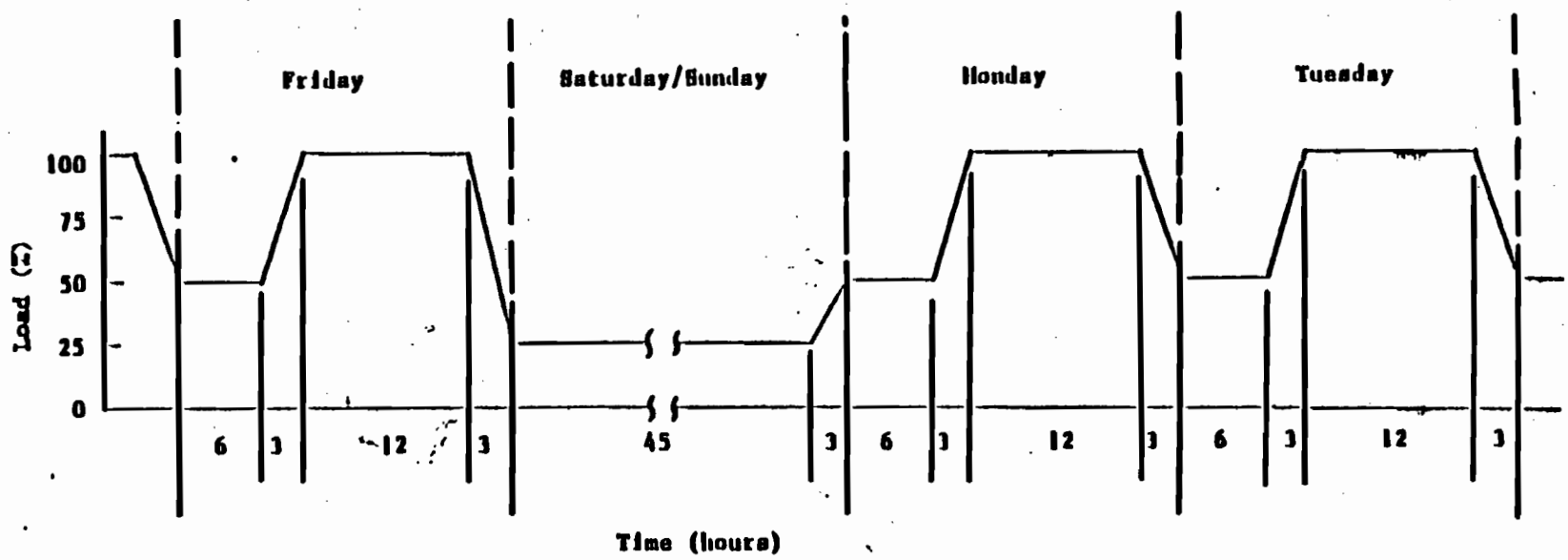


Table 1-2

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.

The system shall function through the design transients provided in Table 1-3. (3202.0102.025)

The Safety Protection Subsystem shall sense process variables to detect abnormal plant conditions and actuate equipment to maintain plant parameters within the plant damage thresholds established for the components listed in Table 1-4, preventing damage to components essential for the protection of the public health and safety and plant investment. (3202.0102.026)

The Safety Protection Subsystem shall be designed to be administered, operated, and maintained by a minimum plant staff consistent with the plant availability and safety goals. (3202.0102.027)

1.2.3 Structural Requirements

1.2.3.1 Mechanical

Safety 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. (3202.0102.200)

1.2.3.2 Seismic

The Safety Protection Subsystem shall be designed, fabricated, and erected to performance standards that will enable it to withstand the forces that might be imposed by an earthquake with ground acceleration levels corresponding to an Operating Basis Earthquake (OBE) with a maximum 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

*Numbers in { } are estimated and subject to change.

Table 1-3

HTGR PLANT TRANSIENTS

[LATER]

Table 1-4

PLANT EQUIPMENT DAMAGE LIMITS FOR USE IN DESIGNING THE SAFETY PROTECTION SUBSYSTEM

Component	Requirements*
Fuel particles	Maintain fuel particle temperature ≤{2912}°F (3202.0102.050)

*Numbers in { } are estimates and subject to change.

{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. (3202.0102.210)

The system components shall be designed to meet the seismic response spectra provided in [later]. (3202.0102.211)

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: (3202.0102.212)

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. (3202.0102.215)

1.2.4 Environmental Requirements

The Safety Protection Subsystem shall be capable of performing their functions before, during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions shown in Tables 1-5, 1-6, 1-7. (3202.0102.220)

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.

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.

1.2.5 Instrumentation and Control Requirements

Controls and instrumentation capable of manually initiating a reactor trip and monitoring the achievement of this function shall be provided at a location outside the main control room 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. (3202.0102.230)

1.2.6 Surveillance and In-Service Inspection Requirements

The design of Safety Protection Subsystem protective features shall provide for periodic functional testing that will not interfere with normal plant operation. (3202.0102.250)

An in-service inspection program shall be defined and documented. Anticipated man-hour requirements shall be documented to accomplish the in-service inspection program. Anticipated health physics man-hours required to support the ISI Program shall be documented. The use of models should be considered to facilitate assessments of inspectability. Estimated man-hours shall include equipment/system isolation, preparation for inspection, and return to service. (3202.0102.251)

The design of the Safety Protection Subsystem shall include in-service inspection configurations, plant, and procedures for identification of inspection equipment to be used to accomplish the inspections. Special equipment not commercially available shall be furnished by the equipment vendor. (3202.0102.252)

Plant piping design shall minimize the need for snubbers and restraints. The design shall be reviewed by an ISI specialist to ensure inspectability. (3202.0102.253)

1.2.7 Availability Assurance Requirements

The Safety 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. (3202.0102.270)

The subsystem shall be designed to meet its planned outage allocation given in Table 1-8. (3202.0102.271)

The subsystem shall be designed to meet its overall reliability allocation given in Table 1-8. (3202.0102.272)

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. (3202.0102.273)

1.2.8 Maintenance Requirements

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. (3202.0102.280)

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.

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
Safety Protection	{4,800}*	{12}	{18.6}			{18.6}	

*{ } = Number is estimated and subject to change.

Anticipated tasks, methods, personnel skills, and man-hours required to achieve the scheduled durations shall be determined and documented.

(3202.0102.281)

Anticipated tasks, methods, personnel skills, and man-hours requirements to accomplish unscheduled maintenance shall be documented for the Safety 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.

(3202.0102.283)

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. (3202.0102.284)

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.

(3202.0102.285)

The design of Safety Protection Subsystem mechanical and electrical systems, components, and parts shall provide for reasonable and necessary interchangeability. (3202.0102.286)

The Safety Protection Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3202.0102.287)

The Safety Protection Subsystem shall be designed to facilitate hands-on maintenance. (3202.0102.288)

Provisions shall be made in the Safety Protection Subsystem for monitoring plant status, configuration, and performance as a basis for maintenance diagnostics and decision-making. (3202.0102.289)

The Safety 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. (3202.0102.290)

Remote maintenance technique shall be considered in the Safety Protection Subsystem design where improved availability may result from time savings. (3202.0102.291)

Where practicable, the design of the Safety 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. (3202.0102.292)

1.2.9 Safety Requirements

1.2.9.1 Deterministic

The Safety Protection Subsystem is classified as safety-related. Certain features of the Safety Protection Subsystem (for example, selected trip input parameters and test provisions) are not required for safety and are classified nonsafety-related.

Equipment classification requirements shall be in accordance with Table 1-9. (3202.0102.310)

Table 1-9

EQUIPMENT CLASSIFICATION
(SAFETY PROTECTION SUBSYSTEM)

	Equipment Classification	Seismic Category	QAL Level
Safety Protection	Class 1E	CAT I	QAL I

1.2.9.2 Probabilistic

The Safety Protection Subsystem shall meet the (safety) reliability requirements allocation shown in Table 1-8. (3202.0102.311)

1.2.10 Codes and Standards Requirements

Design, analysis, fabrication, and construction shall comply with applicable Codes of Federal Regulation and with Industry Codes and Standards that are needed to meet the four goals of the Integrated Approach. (3202.0102.319)

1.2.10.1 Code of Federal Regulations (10CFR)

Table 1-10 lists the 10CFR regulations that apply to the Safety Protection Subsystem design, including comments on required modifications. (3202.0102.320)

Design and licensing documentation shall be developed as necessary to obtain design certification of the Standard Nuclear Island by the NRC. (3202.0102.321)

1.2.10.2 Industrial Codes and Standards

The design of the Safety Protection Subsystem shall meet the industrial standards given in Table 1-11. (3202.0102.331)

The design of the Safety Protection Subsystem shall consider the industrial standards given in Table 1-12. (3202.0102.332)

Table 1-10

CODE OF FEDERAL REGULATION (10CFR) APPLICABILITY TO SAFETY PROTECTION SUBSYSTEM DESIGN

Part/Para.	Subject	Modifications
20/101	Radiation dose standards for individuals in restricted areas.	None.
20/103	Exposure of individuals to concentrations of radioactive materials in air in restricted areas.	None.
20/105	Permissible levels of radiation in unrestricted areas.	None.
20/106	Radioactivity in effluents to unrestricted areas.	None.
21	Reporting of defects and noncompliance.	None.
50	Domestic licensing of production and utilization facilities.	
	50.2(v), Definitions.	Change terminologies to HTGR specific.
	50.34a, Design Objectives for Equipment to Control Releases of Radioactive Material in Effluents - Nuclear Power Reactors.	
	50.36, Technical Specifications.	
	50.36a, Technical Specifications on Effluents from Nuclear Power Reactors.	--
	50.47, Emergency Plans.	--
	50.49, Qualification of Electric Equipment	--
	50.55a, Codes and Standards	--
50/Appendix B	Quality Assurance Criteria for Nuclear Power Plants and and Fuel Reprocessing Plants.	None.
50/Appendix I	Numerical Guides for Design Objectives and Limiting Conditions for Operation to Meet the Criterion "As Low As Is Reasonably Achievable" for Radioactive Material in Light Water Cooled Nuclear Power Reactor Effluents.	None.
100	Reactor Site Criteria	None.

0/8498/0

Table 1-11

INDUSTRIAL CODES AND STANDARDS APPLICABLE TO THE SAFETY PROTECTION SUBSYSTEM DESIGN

ANSI/IEEE Std. 603*	"IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."**

*The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

**IEEE-279 is required by 10CFR50.55a; however, it has been withdrawn by IEEE as IEEE-603 supersedes IEEE-279.

Table 1-12

INDUSTRIAL CODES AND STANDARDS FOR CONSIDERATION IN THE SAFETY 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. 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."
IEEE Std. 381	"Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations."

*The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

Table 1-12 (Continued)

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."
ANSI/IEEE Std. 494	"Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear 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 1-12 (Continued)

NSI/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."

1.2.11 Quality Assurance Requirements

All items designated safety-related, seismic category I, and/or electrical class 1E shall come under a quality assurance program which fully complies with the requirements of Title 10 Code of Federal Regulations Part 50 (10CFR50), Appendix B. The basic requirements and supplements of ANSI/ASME NQA-1 and the four additional supplements from NE F2-10 regarding engineering holds, engineering drawing lists, design reviews, and management assessment shall be implemented on activities that affect the quality of such items. These items are designated as Quality Assurance Level (QAL) I. (3202.0102.350)

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 NQA-1 and the four additional supplements identified above. 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. (3202.0102.351)

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 I.

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. (3202.0102.370)

The design of Safety 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. (3202.0102.371)

The Safety 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. (3202.0102.372)

The Safety Protection Subsystem and its equipment and arrangement features shall facilitate installation, removal, and reinstallation. (3202.0102.373)

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. (3202.0102.374)

1.2.13 Decommissioning Requirements

An analysis shall be performed to estimate the cost of decontaminating and dismantling the Plant Protection and Instrumentation System. (3202.0102.380)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The Safety Protection Subsystem provides the safety system sense and command features necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant protective actions required to mitigate the consequences of design basis events, protecting the public health and safety. The Safety Protection Subsystem is a nuclear safety-related protection system. As such, it meets the requirements of Institute of Electrical and Electronic Engineers (IEEE) Standard 603. Each reactor module has a separate and independent Safety Protection Subsystem.

The Safety Protection Subsystem includes the following:

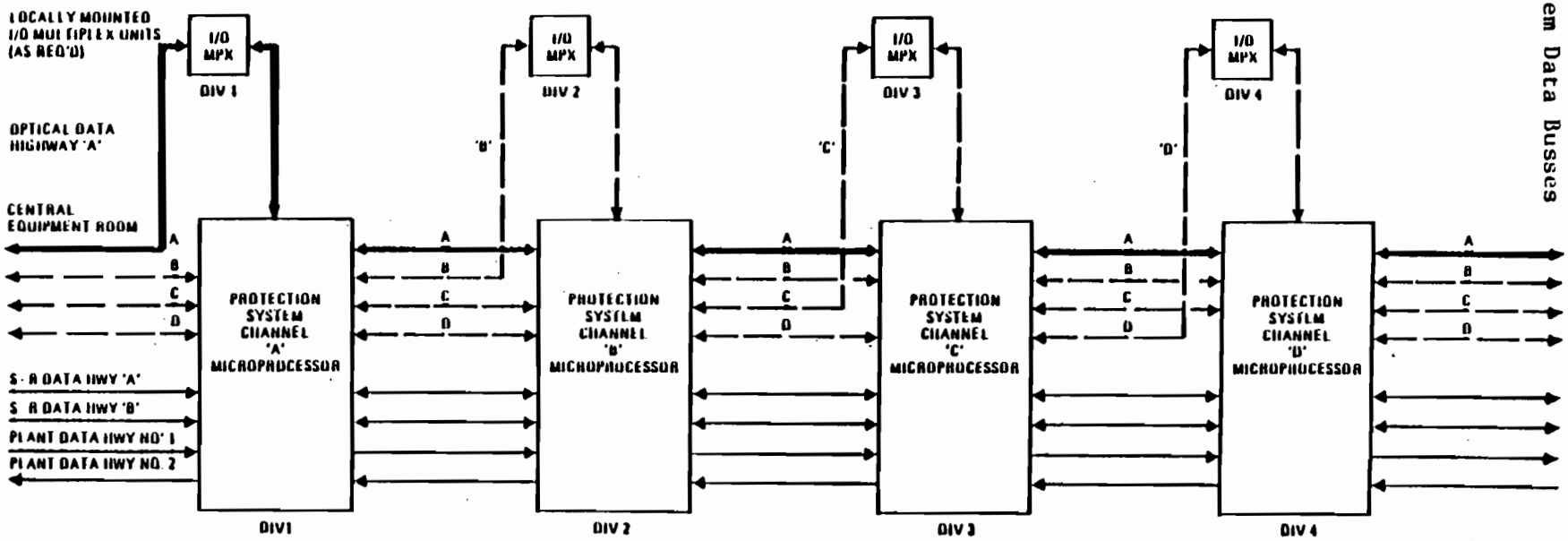
1. Reactor trip using outer control rods.
2. Reactor trip using reserve shutdown system.

2.2 SUBSYSTEM CONFIGURATION

The Safety 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 public health and safety.

The safety 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.

Fig. 2-1 Protection System Data Busses



908498/0

The operator interfaces for the Safety 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. Since no operator action is required for safety, these interfaces are not classified as safety-related. However, these operator interfaces are provided as part of the PPIS and they are separate and independent of all other plant instrumentation and controls. The remote shutdown area operator interfaces provide the reactor operator the capability of tripping the reactor with the safety-related reactor trip, from a position remote from the main control room in the event the main control room becomes uninhabitable. This function is not safety-related.

The design parameters of the Safety Protection Subsystem is based on the results of transient analysis and are discussed in greater detail in Section 2.3.

2.2.1 Safety Protection Subsystem

Each reactor module has a separate and independent Safety Protection Subsystem which consists of four separate (redundant) safety channels and redundant two-out-of-four coincidence solid-state logic to command initiation of a protective action. Each safety channel includes the field mounted process variable sensors (e.g., resistance thermometers, flow transducers, pressure transducers, neutron detectors, etc.), electronic signal conditioning equipment, and electronic trip setpoint comparators to provide a trip signal when the process variable value reaches the trip setpoint. The two-out-of-four coincidence logic circuitry provides a protective action initiation signal when any two or more separate safety system channels reach the trip setpoint. The protective action initiation signal is sent to separate and redundant actuation devices. The boundaries of the safety protection subsystem are generally from, and including, the safety system sensors to the input of the actuation devices.

The Safety Protection Subsystem is required to meet the requirements of "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE-603, which includes criteria for equipment qualification, system integrity, independence, capability for test and calibration, information displays, manual and automatic control, interaction with other systems, operating bypass, etc.

The Safety Protection Subsystem is composed of the following subsystems for each reactor module.

2.2.1.1 Reactor Trip Using Outer Control Rods

This safety-related subsystem initiates a rapid reduction in reactor power following reactivity excursions, loss of adequate core cooling, water ingress events, or breach of the primary coolant barrier by initiating the automatic insertion of all outer control rods including any that may be in the process of being withdrawn.

The outer control rod reactor trip subsystem trip inputs, each derived from four separate and redundant sensor channels are:

1. Neutron flux to helium mass flow ratio high.

2. Primary coolant pressure low.

3. Primary coolant pressure high.

4. Primary coolant moisture concentration high (not required for safety).

5. Main loop trip signal (not required for safety).

6. Steam generator inlet helium temperature high (not required for safety).

7. Manual initiation (not required for safety).

The outer control rod reactor trip subsystem actuated equipment are the outer control rods and their release mechanisms. Upon initiation of the reactor trip signal all outer control rods are fully inserted in the core. On occurrence of a reactor trip, the reactor trip subsystem sends signals to the NSSS control system to initiate a nonsafety-related feedwater flow reduction to aid in an orderly ramp down of the steam supply system. Reactor power inputs to the reactor trip subsystem are derived from excore neutron flux detectors. Detector outputs are conditioned into a linear signal required for the reactor trip module input.

The outer control rods and the safety-related neutron detectors and detector electronics are safety-related equipment provided by the reactor system.

2.2.1.2 Reactor Trip Using Reserve Shutdown System

This safety-related subsystem actuates the reserve shutdown system to perform reactor trip whenever the outer control rod reactor trip system fails to trip when commanded (anticipated transient without scram) or when unlimited water ingress enters the reactor core.

The reserve shutdown system reactor trip inputs are:

1. Reactor neutron flux to main helium circulator speed ratio high (with appropriate delay time to allow the outer control rod reactor trip system to correct the transient).

2. Primary coolant pressure high.

3. Manual initiation (not required for safety).

The actuated equipment for this reactor trip subsystem are the reserve shutdown system fusable links. Upon actuation the fusable links open and the reserve shutdown material is released into the reactor core inner graphite reflector. The protective action is completed when enough negative reactivity has been inserted into the reactor core to ensure a core shutdown margin of at least 0.010 Δk is maintained under all credible post trip conditions.

The reactor neutron flux to circulator speed ratio trip input is inhibited when both neutron flux and circulator speed are low.

On occurrence of a reactor trip using the reserve shutdown system, a signal is sent to the NSSS control subsystem to initiate a nonsafety-related feedwater flow reduction to aid in an orderly rampdown of the steam supply system.

2.3 SUBSYSTEM PERFORMANCE

The design configuration outlined in Section 2.2 for the Safety 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 public health and safety.

The design basis events shown in Table 1-2 govern the design of the Safety Protection Subsystem.

The performance characteristics of major system elements are given in Tables 2-2 and 2-3.

Table 2-1

PLANT DAMAGE LIMITS
FOR USE IN DESIGNING THE SAFETY PROTECTION SUBSYSTEM

Component	Damage Limit
Fuel particles (TRISO coatings)	Maintain fuel particle temperature ≤{2912}°F.

*{ } = Number estimated and subject to change.

Table 2-2

SAFETY PROTECTION SUBSYSTEM
PROTECTIVE ACTIONS

Protective Action	Conditions for Completion of Protective Action	Time for Protection Action to Continue
Reactor Trip Using Outer Control Rods	Insertion of enough negative reactivity to achieve a minimum 0.010 Δk shutdown margin	Sensor channel: Until trip signal sent. Execute features: Indefinitely until manually reset
Reactor Trip Using Reserve Shutdown System	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

908498/0

Table 2-3

SAFETY PROTECTION SUBSYSTEM
ACTUATED EQUIPMENT

Actuated Equipment	Maximum Response Time
Outer Control Rods (Safety-Related)	
Actuating Subsystem: Reactor trip using outer control rods	{25 s}* for full insertion
Reserve Shutdown System (Safety-Related)	
Actuating Subsystem: Reactor trip using reserve shutdown system	{40 s} for full insertion

*{ } = Numbers are estimated and subject to change.

2.3.1 Subsystem Operating Modes

In general the trip portion of the Safety Protection Subsystem is operable during all plant modes. 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 safety system portions of the Safety Protection subsystem out of service is governed by the Plant Technical Specifications.

Table 2-4 gives the operating mode of the Safety Protection Subsystem versus plant conditions.

2.3.2 Subsystem Steady Performance

The steady-state performance is with the subsystem operable, monitoring plant variables, and available for protective functions if needed.

2.3.3 Subsystem Response to Plant Transients

The Safety Protection Subsystem design basis is the subject of continuing design basis analysis. The purpose of this design basis analysis is two-fold:

1. To establish and confirm characteristics of the Safety Protection Subsystem (in particular trip sensing measurements and actuator response).

2. To establish limiting transients that can be imposed on major equipment components.

Safety Protection Subsystem trip parameters used during safety-related design condition (SRDC) analysis and design basis event (DBE) analysis are shown in Table 2-5.

Table 2-4

SAFETY 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	
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	Portion operating tends to relate to control of fission product barriers.
4.0 Emergency Plan Activated	Operable	

[1] Trip portions operate as necessary during abnormal plant events.

Table 2-5 Safety 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 outer control rods	Yes	Neutron flux to helium mass flow ratio high	1.50	1.40	Neutron flux (ϕ)	0 s	[10]* ms	1 s	1 s	Outer control rods	[25] s from full out to full in	
					Primary coolant helium pressure (P)	0 s	[2] s					Helium mass flow is calculated from $C\sqrt{\frac{P\Delta P}{T}}$ where C is a constant
					Core pressure drop (ΔP)	0 s	[2] s					
					Circulator outlet temperature (T)	0 s	[20] s					
	Yes	Primary coolant pressure low	825 psia	835 psia	P (above)			0 s	1 s			
	Yes	Primary coolant pressure high	1025 psia	1015 psia	P (above)			0 s	1 s			
	No	Primary coolant moisture high	1200 ppmv	1000 ppmv	Moisture concentration (M)	[20] s	[5] s	0 s	1 s			Moisture concentration measurement from S/G isolation and dump
	No	Main loop trip	N/A	N/A	Main loop trip signal	N/A	N/A	0 s	1 s			
	No	S/G inlet helium temperature high	[1400] °F	[1375] °F	S/G inlet helium temperature (T_{SG})	0 s	[20] s	0 s	1 s			

*[ ] = Number Tentative and Subject to Change

Table 2-5 Safety 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 reserve shutdown system	Yes	Neutron flux to HTS circulator speed ratio high and time delay ≤50 s and	1.90 and 50 s time delay	1.80 and 30 s time delay	Neutron flux (ϕ_R)	0 s	[10]* ms	1 s	1 s	Reserve shutdown hopper release	5 s to open hopper 35 s to empty hopper	Neutron flux measurement independent and diverse from reactor trip neutron measurements
					HTS circulator speed (s)	0 s	[10] ms					
					time (t)	0 s	0 s					
		Inhibit at low HTS circulator speed and low neutron flux	Inhibit at ≤7% circulator speed and ≤14% neutron flux	Inhibit at ≤5% circulator speed and ≤10% neutron flux								
	Yes	Primary coolant helium pressure high	1025 psia	1015 psia	Primary coolant helium pressure (P)	0 s	[2] s	0 s	1 s			Helium-pressure measurement from reactor trip pressure instrument

*[ ] = Number Tentative and Subject to Change

2.3.3.1 AOO Performance

The response of the Safety 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. After loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high and a reactor trip using the outer control rods is commanded.

AOO No. 1(B) Loss of Offsite Power and Turbine Trip. Loss of offsite power and turbine trip causes the main loop helium circulator to lose electrical power and coastdown. The neutron flux to helium mass flow measurement is detected as high and a reactor trip using the outer control rods is commanded.

AOO No. 1(C) Spurious Reactor Trip With Cooling on HTS. The Safety Protection Subsystem has no response to AOO 1(C) other than to continue to be operable.

AOO No. 1(D) Main Loop Transient Without Reactor Trip. The Safety Protection Subsystem has no response to AOO 1(D) other than to continue to be operable.

AOO No. 2 Loss of Main Loop Cooling and Shutdown Cooling. After loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high and a reactor trip using the outer control rods is commanded. This response is identical to AOO No. 1(A).

AOO No. 3 Rod Withdrawal With Reactor Trip and Cooling on HTS. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint and a reactor trip using the outer control rods is commanded.

AOO No. 4 Small Steam Generator Leak. A small steam generator leak causes a slow moisture ingress. The high primary coolant moisture concentration is reached at the nonsafety-related moisture monitors and a reactor trip using the outer control rods is commanded.

AOO No. 5 Small Primary Coolant Leak. A small primary coolant leak causes a slow depressurization of the primary coolant. When the primary coolant pressure reaches the low pressure setpoint a reactor trip using the outer control rods is commanded.

2.3.3.2 DBE Performance

The Safety Protection Subsystem's response to DBEs is described in this section. No other system's performance is described even though other systems may also respond to the DBEs.

DBE No. 1 Loss of HTS and SCS Cooling. The initiating event for DBE No. 1 is loss of offsite power and turbine trip. A loss of offsite power and turbine trip causes a loss of all primary ac power supplies. This causes the main loop helium circulator to coast down due to loss of power. This loss of primary coolant flow is detected as a high neutron flux to helium mass flow measurement and a reactor trip using the outer control rods is commanded. The safety protection subsystem takes no further action for this DBE. If primary ac power is not restored and standby ac power is not available, the safety protection subsystem loses battery backup power after approximately one hour. At this time the Safety Protection Subsystem fails "as is" since it has no further safety function to perform. Environmental conditions or other plant service conditions experienced during DBE No. 1 have no affect on the ability of the safety protection subsystem to perform its safety function.

DBE No. 2 HTS Transient Without Control Rod Trip. The initiating event for DBE No. 2 is main loop cooling rampdown with a failure of reactor trip

using the outer control rods to take place. This event is an anticipated transient without scram (ATWS). This ATWS event is detected as a high neutron flux to circulator speed ratio measurement. If after a time delay the reactor trip using the outer control rods has not executed protective action, reactor trip using the reserve shutdown system is commanded. Environmental conditions or other plant service conditions experienced during DBE No. 2 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

DBE No. 3 Control Rod Withdrawal Without HTS Cooling. The initiating event for DBE No. 3 is an inadvertent control rod bank withdrawal. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint and a reactor trip using the outer control rods is commanded. Environmental conditions or other plant service conditions experienced during DBE No. 3 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

DBE No. 4 Control Rod Withdrawal Without HTS and SCS Cooling. The initiating event for DBE No. 4 is an inadvertent control rod bank withdrawal. An inadvertent control rod bank withdrawal causes the neutron flux to helium mass flow measurement to exceed the high setpoint and a reactor trip using the outer control rods is commanded. Core cooling on the reactor cavity cooling system may cause the primary coolant pressure to exceed the high pressure setpoint and a reactor trip using the reserve shutdown system may also be commanded. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods. Environmental conditions or other plant service conditions experienced during DBE No. 4 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

DBE No. 5 Large Earthquake With SCS Cooling. The initiating event for DBE No. 5 is a large earthquake. It is assumed that main loop cooling is eventually lost.

After loss of main loop cooling the neutron flux to helium mass flow measurement is detected as high and a reactor trip using the outer control rods is commanded.

The Safety Protection Subsystem and its safety-related auxiliary supporting features are qualified to withstand a safe shutdown earthquake (SSE) and perform their safety functions. No other environmental conditions or other plant service conditions experienced during DBE No. 5 have an effect on the ability of the Safety Protection Subsystem to perform its safety function.

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. This event is detected as high primary coolant moisture measurement by the nonsafety-related moisture monitors. When the nonsafety-related high moisture setpoint is reached, a reactor trip using the outer control rods is commanded. Environmental conditions or other plant service conditions experienced during DBE No. 6 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

DBE No. 7 Moisture Inleakage Without SCS Cooling. The initiating event for DBE No. 7 is a moderate steam generator leak and subsequent moderate moisture ingress rate. The response of the Safety Protection Subsystem to this event is identical to DBE No. 6 except as follows: Core cooling on the reactor cavity cooling system may cause the primary coolant pressure to exceed the high pressure setpoint and a reactor trip using the reserve shutdown system may also be commanded. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods.

DBE No. 8 Moisture Inleakage With Moisture Monitor Failure. The initiating event for DBE No. 8 is a small steam generator leak and subsequent small moisture ingress rate. DBE No. 8 also includes a failure of the nonsafety-related investment protection moisture monitors. The moisture ingress causes the primary coolant pressure to slowly increase.

The primary coolant pressure reaches the high pressure setpoint and a reactor trip using the outer control rods and the reserve shutdown system is commanded. Environmental conditions or other plant service conditions experienced during DBE No. 8 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

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. In this DBE the nonsafety-related investment protection moisture monitors detect this leak and command steam generator isolation and dump. The steam generator dump valves fail to reclose, thereby causing a small primary coolant leak. Therefore, this DBE degenerated to DBE No. 11 and the response of the Safety Protection Subsystem to DBE No. 9 is identical to DBE No. 11.

DBE No. 10 Primary Coolant Leak With HTS Cooling. The initiating event for DBE No. 10 is a moderate primary coolant leak. A moderate primary coolant leak causes a rapid depressurization of the primary coolant. When the primary coolant pressure reaches the low pressure setpoint a reactor trip using the outer control rods is commanded. Environmental conditions or other plant service conditions experienced during DBE No. 10 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

DBE No. 11 Primary Coolant Leak Without HTS and SCS Cooling. The initiating event for DBE No. 11 is a small primary coolant leak. A small primary coolant leak causes a slow depressurization of the primary coolant. The response of the Safety Protection Subsystem to this event is identical to DBE No. 10.

2.3.3.3 SRDC Performance

The performance of the Safety Protection Subsystem under SRDCs is described. No other system's performance is described even though other systems' designs may also be affected by these SRDCs.

SRDC No. 1 Pressurized Conduction Cooldown (Station Blackout). The performance of the Safety Protection Subsystem under SRDC No. 1 is identical to its response to DBE No. 1. Environmental conditions or other plant service conditions experienced during SRDC No. 1 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 2 Loss of Forced Circulation Without Control Rod Trip. The performance of the Safety Protection Subsystem under SRDC No. 2 is identical to its response to DBE No. 2. Environmental conditions or other plant service conditions experienced during SRDC No. 2 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 3 Pressurized Conduction Cooldown With Control Rod Withdrawal. The performance of the Safety Protection Subsystem under SRDC No. 3 is identical to its response to DBE No. 3 except core cooling on the reactor cavity cooling system may cause the primary coolant pressure to exceed the high pressure setpoint and a reactor trip using the reserve shutdown system may be commanded. This reactor trip is not required for this event since the reactor is already tripped with the outer control rods. Environmental conditions or other plant service conditions experienced during SRDC No. 3 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 4 Pressurized Conduction Cooldown With Control Rod Withdrawal. The performance of the Safety Protection Subsystem under SRDC No. 4 is identical to its performance under SRDC No. 3. Environmental conditions or

other plant service conditions experienced during SRDC No. 4 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 5 Earthquake With RCCS Cooling. The performance of the Safety Protection Subsystem under SRDC No. 5 identical to its response to DBE No. 5. Environmental conditions or other plant service conditions experienced during SRDC No. 5 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 6A Large Unterminated Moisture Ingress. The initiating event for SRDC No. 6A is a steam generator offset tube rupture and subsequent large moisture ingress rate. The large water ingress rate causes the neutron flux to helium mass flow measurement to exceed the high setpoint and a reactor trip using the outer control rods is commanded. The primary coolant pressure also increases and when the high pressure setpoint is reached, a reactor trip using the reserve shutdown system is commanded.

SRDC No. 6B Large Unterminated Measure Ingress. The performance of the Safety Protection Subsystem under SRDC No. 6B is identical to its performance under SRDC No. 6A. Environmental conditions or other plant service conditions experienced during SRDC No. 6B have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 7 Small Unterminated Moisture Ingress. The performance of the Safety Protection Subsystem under SRDC No. 7 is identical to the response to DBE No. 8. Environmental conditions or other plant service conditions experienced during SRDC No. 7 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 8 Small Unterminated Moisture Ingress. The performance of the Safety Protection Subsystem under SRDC No. 8 is identical to its performance under SRDC No. 7. Environmental conditions or other plant

service conditions experienced during SRDC No. 8 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 9 Small Moisture Ingress With Open Dump Tank Vents. The performance of the Safety Protection Subsystem under SRDC No. 9 is identical to its performance under DBE No. 9. Environmental conditions or other plant service conditions experienced during SRDC No. 9 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 10 Depressurized Conduction Cooldown With Moderate Primary Coolant Leak. The performance of the Safety Protection Subsystem under SRDC No. 10 is identical to the response to DBE No. 10. Environmental conditions or other plant service conditions experienced during SRDC No. 10 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

SRDC No. 11 Depressurized Conduction Cooldown With Small Primary Coolant Leak. The performance of the Safety Protection Subsystem under SRDC No. 11 is identical to the response to DBE No. 11. Environmental conditions or other plant service conditions experienced during SRDC No. 11 have no effect on the ability of the Safety Protection Subsystem to perform its safety function.

2.3.4 Failure Modes and Effects

The Safety 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 through the special nuclear area instrumentation 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 Safety Protection Subsystem is designed to fail into a safe state (or into a state demonstrated to be acceptable) on conditions such as disconnection of the system, loss of electric power, and loss of HVAC.

Reactor trip using outer control rods trips on loss of all electrical power.

Reactor trip using the reserve shutdown system requires electric power to trip. This design is adequate to meet the safety function and also meet plant availability requirements by avoiding spurious reserve shutdown system insertions.

The general failure modes of the system are given in Table 2-6.

2.4 SYSTEM ARRANGEMENT

The Safety Protection Subsystem is arranged into modular electronic components with four separate safety-related channels. Each of the four MHTGR reactor modules has a separate four channel safety-related protection system. The safety-related components for each reactor module are associated with that reactor module. The nonsafety-related operator interface equipment for the Safety 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 Safety Protection Subsystem equipment is shown in Table 2-7.

Table 2-6

FAILURE MODES OF SAFETY PROTECTION SUBSYSTEM

Subsystem	Subsystem Design Characteristic
Reactor trip using outer control rods	De-energize to trip
Reactor trip using reserve shutdown system	Energize to trip

Figure 2-2 ARRANGEMENT OF PLANT PROTECTION AND INSTRUMENTATION SYSTEM EQUIPMENT

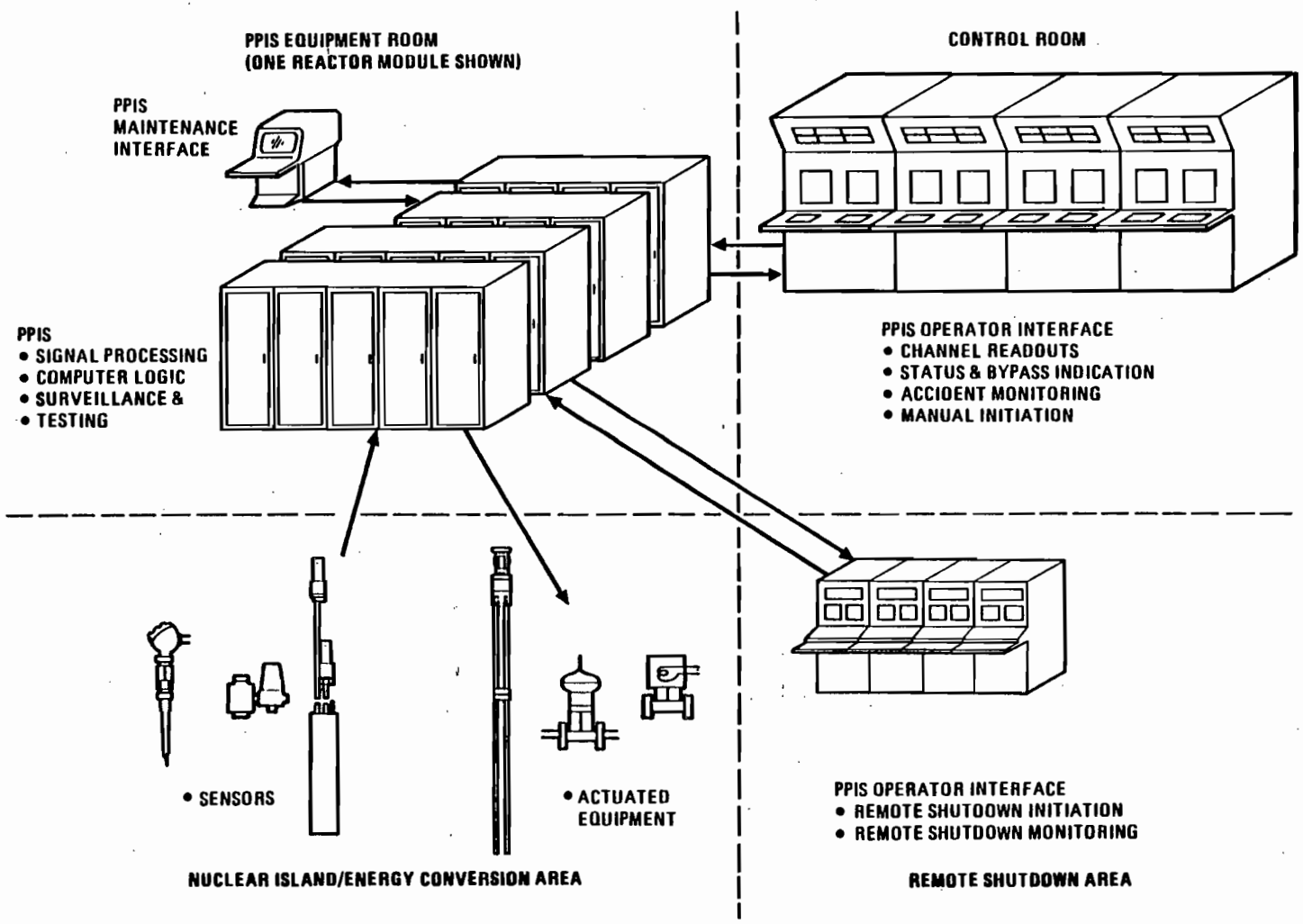


Table 2-7

SAFETY PROTECTION SUBSYSTEM EQUIPMENT

Equipment Number	Equipment Name	Quantity Required for MHTGR Plant	Equipment Location
I-3202-1/4-A/D	Safety protection cabinets	16	PPIS equipment room
I-3205-1/4-A/D	Safety protection remote instrumentation	16	Reactor building
Z-3205-A/D	Instruments, hardware, and software	4 lots	All of the above

2.5 INSTRUMENTATION AND CONTROL

[This section not used because this entire system is an instrumentation and control system.]

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

3.1 COMPONENT FUNCTIONS

[Later]

3.2 COMPONENT DESIGN REQUIREMENTS

[Later]

SECTION 4

SYSTEM AND SUBSYSTEM INTERFACES

4.1 INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interface requirements imposed on other systems are presented in Table 4-1. These are given on a per reactor module basis as the Safety Protection Subsystem is independent for each reactor module.

4.2 SUBSYSTEM BOUNDARY DEFINITION

The Safety Protection Subsystem is the sense and command portion of a safety system. It interfaces with various plant subsystems which provide the actuate portion of the safety system.

The Safety Protection Subsystem (along with other plant systems) provides signal inputs to the Special Nuclear Area Instrumentation Subsystem.

Table 4-1

SAFETY 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 System (1000)			
Neutron Control Subsystem (1012)	Provide for installation of control rod holding coil current relay/contactors in both sides of the current loop to act as the actuation devices for the reactor trip subsystem.	Electrical signals.	Quantity: Two two-out-of-four logic matrices. (3202.0401.002)
	Provide neutron detector safety system sensor channel input to the reactor trip subsystem.	Electrical signals.	Quantity: Twelve neutron flux detectors required, arranged in four independent channels to measure reactor power. (3202.0401.003) Location: Twelve sensors required (three sensors/channel), located in six equally spaced wells in the reactor vessel cavity. The two sensors in each well will be located in the top half and the bottom half of the well. (3202.0401.004)

908498/0

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
	Provide for automatic control of reactor trip reserve shutdown.	Electrical signals.	Quantity: Two fuse link release signals. (3202.0401.005)
4.1.1.2 Heat Transport System (2100)			
Main Circulator Subsystem (2101)	Provide for installation of separate safety system circulator speed sensors in the circulator.	Electrical signals.	Quantity: Four circulator speed sensors. (3202.0401.010)
Steam Generator Subsystem (2102)	Provide for installation of protection system sensors to measure primary coolant parameters.	Pipe connection.	Quantity: Four reactor pressure transmitters to measure primary coolant pressure. (3202.0401.011) Four core differential pressure transmitters. (The measurement is used in calculating main loop helium mass flow.) (3202.0401.012)
	Provide steam generator penetrations to accommodate safety protection subsystem sensors.	Steam generator penetrations.	Quantity: Four thermowell access penetrations in the circulator outlet duct. (3202.0401.013)
4.1.1.3 Plant Protection and Instrumentation System (3200)			
Special Nuclear Area Instrumentation Subsystem (3203)	Provide monitoring of input channels and system	Isolated output electrical signals.	Quantity: Each input, each bypass, each output. (3202.0401.020)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.4 Plant Control, Data, and Instrumentation System (3700)			
NSSS Control Subsystem (3701)	Adjust control system settings following trips.	Electrical signals.	Quantity: Two (reactor trip outer rods and reactor trip reserve shutdown). (3202.0401.030)
4.1.1.5 Building, Structures, and Building Service Group (7000)			
Reactor Building (7001)	Provide building space and structural support to accommodate Safety Protection Subsystem equipment.	Floor mounting.	Quantity: Eight cabinets. (3202.0401.040)
4.1.1.6 Mechanical Service Group (9000)			
HVAC (9011)	Provide HVAC to support the normal operation of the Safety Protection Subsystem.	None.	Quantity: Two. (3202.0401.050)
4.1.1.7 Electrical Group (9200)			
Class 1E Uninterruptible Power Supply (9205)	Provide separate Class 1E uninterruptible power distribution channels to power the Safety Protection Subsystem.	Electric feeders.	Quantity: Four separate Class 1E sources. (3202.0401.060)

0/8498/0

SECTION 5

SYSTEM CONSTRUCTION

The construction of the Safety Protection Subsystem will be planned and scheduled so that its components will fit up properly with all its interfacing components, subsystems, and systems. This will require a detailed plan for installing the proper components at the proper time in the plant construction sequence.

5.1 PACKAGING AND SHIPPING

The design of the Safety 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 Safety 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 Safety 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 Safety 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 Safety 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 Safety 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 Safety 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 Safety 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 vessels 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 Safety 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 SUBSYSTEM 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 setpoints and damage limits. The limiting protection system settings (allowable values) conservatively bound component damage thresholds so that if the limiting protection system setting in 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 Safety Protection Subsystem are shown in Table 6-1.

6.1.2 Precautions

Design features are included to assist the operator in verifying that Safety Protection Subsystem degree of redundancy of at least one is always maintained. For example, whenever any essential safety system component is bypassed, such that a safety group is inoperable, a continuous safety system bypass indication/alarm is displayed in the main control room.

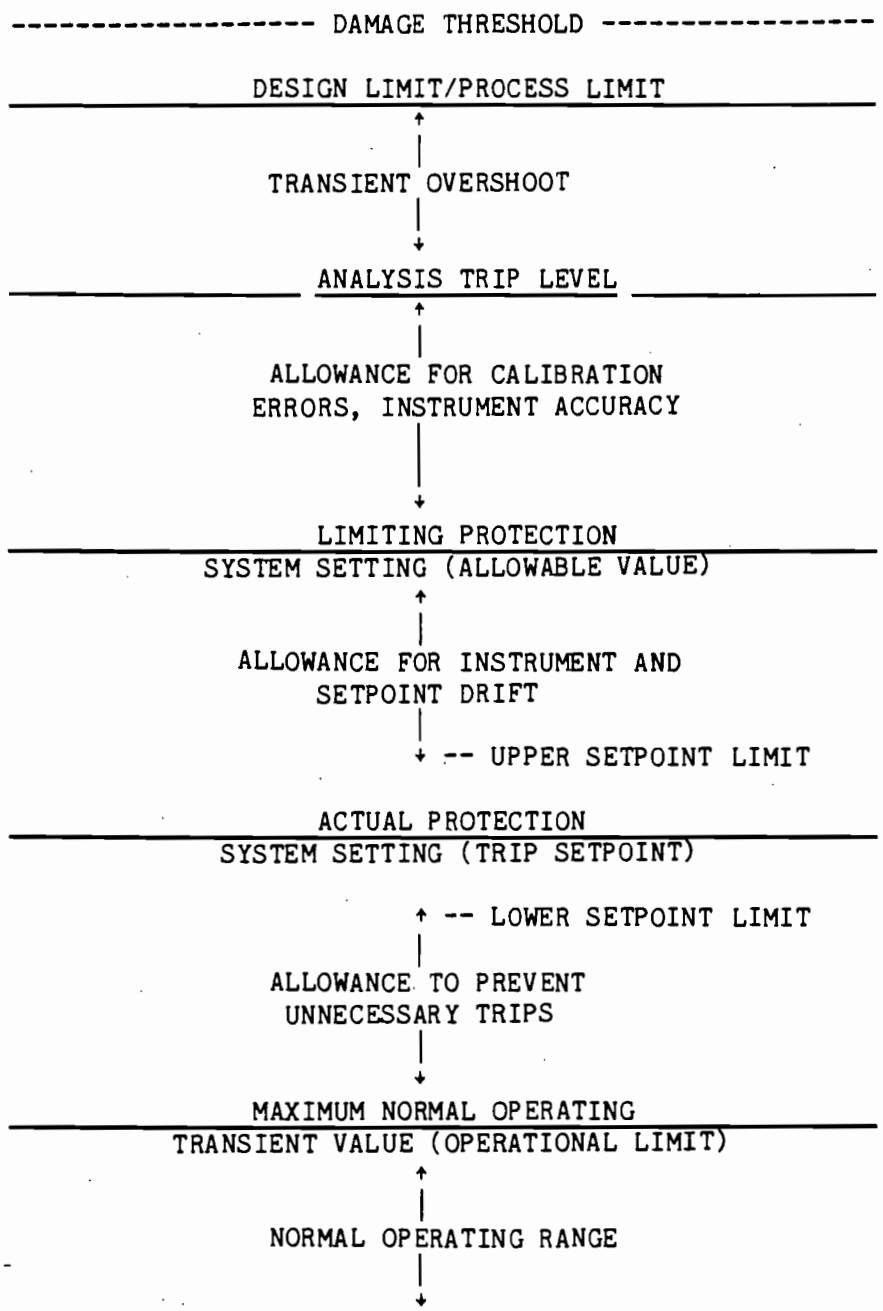


Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS AND COMPONENT DAMAGE LIMITS

Table 6-1

OPERATING LIMITS AND SETPOINTS FOR THE SAFETY PROTECTION SUBSYSTEM

Parameter	Operating Limit (Limiting Protection System Setting)	System Setpoint (Actual Protection System Setting)	Remarks
REACTOR TRIP			
Reactor power to helium mass flow ratio	[TBD]	{1.4}*	
Steam generator helium inlet temperature, °C (°F)	[TBD]	{746 (1375)}	
Primary coolant pressure, MPa (psia)	[TBD]	high {6.998 (1015)} low {5.757 (835)}	
Primary coolant moisture concentration, ppmv	[TBD]	{1000}	
RESERVE SHUTDOWN SYSTEM			
Reactor power to circulator speed ratio	[TBD]	{1.8}	
Primary coolant pressure, MPa (psia)	[TBD]	{6.998 (1015)}	

*{ } = Numbers are estimated and subject to change.

Whenever one safety channel of the two-out-of-four logic is disconnected or bypassed, the remainder of the system maintains a degree of redundancy of one. Whenever a one-out-of-two safety system actuation device is disconnected or bypassed, the time of inoperability must be kept to a minimum and will be within acceptable safety system reliability analysis constraints.

Whenever the two-out-of-four logic safety system is operated with one safety 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 Safety Protection Subsystem and its components prior to nuclear fuel loading and power operation.

Initial preoperational test procedures will be written to demonstrate operational and instrumentation capability for at least the following:

1. Reactor Trip Subsystem

2. Reserve Shutdown Subsystem

6.2.2 Routine Preoperational Checkout

The following prerequisites are required for routine preoperational checkout:

1. Reactor Building Instrument Equipment Area operable.

2. Uninterruptible power sources operable.

3. Special Nuclear Area Instrumentation Subsystem operating.

4. Neutron Control System operable.

5. Heat Transport System Instrumentation operable.

6. Main Steam and Turbine Bypass Instrumentation operable.

Checkout Procedure

In general, the following steps are governed by the plant procedures. Some steps may be bypassed during any specific plant startup provided that the system is still current in accordance with the plant procedures (for example, sensor calibration or actuation device exercising need not be performed upon each startup if the plant 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 (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., 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. Safety Protection Subsystem current per Plant Technical Specifications.

3. Electrical systems operating.

4. Heat Transport System operating.

5. Reactor Cavity Cooling System operating.

6. HVAC operating.

7. Heat Rejection Group operating.

8. Power Conversion Group operating.

9. Reactor Vessel System operating.

10. Shutdown Cooling System operable.

11. Reactor System operable.

12. Plant Control Data and Instrumentation System operating.

6.3.1.2 Procedure

Initial plant startup, criticality testing, etc., employs an additional high startup range reactor trip input. Provisions exist in the instrumentation system to facilitate this; however, it must be physically connected/unconnected as it is not considered a normal reactor trip sensor input. The startup procedure includes:

1. Reset reactor trip circuitry.

2. Reset any first-in trip annunciators.

3. Withdraw control rods in prescribed sequences as determined by Reactivity Control System, equipment heatup rates, etc.

4. Ensure instrumentation readings increase appropriately throughout plant startup on all redundant channels.

6.3.2 Shutdown from 25% Steam Flow

The shutdown procedure includes:

1. Inserting control rods in prescribed sequences as determined by the Reactivity Control System at a low power level.

2. Monitoring plant safety status periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

6.4 NORMAL OPERATION

The procedures for normal operation are as follows:

Periodically monitor systems to ensure that all portions are operating normally.

Perform periodic surveillance, testing, and calibration in accordance with the plant procedures.

6.5 REFUELING

Monitor plant safety status periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

The reactor trip contactors are to remain open during plant shutdowns (exclusive of any testing that may be performed). Control rod/drive mechanism removal for refueling, which requires powering of the control rod drive brake and motor to facilitate removal, can be accomplished on a one-at-a-time basis using plug-in temporary controls provided on the reactor refueling floor as part of the Neutron Control Subsystem.

6.6 SHUTDOWN

A plant shutdown can be initiated either with the normal station controls (planned shutdown) or automatically by the Protection Subsystems (emergency shutdown). During plant shutdown the plant safety status must be monitored by the operator periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

Shutdown of the entire Safety Protection Subsystem to perform maintenance is generally not required due to the redundancy of the channels. To the extent possible, maintenance and surveillance should be done during scheduled plant shutdowns. Inadvertent shutdowns of redundant portions of the Safety Protection Subsystem can result in a reactor trip due to the fail-safe characteristics of the design.

6.6.1 Automatic Plant Shutdowns

The Safety Protection Subsystem automatically initiate reactor trip upon detection of abnormal plant conditions. All automatic trips to the extent possible are preceded by early warning alarms. The operator should take

immediate corrective action, where possible, to prevent a plant trip. This is not possible in all circumstances due to the nature of the various design basis events. Following automatic protective action, the following operator actions should be taken:

1. Verify that redundant portions of the Safety Protection Subsystem have tripped. (Note any abnormal or suspicious Plant Protection and Instrumentation System behavior for future review.)

2. Verify that the outer 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, core cooling and fission product containment are satisfactory and under control.

4. Note the cause of the event and the need for additional operator actions.

5. Continue the plant shutdown per the plant emergency procedures.

6. Plant restart shall not be initiated until the cause for the trip has been positively established, necessary corrections, repairs have been performed, and it has been ascertained that the Safety Protection Subsystem performance was per design.

6.6.2 Safety Protection Subsystem Shutdown

Planned plant shutdown generally involves a reactor trip from a low power level.

1. Ensure that all control rods release and insert on a timely basis following a reactor trip from low power level.

2. Ensure plant is shut down prior to shutting off electrical power (loss of electrical power in more than one of a redundant group can cause a system trip.)

6.7 ABNORMAL OPERATION

Abnormal operation of the Safety Protection Subsystem is limited to plant operation with the systems operating in a degraded mode (failed or inoperable equipment). Generally operation in a degraded mode is governed by the Plant Technical Specifications.

The Safety Protection Subsystem is configured so as to not adversely affect plant safety or plant availability due to a single failure. Therefore, a single failed component or input channel will not cause an unwanted (spurious) system trip nor prevent a required one.

The cause for spurious channel trips should be determined, corrected, and the channel reset in a timely fashion. Continued plant operation with an input channel in a trip condition is undesirable because a second channel trip will result in an unwanted system trip. However, for Technical Specification purposes, a tripped channel is generally defined as operable and this may be employed in some instances to delay plant shutdown for a more appropriate time (i.e., the weekend, to receive spare parts, etc.). The Safety 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, March 1986, (HFS-20100, Rev. 2) (908397, Rev. 2).

APPENDIX A

TRACEABILITY OF REQUIREMENTS

1. INTRODUCTION

This Appendix provides traceability of requirements to sources within the Safety 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., 3202); 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

SAFETY PROTECTION SUBSYSTEM TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3202.0102.001	Formal design	1	3.2.2
3202.0102.002	Nuclear island configuration	1	3.2.2
3202.0102.003	Minimize inaccessible areas	1	3.2.2
3202.0102.004	Control and protection independence	1	3.2.2
3202.0102.005	Safety Protection Subsystem configuration of two subsystems	1	3.2.2
3202.0102.006	Two-out-of-four sense and command logic	1	3.2.2
3202.0102.007	Safety Protection Subsystem configuration	1	3.2.2
3202.0102.008	Safety Protection Subsystem configuration	1	3.2.2
3202.0102.009	Safety Protection Subsystem configuration	1	3.2.2
3202.0102.010	Safety Protection Subsystem configuration	1	3.2.2
3202.0102.011	Safety Protection Subsystem configuration	1	3.2.2
3202.0102.012	Sensor channel requirements	1	3.2.2
3202.0102.020	Mid 1990's start of operation	1	3.2.2
3202.0102.021	40-year load cycle	1	3.2.2
3202.0102.022	Duty cycle events	1	3.2.2
3202.0102.023	Reactor/turbine generator combinations	1	3.2.2
3202.0102.024	Confirmation through analysis	1	3.2.2
3202.0102.025	Design transients	1	3.2.2

Table A-1 (continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3202.0102.026	Overall functional requirement for the design of the Safety Protection Subsystem	1	3.2.2
3202.0102.027	Operation by minimum staff	1	3.2.2
3202.0102.050	Fuel particle temperature limits	1	3.2.2
3202.0102.200	Mechanical requirements for cabinet, rack, and panel design	1	3.2.2
3202.0102.210	Seismic design	1	3.2.2
3202.0102.211	Seismic response spectra	1	3.2.2
3202.0102.212	Seismic damping coefficients	1	3.2.2
3202.0102.215	Materials	1	3.2.2
3202.0102.220	Operating environments	1	3.2.2
3202.0102.230	Requirement for remote shutdown	1	3.2.2
3202.0102.250	In-service inspection	1	3.2.2
3202.0102.251	In-service inspection with plant on-line	1	3.2.2
3202.0102.252	In-service inspection of reactor coolant pressure boundary	1	3.2.2
3202.0102.253	Pipe restraints	1	3.2.2
3202.0102.270	Availability	1	3.2.2
3202.0102.271	System outage requirements allocation	1	3.2.2

Table A-1 (continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3202.0102.272	System reliability requirements allocation	1	3.2.2
3202.0102.273	Design modifications for availability improvement	1	3.2.2
3202.0102.280	Hands-on maintenance	1	3.2.2
3202.0102.281	Planned outage schedule	1	3.2.2
3202.0102.283	Man-hour requirements	1	3.2.2
3202.0102.284	"Off-the shelf" components	1	3.2.2
3202.0102.285	Spare parts listing	1	3.2.2
3202.0102.286	Parts interchangeability	1	3.2.2
3202.0102.287	Arrangement to facilitate on-line maintenance	1	3.2.2
3202.0102.288	Design to facilitate hands-on maintenance	1	3.2.2
3202.0102.289	Monitoring as basis for maintenance diagnostics	1	3.2.2
3202.0102.290	Plant staffing	1	3.2.2
3202.0102.291	Remote maintenance	1	3.2.2
3202.0102.292	On-line in-service inspection	1	3.2.2
3202.0102.310	Equipment classification	1	3.2.2
3202.0102.311	Safety/reliability	1	3.2.2
3202.0102.319	Codes and standards	1	3.2.2
3202.0102.320	Codes and standards	1	3.2.2

Table A-1 (continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3202.0102.321	Certification as a standard Nuclear Island	1	3.2.2
3202.0102.330	Codes and standards	1	3.2.2
3202.0102.331	Codes and standards	1	3.2.2
3202.0102.332	Codes and standards	1	3.2.2
3202.0102.350	Quality assurance requirements	2	3.2.2
3202.0102.351	Quality identification (QAL II, III)	2	3.2.2
3202.0102.370	Construction plan and schedule	1	3.2.2
3202.0102.371	Parallel construction	1	3.2.2
3202.0102.372	Utilization of shop, factory or field fabricated parts	1	3.2.2
3202.0102.373	Arrangement features	1	3.2.2
3202.0102.374	Materials, processes and parts	1	3.2.2
3202.0102.380	Decommissioning requirements	1	3.2.2
3202.0401.002	Installation of control rod holding current contactors	2	2.2.1.1
3202.0401.003	Neutron detectors for input to Reactor Trip Subsystem	2	2.2.1.1
3202.0401.004	Neutron detectors for input to Reactor Trip Subsystem	2	2.2.1.1
3202.0401.005	Control signals to reserve shutdown equipment	2	2.2.1.2
3202.0401.010	Provide circulator speed sensors.	2	2.2.1.2

Table A-1 (continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3202.0401.011	Installation provisions for primary coolant pressure transmitters	2	2.2.1.1
3202.0401.012	Provide core differential pressure transmitter installation	2	2.2.1.1
3202.0401.013	Provide for circulator outlet thermowell installation	2	2.2.1.1
3202.0401.020	Provide monitoring for Safety Protection Subsystem	2	2.2.1
3202.0401.030	Adjust control settings following trips	2	2.2.1
3202.0401.040	Provide building space for Safety Protection Subsystem equipment	2	2.4
3202.0401.050	Provide HVAC for Safety Protection Subsystem equipment	2	2.2
3202.0401.060	Provide 1E UPS for Safety Protection Subsystem equipment	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. "Safety Protection Subsystem Design Description," HFD-43202, Rev. 0 (908498, 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]

HTGR-86-050

HTGR

SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION

[redacted]

[redacted] Divisions of [redacted] HTR Development [redacted] rgy.

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

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 the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HTGR–86–050
908499/1

SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION

[redacted]
Any Further Distribution by any Holder of this Document
[redacted]
HTR
[redacted]

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					
SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION				☐ R & D ☐ DV & S ☒ DESIGN	APPROVAL LEVEL 5
DISCIPLINE	SYSTEM	DOC. TYPE	PROJECT	DOCUMENT NO.	ISSUE NO./LTR.
0	32 03	SSDD	6300	908499	1

QUALITY ASSURANCE LEVEL	SAFETY CLASSIFICATION	SEISMIC CATEGORY	ELECTRICAL CLASSIFICATION
QAL II	NNS	Non CAT I	OSRE

INFO 11

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.Bramblett		Initial issue (HFD-43203 Rev. 0) 6352-320-103

[redacted]Y

[redacted]ument [redacted]g [redacted] [redacted]ies or Foreign Divisions of U.S. [redacted] HTR [redacted] Division, U.S. Department of Energy.

CONTINUE ON GA FORM 1485-1

Cover Sheets	2 (Unnumbered)		
Issue Summary 1,1a	2		
ii through xvii	16	A-1 through A-6	6
1-1 through 1-20	20	B-1	1
2-1 through 2-12	12	C-1	1
3-1	1	D-1	1
4-1 through 4-6	6	E-1	1
5-1 through 5-3	3	F-1	1
6-1 through 6-6	6		
7-1	1	Total	82
8-1	1		
9-1	1		

NEXT INDENTURED DOCUMENTS

908444

(HFD-33200)

REV	1		0	←	→	0																					
SH	1a		57	THRU		82																					
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

TITLE	DOCUMENT NO.	ISSUE NO./LTR.
SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN DESCRIPTION	908499	1

INFO 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 J.Bauer	C.Rodriguez F.Silady Interface Assurance	G.P.Connors	G.C.Bramblett		HTGR cover added HTGR-86-050/0 (HFD-43203,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 1-20	0	6/30/86
2	2-1 through 2-12	0	6/30/86
3	3-1	0	6/30/86
4	4-1 through 4-6	0	6/30/86
5	5-1 through 5-3	0	6/30/86
6	6-1 through 6-6	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-6	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

	PAGE
LIST OF EFFECTIVE PAGES	ii
LIST OF APPENDICES	vii
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS AND ACRONYMS	x
DEFINITIONS	xi
PREFACE	xv
SUMMARY	xvii
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Integrated Approach Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-3
1.2.3 Structural Requirements	1-3
1.2.4 Environmental Requirements	1-6
1.2.5 Instrumentation and Control Requirements	1-6
1.2.6 Surveillance and In-Service Inspection Requirements	1-6
1.2.7 Availability Assurance Requirements	1-6
1.2.8 Maintenance Requirements	1-11
1.2.9 Safety Requirements	1-13
1.2.10 Codes and Standards Requirements	1-13
1.2.11 Quality Assurance Requirements	1-13
1.2.12 Construction Requirements	1-19
1.2.13 Decommissioning Requirements	1-20

CONTENTS (Continued)

		PAGE
2.	DESIGN DESCRIPTION	2-1
2.1	Summary Description	2-1
2.2	Subsystem Configuration	2-3
2.2.1	Reactor Vessel Pressure Relief Block Valve Closure Interlock	2-3
2.2.2	Safety System Information Displays	2-3
2.2.3	Investment Protection Information Displays	2-4
2.2.4	Post Accident Monitoring Instrumentation	2-5
2.3	Subsystem Performance	2-5
2.3.1	Subsystem Operating Modes	2-5
2.3.2	Subsystem Steady-State Performance	2-6
2.3.3	Subsystem Response to Plant Transients	2-6
2.3.4	Subsystem Failure Modes and Effects	2-9
2.4	Subsystem Arrangement	2-9
2.5	Instrumentation and Control	2-10
3.	COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS	3-1
3.1	Component Functions	3-1
3.2	Component Design Requirements	

CONTENTS (Continued)

		PAGE
4.	SUBSYSTEM AND COMPONENT INTERFACES	4-1
	4.1 Subsystem Interface Requirements	4-1
	4.2 Component Boundary Definition	4-1
5.	SUBSYSTEM CONSTRUCTION	5-1
	5.1 Packaging and Shipping	5-1
	5.2 Handling at Delivery	5-1
	5.3 Receiving Inspection	5-2
	5.4 Storage	5-2
	5.5 Access	5-2
	5.6 Installation and/or Field Fabrication	5-2
	5.7 Construction Testing	5-3
	5.8 As-Built Drawings	5-3
6.	SUBSYSTEM OPERATION	6-1
	6.1 Subsystem Limitations, Setpoints, and Precautions	6-1
	6.1.1 Operating Limits and Setpoints	6-1
	6.1.2 Precautions	6-1
	6.2 Preoperational Checkout	6-2
	6.2.1 Initial Preoperational Checkout	6-2
	6.2.2 Routine Preoperational Checkout	6-2

CONTENTS (Continued)

		PAGE
6.3	Startup/Shutdown	6-4
6.3.1	Startup to 25% Steam Flow	6-4
6.3.2	Shutdown from 25% Steam Flow	6-4
6.4	Normal Operation	6-5
6.5	Refueling	6-5
6.6	Shutdown	6-5
6.7	Abnormal Operation	6-6
6.8	Casualty Events and Recovery Procedures	6-6
7.	SUBSYSTEM MAINTENANCE	7-1
8.	SUBSYSTEM DECOMMISSIONING	8-1
9.	REFERENCES	9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability of Requirements	A-1
B	Drawings	B-1
C	Transients	C-1
D	Design Basis Seismic Inputs	D-1
E	Parameter Lists	E-1
F	Proprietary Claims	F-1

LIST OF ILLUSTRATIONS

FIGURE		PAGE
2-1	Arrangement of PPIS Equipment	2-11

LIST OF TABLES

TABLE		PAGE
1-1	HTGR Plant Transients	1-4
1-2	External Environmental Conditions, Normal	1-7
1-3	External Environmental Conditions, Abnormal	1-8
1-4	External Environmental Conditions, Design Basis Event	1-9
1-5	Unavailability/Reliability Allocations	1-10
1-6	Equipment Classification	1-14
1-7	Industrial Codes and Standards Applicable to the Special Nuclear Area Instrumentation Subsystem Design	1-15
1-8	Industrial Codes and Standards for Consideration in Special Nuclear Area Instrumentation Subsystem Design	1-16
2-1	Special Nuclear Area Instrumentation Operating Mode Versus Plant Conditions	2-7
2-2	Special Nuclear Area Instrumentation Equipment	2-12
4-1	Interface Requirements Imposed on Other Systems	4-1

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. 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation includes the reactor vessel pressure relief block valve closure interlock, displays that monitor plant protection systems status, displays that monitor the plant safety and investment under normal operating and accident conditions, and controls which allow control of reactor shutdown from a remote shutdown area.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 INTEGRATED APPROACH SUBSYSTEM FUNCTIONS

The function of the Special Nuclear Area Instrumentation Subsystem is to actuate preventive features to verify that safety systems are operable, to monitor plant safety and investment under normal and accident conditions and enable control of reactor shutdown from a remote shutdown area.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Formal utility/user reviews of the Special Nuclear Area Instrumentation 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.

(3203.0102.001)*

The Special Nuclear Area Instrumentation Subsystem shall be compatible with a configuration whereby reactor modules are located within a Nuclear Island that is physically separated from the remaining portions of the plant.

(3203.0102.002)

The Special Nuclear Area Instrumentation 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. (3203.0102.003)

---

*Requirements traceability number.

The Special Nuclear Area Instrumentation Subsystem shall provide preventive feature interlocks and instrumentation that monitors protection systems status and the plant under normal operating and accident conditions. (3203.0102.004)

The preventive feature interlock shall be the Reactor Vessel pressure relief block valve closure interlock. (3203.0102.005)

The pressure relief block valve closure interlock shall consist of redundant electrical sensors, logic, and electrical interlocks to prevent the simultaneous closure of both reactor vessel pressure relief valve trains, thereby preventing the complete bypass of the reactor vessel over-pressure protection. The general configuration shall be as shown on the Reactor Vessel Relief Block Valve Interlock Instrument Block Diagram. (For drawings see Appendix B.) (3203.0102.006)

The protection systems information displays shall consist of field mounted electronic sensors, electronic multiplexer modules, redundant digital data highways, and field mounted and main control room instrumentation displays to provide the integration of protection system sensor channel readouts, protection system status (e.g., trip, alarm, normal, etc.) indication, and protection system bypass indication. (3203.0102.007)

The protection system information displays shall be integrated as shown in Protection System Display, Instrumentation Block Diagram Drawing. (For drawings, see Appendix B.) (3203.0102.008)

The reactor vessel pressure relief block valve closure interlock shall be powered from the same electrical power source which powers the reactor vessel pressure relief block valves. (3203.0102.009)

1.2.2 Operational Requirements

The design, development, fabrication/construction, and installation of the Special Nuclear Area Instrumentation Subsystem shall accommodate a mid-1990s start-of-operation date. (3203.0102.020)

The Special Nuclear Area Instrumentation Subsystem shall be designed for an operating life of 40 calendar years from start of operation. (3203.0102.021)

The system shall function through the design transients provided in Table 1-1. (3203.0102.022)

The Special Nuclear Area Instrumentation Subsystem shall be designed to be administered, operated, and maintained by a minimum plant staff consistent with the plant availability and safety goals. (3203.0102.023)

1.2.3 Structural Requirements

1.2.3.1 Mechanical

Special Nuclear Area Instrumentation 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. (3203.0102.030)

1.2.3.2 Seismic

The Special Nuclear Area Instrumentation 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 horizontal ground acceleration of 0.15 g and vertical

Table 1-1

HTGR PLANT TRANSIENTS

[LATER]

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. (3203.0102.040)

The system components shall be designed to meet the seismic response spectra provided in [later]. (3203.0102.041)

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: (3203.0102.042)

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. (3203.0102.050)

*Numbers in { } are estimated and subject to change.

1.2.4 Environmental Requirements

The Special Nuclear Area Instrumentation Subsystem shall be capable of performing their functions before, during, and for an adequate time after being subjected to the normal, abnormal, and design basis event environmental conditions shown in Tables 1-2, 1-3, 1-4. (3203.0102.060)

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 at a location outside the main control room 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. (3203.0102.070)

1.2.6 Surveillance and In-Service Inspection Requirements

This section not used as this subsystem is nonsafety-related.

1.2.7 Availability Assurance Requirements

The Special Nuclear Area Instrumentation 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. (3203.0102.090)

The subsystem shall be designed to meet its planned outage allocation given in Table 1-5. (3203.0102.091)

The subsystem shall be designed to meet its overall reliability allocation given in Table 1-5. (3203.0102.092)

Table 1-2

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.

908499/0

Table 1-3

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 1-4

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 1-5

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
Special Nuclear Area Instrumentation	{89,000}*	{12}	{1.0}			{1.0}	

*Numbers in { } are estimated and subject to change.

908499/0

1.2.8 Maintenance Requirements

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. (3203.0102.100)

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. (3203.0102.101)

Anticipated tasks, methods, personnel skills, and man-hours requirements to accomplish unscheduled maintenance shall be documented for the Special Nuclear Area Instrumentation 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. (3203.0102.102)

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. (3203.0102.103)

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.

(3203.0102.104)

The design of Special Nuclear Area Instrumentation Subsystem mechanical and electrical systems, components, and parts shall provide for reasonable and necessary interchangeability. (3203.0102.105)

The Special Nuclear Area Instrumentation Subsystem shall be designed and arranged and equipment and components located in the plant to facilitate on-line maintenance. (3203.0102.106)

The Special Nuclear Area Instrumentation Subsystem shall be designed to facilitate hands-on maintenance. (3203.0102.107)

Provisions shall be made in the Special Nuclear Area Instrumentation Subsystem for monitoring plant status, configuration, and performance as a basis for maintenance diagnostics and decision-making. (3203.0102.108)

The Special Nuclear Area Instrumentation 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. (3203.0102.109)

Remote maintenance technique shall be considered in the Special Nuclear Area Instrumentation Subsystem design where improved availability may result from time savings. (3203.0102.110)

Where practicable, the design of the Special Nuclear Area Instrumentation 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. (3203.0102.111)

1.2.9 Safety Requirements

Since the Special Nuclear Area Instrumentation does not perform any 10CFR100 related radionuclide control functions, no special classification is applied to it. However, the subsystem will have appropriate reliability to meet other top-level regulatory criteria and user requirements.

Equipment classification requirements shall be in accordance with Table 1-6. (3203.0102.120)

1.2.10 Codes and Standards Requirements

Design and licensing documentation shall be developed as necessary to obtain design certification of the Standard Nuclear Island by the NRC. (3203.0102.130)

The design of the Special Nuclear Area Instrumentation Subsystem shall meet the industrial standards given in Table 1-7. (3203.0102.131)

The design of the Special Nuclear Area Instrumentation Subsystem shall consider the industrial standards given in Table 1-8. (3203.0102.132)

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. (3203.0102.140)

Table 1-6

EQUIPMENT CLASSIFICATION
(SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM)

	Equipment Classification	Seismic Category	QAL Level
Special Nuclear Area Instrumentation	Non Class 1E	Non CAT I	QAL II

Table 1-7

INDUSTRIAL CODES AND STANDARDS APPLICABLE TO THE SPECIAL NUCLEAR AREA INSTRUMENTATION SUBSYSTEM DESIGN

ANSI/IEEE Std. 603*	"IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."**

*The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

**IEEE-279 is required by 10CFR50.55a; however, it has been withdrawn by IEEE as IEEE-603 supersedes IEEE-279.

Table 1-8

INDUSTRIAL CODES AND STANDARDS FOR CONSIDERATION IN THE SPECIAL NUCLEAR AREA INSTRUMENTATION 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. 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."
IEEE Std. 381	"Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations."

*The actual issue date, edition, addenda, etc., of applicable industrial codes and standards shall be specified at the time of plant site selection.

Table 1-8 (Continued)

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. 497	"Criteria for Accident Monitoring Instrumentation for Nuclear 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."
ANSI/ISA-S67.01	"Transducer and Transmitter Installation for Nuclear Safety Applications."

Table 1-8 (Continued)

ISA-S67.02	"Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use 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."

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 constructibility, particularly in congested areas. (3203.0102.150)

The design of Special Nuclear Area Instrumentation 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. (3203.0102.151)

The Special Nuclear Area Instrumentation Subsystem design shall utilize shop factory, or field fabricated, assembled and erected components and subsystems to reduce erection costs and to enhance quality controls. (3203.0102.152)

The Special Nuclear Area Instrumentation Subsystem and its equipment and arrangement features shall facilitate installation, removal, and reinstallation. (3203.0102.153)

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. (3203.0102.154)

1.2.13 Decommissioning Requirements

An analysis shall be performed to estimate the cost of decontaminating and dismantling the Special Nuclear Area Instrumentation Subsystem.

(3203.0102.160)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The Special Nuclear Area Instrumentation Subsystem provides the reactor vessel pressure relief block valve closure interlock, instrumentation that monitors protection systems' status and the plant under normal operating and accident conditions and enable control of reactor shutdown from an area remote from the control room. It is not safety-related.

The Special Nuclear Area Instrumentation includes the following:

1. Reactor vessel pressure relief block valve closure interlock.
2. Safety system information displays.
3. Investment protection information displays.
4. Post-accident monitoring instrumentation.

2.2 SUBSYSTEM CONFIGURATION

The interlock feature of the Special Nuclear Area Instrumentation is the reactor vessel pressure relief block valve closure interlock. The vessel pressure relief block valve closure interlock consists of redundant electrical sensors, and electrical interlocks to prevent the simultaneous closure of both vessel relief valve trains. This prevents the complete bypass of the vessel overpressure protection.

The safety system information equipment consists of field mounted electronic multiplexer modules, redundant digital data highways, and local and main control room instrumentation displays to provide the integration of safety system sensor channel readouts, safety system status (e.g., trip, alarm, normal, etc.) indication, and safety system bypass indication. These displays assist the operator in verifying that the plant safety

systems are operable, that the proper degree of redundancy is maintained, and that protective action has been completed after a design basis event. The displays also are used in performing safety system calibration, testing, and maintenance.

These displays also provide a continuous, dedicated display of a minimum set of plant parameters or derived variables used by the operator in the main control room during all plant conditions to assess the plant safety status. These displays are also accessible to other locations in the plant through digital data highways.

The post accident monitoring (PAM) instrumentation indicates plant variables which are required by the control room operating personnel during accident situations to (1) provide information required to permit the operator to assess that the reactor is safely shut down and is being cooled; (2) determine whether reactor trip and other safety systems are performing their intended functions; and (3) provide information to the operators that will enable then to determine the adequacy and status of radioactivity barriers. In addition to the above, the post accident monitoring instrumentation indicates plant variables that provide information on the operation of plant safety systems and other systems that are required by the control room operating personnel during an accident to (1) furnish data regarding the operation of plant systems in order that the operator can make appropriate decisions as to their use and to (2) provide information regarding the release of radioactive materials. The post accident monitoring instrumentation includes a subset of safety system parameters plus additional parameters such as site radiological and site meteorological parameters. The post accident monitoring instrumentation uses field mounted electronic multiplexer modules to acquire plant signals and convert the signals to a digital format. These signals are transmitted over redundant PPIS digital data highways to microprocessor driven displays located in the control room. These displays are part of the PPIS and are separate and independent of all other plant instrumentation and control

displays. These displays are also accessible at other locations throughout the plant through the digital data highways.

The Special Nuclear Area Instrumentation Subsystems are as follows:

2.2.1 Reactor Vessel Pressure Relief Block Valve Closure Interlock

This subsystem prevents the simultaneous closure of both reactor vessel relief block valves to ensure that at least one vessel relief valve is always available to protect the reactor vessel and primary coolant boundary.

The reactor vessel pressure relief block valve closure interlock is actuated whenever either vessel pressure relief block valve is not fully open, and prevents the simultaneous closure of both reactor vessel pressure relief block valves. The interlock function is accomplished when the power necessary to drive the block valves closed is interrupted. The interlock does not interfere with opening the block valves individually or simultaneously. Actuation of the interlock is alarmed in the control room.

The reactor vessel pressure relief block valve interlock consists of a redundant train of two sensors and logic for each block valve. Two limit switches (one in each train) for each block valve sense when the block valve is not fully open. Actuation of either redundant logic train interrupts the block valve power for closing the valve. At no time does the reactor vessel pressure relief block valve interlock prevent power from being used to open the block valve.

2.2.2 Safety System Information Displays

Safety system information displays consist of an integrated system using digital data highways and computer-based displays to provide:

1. All safety system channel readouts.

2. All safety system status indications including status indications for safety system actuation devices, actuated equipment, and safety system auxiliary supporting features.

3. All safety system bypass indications including bypass indications for safety system actuation devices, actuated equipment, and safety system auxiliary supporting features.

In general, the system provides those displays which enable the reactor operator to perform the equipment surveillance and plant conditions monitoring necessary to determine that the plant safety systems are operable during normal operation, and that they have performed their function, that the plant is safely shutdown, and that core cooling and fission product barrier integrity is maintained during normal shutdown and following the occurrence of a design basis event (DBE).

2.2.3 Investment Protection Information Displays

Investment protection information displays function similarly to the safety system information displays. However, they include supplemental monitoring to facilitate plant restarts for the purpose of verifying that plant equipment has not been damaged in various operating events. Investment protection information displays consist of an integrated system using digital data highways and computer-based displays to provide:

1. All investment protection channel readouts.

2. All investment protection status indications including status indications for investment protection actuation devices, actuated equipment, and investment protection auxiliary supporting features.

3. Bypass indications for all investment protection actuation devices, actuated equipment, and auxiliary supporting features.

In general, the system provides those displays which enable the reactor operator to perform the equipment surveillance and plant condition monitoring necessary to determine that the plant investment protection systems are operable during normal operation, and that they have performed their function, that the plant investment is protected during transient events. The investment protection information displays provide information which may allow the reactor operator to take manual actions which are important to protecting plant investment.

2.2.4 Post Accident Monitoring Instrumentation

The post accident monitoring instrumentation includes a subset of safety system parameters plus additional parameters such as site radiological and site meteorological parameters. The post accident monitoring instrumentation uses field mounted electronic multiplexer modules to acquire plant signals and convert the signals to a digital format. These signals and other safety-related signals are transmitted over redundant digital data highways to microprocessor driven PPIS displays located in the control room. These displays are also accessible at other locations throughout the plant through the digital data highways.

2.3 SUBSYSTEM PERFORMANCE

2.3.1 Subsystem Operating Modes

The Special Nuclear Area Instrumentation is operable during all plant modes. The status of the plant is monitored at all times and interlock actions are initiated as required. Portions of the system may be bypassed for surveillance, testing, and maintenance; however, due to the system's redundancy this does not necessitate loss of the function. Operation of the plant with portions of the Special Nuclear Area Instrumentation out of service is governed by the plant technical specifications.

Table 2-1 gives the operating modes of the Special Nuclear Area Instrumentation versus plant conditions.

2.3.2 Subsystem Steady State Performance

The steady-state performance is with the system operating and continuously monitoring inputs. Output signals and display as required are generated for use on demand. The general use of this system is for determining the status of protection systems, performance of protection systems, status of bypasses, and accident monitoring.

2.3.3 Subsystem Response to Plant Transients

2.3.3.1 AOO Performance

The response of only the Special Nuclear Area Instrumentation is described in this section. The response of the Special Nuclear Area Instrumentation to all AOOs is as follows:

1. Monitors and displays all Safety Protection and Investment Protection Subsystem sensor channels before, during, and after all AOOs.

2. Monitors and displays Safety Protection and Investment Protection Subsystem actuated device states before, during, and after all AOOs.

3. Monitors and displays Safety Protection and Investment Protection Subsystem operability and status before, during, and after all AOOs.

4. Monitors and displays the minimum set of parameters necessary to determine that plant radionuclide control is maintained before, during, and after all AOOs.

Table 2-1

SPECIAL NUCLEAR AREA INSTRUMENTATION
OPERATING MODE VERSUS PLANT CONDITION

Plant Condition		Operating Mode	Remarks
1.1	Energy production	Operable	
1.2	Shutdown	Shutdown/operable	Portions of system may be shut down for maintenance
1.3	Refueling	Operable	
1.4	Startup and shutdown	Operable	
2.0	Maintain plant protected	Operating	Portion operating depends upon portion of plant in need of protection
3.0	Radiological release controlled	Operating	
4.0	Emergency plan activated	Operating	

2.3.3.2 DBE Performance

The response of only the Special Nuclear Area Instrumentation is described in this section. The response of the Special Nuclear Area Instrumentation DBEs is identical, except where noted, and is as follows:

1. Monitors and displays all Safety Protection and Investment Protection Subsystem sensor channels before, during, and after all DBEs.

2. Monitors and displays Safety Protection and Investment Protection Subsystem actuated device states before, during, and after all DBEs.

3. Monitors and displays Safety Protection and Investment Protection Subsystem operability and status before, during, and after all DBEs.

4. Monitors and displays the minimum set of parameters necessary to determine that plant radionuclide control is maintained before, during, and after all DBEs.

In DBE No. 1, station blackout, the Special Nuclear Area Instrumentation continues to operate from the uninterruptible power system.

For DBE No. 5, large seismic event, the Special Nuclear Area Instrumentation is seismically qualified to be operable following (but not necessarily during) a large seismic event.

Except as noted above environmental conditions or the plant service conditions experienced during DBEs have no effect on the ability of the special nuclear area instrumentation to perform its function.

2.3.3.3 SRDC Performance

The Special Nuclear Area Instrumentation is not classified as safety-related; therefore, this section is not applicable.

2.3.4 Subsystem Failure Modes and Effects

The Special Nuclear Area Instrumentation Subsystem is a redundant system for high reliability, therefore a single failure will not prevent its operation.

2.3.4.1 Reactor Vessel Relief Valve Block Valve Closure Interlock

The interlock function is accomplished when the power necessary to drive the block valves closed is interrupted. The interlock does not interfere with opening the block valves individually (or simultaneously). The system is a one-out-of-two logic arrangement where actuation of either logic train interrupts the block valve power for closing the valve. Loss of power or circuit failures could prevent valve closure which is the fail safe mode.

2.3.4.2 Information Displays

The safety system, investment protection and accident monitoring information displays are configured using a redundant computer based acquisition processing and display system. Therefore failure of any single component will not result in failure of the system. Portions of the system required for accident monitoring will be qualified for the accident conditions during which it is expected to perform.

2.4 SUBSYSTEM ARRANGEMENT

The Special Nuclear Area Instrumentation Subsystem is arranged into modular electronic components with two separate channels. Each of the four MHTGR reactor modules has separate Special Nuclear Area Instrumentation

associated with that reactor module. The Special Nuclear Area Instrumentation equipment includes its own operator interface equipment, operator interface equipment for the Safety Protection Subsystem, and operator interface equipment for the Investment Protection Subsystem. This operator interface equipment is located in the 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. 2-1.

The reactor vessel pressure relief block valve interlock utilizes interlock limit switches located on the valve actuator (gear/cam operated). (Alternately valve shaft mounted limit switches may be used.) The actuator relays are located in the motor control centers associated with the block valves.

A list of and locations of the Special Nuclear Area Instrumentation equipment is given in Table 2-2.

2.5 INSTRUMENTATION AND CONTROL

[This section not used because this entire system is an Instrumentation and Control System.]

Fig. 2-1 Arrangement of PPIS Equipment

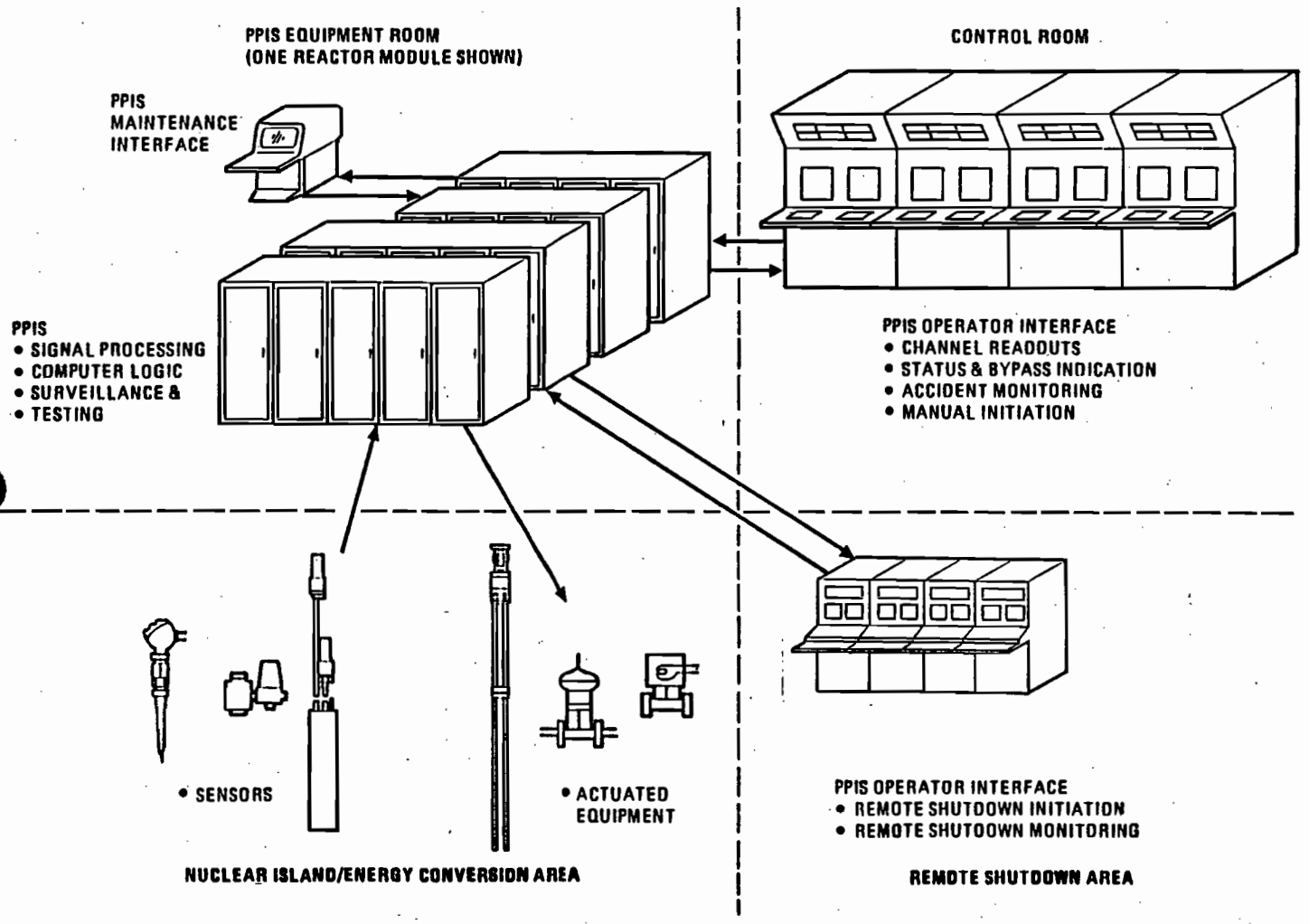


Table 2-2

SPECIAL NUCLEAR AREA INSTRUMENTATION EQUIPMENT

Equipment Number	Equipment Name	Quantity Required for MHTGR Plant	Equipment Location
I-3201-A/D	PPIS maintenance consoles	4	PPIS equipment room
I-3203-A/D	PPIS control room panels	4	Control room
I-3204-A/D	PPIS remote shutdown panels	4	Remote shut-down area
I-3206/9-A/D	Special nuclear area instrumentation	16	Reactor building
I-3217-1/2-A/D	Special nuclear area modules	8	PPIS equipment room
Z-3217-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 Special Nuclear Area Instrumentation Subsystem is independent for each reactor module.

4.2 COMPONENT BOUNDARY DEFINITION

The Special Nuclear Area Instrumentation Subsystem interfaces with various plant systems to obtain signal inputs.

Table 4-1

SPECIAL NUCLEAR AREA INSTRUMENTATION 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 System (1000)			
(Neutron Control Subsystem) (1012)	Provide signals to indicate when the control rod is fully inserted into the reactor core to act as a sensor input to the Special Nuclear Area Instrumentation.	Electrical signals.	Quantity: Two per control rod drive. (3203.0401.001)
	Provide signals to indicate when the reserve shutdown hopper gate is opened to act as a sensor input to the Special Nuclear Area Instrumentation.	Electrical signals.	Quantity: One per reserve shutdown mechanism. (3203.0401.002)
	Provide wide range neutron flux signals to act as inputs to the Special Nuclear Area Instrumentation.	Electrical signals.	Quantity: Three. (3203.0401.003)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.2 Reactor Vessel System (1100)			
(Pressure Relief Subsystem) (1105)	Provide signals from pressure relief block valves to indicate when either valve is not in the full open position. This signal acts as an input to the pressure relief block valve closure interlock.	Electrical signals.	Quantity: Two (redundant) and electrically separate limit switches from each pressure relief valve. (3203.0401.010)
	Provide signals from each pressure relief valve to the Special Nuclear Area Instrumentation to indicate if the relief valve is not fully closed.	Electrical signals.	Quantity: Two (redundant) per valve. (3203.0401.012)
4.1.1.3 Reactor Service System (2000)			
(Helium Purification) (2023) (Essential Cooling Water) (2042) (Gaseous Radioactive Waste) (2064)	Provide for status signals of those essential systems which support the moisture monitors to act as input to the Special Nuclear Area Instrumentation Subsystem information displayed.	Electrical signals.	Quantity: {Six.}* (3203.0401.020)

*Numbers in { } are estimated and subject to change.

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.4 Heat Transport System (2100)			
(Main Circulator Subsystem) (2101)	Provide sensor signals to indicate the status of the main loop shutoff valve to act as an input to the Special Nuclear Area Instrumentation Subsystem information displays.	Electrical Signals.	Quantity: Two (redundant) main loop shutoff valves. (3203.0401.050)
4.1.1.5 Miscellaneous Control and Insrumentation Group (3000)			
(Radiation Monitoring) (3003) (Meteorological Monitoring) (3005)	Provide information, trip status, and bypass status to the Special Nuclear Area Instrumentation Subsystem information displays.	Electrical signals.	Quantity: {Twelve.} (3203.0401.060)
4.1.1.6 Plant Protection and Instrumentation System (3200)			
(Investment Protection Subsystem) (3201) (Safety Protection Subsystem) (3202)	Provide information, trip status, and bypass status to the Special Nuclear Area Instrumentation Subsystem information displays.	Electrical signals.	Quantity: [TBD]. (3203.0401.080)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
4.1.1.7 Power Conversion Group (5000)			
(Feedwater and Condensate) (5002) (Main and Bypass Steam) (5004) (Steam and Water Dump (Subsystem) (5013)	Provide status and bypass signals to the Special Nuclear Area Instrumentation Subsystem information display.	Electrical signals.	Quantity: {Sixteen.} (3203.0401.100)
4.1.1.8 Reactor Cavity Cooling System (5600)	Provide status and performance information to Special Nuclear Area information displays.	Electrical signals.	Quantity: 2 flow; 10 temperature. (3203.0401.120)
4.1.1.9 Shutdown Cooling System (5700)			
(Shutdown Heat Removal Control Subsystem) (5703)	Provide information, trip status, and bypass status to the Special Nuclear Area Instrumentation Subsystem information displays.	Electrical signals.	Quantity: {Four.} (3203.0401.130)
4.1.1.10 Buildings, Structures, and Building Service Group (7000)			
(Reactor Building) (7001)	Provide building space and structural support to accommodate Special Nuclear Area Instrumentation Subsystem equipment.	Floor mounting.	Quantity: Eight cabinets. (3203.0401.150)

Table 4-1 (Continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
(Operations Center) (7008)	Provide main control room space to house Special Nuclear Area Instrumentation Subsystem main control room equipment.	Floor mounting.	Quantity: One cabinet. (3203.0401.160)
4.1.1.11 Mechanical Service Group (9000)			
(HVAC) (9011)	Provide HVAC to support the normal operation of the Special Nuclear Area Instrumentation Subsystem	None.	Quantity: {Two.} (3203.0401.170)
4.1.1.12 Electrical Group (9200)			
(Class 1E Uninterruptible) Power Supply) (9205)	Provide separate Class 1E uninterruptible power distribution channels to power the Special Nuclear Area Instrumentation Subsystem as a 1E associated circuit.	Electric feeders.	Quantity: Two separate Class 1E sources. (3203.0401.180)
	Provide status and bypass sensors for all Class 1E power buses to act as an input signals to the Special Nuclear Area Instrumentation Subsystem information displays.	Electrical signals.	Quantity: {Sixteen.} (3203.0401.190)

SECTION 5

SUBSYSTEM CONSTRUCTION

The construction of the Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation Subsystem components located in the reactor building. Access requirements in other buildings and lifting equipment requirements are [TBD].

5.6 INSTALLATION AND/OR FIELD FABRICATION

The installation of the Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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 Special Nuclear Area Instrumentation 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. 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 Special Nuclear Area Instrumentation 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 SUBSYSTEM LIMITATIONS, SETPOINTS, AND PRECAUTIONS

6.1.1 Subsystem Limits and Setpoints

The Special Nuclear Area Instrumentation is a two channel system. Since it has a degree of redundancy of one it is limited to being able to perform its function with one of the redundant channels failed.

Setpoints are generally established by the systems and subsystems that are monitored by the Special Nuclear Area Instrumentation Subsystem. Malfunction and other setpoints established within this subsystem will be delineated later in the design.

6.1.2 Precautions

Periodic surveillance is required of this subsystem to assure its continuing operability especially as it is not relied upon for the day-to-day normal plant operations.

Attention needs to be given to the validity of the data furnished by the system even though provisions have been made for validation of input data, etc. Suspect data should be investigated further or cross checked with the redundant portions of the subsystems.

Maintenance, when performed, should be limited to disabling as little as possible of the subsystem.

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 Special Nuclear Area Instrumentation Subsystem and its 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. PCRV Pressure Relief Block Valve Closure Interlock.
2. Safety Protection Information Displays.
3. Investment Protection Information Displays.
4. Accident Monitoring Displays.

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. Safety Protection Subsystem operable.
5. Investment Protection Subsystem operable.
6. Neutron Control System operable.
7. PCRV Pressure Relief System operable.
8. Heat Transport System Instrumentation operable.
9. Feedwater and Condensate System Instrumentation operable.
10. Main Steam and Turbine Bypass Instrumentation operable.
11. Steam and Water Dump Subsystem operable.
12. Radiation Monitoring Subsystem operable.
13. Meteorological Monitoring Subsystem 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 procedures (for example, calibration need not be performed upon each startup if the plant procedural requirement is a yearly calibration):

1. Check that any test instrumentation utilized has a current calibration.

2. Energize system.

3. Calibrate sensors, record as-found and as-left data.

4. Calibrate readout instruments.

5. Confirm input channel operability.

6. Monitor video displays for operability.

7. Check automatic logic test circuitry, run diagnostics programs.

8. Monitor automatic testing as provided, reset system as required.

9. Check that all signals, actuators, etc., are returned to their correct positions and confirm that all redundant portions of the system are operable.

10. 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 subsystem startup:

1. Routine preoperational checkout performed.

2. Electrical systems operating.

3. HVAC systems operating.

4. Reactor vessel pressure relief system operable.

6.3.1.2 Procedure

The startup procedure includes:

1. Ensuring instrumentation is operating.

2. Ensuring that reactor vessel block valve interlock is operable.

3. Ensuring periodically that instrumentation readings respond as expected during plant startup.

4. Ensuring that protection system status (bypasses of trips, etc.) change as expected during plant startup.

6.3.2 Shutdown from 25% Steam Flow

During the process of shutting the plant down from 25 percent steam flow the special nuclear area instrumentation is operating in its normal mode.

6.4 NORMAL OPERATION

The procedures for normal operation are as follows:

Periodically monitor subsystem status to ensure that all portions are operating normally.

Perform periodic surveillance, testing, and calibration in accordance with the plant procedures.

6.5 REFUELING

Monitor plant and protection system status periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

6.6 SHUTDOWN

During plant automatic shutdowns the plant safety status should be monitored by the operator periodically to ascertain that reactivity, core cooling, fission product barrier, and fission product release control are being maintained.

Shutdown of the entire special nuclear area instrumentation to perform maintenance is generally not required due to the redundancy of the subsystem. To the extent possible, maintenance and partial shutdown of the special nuclear area instrumentation should be done during scheduled plant shutdowns.

6.7 ABNORMAL OPERATION

Abnormal operation of the special nuclear area instrumentation is limited to operation with the subsystem operating in a degraded mode (failed or inoperable equipment).

Special Nuclear Area Instrumentation Subsystem is configured so as to not adversely affect plant safety or plant availability with a single failure.

The cause for failed equipment or input channel measurements should be determined, corrected, and the equipment repaired in a timely fashion.

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 Special Nuclear Area Instrumentation 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., 3203); 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

SPECIAL NUCLEAR AREA INSTRUMENTATION TECHNICAL REQUIREMENTS TRACEABILITY SUMMARY

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3203.0102.001	Formal design	1	3.2.3
3203.0102.002	Nuclear island configuration	1	3.2.3
3203.0102.003	Minimize inaccessible areas	1	3.2.3
3203.0102.004	Special nuclear area instrumentation essential features	1	3.2.3
3203.0102.005	Essential preventive features	1	3.2.3
3203.0102.006	Preventive features configuration	1	3.2.3
3203.0102.007	Configuration of protection systems information displays	1	3.2.3
3203.0102.008	Integration of protection systems information displays	1	3.2.3
3203.0102.009	Reactor vessel pressure relief block valve closure interlock electrical power	1	3.2.3
3203.0102.020	Mid 1990's start of operation	1	3.2.3
3203.0102.021	40-year load cycle	1	3.2.3
3203.0102.022	Design transients	1	3.2.3
3203.0102.023	Minimum plant staffing	1	3.2.3
3203.0102.030	Mechanical requirements for cabinet, rack, and panel design	1	3.2.3
3203.0102.040	Seismic design	1	3.2.3
3203.0102.041	Seismic response spectra	1	3.2.3
3203.0102.042	Seismic damping coefficients	1	3.2.3

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3203.0102.050	Materials	1	3.2.3
3203.0102.060	Operating environments	1	3.2.3
3203.0102.070	Requirement for remote shutdown	1	3.2.3
3203.0102.090	Availability	1	3.2.3
3203.0102.091	System outage requirements allocation	1	3.2.3
3203.0102.092	System reliability requirements allocation	1	3.2.3
3203.0102.100	Hands-on maintenance	1	3.2.3
3203.0102.101	Planned outage schedule	1	3.2.3
3203.0102.102	Man-hour requirements	1	3.2.3
3203.0102.103	"Off-the shelf" components	1	3.2.3
3203.0102.104	Spare parts listing	1	3.2.3
3203.0102.105	Parts interchangeability	1	3.2.3
3203.0102.106	Arrangement to facilitate on-line maintenance	1	3.2.3
3203.0102.107	Design to facilitate hands-on maintenance	1	3.2.3
3203.0102.108	Monitoring as basis for maintenance diagnostics	1	3.2.3
3203.0102.109	Plant staffing	1	3.2.3
3203.0102.110	Remote maintenance	1	3.2.3
3203.0102.111	On-line in-service inspection	1	3.2.3

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3203.0102.120	Equipment classification	1	3.2.3
3203.0102.130	Certification as a standard Nuclear Island	1	3.2.3
3203.0102.131	Codes and standards	1	3.2.3
3203.0102.132	Codes and standards	1	3.2.3
3203.0102.133	Codes and standards	1	3.2.3
3203.0102.140	Quality identification (QAL II, III)	1	3.2.3
3203.0102.150	Construction plan and schedule	1	3.2.3
3203.0102.151	Parallel construction	1	3.2.3
3203.0102.152	Utilization of shop, factory or field fabricated parts	1	3.2.3
3203.0102.153	Arrangement features	1	3.2.3
3203.0102.154	Materials, processes and parts	1	3.2.3
3203.0102.160	Decommissioning	1	3.2.3
3203.0401.001	Provide control rod inserted signals	2	2.2.2
3203.0401.002	Provide reserve shutdown hopper gate position signals	2	2.2.2
3203.0401.003	Provide wide range neutron signals	2	2.2.4

Table A-1 (Continued)

Traceability Number	Summary Requirement Description	Source Description/Reference Ref.	Section
3203.0401.010	Provide pressure relief valve position signals for block valve interlock	2	2.2.1
3203.0401.012	Provide pressure relief valve position signals	2	2.2.3
3203.0401.020	Provide moisture monitor support system status signals	2	2.2.3
3203.0401.050	Provide main loop shutoff valve status signals	2	2.2.3
3203.0401.060	Provide information from radiation monitoring, and meteorological subsystems for display	2	2.2.4
3203.0401.080	Provide protection system status and information for display	2	2.2.2 and 2.2.3
3203.0401.100	Provide status signals from feedwater, steam, and steam water dump subsystems for display	2	2.2.3
3203.0401.120	Provide status signals from RCCS system.	2 3	2.2.2 2.5
3203.0401.130	Provide information on SCS for display	2	2.2.3
3203.0401.150	Provide building space for Special Nuclear Area Instrumentation equipment	2	2.4
3203.0401.160	Provide control room space for Special Nuclear Area Instrumentation equipment	2	2.4
3203.0401.170	Provide HVAC for Special Nuclear Area Instrumentation equipment	2	2.2
3203.0401.180	Provide UPS for Special Nuclear Area Instrumentation equipment	2	2.2
3203.0401.190	Provide electric power system status signals	2	2.2.2 and 2.2.3

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. "Special Nuclear Area Instrumentation Subsystem Design Description," HFD-43203, Rev. 0 (908499, Rev. 0).

3. "Reactor Cavity Cooling System Design Description," HFD-35600, Rev. 0 (908442, Rev. 0).

APPENDIX B

DRAWINGS

Drawing Number	Title
GA Drawing [later]	IB Diagram - Protection System Display Instrumentation
GA Drawing [later]	IB Diagram - Reactor Vessel Pressure Relief Block Valve Interlock

APPENDIX C

TRANSIENTS

[LATER]

APPENDIX D

DESIGN BASIS SEISMIC INPUTS

[LATER]

APPENDIX E

PARAMETER LISTS

[LATER]

APPENDIX F

PROPRIETARY CLAIMS

[LATER]

DOE-HTGR-87-074
REVISION 0

HTGR

RADIATION MONITORING SUBSYSTEM DESIGN DESCRIPTION

[redacted]GY

Any Further Distribution [redacted]nt or [redacted]eign [redacted]nd For- [redacted]es Shall Be Approved [redacted]ion, U.S. [redacted]

AUTHOR/CONTRACTOR

BECHTEL NATIONAL, INC.

ISSUED BY: BECHTEL NATIONAL, INC.,
UNDER SUBCONTRACT TO GAS-COOLED REACTOR ASSOCIATES,
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

JULY 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HFD-43003

RADIATION MONITORING
SUBSYSTEM DESIGN DESCRIPTION
4 x 350 MWT MODULAR HTGR PLANT

[redacted]

Author/Contractor

Bechtel National, Inc.

Issued by: Bechtel National, Inc.

Under Subcontract to Gas-Cooled Reactor Associates

For The Department of Energy

Contract DE-AC03-78SF02034

July 1986

LIST OF EFFECTIVE PAGES

SECTION/ APPENDIX	PAGE(S)	REV.	DATE
—	Title Page	0	7/86
—	i through viii	0	7/86
—	Preface (ix)	0	7/86
—	Summary (xi)	0	7/86
1	1-1 through 1-5	0	7/86
2	2-1 through 2-8	0	7/86
3	3-1	0	7/86
4	4-1 through 4-3	0	7/86
5	5-1	0	7/86
6	6-1	0	7/86
7	7-1	0	7/86
8	8-1	0	7/86
9	9-1	0	7/86
A	A-1 through A-2	0	7/86
B	B-1	0	7/86
C	C-1	0	7/86
D	D-1	0	7/86
E	E-1	0	7/86
F	F-1	0	7/86
G	G-1	0	7/86

TABLE OF CONTENTS

Section	Page
LIST OF APPENDICES	iii
LIST OF ILLUSTRATIONS	iv
LIST OF TABLES	v
LIST OF ABBREVIATIONS AND ACRONYMS	vi
DEFINITIONS	viii
PREFACE	ix
SUMMARY	xi
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-2
1.2.3 Structural Requirements	1-2
1.2.4 Environmental Requirements	1-2
1.2.5 Instrumentation and Control Requirements	1-3
1.2.6 Surveillance and In-Service Inspection Requirements	1-3
1.2.7 Availablilty Assurance Requirements	1-3
1.2.8 Maintenance Requirements	1-3
1.2.9 Safety Requirements	1-3
1.2.10 Codes and Standards Requirements	1-3
1.2.11 Quality Assurance Requirements	1-4
1.2.12 Construction Requirements	1-4
1.2.13 Decommissioning Requirements	1-4
2. DESIGN DESCRIPTIONS	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-2

TABLE OF CONTENTS (cont'd)

Section	Page
2.3 Subsystem Performance Characteristics	2-5
2.3.1 Subsystem Operating Modes	2-5
2.3.2 Subsystem Steady-State Performance	2-6
2.3.3 Subsystem Response to Plant Transients	2-6
2.3.4 Subsystem Failure Modes and Effects	2-6
2.4 Subsystem Arrangement	2-6
2.5 Instrumentation and Control	2-8
3. COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS (TBD)	3-1
4. SUBSYSTEM AND COMPONENT INTERFACES	4-1
4.1 Subsystem Interface Requirements	4-1
4.2 Component Boundary Definition	4-3
5. SUBSYSTEM CONSTRUCTION	5-1
6. SUBSYSTEM OPERATION	6-1
7. SUBSYSTEM MAINTENANCE	7-1
8. SUBSYSTEM DECOMMISSIONING	8-1
9. REFERENCES	9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability Requirements	A-1
B	Drawings	B-1
C	Transients	C-1
D	Design Basis Seismic Inputs	D-1
E	Equipment List	E-1
F	Paremeter List	F-1
G	Proprietary Claims	G-1

LIST OF ILLUSTRATIONS

FIGURE PAGE

[TBD]

LIST OF TABLES

TABLE		PAGE
1-1	Codes and Standards	1-5
2-1	Potential Location of Radiation Monitors	2-3

LIST OF ABBREVIATIONS AND ACRONYMS

ALARA	As Low As Reasonably Achievable
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrences
ASME	American Society of Mechanical Engineers
BSDD	Building and Structures Design Description
CDS	Component Design Specification
CFR	Code of Federal Regulations
CRP	Central Radiation Processor
DBE	Design Bases Event
DMS	Data Management System
HPS	Helium Purification Subsystem
HTGR	High Temperature Gas-Cooled Reactor
HTS	Heat Transport System
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrument Society of America
LRP	Local Radiation Processors
MCR	Main Control Room
MHTGR	Modular High Temperature Gas-Cooled Reactor
NBS	National Bureal of Standards
NEMA	National Electrical Manufacturers Association
NICWB	Nuclear Island Cooling Water Building
NSSS	Nuclear Steam Supply System
OBE	Operating Basis Earthquake
OPDS	Overall Plant Design Specification
PCDIS	Plant Control and Data Information System
PPIS	Plant Protection and Instrumentation Subsystem
PRA	(TBD)
QA	Quality Assurance
QAL	Quality Assurance Level

LIST OF ABBREVIATIONS AND ACRONYMS (Cont'd)

RAB	Reactor Auxiliary Building
RB	Reactor Building
RCCS	Reactor Cavity Cooling System
RMS	Radiation Monitoring System
RPCWS	Reactor Plant Cooling Water Subsystem
RSB	Reactor Service Building
SCS	Shutdown Cooling System
SCWS	Shutdown Cooling Water System
SDD	Subsystem Design Description
SRDC	(TBD)
SSDD	Subsystem Design Description
SWS	Service Water Subsystem
TBD	To Be Determined

DEFINITIONS

[TBD]

PREFACE

The objectives of the MHTGR plant project is to produce safe, economical power. Supporting this objective, four major goals and their associated plant states are identified as follows:

1. Maintain Plant Operation
1.1 Maintain Safe Energy Production
1.2 Maintain Safe Shutdown
1.3 Maintain Safe Refueling
1.4 Maintain Safe 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 radionculide).

The Overall Plant Design Specificaion (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, interface, operational, safety, maintenance, inspection, and decommissioning requirements for design of the plant.

In response to the OPDS, a series of lower tier documents, System Design Descriptions (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDD), Component Design Specifications (CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability of requirement source from plant-level requirements to equipment-level requirements shall be maintained throughout this hierarchy of design documents.

SUMMARY

The Radiation Monitoring Subsystem (RMS) consists of area monitors, airborne monitors and process monitors located throughout the plant and at the site boundary. Certain monitors, located at specific areas in the plant, in-plant effluents, and at the site boundary, are capable of monitoring post-accident conditions. A Central Radiation Processor (CRP) includes RMS control and monitoring consoles and instrumentation cabinets located in the Reactor Service Building. All RMS displays and alarms are provided to the Plant Control and Data Information System (PCDIS) for presentation in the Main Control Room (MCR) and in the health physics/access control area in the Personnel Service Building.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 Subsystem Functions

The RMS serves to control both onsite and public radiation exposure by monitoring the dose levels and effluent radionuclide concentrations at various locations in the plant and at the site boundary.

The RMS provides alarm for assessment and response to abnormal radiation conditions.

The RMS has no power generation functions.

1.2 Subsystem Design Requirements

The subsystem design requirements discussed below include specific requirements and applicable top-level utility and regulatory requirements.

1.2.1 Subsystem Configuration and Essential Features Requirements

The RMS shall be capable of continuously detecting, indicating, and reporting radionuclide concentrations and radiation levels.

(3003.0102.011)*

The RMS shall provide for:

- o Area Radiation Monitoring
- o Airborne Radioactivity Monitors
- o Portable Monitors
- o Process Radioactivity Monitoring
- o Site Boundary Monitoring

(3003.0102.012)

---

* Traceability Number

1.2.2 Operational Requirement

[Component ranges, response characteristics, and accuracies shall meet the best time response and good stability on a long-term basis.]

(3003.0102.021)

[The RMS shall provide input to the PPIS.]

(3003.0102.022)

The RMS shall monitor classified zone areas requiring personnel access.

(3003.0102.023)

For generic and plant level operational requirements refer to OPDS (Ref. 1).

(3003.0102.024)

1.2.3 Structural Requirements

For generic and plant level structural requirements refer to OPDS (Ref. 1).

(3003.0102.031)

1.2.4 Environmental Requirements

[The RMS shall be designed to perform its function over a temperature range of 0° C (32° F) to 40° C (104° F) and a relative humidity range of 0 to 95 percent.]

(3003.0102.041)

[Many RMS components are exposed to significant radiation from surface and airborne contamination. The design of the affected components shall be able to withstand the effects of radiation being monitored and alarmed.]

(3003.0102.042)

For generic and plant level environmental requirements refer to OPDS (Ref. 1).

(3003.0102.043)

1.2.5 Instrumentation and Control Requirements

[The RMS is part of plant miscellaneous I&C. Thus, there are no I&C requirements.]

1.2.6 Surveillance and In-Service Inspection Requirements

The RMS local processor(s) shall contain fault diagnostics and/or supervised sensors and instrumentation to alert operators of equipment failures.

(3003.0102.061)

The RMS shall receive receive regular periodic calibration and operational checks.

(3003.0102.062)

1.2.7 Availability Assurance Requirements

For generic and plant level availability assurance requirements refer to OPDS (Ref. 1)

(3003.0102.071)

1.2.8 Maintenance Requirements

For generic and plant level maintenance requirements refer to OPDS (Ref. 1).

(3003.0102.081)

1.2.9 Safety Requirements

The RMS is not safety related. Thus, there are no requirements.

1.2.10 Codes and Standard Requirements

[The analyses and trade studies for determining the codes and standards and other industry and regulatory requirements which should be applied to the engineering of systems, structures, and components have not yet been

performed. However, it is anticipated that those listed on Table 1-1 will be found applicable.]

1.2.11 Quality Assurance Requirements

[TBD]

1.2.12 Construction Requirements

For generic and plant level construction requirements refer to OPDS (Ref. 1).
(3003.0102.121)

1.2.13 Decommissioning Requirements

For generic and plant level decomissioning requirements refer to OPDS (Ref. 1).
(3003.0102.131)

Table 1-1

CODES AND STANDARDS

1. ANSI - N13.1 - 1969, Sampling Airborne Radioactive Materials in Nuclear Facilities, Guide 10.

2. ANS-18-20, Nuclear Plant Reliability Data Collection and Reporting System.

3. ANS-58-4, Criteria for Technical Specifications for Nuclear Power Stations.

4. ISA-RP25.1, Materials for Instruments in Radiation Service, Recommended Practice.

5. NEMA-ICS 1, General Standards for Industrial Control and Systems.

6. NEMA-ICS 2, Standards for Industrial Control Devices, Controllers, and Assemblies.

SECTION 2

DESIGN DESCRIPTION

2.1 Summary Description

Area Radiation Monitoring. The area radiation monitoring subsystem supplements the personnel and area radiation survey provisions of the plant radiation protection program (see TBD) by serving to alert plant personnel entering or working in normally non-radiation or low-radiation areas, inform the Main Control Room (MCR) operators of the occurrence and approximate location of an abnormal radiation flux increase in non- radiation or low-radiation areas, and assist in maintaining personnel exposure as low as reasonably achievable (ALARA).

Airborne Radioactivity Monitors. Airborne radioactivity is monitored within an enclosure by either direct measurement by measurement of the enclosure atmosphere or of the exhaust air from the enclosure. The type of airborne radioactivity monitors are based upon the nature and type of radioactivity expected, and the location being monitored.

Portable Monitors. Portable air activity samplers are provided to allow periodic localized monitoring of specific air volumes of interest independent of the fixed monitor subsystems. The samplers are used to verify that airborne activity concentrations within the plant operating spaces are within allowable limits and also to verify the proper operation of fixed monitor subsystems.

Process Radioactivity Monitoring. Process radioactivity monitoring keeps the operators informed about the condition of routine or potential sources of radiation or radionuclide releases.

Site Boundary Monitoring. Site boundary monitoring keeps operators informed about the extent of routine airborne radionuclide releases and provides information for realistic assessment of radiological consequences following an accidental release of radioactive materials to the atmosphere (see TBD).

2.2 Subsystem Configuration

The RMS is intended to detect, indicate, and report radionuclide concentrations and radiation levels at various locations in the plant buildings, structures and subsystems, and at the site boundary. The monitors are controlled by Local Radiation Processors (LRP) which transmit data on a data bus (or loop) to a Central Radiation Processor (CRP). The CRP provides display and control functions and optionally can prepare release reports for normal and abnormal conditions. The RMS also provides input to the PPIS, with post-accident monitoring providing input to the Special Nuclear Area Instrumentation Subsystem, while airborne radioactivity monitors in the blowdown vent path for each reactor building provide input to the primary coolant pressure pumpdown portion of the Investment Protection Subsystem.

Additional configuration requirements follow:

Area Radiation Monitoring. This subsystem has no function related to the quantitative monitoring of releases of radioactive material to the environment; thus, this subsystem is configured only to supplement the plant radiation protection program only. See Section 4.2 for the location of monitors for this subsystem.

Airborne Radioactivity Monitors. Where ingestion of radioactive airborne materials by plant personnel is a possibility, combination particulate/halogen/gaseous monitors are used to analyze, record and alarm should the radioactivity approach the limits established by 10 CFR 20. See Table 2-1 for potential location of monitors for this subsystem.

Portable Monitors. This subsystem has no function related to the quantitative monitoring of releases of radioactive material to the

Table 2-1

POTENTIAL LOCATION OF RADIATION MONITORS

Area Monitors

- Main control room
- PPIS cabinet rooms
- Radwaste building corridors and processing areas
- Reactor building corridors
- Fuel storage and handling area
- Local control panels in each reactor building and in the reactor service building (RSB)
- Radwaste pipeway
- Helium purification system (HPS) area
- Reactor equipment service facility
- Radwaste shipment area
- Radwaste solidification area
- Sampling rooms and radioactive chemistry laboratory

Airborne Radioactivity Monitors

- Normal ventilation exhaust duct from each reactor building
- Blowdown vent path from each reactor building
- Reactor cavity cooling system (RCCS) exhaust ducts from each reactor silo
- Ventilation exhaust duct from the fuel handling area
- Ventilation exhaust duct(s) from the radwaste building
- Control room air supply intake (if necessary to protect operators)
- Exhaust from each turbine plant air ejector (if required for tritium or other releases)
- Two monitors located at grade between reactor modules 1 and 2 and 3 and 4.

Table 2-1 (Cont'd)

Process Radioactive Monitors

- Effluent from each helium purification system (HPS)
- Sample flow from the primary coolant system in each reactor module (to determine level of circulating activity)
- Reactor plant cooling water system (RPCWS) exit flow from each HPS, main helium circulators and moisture monitor instrumentation
- Exit water stream from each spent fuel pool
- Shutdown cooling water system (SCWS) exit flow from each shutdown cooling system (SCS) heat exchanger
- Service water system (SWS) exit flow from each SCWS heat exchanger

Site Boundary Monitors

- Meteorological tower and other selected locations

environment; thus, the sampling subsystem and portable monitors are provided for a back-up means of monitoring only.

Process Radioactivity Monitoring. This subsystem is concerned with detecting leaks between isolated process barriers. For example, heat exchangers that are used between processes that may contain radioactive materials and those that do not contain radioactive materials may develop leaks. Such leaks can be detected owing to the inherent sensitivity of the monitors for detecting radioactive materials. When such leakage is detected, alarms are actuated in the main control room so that corrective maintenance or other appropriate action can be taken. The RMS provides a continuous record of any such radioactivity. See Section 4.2 for the location of monitors for this subsystem.

Site Boundary Monitoring. In conjunction with meteorological data, radionuclide levels at the site boundary will be routinely assessed to verify that the dose due to airborne effluents does not exceed that permitted by the top level regulatory criteria (see TBD). A continuous air monitor provides the input to the RMS for the Site Boundary radionuclide level measurement. See Section 4.2. for the location of the monitor for this subsystem.

2.3 Subsystem Performance Characteristics

2.3.1 Subsystem Operating Modes

2.3.1.1 Normal Operation

During normal RMS operation, "on-line" monitors provide continuous information about the condition of routine or potential sources of radionuclide release.

Portable particulate, iodine, and gaseous continuous air monitors will be used to monitor the local areas where there is a possibility of airborne radioactivity during maintenance on the radioactive subsystems. Abnormal operation involving the spread of airborne radioactivity will be monitored locally using the portable monitors. Periodic grab samples for particulate,

iodine, and noble gases will be taken throughout the plant and analyzed in the radioactive chemistry laboratory in the Personnel Service Building to ensure that the fixed monitors are operating properly. In addition, all monitors will be calibrated on a quarterly schedule using radioactive transfer sources. The periodic recalibration will be based on primary calibration traceable to NBS standard sources.

2.3.1 Subsystem Steady State Performance

Prior to fuel loading, the RMS is completely operational and provides continuous and periodic localized monitoring through all modes of plant operation and post-accident condition.

2.3.2 Subsystem Response to Plant Transients

The RMS is not required to respond to plant transients. However, the RMS is powered from the non-class 1E UPS to provide continuous operation following loss of normal power.

2.3.3 Subsystem Failure Modes and Effects

The RMS has built in diagnostics, testing, and regular calibration to minimize pending signal failures.

Main Control Room (MCR) operator is alerted of any pending failures to aid in initiating corrective actions. If the RMS monitors fail to provide the operator with continuous information of the radioactivity levels, it does not affect short term reactor operation. During this term, portable monitors and/or sampling subsystem provides a back-up means of monitoring.

2.4 Subsystem Arrangement

Potential locations for radiation monitors are shown in Section 4. Specific locations and numbers of monitors will be determined based on plant subsystem layouts and the results of the shielding assessments. The location of the principal radiation monitors will be shown on the radiation zoning drawings.

The subsystem control and monitoring console is located in the Reactor Service Building in a location with convenient and continuous personnel access. Monitoring and interpretation of the radiation monitoring displays and reports will be performed by personnel other than main control room operating personnel. Selected output data are transmitted to the MCR and health physics/access control area.

Generally, area radiation monitors are provided in areas to which personnel normally have access and for which there is a potential for personnel unknowingly to receive radiation doses in excess of 10 CFR 20 limits in a short period of time because of subsystem failure or improper personnel action. Any plant area which meets one or more of the following criteria is monitored:

1. Zone I areas which, during normal plant operation, including refueling, could exceed the radiation limit of 0.25 mR/hr upon subsystem failure or personnel error or which will be continuously occupied following an accident requiring plant shutdown.
2. Zone II areas where personnel could otherwise unknowingly receive high levels of radiation exposure due to subsystem failure or personnel error.
3. Areas in which the new and spent fuel is received and stored.

The locations of fixed airborne radioactivity monitors are dependent upon the point of leakage, the ability to identify the source of radioactivity so that corrective action may be performed, and whether personnel may be exposed to the airborne radioactivity.

1. Airborne radioactivity monitors sample normally accessible personnel operating areas for which there is a potential for airborne radioactivity.
2. Exhaust ducts will be monitored which serve an area containing processes which, in the event of major leakage, could result in concentrations within the plant approaching the limits established by 10 CFR 20 for plant workers.

3. Dilution from other exhaust ducts is considered when locating monitors in exhausted subsystems to ensure maximum coverage and still be able to detect 10 CFR 20 airborne radioactivity limits in the area with the lowest ventilation flow.
4. Outside air ducts for the control building will be monitored to measure possible introduction of radioactive materials into the control building to ensure habitability of those areas requiring personnel occupancy.
5. Exhaust to the environment will be monitored to determine that concentrations exceeding those of the top level regulatory criteria are not released.

Areas not normally accessible are monitored prior to personnel entry with portable monitors or samplers depending upon the potential for airborne radioactivity and work to be performed in the area.

The location of process radioactivity monitors is dependent on the types of processes, the process fluids, the location of the potential leaks, the capability of available radioactivity detectors, the type of corrective action possible, and potential hazards to personnel.

The site boundary monitors are located on the meteorological tower and other selected locations depending upon the prevailing meteorological conditions.

2.5 Instrumentation and Control

Since the Radiation Monitoring Subsystem is an instrument system, it does not require any additional instruments or controls.

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

(TBD)

SECTION 4

SYSTEM AND COMPONENT INTERFACE

4.1 System Interface Requirements

Interface requirements, at the system level, are presented below for each system (subsystems are also included for information) on which requirements are imposed. The tabulation includes a brief descriptive statement of the nature of the interface, a quantitative requirement, and the physical location of the interface.

Interfacing System	Nature of Interface	Interfacing Component	Interface Requirement
Reactor Service Building	Provide space for, access to, support for the control and monitoring console.	Building Space	Quantity: 1 Space for console, approximately 4'x2' and 19" instrument racks [TBD] in an area with unlimited personnel access.
Plant Operation Support	Operate and maintain the Radiation Monitoring System.	Plant Personnel	Quantity: [TBD] Physical Interface: In the Reactor Service Building and at each monitor location.

Interfacing System	Nature of Interface	Interfacing Component	Interface Requirement
Data Management System	Transmits, processes and stores radioactive data.	Data Highway	Accept signals from RMS for transmission to MCR. Post accident monitoring data is transmitted to the Special Nuclear Area Instrumentation System.
Non-Class 1E UPS Power	Provides power to RMS.	UPS source distribution panel	Quantity: 120 V ac, 60 Hz, 1 Ph, 8000 W Physical Interface: In the Reactor Service Building and at each monitor location.
Heating Ventilation and Air Conditioning	Provide Environmental Control.	Building Space	Control temperature 10°C to 27°C. Relative humidity maximum of 95 percent noncondensing.
Meteorological Monitoring	Provide space for access to, support for radiation monitors.	Tower structure	Space and support for monitors on tower, etc.

4.2 Component Boundary Definition

[TBD]

SECTION 5

SUBSYSTEM CONSTRUCTION

[TBD]

SECTION 6

SYSTEM OPERATION

[TBD]

SECTION 7

SYSTEM MAINTENANCE

[TBD]

SECTION 8

SYSTEM DECOMMISSIONING

[TBD]

SECTION 9

REFERENCES

1. U.S. Department of Energy, Overall Plant Design Specification, Modular High Temperature Gas Cooled Reactor, HTGR-86-004, Revision 1, Issued by GA Technologies, San Diego, CA, February 1986.

APPENDIX A

TRACEABILITY REQUIREMENTS

Traceability Number	Requirement	Source Ref.	Source Section
3003.0102.011	The RMS shall have capability of detecting, inducting and reporting radiation levels	1	
3303.0102.012	The RMS shall provide for various monitoring	1	
3003.0102.021	[Shall have best response time and good stability]		*
3003.0102.022	[RMS shall input to the PPIS]		*
3003.0102.023	RMS shall monitor personnel access areas and classified zones	1	
3003.0102.024	Generic and plant level operational requirements	1	
3003.0102.031	Generic and plant level structural requirements	1	
3003.0102.041	[The RMS shall meet temperature and humidity requirements]		*
3003.0102.042	Shall withstand radiation environment		*
3003.0102.043	Generic and plant level environmental requirements	1	
3003.0102.061	The RMS local processors shall contain fault diagnostics	1	
3003.0102.062	Shall require regular calibration and operational checks	1	

* At present these requirements are anticipated and will be confirmed by Functional Analyses.

APPENDIX A, Cont'd.

TRACEABILITY REQUIREMENTS

Traceability Number	Requirement	Source Ref.	Source Section
3003.0102.071	Generic and plant level availability assurance requirements	1	
3003.0102.081	Generic and plant level maintenance requirements	1	
3003.0102.121	Generic and plant level construction requirements	1	
3003.0102.131	Generic and plant level decommissioning requirements	1	

APPENDIX B

DRAWINGS

Drawings are included as part of the Reactor Building and Reactor Service Building Design Descriptions.

APPENDIX C

TRANSIENTS

There are no transients that affect the RMS.

APPENDIX D

DESIGN BASIS SEISMIC INPUT

(TBD)

APPENDIX E

EQUIPMENT LIST

[TBD]

APPENDIX G

PROPRIETARY CLAIMS

[TBD]

APPENDIX F

PARAMETER LIST

[TBD]

DOE-HTGR-87-075
REVISION 0

HTGR

SEISMIC MONITORING SUBSYSTEM DESIGN DESCRIPTION

[redacted]
An[redacted]nt or
of Other[redacted]
In[redacted] Foreign Companies and For-
eign Sub[redacted]nies Shall
B[redacted]ision, U.S.
D[redacted]

AUTHOR/CONTRACTOR

BECHTEL NATIONAL, INC.

~~ISSUED BY: BECHTEL NATIONAL, INC.~~,
UNDER SUBCONTRACT TO GAS-COOLED REACTOR ASSOCIATES,
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

JULY 1987

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HFD-43004

SEISMIC MONITORING SUBSYSTEM DESIGN DESCRIPTION

4 x 350 MWT MODULAR HTGR PLANT

[redacted]

Author/Contractor

Bechtel National, Inc.

Issued by: Bechtel National, Inc.

Under Subcontract to Gas-Cooled Reactor Associates

For The Department of Energy

Contract DE-AC03-78SF02034

July 1986

LIST OF EFFECTIVE PAGES

SECTION/ APPENDIX	PAGE(S)	REV.	DATE
—	Title Page	0	7/86
—	i through vii	0	7/86
—	Preface (viii)	0	7/86
—	Summary (x)	0	7/86
1	1-1 through 1-5	0	7/86
2	2-1 through 2-6	0	7/86
3	3-1	0	7/86
4	4-1 through 4-2	0	7/86
5	5-1	0	7/86
6	6-1	0	7/86
7	7-1	0	7/86
8	8-1	0	7/86
9	9-1	0	7/86
A	A-1 through A-2	0	7/86
B	B-1	0	7/86
C	C-1	0	7/86
D	D-1	0	7/86
E	E-1	0	7/86
F	F-1	0	7/86
G	G-1	0	7/86

TABLE OF CONTENTS

Section	Page
LIST OF APPENDICES	iii
LIST OF ILLUSTRATIONS	iv
LIST OF TABLES	v
LIST OF ABBREVIATIONS AND ACRONYMS	vi
DEFINITIONS	vii
PREFACE	viii
SUMMARY	x
1. SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsytem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-1
1.2.3 Structural Requirements	1-2
1.2.4 Environmental Requirements	1-2
1.2.5 Instrumentation and Control Requirements	1-2
1.2.6 Surveillance and In-Service Inspection Requirements	1-3
1.2.7 Availablilty Assurance Requirements	1-3
1.2.8 Maintenance Requirements	1-3
1.2.9 Safety Requirements	1-3
1.2.10 Codes and Standards Requirements	1-3
1.2.11 Quality Assurance Requirements	1-3
1.2.12 Construction Requirements	1-5
1.2.13 Decommissioning Requirements	1-5
2. DESIGN DESCRIPTIONS	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-2

TABLE OF CONTENTS (cont'd)

Section	Page
2.3 Subsystem Performance Characteristics	2-3
2.3.1 Subsystem Operating Modes	2-4
2.3.2 Subsystem Steady-State Performance	2-4
2.3.3 Subsystem Response to Plant Transients	2-5
2.3.4 Subsystem Failure Modes and Effects	2-5
2.4 Subsystem Arrangement	2-5
2.5 Instrumentation and Control	2-5
3. COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS	3-1
3.1 Component Functions	
3.2 Component Design Requirements	
4. SUBSYSTEM AND COMPONENT INTERFACES	4-1
4.1 Subsystem Interface Requirements	4-1
4.2 Component Boundary Definition	
5. SUBSYSTEM CONSTRUCTION	5-1
6. SUBSYSTEM OPERATION	6-1
7. SUBSYSTEM MAINTENANCE	7-1
8. SUBSYSTEM DECOMMISSIONING	8-1
9. REFERENCES	9-1

LIST OF APPENDICES

APPENDIX		PAGE
A	Traceability Requirements	A-1
B	Drawings	B-1
C	Transients	C-1
D	Design Basis Seismic Inputs	D-1
E	Equipment List	E-1
F	Paremeter List	F-1
G	Proprietary Claims	G-1

LIST OF ILLUSTRATIONS

FIGURE		PAGE
2-1	Location of Seismic Instrumentation Sensors	2-6

LIST OF TABLES

TABLE		PAGE
1-1	Codes and Standards	1-4

LIST OF ABBREVIATIONS AND ACRONYMS

AOO	Anticipated Operational Occurrence
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CFR	Code of Federal Regulations
DMS	Data Management System
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrument Society of America
ICD	Interface Control Document
MCR	Main Control Room
MHTGR	Modular High Temperature Gas-Cooled Reactor
NFPA	National Fire Protection Association
OPDS	Overall Plant Design Specification
PA	Peak Accelerograph
PPIS	Plant Protection and Instrumentation Subsystem
PSG	Peak Strain Gage
QA	Quality Assurance
QAL	Quality Assurance Level
OBE	Operating Basis Earthquake
RB	Reactor Building
RAB	Reactor Auxiliary Building
SDD	System Design Description
SMS	Seismic Monitoring System
SS	Seismic Switch
SSDD	Subsystem Design Description
SSE	Safe Shutdown Earthquake
SWS	Service Water Subsystem
TBD	To Be Determined
THA	Time History Accelerometer

DEFINITIONS

[TBD]

PREFACE

The objectives of the MHTGR plant project is to produce safe, economical power. Supporting this objective, four major goals and their associated plant states are identified as follows:

1. Maintain Plant Operation
1.1 Maintain Safe Energy Production
1.2 Maintain Safe Shutdown
1.3 Maintain Safe Refueling
1.4 Maintain Safe 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 radionculide).

The Overall Plant Design Specificaion (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, interface, operational, safety, maintenance, inspection, and decommissioning requirements for design of the plant.

In response to the OPDS, a series of lower tier documents, System Design Descriptions (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDD), Component Design Specifications (CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability of requirement source from plant-level requirements to equipment-level requirements shall be maintained throughout this hierarchy of design documents.

SUMMARY

The Seismic Monitoring System (SMS) consists of an array of sensors and a system control and monitoring console housing data handling and recording equipment.

The Seismic Monitoring System acquires and processes seismic data for use in assessing the consequences of earthquakes which exceed an operating basis earthquake (OBE) or a safe shutdown earthquake (SSE).

SECTION 1

SYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SYSTEM FUNCTIONS

The SMS permits assessment of the continued functionality of systems, subsystems, and components significant to the protection, public health, and safety to allow plant restart following a seismic event, in support of integrated approach goals 1 and 2.

1.2 SYSTEM DESIGN REQUIREMENTS

The system design requirements discussed below include specific requirements and applicable top-level utility and regulatory requirements.

1.2.1 System Configuration and Essential Features Requirements

The SMS shall be capable of continuously detecting, indicating, and reporting seismic activity for the facility.

(3004.0102.011)

[The SMS shall consist of seismic sensing and monitoring instrumentation.]

(3004.0102.012)

1.2.2 Operational Requirement

[The SMS shall provide continuous monitoring through all modes of plant operation and post-earthquake conditions.]

(3004.0102.021)

[The SMS shall have built-in diagnostics, testing and calibration features to minimize pending special failures.]

(3004.0102.022)

[The SMS shall provide selected data to the Data Management System (DMS).]

(3004.0102.023)

[Seismic Switches shall be installed adjacent to each of the Time History Accelerometers.]

(3004.0102.024)

For generic and plant level operational requirements refer to OPDS (Ref. 1).

(3004.0102.025)

1.2.3 Structural Requirements

For generic and plant level requirements refer to OPDS (Ref. 1).

(3004.0102.031)

1.2.4 Environmental Requirements

[The SMS shall be designed to perform its function and operate continuously over a temperature range of 0°C (32°F) to 40°C (104°F) and a relative humidity range of 0 to 95 percent.]

(3004.0102.041)

For generic and plant level I&C requirements, refer to OPDS (Rev.1)

(3004.0102.042)

1.2.5 Instrumentation and Control Requirements

[The SMS is part of plant miscellaneous I&C. Thus, there are not I&C requirements.]

---

* Traceability Number.

1.2.6 Surveillance and In-Service Inspection Requirements

[The SMS local processor(s) shall contain fault diagnostics and/or supervised sensors and instrumentation to alert operators of equipment failures.]

(3004.0102.061)

The SMS shall receive regular periodic calibration and operational checks.

(3004.0102.062)

1.2.7 Availability Assurance Requirements

For generic and plant level availability assurance requirements refer to OPDS (Ref. 1)

(3004.0102.071)

1.2.8 Maintenance Requirements

For generic and plant level maintenance requirements refer to OPDS (Ref. 1).

(3004.0102.081)

1.2.9 Safety Requirements

The SMS is not safety-related. Thus, there are no safety requirements.

1.2.10 Codes and Standard Requirements

[The analyses and trade studies for determining the codes and standards and other industry and regulatory requirements which should be applid to the engineering of systemns, structures, and components have not yet been performed. However, it is anticipated that those listed on Table 1-1 will be found appliable.]

1.2.11 Quality Assurance Requirements

[TBD]

TABLE 1-1

CODES AND STANDARDS

1. ANS-18-20, Nuclear Plant Reliability Data Collection and Reporting System.

2. ANS-58-4, Criteria for Technical Specifications for Nuclear Power Stations.

3. NEMA-ICS 1, General Standards for Industrial Control and Systems.

4. NEMA-ICS 2, Standards for Industrial Control Devices, Controllers, and Assemblies.

5. ANSI/ANS 2.2, Earthquake Instrumentation Criteria for Nuclear Power Plants

1.2.12 Construction Requirements

For generic and plant level construction requirements refer to OPDS (Ref. 1).

(3004.0102.121)

1.2.13 Decommissioning Requirements

For generic and plant level decomissioning requirements refer to OPDS (Ref. 1).

(3004.0102.131)

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

The SMS is configured using the following sensing and monitoring instrumentation:

Peak accelerographs (PA). These sensors are manually retrieved following an earthquake and are used in the detailed investigations for particular structures, systems, and equipment.

Peak Strain Gages (PSG). These sensors are mounted directly on equipment, supports, or piping as necessary to verify the continued availability of seismic category I systems and equipment.

Seismic Switches (SS). These devices actuate the seismic monitoring subsystem when seismic accelerations exceed selected set points.

Response Spectrum Analyzer (RSA). The response spectrum analyzer determines the response spectra attained in three mutually orthogonal directions at any THA location.

Time History Accelerometers (THA). Time history accelerometers produce a record of the time varying acceleration at the sensor location.

System control and monitoring console. A console located in the Reactor Service Building houses the recording, playback, and calibration units which are used in conjunction with the THA sensors to produce a time/history record of an earthquake. The console location is shown in Appendix E.

2.2 SYSTEM CONFIGURATION

The SMS is intended to detect, indicate, and record the seismic accelerations experienced by structures and equipment [significant to the protection of public health and safety] during an earthquake. The basic set of SMS sensors is provided for two of the four identical Reactor Buildings. Because the Reactor Buildings are identical, the data from the instrumented ones will be applicable to all. The seismic instruments are designed to respond to the reactor building design acceleration levels. Two redundant sets of reactor building seismic sensors permit major maintenance on any reactor module, including removing a set of sensors from service, without jeopardizing seismic surveillance of the plant.

Additional configuration requirements follow.

Peak Accelerographs. Each sensor contains three accelerographs mounted in a mutually orthogonal array. PAs which are mounted directly on equipment have one axis coincident with the principal equipment axis. All other PAs have their principal axes oriented identically, with one horizontal axis parallel to the major horizontal axis assumed in the seismic analysis. Specific sensor locations are chosen which exhibit significant responses to seismic motion. These sensors do not require a power source but have the capability of permanently recording peak acceleration. The seismic instrument type and location are shown in Appendix E.

Peak Strain Gages. These gages are mounted directly on the equipment, equipment supports, or piping at a point chosen to display the maximum earthquake-induced strain. Data from PSGs must be manually retrieved following an earthquake and are used in the detailed investigation of particular systems and equipment. The seismic instrument type and location are shown in Appendix E.

Seismic Switches. Switch contacts open (fail safe) when seismic accelerations exceed the switch setpoint. Information of the exceeded setpoints is presented in the main control room. The seismic switches have independently

adjustable setpoints for the vertical and horizontal axes. These switches are installed adjacent to each of the Time History Accelerometers (THA). The seismic instrument type and location are shown in Appendix E.

Response Spectrum Analyzer. This instrument analyzes the response spectra obtained at any THA location and displays this information at the monitoring console. The display unit is either an X-Y or stripchart recorder that plots response acceleration versus frequency or a hard copy printer that prints the response acceleration values and their respective frequencies. The seismic instrument type and location are shown in Appendix E.

Time History Accelerometers. The response data obtained from a THA is used directly for analysis and comparison with reference information, and may be converted to response spectra form for spectral comparisons with design parameters.

Each sensor unit contains three accelerometers mounted in a mutually orthogonal array. All accelerometers have their principal axes oriented identically, with one horizontal axis parallel to the major horizontal axis assumed in the seismic analysis.

A magnetic tape recording and playback unit is provided for multiple channel recording and playback of the signals from time history accelerometers. The data recordings include an additional recording channel which contains a timing signal. The recording and playback system has a special cabinet furnished for these instruments and devices necessary for system testing, annunciating, calibration, and control. This cabinet is located adjacent to the monitoring console. The seismic and instrument type and location are shown in Appendix E.

System Control and Monitoring Console. This console and its associated equipment is used in conjunction with THA sensors. The console contains signal conditioning and display equipment associated with the remote indicating response spectrum recorder, audible and visual annunciators associated with the seismic switches, audible and visual annunciators wired to

display initiation of the THA recorder, and the power supply components for all equipment contained within the console. The console location is shown in Appendix E.

2.3 SYSTEM PERFORMANCE CHARACTERISTICS

2.3.1 System Operating Mode

2.3.1.1 Normal Operation

During normal SMS operation, monitors provide continuous information about seismic conditions (seismic accelerations experienced by structures and equipment during an earthquake).

During normal SMS operation equipment-mounted peak recording accelerographs and peak strain gages are used to determine if the design limitation of the specific equipment to which they are fastened has been exceeded. If the measured responses are less than the values used in the design and qualification of structures, systems, and equipment [significant to the protection of the public health and safety], the structure, system, or equipment is considered adequate for future operations. Otherwise, further analysis is made to check the adequacy of these items for future use. Initial determination of the earthquake severity is performed immediately after the earthquake by comparing the measured response spectra with the OBE and SSE response spectra for the corresponding location. If the measured spectra exceed the OBE response spectra by a significant amount, the plant will be shut down and a detailed analysis of the earthquake motion will be undertaken.

2.3.2 System Steady State Performance

The system performance characteristics are as specified in [ANSI/ANS 2.2, Section 5,] which defines the requirements for the acceleration sensors, recorders, seismic switches, time history accelerographs, peak accelerographs and the response spectrum recorder.

Prior to startup, the SMS is completely operational and provides continuous monitoring through all modes of plant operation and post-earthquake conditions.

2.3.3 System Response to Plant Transient

The SMS is not required to respond to plant transients. However, it is designed to be operable during and after a DBE-5 event.

2.3.4 System Failure Modes and Effects

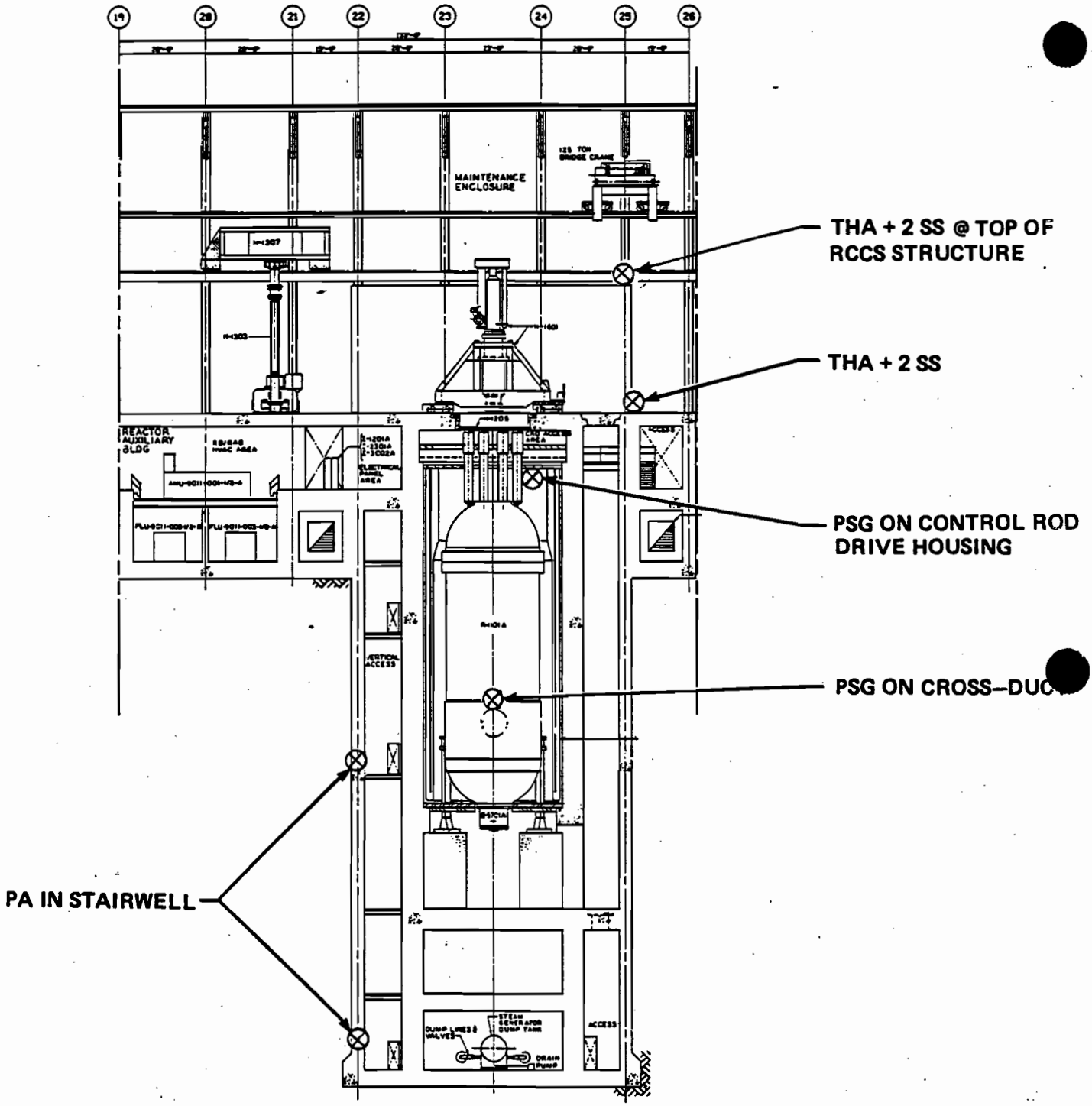
During normal operation the SMS provides continuous monitoring to determine if the design limitation of the structures systems or equipment has been exceeded. If the SMS sensors fail to provide continuous information about seismic accelerations the operator is alerted and will initiate corrective actions. Prolonged outage of the SMS fails to provide the operator with the necessary data to carry out a detailed analysis should an earthquake occur.

2.4 SYSTEM ARRANGEMENT

The seismic sensors are located as shown in Figure 2-1. The subsystem control and monitoring console is located in the Reactor Service Building in a location with convenient personnel access. Monitoring and interpretation of the seismic monitoring displays and recordings will be performed by personnel other than main control room the operating personnel.

2.5 INSTRUMENTATION AND CONTROL

Since the Seismic Monitoring System is an instrument system, it does not require any additional instruments and controls.



⊗ Seismic instrumentation sensors

THA	Time-history accelograph
PA	Peak accelograph
SS	Seismic switch
PSG	Peak strain gage

Figure 2-1

LOCATION OF SEISMIC INSTRUMENTATION SENSORS
(TYPICAL FOR 2 REACTOR SILOS)

SECTION 3

COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS

[TBD]

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACE

4.1 SYSTEM INTERFACE REQUIREMENTS

Interface requirements, at the system level, are presented below for each system (subsystems are also included for information) on which requirements are imposed. The tabulation includes a brief descriptive statement of the nature of the interface, a quantitative requirement, and the physical location of the interface.

Interfacing System	Nature of Interface	Interfacing Component	Interface Requirement
Building Structures and Building Service Group	Provide and maintain space for the control and monitoring console in the Reactor Service Building	Building space	Space for console approximately 1m x 2m (3' x 6') and one and one instrument rack in an area with unlimited personnel access. Space to remain functional and, habitable during all seismic events including SSE.
Plant Operation Support	Operate and maintain the Seismic Monitoring Subsystem	Plant personnel	Plant, O&M staff including instrument technician.

Interfacing System	Nature of Interface	Interfacing Component	Interface Requirement
Data Processing	Transmits, processes and stores seismic data	Data highway	Accepts signals from SMS for transmission to MCS
Non-Class 1E power	Provides Power to SMS	Uninterruptable power source (UPS) bus	110/240 V AC, 60 Hz 1200 W. UPS to remain operable through SSE.

4.2 COMPONENT BOUNDARY DEFINITIONS

[TBD]

SECTION 9

REFERENCES

1. U.S. Department of Energy, Overall Plant Design Specification, Modular High Temperature Gas Cooled Reactor, HTGR-86-004, Revision 1. Issued by GA Technologies, San Diego, CA, February 1986.

APPENDIX A

TRACEABILITY REQUIREMENTS

Traceability Number	Requirement	Source Ref.	Source Section
3004.0102.011	The SMS shall have the capability of detecting, indicating and reporting seismic activity	1	
3004.0102.012	[The SMS shall consist of seismic sensing and monitoring equipment]		*
3004.0102.021	[The SMS shall provide continuous monitoring]		*
3004.0102.022	[The SMS shall have built-in diagnostics]		*
3004.0102.023	[The SMS shall interface the DMS]		*
3004.0102.024	[The seismic switches shall be installed next to THAs]		*
3004.0102.025	Generic and plant level operational requirements	1	
3004.0102.031	Generic and plant level structural requirements	1	
3004.0102.041	[The SMS shall meet temperature and humidity requirements]		*
3004.0102.042	Generic and plant level environmental requirements	1	
3004.0102.061	[The SMS local processors shall contain fault diagnostics]		*
3004.0102.062	The SMS shall receive regular calibration and operational checks	1	
3004.0102.071	Generic and plant level availability assurance requirements	1	

Traceability Number	Requirement	Source Ref.	Source Section
3004.0102.081	Generic and plant level maintenance requirements	1	
3004.0102.121	Generic and plant level construction requirements	1	
3004.0102.131	Generic and plant level decommissioning requirements	1	

* At present these requirements are anticipated and will be confirmed by Functional Analyses.

APPENDIX B

DRAWINGS

Drawings are included as part of the Reactor Building and Reactor Service Building Design Descriptions.

APPENDIX C

TRANSIENTS

[TBD]

APPENDIX D

DESIGN BASIS SEISMIC INPUT

(TBD)

APPENDIX E

EQUIPMENT LIST

Instrument	Quantity/Plant	Location of Seismic Instrumentation Sensors
Time history accelerographs (THA)	4	Reactor Building stairwell
Peak strain gages (PSG)	7	Cross duct, control rod drive housing and reactor building column
Seismic switches (SS)	12	Reactor Building operating floor and fuel handling area
Triaxial time/history accelerometers (THA)	7	Reactor Building operating floor and fuel handling area
Response spectrum (RS)	1	Control and monitoring console in the Reactor Service Building
Recording and playback console	1	Control and monitoring console in the Reactor Service Building

APPENDIX F

PARAMETER LIST

[TBD]

Section G

PROPRIETARY CLAIMS

[TBD]

DOE-HTGR-87-024

HTGR

METEOROLOGICAL MONITORING SUBSYSTEM DESIGN DESCRIPTION

[redacted]

Any Further Distribution by Any Holder of this Document or of Other Data Therein to Third Parties Representing Foreign Interest, Foreign Governments, Foreign Companies and Foreign Subsidiaries or Foreign Divisions of U.S. Companies Shall Be Approved by the Director, HTGR Development Division, U.S. Department of Energy.

AUTHOR / CONTRACTOR

STONE & WEBSTER ENGINEERING CORP.

ISSUED BY STONE & WEBSTER ENGINEERING CORP.
UNDER SUBCONTRACT TO GAS-COOLED REACTOR ASSOCIATES
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

JUNE 1986

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HFD-43005

METEOROLOGICAL MONITORING SUBSYSTEM DESIGN DESCRIPTION

4 x 350 MW(t) MODULAR HTGR PLANT

APP[redacted]OGY

An[redacted]ther Distribution by any Holder of this Document or of Other Data [redacted]ing Foreign Int[redacted]reign Subsidi[redacted]ll Be Approv[redacted] Development [redacted], U.S. De[redacted]

Author/Contractor

Stone & Webster Engineering Corporation

Issued By:
Stone & Webster Engineering Corporation
Under Subcontract to Gas-Cooled Reactor Associates
For the Department of Energy
Contract DE-AC03-78SF02034

June 1986

CONTENTS

	PAGE
LIST OF EFFECTIVE PAGES	iv
LIST OF ACRONYMS	v
LIST OF DEFINITIONS	vi
LIST OF ILLUSTRATIONS	vii
LIST OF TABLES	viii
LIST OF APPENDICES(TBD)	-
PREFACE	ix
SUMMARY	x
1 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operating Requirements	1-1
1.2.3 Structural Requirements	1-1
1.2.4 Environmental Requirements	1-1
1.2.5 Instrumentation and Control Requirements	1-2
1.2.6 Surveillance and In-Service Inspection Requirements	1-2
1.2.7 Availability Assurance Requirements	1-2
1.2.8 Maintenance Requirements	1-2
1.2.9 Safety Requirements	1-3
1.2.10 Codes and Standards Requirements	1-3
1.2.11 Quality Assurance Requirements	1-3
1.2.12 Construction Requirements (TBD)	-
1.2.13 Decommissioning Requirements (TBD)	-
2 DESIGN DESCRIPTION	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-1
2.2.1 Meteorological Tower	2-1
2.2.2 Meteorological Instruments	2-1
2.2.3 Instrument Building	2-2
2.2.4 Data Handling and Processing Equipment	2-2
2.3 Subsystem Performance Characteristics	2-2
2.4 Subsystem Arrangement	2-2
2.5 Instrumentation and Control	2-3
2.5.1 Meteorological Instrument	2-3
2.5.2 Local Instruments	2-3

CONTENTS (continued)

PAGE

3 COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS (TBD) . . . . . -

3.1 Component Functions (TBD) . . . . . -
3.2 Component Design Requirements (TBD) . . . . . -

4 SUBSYSTEM AND COMPONENT INTERFACES 4-1

4.1 Subsystem Interface Requirements 4-1

4.1.1 Interface Requirements Imposed on Other Systems . . . 4-1
4.1.2 Interface Requirements Imposed on Subsystems Within the System 4-1

4.2 Component Boundary Definition (TBD) 4-1

5 SUBSYSTEM CONSTRUCTION (TBD) . . . . . -

5.1 Packaging and Shipping (TBD) . . . . . -
5.2 Handling at Delivery (TBD) . . . . . -
5.3 Receiving Inspection (TBD) . . . . . -
5.4 Storage (TBD) . . . . . -
5.5 Access to Buildings (TBD) . . . . . -
5.6 Installation and/or Field Fabrication (TBD) . . . . . -
5.7 Construction Testing (TBD) . . . . . -
5.8 As-Built Drawings (TBD) . . . . . -

6 SUBSYSTEM OPERATION (TBD) . . . . . -

6.1 Subsystem Limitations, Set Points and Precautions (TBD) . . . -

6.1.1 Subsystem Limitations and Set Points (TBD) . . . . . -
6.1.2 Precautions (TBD) . . . . . -

6.2 Preoperational Checkout (TBD) . . . . . -
6.3 Startup/Shutdown (TBD) . . . . . -
6.4 Normal Operation (TBD) . . . . . -
6.5 Refueling (TBD) . . . . . -
6.6 Shutdown (TBD) . . . . . -
6.7 Abnormal Operation (TBD) . . . . . -
6.8 Casualty Events and Recovery Procedures (TBD) . . . . . -

6.8.1 Casualty Events (TBD) . . . . . -
6.8.2 Design Features to Mitigate Effects of Casualty Events (TBD) . . . . . -
6.8.3 Recovery Procedures (TBD) . . . . . -

7 SUBSYSTEM MAINTENANCE (TBD) . . . . . -

7.1 Maintenance Approach (TBD) . . . . . -
7.2 Corrective Maintenance (TBD) . . . . . -
7.3 Preventive Maintenance (TBD) . . . . . -
7.4 In-Service Inspection (TBD) . . . . . -
7.5 Surveillance (TBD) . . . . . -

CONTENTS (continued)

PAGE

8 SUBSYSTEM DECOMMISSIONING (TBD) . . . . . -

9 REFERENCES 9-1

LIST OF EFFECTIVE PAGES

Page(s)	Rev.	Date
Title page	0	6/86
i through x	0	6/86
1-1 through 1-7	0	6/86
2-1 through 2-7	0	6/86
4-1 through 4-5	0	6/86
9-1	0	6/86

LIST OF ACRONYMS

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
IEEE	Institute of Electrical and Electronics Engineers
NFPA	National Fire Protection Association
NSSS	Nuclear Steam Supply System
OPDS	Overall Plant Design Specification
PPIS	Plant Protection and Instrumentation System
SDD	System Design Description
SSDD	Subsystem Design Description

LIST OF DEFINITIONS

Capable of Measurement	The condition where the entire instrument system will be within the system accuracy and will meet the data recovery requirements.
Chi Over Q (χ/Q)	The degree of dispersion of a radioactive release as it is transported from the point of release to the receptor. It is also called the relative concentration as it is the ratio of the concentration of radioactivity at the receptor (χ) to the radioactivity release rate (Q).
Delta T (ΔT)	The temperature difference between the 60 m (197 ft) and 10 m (33 ft) elevations of the meteorological tower. It is an indication of atmospheric stability in the vertical plane and in the horizontal plane for wind speed below 1.5 m/s (3.4 mi/hr).
Design Basis Event	Postulated abnormal event used in the plant design to establish the acceptable performance requirements of the structures, systems, and components.
Indication of Atmospheric Stability	See delta T and sigma theta
Instrument System	All components of the meteorological monitoring subsystem from the sensor to, and including, data recording and reduction.
Joint Recovery of No Less Than 90 Percent For an Annual Cycle of Wind Speed, Wind Direction, and Stability	For each year (8,760 hours), there will be no less than 7,884 hours for which there will be an hourly average value each for windspeed, wind direction, and an indication of atmospheric stability (ΔT or σ_θ).
System Accuracy	The accuracy to which the meteorological monitoring subsystem provides the true value, as measured by a system traceable to the National Bureau of Standards.
Sigma Theta (σ_θ)	The standard deviation of horizontal wind direction fluctuations determined by statistical analysis of instantaneous values of lateral wind direction. It is an indication of atmospheric stability in the horizontal plane for wind speeds above 1.5 m/s (3.4 mi/hr).

LIST OF ILLUSTRATIONS

TITLE	PAGE
2-1 Meteorological Monitoring Schematic	2-7

LIST OF TABLES

	TITLE	PAGE
1-1	Regulatory Guidance Documents	1-4
1-2	Industry Codes and Standards	1-5
2-1	Meteorological Monitoring Sensors	2-4
2-2	Meteorological Monitoring Instrument Accuracy	2-5
2-3	Local Instruments	2-6
4-1	Interface Requirements Imposed on Other Systems	4-2
4-2	Interface Requirements Imposed on Other Subsystems Within the System.	4-5

PREFACE

The objectives of the HTGR plant project are to produce safe, economical power. Supporting these objectives are four major goals and their associated plant states, 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 Overall Plant Design Specification (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, interface, operational, safety, maintenance, inspection and decommissioning requirements for design of the plant.

In response to the OPDS a series of lower tier documents, System Design Descriptions (SDDs), Subsystems Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDDs), Component Design Specifications (CDSs), and Interface Control Documents (ICDs) describe and control the individual designs. Traceability from plant-level requirements to equipment-level requirements is maintained throughout this hierarchy of design documents.

SUMMARY

Meteorological monitoring acquires and processes meteorological data for use in assessing the following potential environmental effects:

- Site acceptability and adequacy of engineered safety procedures
- Routine radioactive releases
- Design basis accidential releases
- Nonradioactive effects, such as cooling tower effluents (icing, fogging, and salt drift)

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SUBSYSTEM FUNCTIONS

The function of Meteorological Monitoring is to acquire and process meteorological data for use in assessing potential environmental effects for all states of plant operation.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Meteorological Monitoring configuration shall consist of two independent and redundant sets of instruments for parameters requiring joint recovery, i.e., wind speed, wind direction, and indication of atmospheric stability at each elevation.

(3005.0121.001)

1.2.2 Operating Requirements

The nominal voltage for the Meteorological Monitoring instruments shall be non-Class 1E 120 V ac, 60 Hz, single phase.

(3005.0122.001)

The nominal voltage for the meteorological instrument building heating and cooling shall be non-Class 1E 480 V ac, 60 Hz, three phase.

(3005.0122.001)

1.2.3 Structural Requirements

The meteorological tower shall be designed for a horizontal wind pressure of (TBD) kPa ((TBD) psi), on flat surfaces and on ice loading of (TBD) mm ((TBD) in.) of radial (solid) (rime) ice.

(3005.0123.001)

The meteorological tower shall be designed so instrument booms will rotate less than 1 degree in a 50 m/sec (100 mi/hr) wind.

(3005.0123.002)

The meteorological instrument building shall be a Category III nonseismic building.

(3005.0123.003)

1.2.4 Environmental Requirements

Meteorological Monitoring shall be designed to operate over normal outdoor ambient environmental conditions of temperature, pressure, humidity, and radiation for the design life of the instruments.

(3005.0124.001)

1.2.5 Instrumentation and Control Requirements

Meteorological Monitoring shall be monitored and/or alarmed locally and in the control room to provide information on the subsystem status.

(3005.0125.001)

Computer inputs shall be provided to monitor critical parameters which are annunciated, with a hard copy of alarm messages, for documentation of abnormal parameter values and subsystem alarms.

(3005.0125.002)

1.2.6 Surveillance and In-Service Inspection Requirements

Meteorological Monitoring System and component design shall incorporate features necessary for status monitoring and in-service inspection while in service.

(3005.0126.001)

The status of Meteorological Monitoring components shall be monitored, and when in-service inspection activities require removal of equipment from service, design features shall be included to minimize out-of-service duration.

(3005.0126.002)

1.2.7 Availability Assurance Requirements

Meteorological Monitoring shall be designed for a joint recovery of no less than 90 percent of observations of wind speed, wind direction, and indication of atmospheric stability for each sensor elevation and for individual observations of the remaining parameters.

(3005.0127.001)

1.2.8 Maintenance Requirements

Meteorological Monitoring shall be designed and arranged, and components shall be located, to facilitate in-place or on-line maintenance to the greatest degree practicable.

(3005.0128.001)

Meteorological Monitoring components shall be provided with periodic maintenance consistent with the manufacturer's recommendations. In addition, adequate space and maintenance clearances are provided around these components to permit in-place maintenance and facilitate dismantling, removal, or replacement of equipment.

(3005.0128.002)

Meteorological Monitoring shall be provided with an ongoing quality assurance program designed to ensure the various monitoring sensors and electronic instruments remain within their specified limits.

(3005.0128.003)

Meteorological Monitoring spare parts management program shall ensure availability of critical spare parts necessary to facilitate maintenance and to minimize downtime.

(3005.0128.004)

1.2.9 Safety Requirements

Meteorological Monitoring shall be non-safety related.

(3005.0129.001)

1.2.10 Codes and Standards Requirements

Meteorological Monitoring shall be designed and constructed in accordance with the Regulatory Requirements of Regulatory Guidance Documents and Industry Codes and Standards that are listed in Tables 1-1 and 1-2, respectively. Deviations from these requirements may be proposed by the Project Office.

(3005.01210.001)

1.2.11 Quality Assurance Requirements

Items designated non-safety related 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 NEF2-10 regarding engineering holds, engineering drawing lists, design review, and management assessment which shall be implemented on activities that affect the quality of such items. QAL III items shall come under a quality assurance program which complies with selected basic requirements of NQA-1 and the four additional supplements from NEF2-10 identified above.

(3005.0211.001)

System-level documents are assigned the QAL classification that corresponds to the highest QAL of any item in the system. Therefore, this SSDD is classified as QAL III.

(3005.0211.002)

TABLE 1-1

REGULATORY GUIDANCE DOCUMENTS

A. Regulatory Guides (RG)

1.	RG 1.23	Meteorological Measurement Program for Nuclear Power Plants
2.	RG 1.33	Quality Assurance Program Requirements (Operational)
3.	RG 1.97	Instrumentation for Light-Water-Cooled Nuclear Power Plants to Access Plant and Environs Conditions During and Following an Accident

B. NUREG Reports

1.	NUREG 0654, Rev. 1 Appendix 2	Meteorological Criteria for Emergency Preparedness of Operating Nuclear Power Plants

TABLE 1-2

INDUSTRY CODES AND STANDARDS

A. American Concrete Institute (ACI)

1.	ACI 301	Specification for Structural Concrete for Buildings
2.	ACI 318	Building Code Requirements for Reinforced Concrete

B. American Hot Dip Galvanizers Associations (AHDGA) Zinc Institute Inc. (ZI)

1.	AHDGA/ZI Manual	Inspection Manual for Hot Dip Galvanized Products, EZ-2-10M

C. American National Standards Institute (ANSI)

1.	ANSI/ANS 2.5	Standard for Determining Meteorological Information at Nuclear Power Sites
2.	ANSI/AFBMA-9	Load Ratings and Fatigue Life for Ball Bearings
3.	ANSI/AFBMA-11	Load Ratings and Fatigue Life for Roller Bearings
4.	ANSI C37.90	Relays and Relay Systems Associated with Electric Power Apparatus
5.	ANSI N18.7/ANS-3.2	Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants

D. American Society for Testing and Materials (ASTM)

1.	ASTMA 123	Specification for Zinc (Hot-Galvanized) Coatings on Products Fabricated from Rolled, Pressed, and Forged Steel Shapes, Plates, Bars, and Strip
2.	ASTM A 153	Standard Specification for Zinc Coating (Hot Dip) on Iron and Steel Hardware
3.	ASTM A 262	Recommended Practices for Detecting Susceptibility to Intergranular Attack in Stainless Steels
4.	ASTM A 325	Specification for High Strength Bolts for Structural Steel Joints

TABLE 1-2 (continued)

5.	ASTM A 384	Recommended Practice for Safeguarding Against Warpage and Distortion During Hot Dip Galvanizing of Steel Assemblies
6.	ASTM A 615	Specification for Deformed and Plain Billet-Steel Bars for Concrete Reinforcement
7.	ASTM B 8	Specification for Concentric-Lay-Stranded Copper
8.	ASTM C 31	Making and Curing Concrete Compressive and Flexural Strength Test Specimens in the Field
9.	ASTM C 33	Specification for Concrete Aggregates
10.	ASTM C 138	Test for Unit Weight, Yield, and Air Content (Gravimetric) of Concrete
11.	ASTM C 143	Test for Slump of Portland Cement Concrete
12.	ASTM C 150	Standard Specification for Portland Cement
13.	ASTM C 231	Test for Air Content of Freshly Mixed Concrete by the Pressure Method
14.	ASTM C 260	Specification for Air Entraining Admixtures for Concrete
15.	ASTM D 635	Test for Rate of Burning and/or Extent and Time of Burning of Self-Supporting Plastics in a Horizontal Position

E. American Welding Society (AWS)

1.	AWS A5.1	Specification for Carbon Steel Covered Arc-Welding Electrodes
2.	AWS D1.1	Structural Welding Code - Steel

F. Electronic Industries Association (EIA)

1.	EIA-RS 222C	Structural Standards for Steel Antenna Tower and Antenna Supporting Structures

G. Federal Aviation Administration (FAA)

1.	FAA AC-70-7460-1G	Obstruction Marking and Lighting

H. Institute of Electrical and Electronics Engineers (IEEE)

1.	IEEE 112	Standard Test Procedure for Polyphase Inductor Motors and Generators

TABLE 1-2 (continued)

I. National Electrical Manufacturers Association (NEMA)

1.	NEMA ICS-6	Enclosures for Industrial Controls and Systems
2.	NEMA MG1	Motors and Generators

J. National Fire Protection Association (NFPA)

1.	NFPA 70	National Electric Code

K. Steel Structures Painting Council (SSPC)

1.	SSPC PA1	Paint Application Specification No. 1, Shop, Field, and Maintenance Painting*
2.	SSPC PA2	Paint Application Specification No. 2, Method for Measurement of Dry Paint Thickness with Magnetic Gages*
3.	SSPC PT2	Pretreatment Specification No. 2, Cold Phosphate Surface Treatment, Basic Zinc Chromate - Vinyl Butyral Washcoat*
4.	SSPC SP1	Surface Preparation Specification No. 1, Solvent Cleaning*

* Steel Structures Painting Manual Vol. 2, 2nd Edition, 1973

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

Meteorological Monitoring consists of a meteorological tower with an array of meteorological sensors, and an instrument building, housing data handling, recording, and communication equipment, as shown in Figure 2-1.

Meteorological Monitoring acquires data and provides data to the radiation monitoring system as required for making the following assessments:

1. A conservative assessment of the radiological consequences of airborne releases from design basis accidents to aid in the evaluation of the acceptability of the site and the adequacy of the engineered safety features.

2. A realistic assessment of the potential radiation dose to the public resulting from the routine releases of radioactive materials in airborne effluents, to assist in demonstrating that the operation of the plant is being conducted safely and the effluent control equipment meets its design objectives, and is being operated properly.

3. A realistic assessment of the potential radioactive consequences of an actual or projected accidental release of radioactive material to the atmosphere.

4. A realistic assessment of the potential dispersion of radioactive materials from, and the radiological consequences of, a spectrum of accidents to aid in evaluating the environmental risk posed by the nuclear power plant.

5. A realistic assessment of potential nonradioactive environmental effects such as fogging, icing, and salt drift from cooling towers, to aid in evaluating the environmental impact of the plant.

2.2 SUBSYSTEM CONFIGURATION

2.2.1 Meteorological Tower

The tower is a guyed triangular 60 m (197 ft) tower with instrument elevator. A grounding system ties together the tower, lightning rod, guy anchors, fence, instrument building, electronic equipment, power distribution system, and communication system.

2.2.2 Meteorological Instruments

The meteorological instruments arrays are mounted on the tower or located near the base of the tower, as shown in Table 2-1.

Redundant sets of temperature sensors measure both reference air temperature at 10 m (33 ft) and the difference in temperature (Δt) between the 60 m (197 ft) and 10 m (33 ft) tower elevations.

Parameters other than those listed in Table 2-1 may be measured to satisfy specific site circumstances.

2.2.3 Instrument Building

The instrument building is climate controlled, located no less than 10 building heights from the tower. It is provided with a security system and a fire protection system.

2.2.4 Data Handling and Processing Equipment

The data handling and processing equipment, which provides monitoring and recording of meteorological data, performs the following functions:

1. Recording instantaneous data on analog recorders
2. Computing and recording 15-minute and hourly averages of meteorological data and standard deviations on digital recorders
3. Providing daily, weekly, monthly, quarterly, and yearly inputs
4. Providing for calibration of system electronics and reporting results
5. Providing data to the data management subsystem for display in the control room
6. Providing data to the data management subsystem, as requested, during a design basis accident.
7. Providing data to PPIS for post accident monitoring
8. Monitoring the local instrumentation and annunciating status and system operation to the control room via the data management subsystem

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

Meteorological Monitoring is operational during all plant operating conditions, with a capability of measurements with a joint recovery of no less than 90 percent for an annual cycle of wind speed, wind direction, and indication of atmospheric stability for each sensor elevation, and for individual observations of the remaining parameters.

2.4 SUBSYSTEM ARRANGEMENT

Meteorological Monitoring is located at approximately the same elevation as finished plant grade in an area where natural or man-made obstructions to wind flow or the plant's heat dissipation system will have little or no effects on the meteorological measurements. Natural or man-made obstructions to air

movement are no higher than the measuring level and with a horizontal separation of 10 times the obstruction heights.

Instrumentation is located on booms oriented into the prevailing wind direction at a minimum distance of two tower widths from the tower. The aspirating temperature shields are pointed downward or laterally toward the north. The precipitation collector is located so that obstructions do not interfere with the collection of precipitation. The solar intensity instrument is located so that shadows from obstructions do not fall upon it.

2.5 INSTRUMENTATION AND CONTROL

2.5.1 Meteorological Instruments

The meteorological instrument type, range, and accuracy are shown in Table 2-2. Primary readout is on a digital recorder, with analog stripchart or multipoint recorder backup located in the instrument building. Analog recorder accuracy is ±0.25 percent. The data are also provided, stored,and reported to the data management subsystem for display in the main control room.

2.5.2 Local Instruments

Local instrumentation is shown in Table 2-3.

TABLE 2-1

METEOROLOGICAL MONITORING SENSORS

Parameter	Quantity	Location
Wind Speed	4	Two each at 10 and 60 meters (33 and 197 ft)
Wind Direction	4	Two each at 10 and 60 meters (33 and 197 ft)
Temperature	4	Two each at 10 and 60 meters (33 and 197 ft)
Dew Point	2	One each at 10 and 60 meters (33 and 197 ft)
Solar Radiation	1	10 meters (33 ft)
Precipitation	1	Ground Level

TABLE 2-2

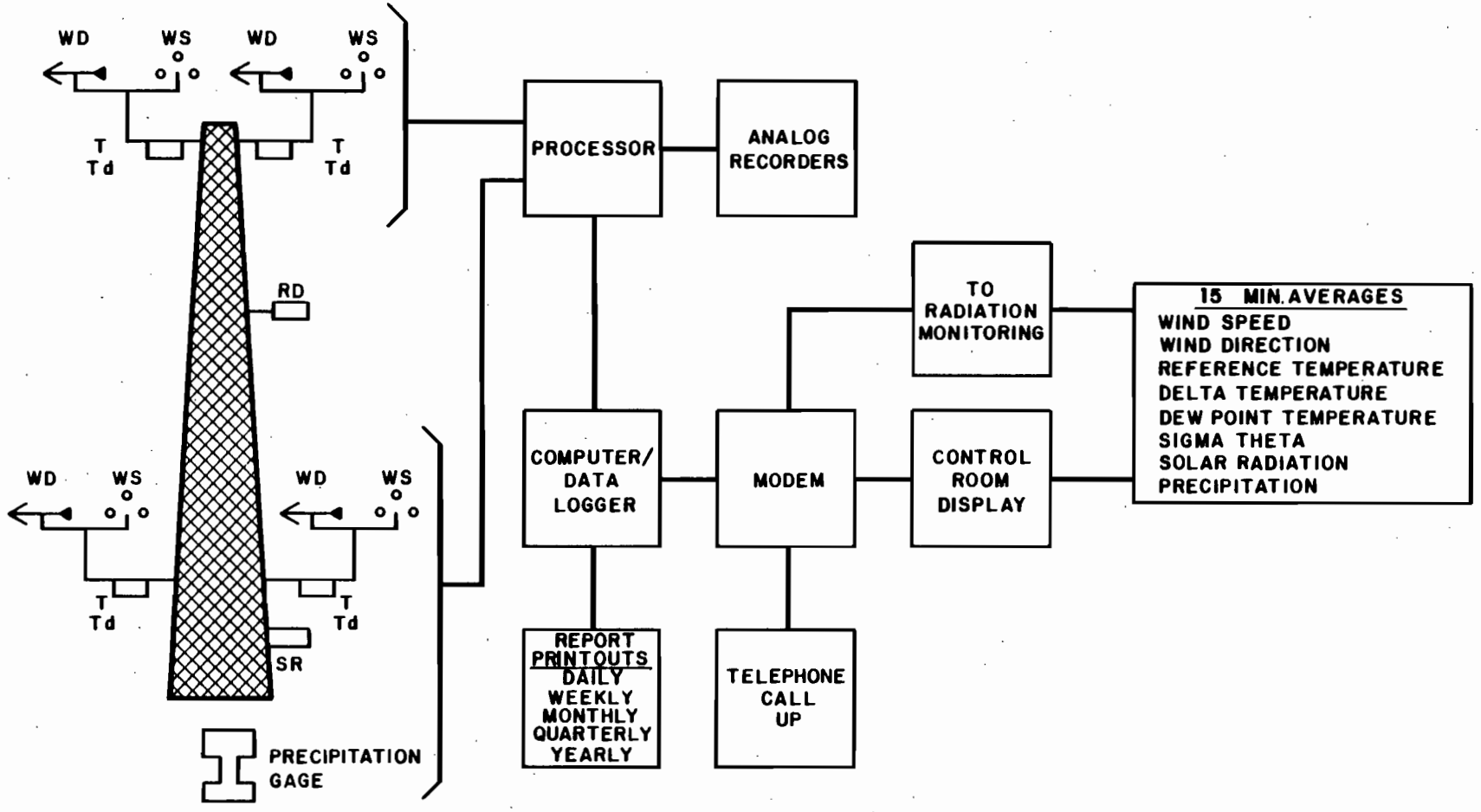
METEOROLOGICAL MONITORING INSTRUMENT ACCURACY

Parameter	Type	Range	Accuracy
Wind Speed	3-Cup Anemometer	0 to 50 m/s (100 mi/hr)	±0.22 m/s (0.5 mi/hr) up to 2.2 m/s (5.0 mi/hr); ±10% above 2.2 m/s (5.0 mi/hr)
Wind Direction	Counterbalanced Vane	0 to 540°	±5% of azimuth
Temperature	100 ohm at 0°C (32°F) Duplex Platinum RTD	-50°C to + 50°C (-58°F to +122°F)	±0.5°C (0.9°F)
Delta T	100 ohm at 0°C (32°F) Duplex Platinum RTD	-5°C to +5°C (-9°F to +9°F)	±0.15°C/50 m (0.27°F/ 164 ft)
Dew Point	Lithium Chloride	-50°C to +50°C (-58°F to +122°F)	±1.5°C (2.7°F), when relative humidity is higher than 60%, and temperature is between -30°C and +30°C (-22°F and +86°F)
Solar Radiation	Black and White Pyranometer	0 to 8.2 joules/ m^2 -min (2 langley/min)	±5% FS
Precipitation	Heated Tipping Bucket	Infinite, with a resolution of 0.25 mm (0.01 in)	±10% of catch in access of 5 mm (0.2 in)

TABLE 2-3

LOCAL INSTRUMENTS

Parameter	Type	Range	Accuracy	Location of Readout
Status of Aspirated Shields	Contact Closure	Flow/ No Flow	NA	Instrument Building
Instrument Building Temperature	RTD	0 to 50°C (32-122°F)	± 1%	Instrument Building
Others to be Determined				



LEGEND

WS - WIND SPEED SENSOR
WD - WIND DIRECTION SENSOR
T - TEMPERATURE SENSOR
Td - DEW POINT TEMPERATURE SENSOR
SR - SOLAR RADIATION SENSOR
RD - RADIATION DETECTOR

Figure 2-1
METEOROLOGICAL MONITORING SCHEMATIC

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACES REQUIREMENTS

4.1.1 Interface Requirements Imposed on Other Systems

Interface requirements, at the system level, are presented in Table 4-1 showing the interfacing systems on which the requirements are imposed, the nature of the interface, the interfacing component, and the interface requirements.

4.1.2 Interface Requirements Imposed on Subsystems Within the System

Interface requirements, at the subsystem level, are presented in Table 4-2 showing the interfacing subsystems within the Miscellaneous Control and Instrumentation Group on which the requirements are imposed, the nature of the interface, the interfacing component, and the interface requirements.

4.2 COMPONENT BOUNDARY DEFINITION

(TBD)

TABLE 4-1

INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
1. Reactor System (10)	No interface	NA	NA
2. Reactor Vessel System (11)	No interface	NA	NA
3. Reactor Services Group (20)	No interface	NA	NA
4. Heat Transport System (21)	No interface	NA	NA
5. Shutdown Cooling System (22)	No interface	NA	NA
6. Miscellaneous Control and Instrumentation System (30)	See Table 4-2 for interface requirements imposed on subsystems within the Miscellaneous Control and Instrumentation System.		
7. Plant Protection and Instrumentation System (32)	No interface	NA	NA
8. Fuel Handling, Storage and Shipping System (34)	No interface	NA	NA

TABLE 4-1 (continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
9. Plant Control, Data and Instrumentation System (37)			
(Plant Operational Support)	Operates and maintains meteorological monitoring	Meteorological Building	TBD
(Data Processing)	Processes and stores Meteorological Data System	Communication	TBD
10. Reactor Cavity Cooling System (48)	No interface	NA	NA
11. Power Conversion System (50)	No interface	NA	NA
12. Heat Rejection Group (52)	No interface	NA	NA
13. Building Structures and Building Services System (70)			
(Other Buildings)	Provides non-seismic Category III structure	Inside Meteorological Fence	TBD
(Meteorological Monitoring)			
14. Mechanical Services System (90)			
(Plant Fire Protection)	Provides fire protection	Meteorological Building	TBD
15. Electrical Group 1E (91)	No interface	NA	NA

TABLE 4-1 (continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
16. Electrical Group (92)			
(Non Class IE AC Distribution System)	Provides ac power	Meteorological Building Service Entrance	TBD
(Non Class IE Uninterruptible Power Sypply System)	Provides backup power	Meteorological Building Service Entrance	TBD
(Communication System)	Transmits data and status	Meteorological Building Service Entrance	TBD
(Plant Security)	Provides security	Meteorological Tower and Building	TBD
(Grounding, Lightning, Heat Tracing and Cathodic Protection)	Provides grounding and lightning protection	Meteorological Tower Fence, Instruments, and Building	TBD

TABLE 4-2

INTERFACE REQUIREMENTS IMPOSED ON
OTHER SUBSYSTEMS WITHIN THE SYSTEM

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Miscellaneous Control And Instrumentation Group (30)			
(NSSS Analytical Instruments)	No interface	NA	NA
(Radiation Monitoring)	See Radiation Monitoring SSDD, Section 4	See Radiation Monitoring SSDD, Section 4	No interface requirements are imposed on this subsystem. However, this subsystem imposes interface requirements on meteorological monitoring, as shown in the SSDD, Section 4.
(Seismic Monitoring)	No interface	NA	NA
(Fire Detection and Alarm)	Provides fire detection and alarm	Communication System	TBD
(Security Monitoring)	Provides security	Communication System	TBD

SECTION 9

REFERENCES

1. Gas-Cooled Reactor Associates (GCRA). Utility/User Design Requirements for Modular High Temperature Gas-Cooled Reactor Plant, GCRA 86-002, Rev. 1. GCRA, San Diego, CA, March 1986.

2. GA Technologies, Inc. (GA) et al. Overall Plant Design Specification Modular High Temperature Gas-Cooled Reactor, HTGR-86-004, Rev. 1. GA, San Diego, CA, February 1986.

3.. Stone & Webster Engineering Corporation (SWEC). Security Monitoring, HFD-43007, SWEC, Boston, MA, June 1986.

4. Quality Assurance Requirements, HP-20801, Rev. 1. September 1984.

DOE-HTGR-87-025

HTGR

FIRE DETECTION AND ALARM SUBSYSTEM DESIGN DESCRIPTION

[redacted]

[redacted]

AUTHOR / CONTRACTOR

STONE & WEBSTER ENGINEERING CORP.

ISSUED BY STONE & WEBSTER ENGINEERING CORP.
UNDER SUBCONTRACT TO GAS-COOLED REACTOR ASSOCIATES
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

JUNE 1986

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HFD-43006

FIRE DETECTION AND ALARM SUBSYSTEM DESIGN DESCRIPTION

4 x 350 MW(t) MODULAR HTGR PLANT

[redacted]

[redacted] to Third Parties Representing Foreign [redacted] the Director, HTGR Development Division, U.S. [redacted]

Author/Contractor

Stone & Webster Engineering Corporation

Issued By:
Stone & Webster Engineering Corporation
Under Subcontract to Gas-Cooled Reactor Associates
For the Department of Energy
Contract DE-AC03-78SF02034

June 1986

CONTENTS

	Page
LIST OF EFFECTIVE PAGES	iv
LIST OF ACRONYMS	v
DEFINITIONS	vi
LIST OF ILLUSTRATIONS	vii
LIST OF TABLES	viii
LIST OF APPENDICES. (TBD)	-
PREFACE	ix
SUMMARY	x
1 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-1
1.2.3 Structural Requirements	1-1
1.2.4 Environmental Requirements	1-1
1.2.5 Instrumentation and Control Requirements	1-2
1.2.6 Surveillance and In-Service Inspection Requirements	1-2
1.2.7 Availability Assurance Requirements	1-2
1.2.8 Maintenance Requirements	1-2
1.2.9 Safety Requirements	1-2
1.2.10 Codes and Standards Requirements	1-2
1.2.11 Quality Assurance Requirements	1-3
1.2.12 Construction Requirements	1-3
1.2.13 Decommissioning Requirements (TBD)	1-3
2 DESIGN DESCRIPTION	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-1
2.3 Subsystem Performance Characteristics	2-1
2.3.1 Subsystem Operating Modes	2-1
2.3.2 Subsystem Steady-State Performance	2-1
2.3.3 Subsystem Response to Plant Transients	2-1
2.3.4 Subsystem Failure Modes and Effects	2-2
2.4 Subsystem Arrangement	2-2
2.5 Instrumentation and Control	2-2

CONTENTS (continued)

Page

3 COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS (TBD) . . . . . -

3.1 Component Functions (TBD) . . . . . -
3.1.1 Central Processing Unit Component Functions (TBD) . -
3.1.2 Multiplexer Component Functions (TBD) . . . . . -
3.1.3 Detector Component Functions (TBD) . . . . . -
3.1.4 Annunciator Component Functions (TBD) . . . . . -

3.2 Component Design Requirements (TBD) . . . . . -
3.2.1 Central Processing Unit Component Design Requirements (TBD) . . . . . -
3.2.2 Mutiplexer Component Design Requirements (TBD) . . . -
3.2.3 Detector Component Design Requirements (TBD) . . . . -
3.2.4 Annunciator Component Design Requirements (TBD) . . -

4 SUBSYSTEM INTERFACES 4-1

4.1 Subsystem Interface Requirements 4-1

4.1.1 Interface Requirements Imposed on Other Systems . . 4-1
4.1.2 Interface Requirements Imposed on Subsystems Within the System 4-1

4.2 Component Boundary Definition (TBD) 4-1

5 SUBSYSTEM CONSTRUCTION (TBD) . . . . . -

5.1 Packaging and Shipping (TBD) . . . . . -
5.2 Handling at Delivery (TBD) . . . . . -
5.3 Receiving Inspection (TBD) . . . . . -
5.4 Storage (TBD) . . . . . -
5.5 Access to Building (TBD) . . . . . -
5.6 Installation and/or Field Fabrication (TBD) . . . . . -
5.7 Construction Testing (TBD) . . . . . -
5.8 As-Built Drawings (TBD) . . . . . -

6 SUBSYSTEM OPERATION (TBD) . . . . . -

6.1 Subsystem Limitations, Set Points, and Precautions (TBD) . . . . . -

6.1.1 Subsystem Limitations and Set Points (TBD) . . . . . -
6.1.2 Precautions (TBD) . . . . . -

CONTENTS (continued)

Page

6.2 Preoperational Checkout (TBD) . . . . . -
6.3 Startup/Shutdown (TBD) . . . . . -

6.3.1 Startup to 25 percent Steam Flow. . . . . -
6.3.2 Startup from 25 percent Steam Flow. . . . . -

6.4 Normal Operation (TBD) . . . . . -
6.5 Refueling (TBD). . . . . -
6.6 Shutdown (TBD) . . . . . -
6.7 Abnormal Operation (TBD) . . . . . -
6.8 Casualty Events and Recovery Procedures (TBD). . . . . -

6.8.1 Casualty Events (TBD) . . . . . -
6.8.2 Design Features to Mitigate Effects of Casualty Events (TBD). . . . . -
6.8.3 Recovery Procedures (TBD) . . . . . -

7 SUBSYSTEM MAINTENANCE (TBD). . . . . -

7.1 Maintenance Approach (TBD) . . . . . -
7.2 Corrective Maintenance (TBD) . . . . . -
7.3 Preventive Maintenance (TBD) . . . . . -
7.4 In-Service Inspection (TBD) . . . . . -
7.5 Surveillance (TBD) . . . . . -

8 SUBSYSTEM DECOMMISSIONING (TBD). . . . . -

9 REFERENCES 9-1

LIST OF EFFECTIVE PAGES

Page(s)	Rev	Date
Title page	0	6/86
i through x	0	6/86
1-1 through 1-6	0	6/86
2-1 through 2-4	0	6/86
4-1 through 4-4	0	6/86
9-1	0	6/86

LIST OF ACRONYMS

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CDS	Component Design Specifications
CPU	Central Processing Unit
DOE	Department of Energy
ICD	Interface Control Documents
IEEE	Institute of Electrical and Electronics Engineers
NFPA	National Fire Protection Association
NSSS	Nuclear Steam Supply System
OPDS	Overall Plant Design Specification
SDD	System Design Description
SSDD	Subsystem Design Description
UL	Underwriters Laboratories

LIST OF DEFINITIONS

Alarm	A signal for attracting attention to some abnormal condition
Annunciator	A visual signal device consisting of a number of pilot lights or drops, each one indicating the condition that exists or had existed in an associated circuit, and is labeled accordingly.
Ionization smoke detector	A device which has a small amount of radioactive material which ionizes the air in the sensing chamber, thus rendering it conductive and permitting a current flow through the air between two charged electrodes.
Multiplex	To interleave or simultaneously transmit two or more messages on a single channel.
Photoelectric smoke detector	A photoelectric relay and light source arranged to detect the presence of more than a predetermined amount of smoke in the air.
Thermal (heat) detector	A device which detects abnormally high temperature or rate of temperature rise to initiate a fire alarm.
Ultraviolet flame detector	A device whose sensing element is responsive to radiant energy outside of the range of human vision (below approximately 4000 angstroms).

LIST OF ILLUSTRATIONS

TITLE	PAGE
2-1 Fire Detection and Alarm Subsystem Schematic.	2-4

LIST OF TABLES

	TITLE	PAGE
1-1	Environmental Conditions	1-4
1-2	Regulatory Requirements	1-5
1-3	Industry Codes and Standards	1-6
2-1	Fire Detectors	2-3
4-1	Interface Requirements Imposed on Other Systems	4-2
4-2	Interface Requirements Imposed on Subsystems Within the System	4-4

PREFACE

The objectives of the HTGR plant project are to produce safe, economical power. Supporting these objectives are four major goals and their associated plant states, 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 Overall Plant Design Specification (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, interface, operational, safety, maintenance, inspection and decommissioning requirements for design of the plant.

In response to the OPDS, a series of low tier documents, System Design Descriptions (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSSDs), Component Design Specifications (CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability from plant-level requirements to equipment-level requirements is maintained throughout this hierarchy of design documents.

SUMMARY

Fire Detection and Alarm is an early warning system used to detect and report the presence of a fire within the plant. It detects, annunciates, and records plant-wide fire alarms, subsystem trouble, and fire console operator actions.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SUBSYSTEM FUNCTIONS

The function of Fire Detection and Alarm is to detect and annunciate the presence and location of combustion by-products or presence of fire within the plant. However, the Fire Detection and Alarm provides annunciation only, and does not initiate any fire suppression systems. Fire suppression is provided by the Plant Fire Protection System (SSDD HFD-49004).

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Fire Detection and Alarm shall be a stand-alone system designed for independent and reliable operation. This subsystem shall be configured such that no single event or failure to any component or cable will degrade the operation of the subsystem.

(3006.0121.001)

1.2.2 Operational Requirements

Fire Detection and Alarm shall operate on a continuous basis through all plant modes. This subsystem shall be self-monitoring, reporting any subsystem failures as well as the presence of fire or combustion by-products.

(3006.0122.001)

Fire Detection and Alarm equipment shall be designed to reject radio interference from hand-held, two-way communications equipment.

(3006.0122.002)

Fire Detection and Alarm equipment shall not malfunction in the environment of the power station and shall be capable of passing all specified tests.

(3006.0122.002)

1.2.3 Structural Requirements

Fire Detection and Alarm shall be located in both non-seismic Category I and Seismic Category I structures, and shall be seismically supported within Seismic Category I structures.

(3006.0123.001)

1.2.4 Environmental Requirements

Fire Detection and Alarm equipment shall be capable of operating within the normal and abnormal environmental conditions of temperature, pressure, humidity, and radiation for the design life of the equipment, as indicated in Table 1-1.

(3006.0124.001)

1.2.5 Instrumentation and Control Requirements

Fire Detection and Alarm shall provide annunciation (audible or visual) throughout the plant when a fire is detected.

(3006.0125.001)

Visual alert shall be provided outside the fire zone that is in an alarm state.
(3006.0125.002)

All subsystem alarms and abnormal indications are annunciated in the control room and a hard copy record is made.

(3006.0125.003)

1.2.6 Surveillance and In-Service Inspection Requirements

The design of Fire Detection and Alarm shall incorporate, to the greatest degree practicable, those features necessary for status monitoring and implementing in-service inspection functions with the plant in operation.
(3006.0126.001)

The status of all major system components shall be monitored and displayed, and when in-service inspection activities require removal of equipment from service, design features shall be included to minimize the out-of-service time.
(3006.0126.002)

1.2.7 Availability Assurance Requirements

Fire Detection and Alarm shall not be necessary for electrical generation.
(3006.0127.001)

1.2.8 Maintenance Requirements

Fire Detection and Alarm shall be designed to facilitate in-place or on-line maintenance to the greatest degree practicable.

(3006.0128.001)

Fire Detection and Alarm components shall be provided with periodic maintenance consistent with the manufacturer's recommendations. In addition, adequate floor space and maintenance clearances shall be provided around these components to permit in-place maintenance and facilitate dismantling, removal, or replacement of equipment.

(3006.0128.002)

1.2.9 Safety Regulations

Fire Detection and Alarm shall be non-safety related for component design and Non-Seismic Category I for equipment support in non-Class 1E areas, and Seismic Category I for equipment support in Class 1E areas.

(3006.0129.001)

1.2.10 Codes and Standards Requirements

Fire Detection and Alarm shall be designed and constructed in accordance with the regulatory requirements and the industry codes and standards that are

listed in Tables 1-2 and 1-3. Deviations from these requirements may be proposed for review and approval by the Project Office.

(3006.01210.001)

1.2.11 Quality Assurance Requirements

Items designated nonsafety-related 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 NEF2-10, regarding engineering holds, engineering drawing lists, design review, and management assessment which shall be implemented on activities that affect the quality of such items. 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.

(3006.01211.001)

Subsystem-level documents are assigned the QAL classification that corresponds to the highest QAL of any item in the subsystem. Therefore, this SSDD shall be classified as QAL III.

(3006.01211.002)

1.2.12 Construction Requirements

Fire Detection and Alarm arrangement features shall facilitate the installation, removal, and reinstallation of equipment.

(3006.01212.001)

Fire Detection and Alarm design shall utilize shop, factory, or field fabrication, assembly, or erection as appropriate to minimize erection costs and maintain quality control.

(3006.01212.002)

The design of Fire Detection and Alarm components shall incorporate materials and processes, as required, to meet all packaging, shipping, receiving, storage, handling, construction, and operational functions. Level B and Housekeeping Zone IV is provided from shop fabrication through plant startup.

(3006.01212.003)

1.2.13 Decommissioning Requirements

(TBD)

TABLE 1-1

ENVIRONMENTAL CONDITIONS

A. Normal Environment

Temperature, °C(°F)	15.6-40(60-104)
Pressure, psia	Atmospheric
Humidity, percent	20 - 80
Radiation, rad*	(TBD)
Aging, days/yr	(TBD)
Operating cycles	(TBD)

B. Abnormal Environment

Temperature, °C(°F)	48.9(120)
Humidity, percent	10 - 90
Aging, days/yr	(TBD)

NOTES:

* 40 yr total integrated dose (TID)

TABLE 1-2

REGULATORY REQUIREMENTS

Code of Federal Register	
10CFR50, Appendix R	Licensing of Production and Utilization Facilities, Fire Protection Program

TABLE 1-3

INDUSTRY CODES AND STANDARDS

National Fire Protection Association

1.	NFPA No. 72D	Proprietary Protective Signaling Systems
2.	NFPA No. 72E	Automatic Fire Detectors

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

Fire Detection and Alarm is designed for reliable error-free operation achieved through a redundant design and is designed to the requirements of Subsection 1.2. It provides an alarm response when activated by a fire detector, a failure in the detector's power circuit, or any malfunction which affects the detector's ability to perform properly.

Redundancy is provided by the use of independent transmission cables between remote zone panels and a central processing unit (CPU) located in the Operations Center.

2.2 SUBSYSTEM CONFIGURATION

Fire Detection and Alarm consists of a CPU and remote interface zone panels. A multiplex system is used for communication between the CPU and the remote zone panels, as indicated in Figure 2-1. The remote zone panels receive inputs from various detectors and fire pull stations located in specific fire zone areas throughout the plant.

Various detectors, such as ionization smoke, photoelectric smoke, thermal (heat), and ultraviolet flame type sense the presence of combustion by-products or the presence of fire, and relay a change of state condition to the remote zone panel. Upon receipt of a fire signal from a detector, the zone panel sends a signal to the CPU via the multiplex system. The CPU annunciates the affected fire zone and relates it to the physical location within the plant.

Alarms are provided to alert personnel within the plant to the presence of fire. These alarms are both audible and visual.

Fire pull stations are also located within each fire zone for annual reporting of a fire.

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

Fire Detection and Alarm is operational during all plant operating conditions. In case of loss of ac power, backup generators provide the required power.

2.3.1 Subsystem Operating Modes

Not applicable

2.3.2 Subsystem Steady-State Performance

Not applicable

2.3.3 Subsystem Response to Plant Transients

Not applicable

2.3.4 Subsystem Failure Modes and Effects

The worst case subsystem failure mode is the failure of a fire detection and alarm multiplixer. The effect of this failure would be the inability to monitor fire in the zone that the failed multiplexer services.

2.4 SUBSYSTEM ARRANGEMENT

Fire Detection and Alarm is distributed throughout the plant and arranged so as not to interfere with, nor be interfered by, other systems. Detectors are located according to NFPA 72E. The cabling minimizes the effect of single failures to the balance of the system by providing Class A wiring, as defined in NFPA 72D.

2.5 INSTRUMENTATION AND CONTROL

Fire Detection and Alarm instrumentation and control consists of detectors and annunciators.

Two types of ionization smoke detectors are used to detect products of combustion. In open areas, low voltage detectors with dual ionization chambers capable of detecting products of combustion are used. Standard ionization smoke detectors are used in air ducts.

Photoelectric smoke detectors are also used to detect the products of combustion entering a labyrinth chamber and are set to operate at a density of approximately 1.5 percent per foot.

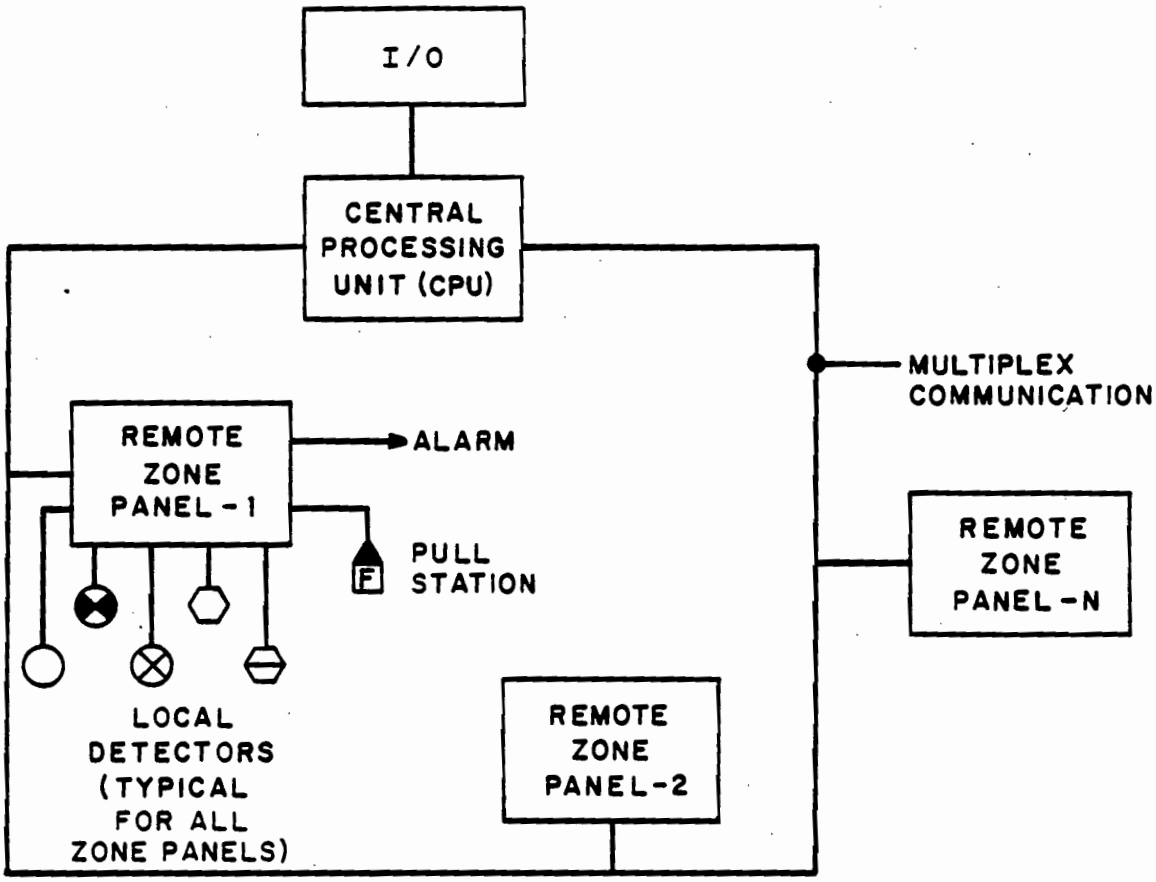
Thermal (heat) detectors are either rate-compensated electric thermostats or fixed thermostats which measure surrounding air temperature and are set to operate at 140°F.

Annunciation is provided at the CPU console and remotely at the remote zone panels. The alarm at the CPU is locked-in until acknowledged by the operator at the console. In addition to providing an audible signal at the CPU, the location and type of device activating the alarm is automatically recorded via an alarm printer. Report alarms in the fire zone are horns, bells, or lights.

TABLE 2-1

FIRE-DETECTORS

Detector Type	Quantity	Location
Ionization	(TBD)	Reactor Building Reactor Service Building Reactor Auxiliary Building Turbine Building Operations Center Makeup Water Treatment and Auxiliary Boiler Building Radioactive Waste Management Building Meteorological Building
Thermal	(TBD)	Reactor Building Reactor Service Building Reactor Auxiliary Building Helium Storage Building Personnel Services Building Turbine Building Transformer Areas Makeup Water Treatment and Auxiliary Boiler Building Operations Center Hydrogen Storage Area Maintenance Building ECA Warehouse Fire Pumphouse Radioactive Waste Management Building Standby Power Building Fuel Oil Storage Tanks
Ultraviolet	(TBD)	Turbine Building Fire Pumphouse Standby Power Building Fuel Oil Storage Tanks
Photoelectric	(TBD)	Reactor Building Reactor Service Building Reactor Auxiliary Building Radioactive Waste Management Building



LEGEND

- SMOKE - PHOTOELECTRIC
- SMOKE - IONIZATION
- HEAT - RATE OF RISE (THERMAL)
- HEAT - FIXED (THERMAL)
- FLAME - ULTRAVIOLET

Figure 2-1
FIRE DETECTION AND ALARM
SUBSYSTEM SCHEMATIC

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

4.1.1 Interface Requirements Imposed on Other Systems

Interface requirements at the system level are presented in Table 4-1 showing the interfacing systems with subsystem identification on which the requirements are imposed, the nature of interface, the interfacing components, and the interface requirements.

4.1.2 Interface Requirements Imposed on Subsystems Within the System

Interface requirements at the subsystem level are presented in Table 4-2 showing the interfacing subsystems within the Miscellaneous Control and Instrumentation Group on which the requirements are imposed, the nature of interface, the interfacing component, and the interface requirements.

4.2 COMPONENT BOUNDARY DEFINITIONS

(TBD)

TABLE 4-1

INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
1. Reactor System (10)	No interface	NA	NA
2. Vessel System (11)	No interface	NA	NA
3. Reactor Services Group (20)	No interface	NA	NA
4. Heat Transport System (21)	No interface	NA	NA
5. Miscellaneous Control and Instrumentation Group (30)	See Table 4-2 for interface requirements imposed on subsystems within the Miscellaneous Control and Instrumentation group.		
6. Plant Protection and Instrumentation System (32)	No interface	NA	NA
7. Fuel Handling, Storage and Shipping System (34)	No interface	NA	NA
8. Plant Control, Data and Instrumentation System (37)	No interface	NA	NA

TABLE 4-1 (continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
9. Power Conversion Group (50)	No interface	NA	NA
10. Heat Rejection Group (52)	No interface	NA	NA
11. Reactor Cavity Cooling System (56)	No interface	NA	NA
12. Shutdown Cooling System (57)	No interface	NA	NA
13. Building Structures and Building Service Group (70)	See Table 2-1 for interface requirements on Building Services.		
14. Mechanical Services System (90)	No interface	NA	NA
15. Electrical Group (92)			
(Non Class IE UPS)	Provides Power to the Fire Detection and Alarm System	UPS bus	120 V, 60 Hz 1 phase UPS
(Grounding, Lightning, Heat Tracing, and Cathodic Protection)	Provides grounding for equipment	Equipment enclosure	TBD

TABLE 4-2

INTERFACE REQUIREMENTS IMPOSED ON
OTHER SUBSYSTEMS WITHIN THE SYSTEM

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Miscellaneous Control And Instrumentation Group (30)			
(NSSS Analytical Instruments)	No interface	NA	NA
(Radiation Monitoring)	No interface	NA	
(Seismic Monitoring)	No interface	NA	NA
(Meteorological Monitoring)	Provides detection	Meteorological Building	TBD
(Security Monitoring)	No interface	NA	TBD

SECTION 9

REFERENCES

1. Gas-Cooled Reactor Associates (GCRA). Utility/User Design Requirements for Modular High Temperature Gas-Cooled Reactor Plant, GCRA-86-002, Rev. 1. GCRA, San Diego, CA, March 1986.

2. GA Technologies, Inc. (GA) et al. Overall Plant Design Specification Modular Hig Temperature Gas-Cooled Reactor, HTGR-86-004, Rev. 1. GA, San Diego, CA, February 1986.

3. GA Technologies, Inc. (GA). NSSS/BOP Interface Requirements for the 4 x 350 MW(t) Modular HTGR Plant, HTGR-86-007, GA, San Diego, CA, April 1986

4. Bechtel National, Inc. (BNI). BNI Input to SWEC on Mechanical Services Group, Letter, GCRA/BEC/81-202, BNI, San Francisco, CA, February 1986.

5. Quality Assurance Requirements, HCP-20801, Rev.1. September 1984.

DOE-HTGR-87-026

HTGR

SECURITY MONITORING SUBSYSTEM DESIGN DESCRIPTION

[redacted]

[redacted] or [redacted] in to third parties representing foreign interests, foreign governments, foreign companies and foreign subsidiaries or foreign divisions of U.S. companies should be coordinated with the Director, HTGR Development Division, U.S. Department of Energy.

AUTHOR / CONTRACTOR

STONE & WEBSTER ENGINEERING CORP.

ISSUED BY STONE & WEBSTER ENGINEERING CORP.
UNDER SUBCONTRACT TO GAS-COOLED REACTOR ASSOCIATES
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-78SF02034

JUNE 1986

DISCLAIMER

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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, mark, 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.

HFD-43007

SECURITY MONITORING SUBSYSTEM DESIGN DESCRIPTION

4 x 350 MW(t) MODULAR HTGR PLANT

[redacted]

Any Further Distribution by any Holder of this Document or of O[redacted]n Interest, Foreign Governments, Foreign Companies and Foreign Subsi[redacted] Be [redacted] Development Division, U.S. [redacted]

Author/Contractor

Stone & Webster Engineering Corporation

Issued By:
Stone & Webster Engineering Corporation
Under Subcontract to Gas-Cooled Reactor Associates
For the Department of Energy
Contract DE-AC03-78SF02034

June 1986

CONTENTS

	Page
LIST OF EFFECTIVE PAGES	iv
LIST OF ACRONYMS	v
LIST OF DEFINITIONS	vi
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES	ix
LIST OF APPENDICES (TBD)	-
PREFACE	x
SUMMARY	xi
1 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS	1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	1-1
1.2.2 Operational Requirements	1-1
1.2.3 Structural Requirements	1-1
1.2.4 Environmental Requirements	1-1
1.2.5 Instrumentation and Control Requirements	1-2
1.2.6 Surveillance and In-Service Inspection Requirements	1-2
1.2.7 Availability Assurance Requirements	1-2
1.2.8 Maintenance Requirements	1-2
1.2.9 Safety Requirements	1-2
1.2.10 Codes and Standards Requirements	1-3
1.2.11 Quality Assurance Requirements	1-3
1.2.12 Construction Requirements	1-3
1.2.13 Decommissioning Requirements (TBD)	1-3
2 DESIGN DESCRIPTION	2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-1
2.3 Subsystem Performance Characteristics	2-4
2.3.1 Subsystem Operating Modes	2-4
2.3.2 Subsystem Steady-State Performance	2-5
2.3.3 Subsystem Response to Plant Transients	2-5
2.3.4 Subsystem Failure Modes and Effects	2-5
2.4 Subsystem Arrangement	2-5
2.5 Instrumentation and Control	2-5

CONTENTS (continued)

Page

3 COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS (TBD) . . . . . -

3.1 Component Functions (TBD) . . . . . -

3.1.1 Central Processing Unit Component Functions (TBD) . -
3.1.2 Multiplexers Component Functions (TBD) . . . . . -
3.1.3 Field Devices Component Functions (TBD) . . . . . -
3.1.4 Alarm Station Console Component Functions (TBD) . . -

3.2 Component Design Requirements (TBD) . . . . . -

3.2.1 Central Processing Unit Component Design Requirements (TBD) . . . . . -
3.2.2 Multiplexers Component Design Requirements (TBD) . . -
3.2.3 Field Devices Component Design Requirements (TBD) . -
3.2.4 Alarm Station Console Component Design Requirements (TBD) . . . . . -

4 SUBSYSTEM INTERFACES 4-1

4.1 Subsystem Interface Requirements 4-1

4.1.1 Interface Requirements Imposed on Other Systems . . 4-1
4.1.2 Interface Requirements Imposed on Subsystems Within the System 4-1

4.2 Component Boundary Definition (TBD) 4-1

5 SUBSYSTEM CONSTRUCTION (TBD) . . . . . -

5.1 Packaging and Shipping (TBD) . . . . . -
5.2 Handling at Delivery (TBD) . . . . . -
5.3 Receiving Inspection (TBD) . . . . . -
5.4 Storage (TBD) . . . . . -
5.5 Access to Buildings (TBD) . . . . . -
5.6 Installation and/or Field Fabrication (TBD) . . . . . -
5.7 Construction Testing (TBD) . . . . . -
5.8 As-Built Drawings (TBD) . . . . . -

6 SUBSYSTEM OPERATION (TBD) . . . . . -

6.1 Subsystem Limitations, Set Points, and Precautions (TBD) . . . . . -

6.1.1 Subsystem Limitations and Set Points (TBD) . . . . . -
6.1.2 Precautions (TBD) . . . . . -

CONTENTS (continued)

Page

6.2 Preoperational Checkout (TBD) . . . . . -
6.3 Startup/Shutdown (TBD) . . . . . -

6.3.1 Startup to 25 percent Steam Flow. . . . . -
6.3.2 Startup from 25 percent Steam Flow. . . . . -

6.4 Normal Operation (TBD) . . . . . -
6.5 Refueling (TBD). . . . . -
6.6 Shutdown (TBD) . . . . . -
6.7 Abnormal Operation (TBD) . . . . . -
6.8 Casualty Events and Recovery Procedures (TBD). . . . . -

6.8.1 Casualty Events (TBD) . . . . . -
6.8.2 Design Features to Mitigate Effects of Casualty Events (TBD). . . . . -
6.8.3 Recovery Procedures (TBD) . . . . . -

7 SUBSYSTEM MAINTENANCE (TBD). . . . . -

7.1 Maintenance Approach (TBD) . . . . . -
7.2 Corrective Maintenance (TBD) . . . . . -
7.3 Preventive Maintenance (TBD) . . . . . -
7.4 In-Service Inspection (TBD) . . . . . -
7.5 Surveillance (TBD) . . . . . -

8 SUBSYSTEM DECOMMISSIONING (TBD). . . . . -

9 REFERENCES 9-1

LIST OF EFFECTIVE PAGES

Page(s)	Rev	Date
Title page	0	6/86
i through xi	0	6/86
1-1 through 1-6	0	6/86
2-1 through 2-10	0	6/86
4-1 through 4-4	0	6/86
9-1	0	6/86

LIST OF ACRONYMS

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BSDD	Buildings and Structures Design Description
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CDS	Component Design Specification
CPU	Central Processing Station
DOE	Department of Energy
GHA	Guardhouse Access Detection
IEEE	Institute of Electrical and Electronics Engineers
MUX	Multiplexer
NFPA	National Fire Protection Association
NSSS	Nuclear Steam Supply System
OPDS	Overall Plant Design Specification
PDS	Perimeter Detection System
SAS	Secondary Alarm Station
SDD	System Design Description
SNM	Special Nuclear Material
SSDD	Subsystem Design Description
TID	Total Integrated Dose
TS	Tamper Switch
VMA	Vital and Material Areas

LIST OF DEFINITIONS

Authorized Individual	Any individual who has been designated in writing to have responsibility for surveillance of, or control over, special nuclear material or to have unescorted access to areas where special nuclear material is used or stored.
Alarm Response Force	Local law enforcement officers that provide the primary response for the protected facility and serve as the secondary response for those facilities using proprietary or commercial guards.
Controlled Access Area	Any temporarily or permanently established area which is clearly demarcated and access to this area is controlled, and which affords isolation of the material or persons within it.
Guard	A uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft, the protection of a plant against radiological sabotage, or both.
Intrusion Alarm	A tamper indicating electrical, electromechanical, electro-optical, electronic, or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and will alert guards or watchmen by means of actuated visible and audible signals.
Isolation Zone	Any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.
Material Access Area	Any location which contains special nuclear material within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.
Physical Barrier	Fence constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire, or similar material, on brackets angled outward between 30 degrees and 45 degrees from the vertical, with an overall height of not less than 8 ft, including the barbed topping;

Physical Barrier (cont)	Building walls, ceilings, and floors constructed of stone, brick, cinder block, concrete, steel, or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described above, with a height of not less than 8 ft; or Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.
Protected Area	An area encompassed by physical barriers and to which access to Nuclear Island is controlled.
Vital Area	Any area which contains vital equipment.
Vital Equipment	Any equipment, system, device, or material; the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.
Security Force	A group of individuals or agencies equipped and trained to respond to security threats.

LIST OF ILLUSTRATIONS

TITLE	PAGE
2-1 Multiplexed Computer Based Security System.	2-9
2-2 CCTV Secondary Alarm Station (SAS).	2-10

LIST OF TABLES

	TITLE	PAGE
1-1	Environmental Conditions	1-4
1-2	Regulatory Requirements	1-5
1-3	Industry Codes and Standards	1-6
2-1	Security Monitoring Sensors	2-7
2-2	Plant/Subsystem Operating Relationships	2-8
4-1	Interface Requirements Imposed on Other Systems	4-2
4-2	Interface Requirements Imposed on Subsystems Within the System	4-4

PREFACE

The objectives of the HTGR plant project are to produce safe, economical power. Supporting these objectives are four major goals and their associated plant states, 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 Overall Plant Design Specification (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, interface, operational, safety, maintenance, inspection, and decommissioning requirements for design of the plant.

In response to the OPDS, a series of low tier documents, System Design Descriptions (SDDs), Subsystem Design Descriptions (SSDDs), Buildings and Structures Design Descriptions (BSDDs), Component Design Specifications (CDSs), and Interface Control Documents (ICDs), describe and control the individual designs. Traceability from plant-level requirements to equipment-level requirements is maintained throughout this hierarchy of design documents.

SUMMARY

Security Monitoring acquires and processes sensor data for use by security personnel in the performance of their function. Security Monitoring is designed and implemented as a part of an overall security plan which is classified as Safeguards Information under 10CFR73.21.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SUBSYSTEM FUNCTIONS

The function of Security Monitoring is to detect and assess through sensory, video, and alarm equipment unauthorized entry and tampering within the plant protected area to secure the plant and ensure public safety for all states of plant operation to maintain safety energy production, shutdown, refueling, and startup/shutdown.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Security Monitoring shall be a stand-alone system designed for independent and reliable operation. This subsystem shall be configured such that no single event or failure to any component or cable will degrade the operation of the subsystem.

(3007.0121.001)

1.2.2 Operational Requirements

Security Monitoring shall operate on a continuous basis through all plant modes. This subsystem shall be self-monitoring, reporting any subsystem failures as well as the presence of security breaches.

(3007.0122.001)

Security Monitoring equipment shall be designed to reject radio interference from hand-held, two-way communications equipment.

(3007.0122.002)

Security Monitoring equipment shall not malfunction in the environment of the power station and shall be capable of passing all specified tests.

(3007.0122.003)

1.2.3 Structural Requirements

Security Monitoring shall be located in both Non-Seismic Category I and Seismic Category I structures, and shall be seismically supported within Seismic Category I structures.

(3007.0123.001)

1.2.4 Environmental Requirements

Security Monitoring equipment shall be capable of operating within the normal and abnormal environmental conditions of temperature, pressure, humidity, and radiation for the design life of the equipment, as indicated in Table 1-1.

(3007.0124.001)

1.2.5 Instrumentation and Control Requirements

Security Monitoring shall provide annunciation (audible or visual) to the alarm stations.

(3007.0125.001)

All subsystem alarms and abnormal indications shall be annunciated at the alarm stations and a hard copy record made.

(3007.0125.002)

1.2.6 Surveillance and In-Service Inspection Requirements

The design of Security Monitoring and its components shall incorporate, to the greatest degree practicable, those features necessary for status monitoring and implementing in-service inspection functions with the plant in operation.

(3007.0126.001)

The status of all major Security Monitoring components shall be monitored, and when in-service inspection activities require removal of equipment from service, design features shall be included to minimize the out-of-service time.

(3007.0126.002)

1.2.7 Availability Assurance Requirements

Security Monitoring shall not be necessary for electrical generation.

(3007.0127.001)

1.2.8 Maintenance Requirements

Security Monitoring shall be designed to facilitate in-place or on-line maintenance to the greatest degree practicable.

(3007.0128.001)

The Security Monitoring components shall be provided with periodic maintenance consistent with the manufacturer's recommendations. In addition, adequate floor space and maintenance clearances shall be provided around these components to permit in-place maintenance and facilitate dismantling, removal, or replacement of equipment.

(3007.0128.002)

1.2.9 Safety Regulations

Security Monitoring shall be non-safety related for component design and Non-Seismic Category I for equipment support in non-Class 1E areas, and Seismic Category I for equipment support in Class 1E areas.

(3007.0129.001)

1.2.10 Codes and Standards Requirements

Security Monitoring shall be designed and constructed in accordance with the regulatory requirements and the industry codes and standards that are listed in Tables 1-2 and 1-3. Deviations from these requirements may be proposed for review and approval by the Project Office.

(3007.01210.001)

1.2.11 Quality Assurance Requirements

Items designated nonsafety-related 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 NEF2-10, regarding engineering holds, engineering drawing lists, design review, and management assessment which shall be implemented on activities that affect the quality of such items. 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.

(3007.01211.001)

Subsystem-level documents are assigned the QAL classification that corresponds to the highest QAL of any item in the subsystem. Therefore, this SSDD shall be classified as QAL III.

(3007.01211.002)

1.2.12 Construction Requirements

Security Monitoring arrangement features shall facilitate the installation, removal, and reinstallation of equipment.

(3007.01212.001)

The Security Monitoring design shall utilize shop, factory, or field fabrication, assembly, or erection as appropriate to minimize erection costs and maintain quality control.

(3007.01212.002)

The design of Security Monitoring components shall incorporate materials and processes, as required, to meet all packaging, shipping, receiving, storage, handling, construction, and operational functions. Level B and Housekeeping Zone IV is provided from shop fabrication through plant startup.

(3007.01212.003)

1.2.13 Decommissioning Requirements

(TBD)

TABLE 1-1

SECURITY MONITORING ENVIRONMENTAL CONDITIONS

A. Normal Environment

Temperature, °C (°F)	15.6 -40 (60-104)
Pressure, psia	Atmospheric
Humidity, percent	20 - 80
Radiation, rad*	(TBD)
Aging, days/yr	(TBD)
Operating cycles	(TBD)

B. Abnormal Environment

Temperature, °C (°F)	48.9 (120)
Humidity, percent	10 - 90
Aging, days/yr	(TBD)

NOTES:

* 40 yr total integrated dose (TID)

TABLE 1-2

REGULATORY REQUIREMENTS

A. Regulatory Guidance Documents

1.	RG 1.17	Protection of Nuclear Power Plants Against Industrial Sabotage
2.	RG 5.12	General Use of Locks in the Protection and Control of Facilities and Special Nuclear Material
3.	RG 5.20	Training, Equipping, and Qualifying of Guards and Watchmen
4.	RG 5.44	Perimeter Intrusion Alarm Systems

B. Codes of Federal Register

1.	10CFR50	Licensing of Production and Utilization Facilities
2.	10CFR73	Physical Protection of Plants and Materials

TABLE 1-3

INDUSTRY CODES AND STANDARDS

A. American National Standards Institute

1. ANSI N18.17 Industrial Security for Nuclear Power Plants

B. Institute of Electrical and Electronic Engineers

1. IEEE 472 Surge Withstand Capability Test

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

Security Monitoring is an integrated system of sensors for perimeter and interior intrusion detection and alarm, with CCTV used for assessment. Supervisory circuits are used to detect tampering and internal system faults. Security Monitoring meets the requirements established in 10CFR50 and 10CFR73.

2.2 SUBSYSTEM CONFIGURATION

The Security Monitoring configuration incorporates multiple detector types and CCTV into a logic multiplex system reporting to central redundant processors and consoles, as shown in Figures 2-1 and 2-2.

All detector alarm points are designed to initiate an alarm signal under any of the following conditions:

1. When sensing a stimulus or condition for which it was designed to react.

2. If primary power fails and secondary power does not take over properly.

3. If the detector's circuitry is opened, shortened, or grounded and if such condition is capable of compromising the device's normal operation.

4. If a tamper switch or triggering mechanism is activated.

Intrusion detection of the Nuclear Island perimeter is provided with the use of the following devices:

- Perimeter (fence) disturbance sensors such as electromechanical switches, piezoelectric transducers, geophones, and electret cables are used to detect intruder penetrations through perimeter fences. They detect mechanical vibrations generated in the fence when an intruder climbs over, cuts through, or lifts up the fence fabric to crawl under.

- Electric field sensors are used to detect fence penetrations when mounted to a perimeter fence, or boundary penetrations when installed in a stand-alone configuration along a zone between the perimeter and the item or structure being protected. They generate an electrostatic field along a combination of parallel field and sense wires. The field and sense wires are either secured to separate fence posts to form a stand-alone electric field fence or they are secured to existing fence posts to form a protected barrier that is part of the existing fence. As an intruder approaches the electric field sensor, his body distorts the electrostatic field generated by the field wire. The resulting field distortions alter the normal electrical

signals on the sense wire. When the change in the signal characteristics satisfies the detector alarm criteria, an alarm is initiated.

- Microwave sensors are invisible barrier detectors used to detect intrusion in the exterior perimeter. These sensors are part of a microwave system composed of a transmitter, receiver, power supply, interconnecting wiring, and alarm annunciator. The microwave transmitter produces a beam-like pattern of microwave energy directed to the receiver, which senses the microwave beam. A partial or total interruption of the beam causes an alarm condition. The microwave beam is modulated to reduce interference from spurious sources of radio frequency energy, to increase sensitivity, and to decrease the vulnerability to defeat from "capture" of the receiver by a false microwave source. Successive microwave links are overlapped so as not to leave gaps.

- Infrared sensors are invisible barrier detectors used to detect intrusion in the exterior perimeter. These sensors are part of an infrared system composed of a transmitter, receiver, power supply, interconnecting wiring, and alarm annunciator. The transmitter directs a narrow beam to a receiver. If the infrared beam between the transmitter and receiver is interrupted, an alarm signal is generated. The infrared beam is modulated. Since it does not diverge significantly, multiple infrared beams between transmitter and receiver are used to define a "wall." If this "wall" is penetrated by an individual, an alarm results.

- Ferrous metal detectors are used to detect perimeter intrusion. These detectors are part of a metal detector system which consists of buried electrical cables, amplifiers, inhibitors, and alarm annunciator. The system is passive and is susceptible to changes in the ambient magnetic field. Such changes are caused either by electromagnetic disturbances or by ferrous metal being carried over the buried cables. The change in the local magnetic field induces a current in the buried cable which is filtered and sensed by the electronics. If the change exceeds a predetermined threshold, an alarm is generated. To reduce nuisance alarms from external electromagnetic sources (e.g., electrical power transmission lines), the electrical cable is laid in loops which are transposed at regular intervals. The inhibitor, buried under a cable loop, senses strong temporary electromagnetic interference (e.g., lightning) and disables the alarm system for approximately one second, thus reducing nuisance alarms.

- Pressure-sensitive sensors/transducers are used to detect small variations in the mechanical stress exerted on the surrounding soil by the presence of an individual passing above the sensor. The signals produced by the transducers are amplified and compared with a pre-established threshold. If the signal exceeds the threshold, an alarm occurs. The transducer is a set of piezoelectric crystals, a fluid-filled flexible tube, or a specially fabricated electrical cable. The sensitive area consists of a narrow corridor, about one meter in width.

- Closed-circuit television (CCTV) cameras are used to observe all areas of the isolation zone. CCTV cameras have pan, tilt, and zoom capabilities, as necessary, with the controls and monitors located in the CAS and SAS.

- CCTV motion detectors are used to detect the presence of an intruder by electronically comparing successive scenes for differences in images. An alarm is initiated when the compared images differ by more than 6 percent. The detectors are capable of desensitizing portions of the viewed area where naturally moving objects occur.

- Balanced magnetic switches are installed on each gate in the perimeter fence and all doors in the protected area. An alarm is initiated with the opening of a gate or door, since the magnetic field is decreased, closing a contact. An alarm is also initiated with an attempted substitution of an external magnetic field, since the magnetic field is increased, closing a contact.

Intrusion detection of all vital and material access areas in the Nuclear Island is provided with the use of the following electronic devices:

- Balanced magnetic switches are installed on all doors leading to vital and material access areas, and entrances to the plant from outside.

- CCTV cameras are located at access ways to vital and material access areas, and in the areas themselves. Visual observation via CCTV provides a positive means of assuring that only individuals who have authorized access to an area pass through the access point into the area. Also, the movements of personnel inside those areas can be followed.

- Ultrasonic motion detectors are used to detect movement of an individual within the area for a distance of 5 ft or less at any velocity between 20 fpm and 600 fpm which causes the control unit to initiate an alarm signal. They consist of transmitter/receiver elements and the necessary control circuitry. The detector senses disturbances in a field of acoustic energy above a frequency of 18 kHz.

- Radiation monitors are used as nuclear material detectors and are located in access passageways to material access areas. These monitors assist in the search of individuals for concealed nuclear material and measure the amount of any radioactive contamination of individuals exiting from a material access area.

- Microwave motion detectors are used to detect movement of man-sized objects in the area. They consist of transmitter/receiver elements and the necessary control circuitry. The detectors operate on the Doppler principle, comparing shifts in frequency in the 2 GHz region between transmitter and receiver.

- Vibration detectors are used to protect walls, ceilings, and floors from forceful entry. The detectors consist of contact microphones and associated electronics for threshold and counting processing.

- Infrared sensors are installed in passageways leading to vital and material access areas. A description of the infrared system is provided under the perimeter intrusion detection and alarm system.

Intrusion detection within the access portal located in the operations center for searching of personnel prior to entry into the protected area is provided with the use of the following devices:

- Metal detectors are located in the secure access passageway so that all individuals entering the protected area pass through the detector. The detectors are walk-through stations. A hand-held metal detector is used to pinpoint the exact location of any metal on a subject.

- X-ray detectors are provided for examination of packages prior to entry to the protected area. The package is placed on a conveyor which passes it by an x-ray generator. The package is either fully exposed to the x-ray beam and the image shown on a fluoroscope screen, or exposed to a sweeping x-ray pencil beam which, through the detector, allows the image to be stored in "memory."

- Explosive detectors are used to search individuals for concealed explosives. They are capable of detecting dynamite, TNT, and similar nitrogen compounds. The guard passes the explosive detectors of the hand-held "sniffer" variety over the individual being searched.

- Radiation monitor/Special Nuclear Material (SNM) detectors are used to provide an efficient, sensitive, and reasonably unobtrusive means of searching individuals for concealed SNM, or measuring the amount of any radioactive contamination of individuals exiting from the protected area. They are composed of a detector unit, associated electronics, and alarm logic. The detector unit is sensitive to the radiations which emanate from a contaminated individual or from SNM, and responds to these radiations by generating current pulses. These pulses are amplified, filtered, and fed to alarm logic which interprets the number (or rate) of pulses in some period of time. If the number (or rate) of pulses exceeds a set level, an alarm condition ensues.

The Security Monitoring sensors, their quantity, and location are listed in Table 2-1.

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

2.3.1 Subsystem Operating Modes

Security Monitoring operates continuously under all plant conditions regardless of plant status. The relationship between system operating modes and plant conditions is shown in Table 2-2.

2.3.2 Subsystem Steady-State Performance

Security Monitoring appears dormant in the steady-state, while providing continuous status of vital and protected areas.

2.3.3 Subsystem Response to Plant Transients

Security Monitoring is oblivious to all other plant systems and operations.

2.3.4 Subsystem Failure Modes and Effects

NOT APPLICABLE

2.4 SUBSYSTEM ARRANGEMENT

Security Monitoring sensors are located at the perimeter fence, the vital and material access areas, and the operations center.

All of the Security Monitoring equipment for the Nuclear Island is housed within the Central Alarm Station (CAS) located within the protected area and the redundant Secondary Alarm Station (SAS) located in the operations center. The CAS is a vital area, isolated by controlled access doors with walls, windows, and doors designed to resist penetration by means of small arms fire, liquids, abrasives, or fire. This room has its own ventilation system separated from the system serving the rest of the building to ensure a secure environment for the personnel attending the security monitors.

The perimeter, vital and material access areas, and access portal detection alarm points are annunciated in the CAS and SAS. The annunciation of a perimeter alarm or an access portal detection alarm indicates the type of alarm (such as microwave system or metal detector) and location. The perimeter alarm annunciates via a graphic display as well as on a printer, while the access portal detection alarm actuates the printer only.

An alarm printer is provided in the CAS and SAS to indicate and log all security-related alarms, location, type, and time of alarm.

All enclosures, housing components which could compromise or neutralize the system, are equipped with tamper switches or triggering mechanism compatible with the alarm systems. The electronics are designed so that tamper-indicating devices remain in operation even though the system itself may be placed in the access mode. All controls that affect the sensitivity of the alarm system are located within a tamper-resistant enclosure. All signal lines connecting the alarm points with alarm monitors are supervised.

2.5 INSTRUMENTATION AND CONTROL

To the extent feasible, each Security Monitoring device is designed to initiate an alarm if any part or component fails, or ages to the extent to render the detector ineffective.

Terminals are located within each detector enclosure and readily accessible to permit wiring for required combinations of detector units. All controls and

terminals which are not required for operation of the detector are not readily accessible.

TABLE 2-1

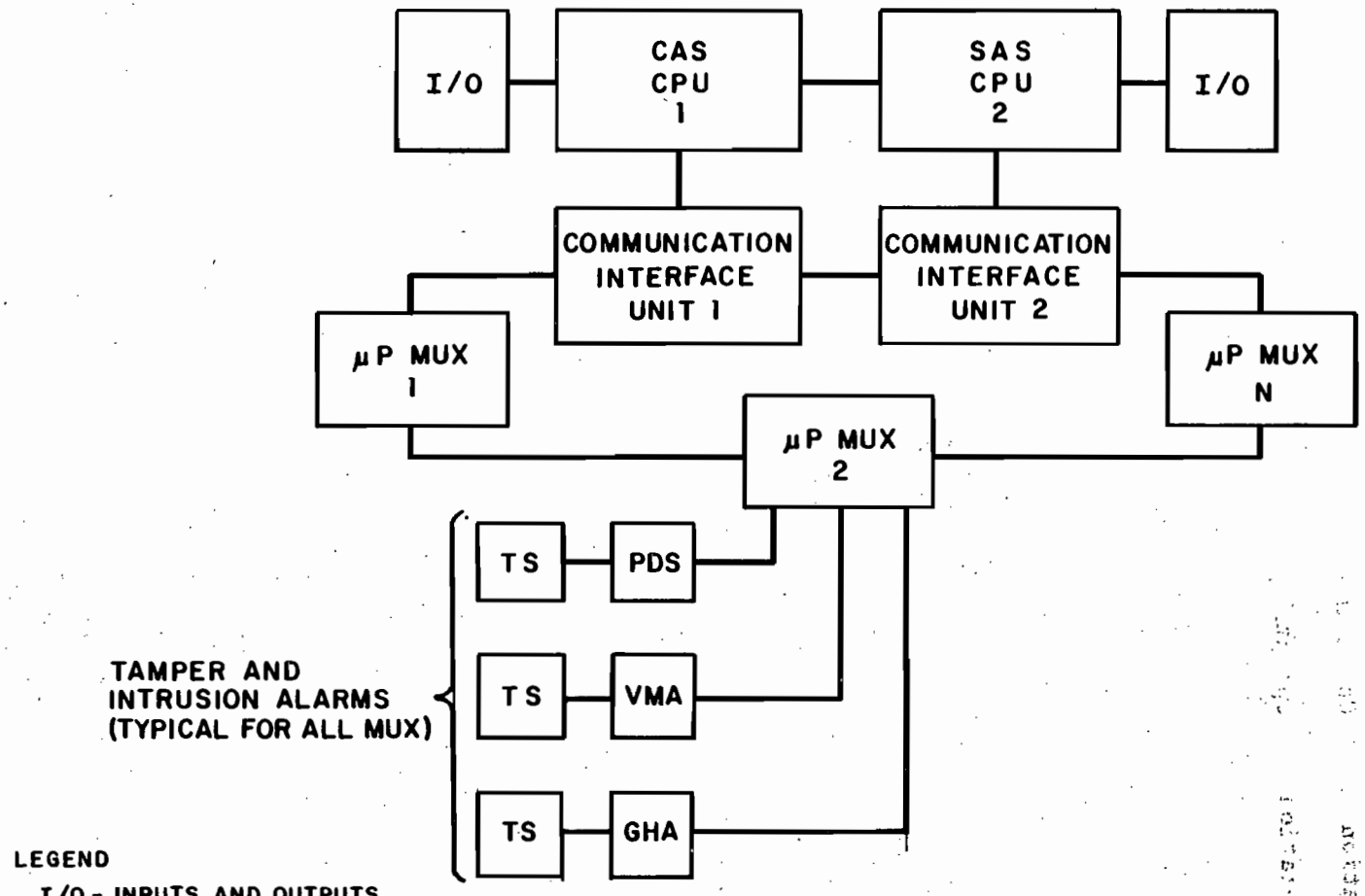
SECURITY MONITORING SENSORS

Parameter	Quantity	Location
Microwave Detectors	(TBD)	Perimeter fence
Microwave Motion Detectors	(TBD)	Vital and material access areas
Infrared Detectors	(TBD)	Perimeter fence and vital and material access areas
Ferrous Metal Detectors	(TBD)	Perimeter fence
Pressure Transducers	(TBD)	Perimeter fence
Vibration or Stress Detectors	(TBD)	Perimeter fence and meteorological tower
Vibration Detectors	(TBD)	Vital and material access areas
CCTV Cameras	(TBD)	Perimeter fence and vital material access areas
CCTV Motion Detectors	(TBD)	Perimeter fence
Balanced Magnetic Switches	(TBD)	Perimeter fence and vital material access areas
Ultrasonic Motion Detectors	(TBD)	Vital material access areas
Radiation Monitors/SNM Detectors	(TBD)	Vital material access areas and access portal
Metal Detectors	(TBD)	Access portal
X-ray Detectors	(TBD)	Access portal
Explosive Detectors	(TBD)	Access portal

TABLE 2-2

PLANT/SUBSYSTEM OPERATING RELATIONSHIPS

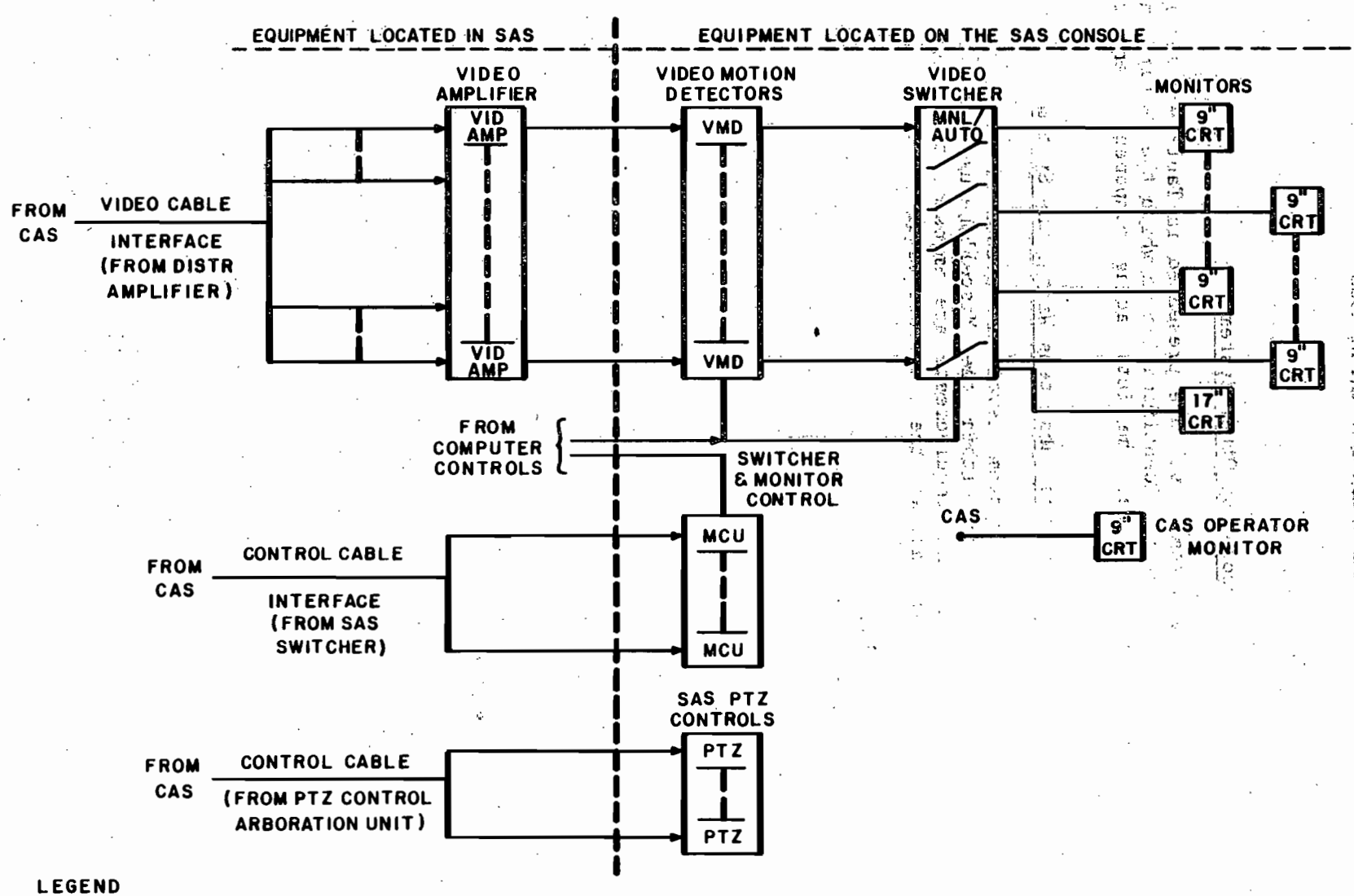
Plant Conditions	Initial Steady-State Mode	Final Steady-State Mode	Remarks
(1) Startup	Operating	Operating	Continuous operation
(2) Shutdown	Operating	Operating	Continuous operation
(3) Normal Operation	Operating	Operating	Continuous operation
(4) Abnormal Operation	Operating	Operating	Continuous operation



LEGEND

- I/O - INPUTS AND OUTPUTS
- CAS - CENTRAL ALARM STATION
- SAS - SECONDARY ALARM STATION
- μP - MICROPROCESSOR
- PDS - PERIMETER DETECTION SYSTEM
- GHA - GUARDHOUSE ACCESS DETECTION
- VMA - VITAL AND MATERIAL ACCESS DETECTION
- TS - TAMPER SWITCH

Figure 2-1
MULTIPLEXED COMPUTER-BASED SECURITY SYSTEM



LEGEND

CAS - CENTRAL ALARM STATION
SAS - SECONDARY ALARM STATION
VMD - VIDEO MOTION DETECTOR
PTZ - PAN, TILT, ZOOM
CRT - CATHODE RAY TUBE

Figure 2-2
CCVT SECONDARY ALARM STATION

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

4.1.1 Interface Requirements Imposed on Other Systems

Interface requirements at the system level are presented in Table 4-1 showing the interfacing systems with subsystem identification on which the requirements are imposed, the nature of interface, the interfacing components, and the interface requirements.

4.1.2 Interface Requirements Imposed on Subsystems Within the System

Interface requirements at the subsystem level are presented in Table 4-2 showing the interfacing subsystems within the Miscellaneous Control and Instrumentation Group on which the requirements are imposed, the nature of interface, the interfacing component, and the interface requirements.

4.2 COMPONENT BOUNDARY DEFINITIONS

(TBD)

TABLE 4-1

INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
1. Reactor System (10)	No interface	NA	NA
2. Vessel System (11)	No interface	NA	NA
3. Reactor Services Group (20)	No interface	NA	NA
4. Heat Transport System (21)	No interface	NA	NA
5. Miscellaneous Control and Instrumentation Group (30)	See Table 4-2 for interface requirements imposed on subsystems within the Miscellaneous Control and Instrumentation Group.		
6. Plant Protection and Instrumentation System (32)	No interface	NA	NA
7. Fuel Handling, Storage and Shipping System (34)	No interface	NA	NA
8. Plant Control, Data and Instrumentation System (37)	No interface	NA	NA

TABLE 4-1 (continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
9. Power Conversion Group (50)	No interface	NA	NA
10. Heat Rejection Group (52)	No interface	NA	NA
11. Reactor Cavity Cooling System (56)	No interface	NA	NA
12. Shutdown Cooling System (57)	No interface	NA	NA
13. Building Structures and Building Service Group (70)	See Table 2-1 for interface requirements on Building Services.		
14. Mechanical Services System (90)	No interface	NA	NA
15. Electrical Group (92)			
(Non Class IE AC Distribution)	Provides ac power	Non-Class IE MCC	480 V, 60 Hz 3 phase
(Plant Security)	Alarm Accessibility	Multiplexers	TBD
(Grounding, Lightning, Heat Tracing, and Cathodic Protection)	Provides grounding for equipment	Equipment enclosures	TBD

TABLE 4-2

INTERFACE REQUIREMENTS IMPOSED ON SUBSYSTEMS WITHIN THE SYSTEM

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
Miscellaneous Control And Instrumentation Group (30)			
(NSSS Analytical Instruments)	No interface	NA	NA
(Radiation Monitoring)	No interface	NA	
(Seismic Monitoring)	No interface	NA	NA
(Meteorological Monitoring)	Provides detection	Meteorological Building and guy wires	TBD
(Fire Detection and Alarm)	No interface	NA	NA

SECTION 9

REFERENCES

1. Gas-Cooled Reactor Associates (GCRA). Utility/User Design Requirements for Modular High Temperature Gas-Cooled Reactor Plant, GCRA-86-002, Rev. 1. GCRA, San Diego, CA, March 1986.

2. GA Technologies, Inc. (GA) et al. Overall Plant Design Specification Modular High Temperature Gas-Cooled Reactor, HTGR-86-004, Rev. 1. GA, San Diego, CA, February 1986.

3. GA Technologies, Inc. (GA). NSSS/BOP Interface Requirements for the 4 x 350 MW(t) Modular HTGR Plant, HTGR-86-007, GA, San Diego, CA, April 1986

4. Stone & Webster Engineering Corporation (SWEC). Meteorological Monitoring, HFD-43005, SWEC, Boston, MA, June 1986.

5. Quality Assurance Requirements, HCP-20801, Rev.1. September 1984.