DOE/HTGR-86-048

HTGR

SAFETY PROTECTION SUBSYSTEM DESIGN DESCRIPTION

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

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

SEPTEMBER 1986

HTGR–86–048
908498/1

SAFETY PROTECTION SUBSYSTEM

DESIGN DESCRIPTION

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

NUCLEAR SAFETY-RELATED

TITLE		APPROVAL LEVEL
SAFETY PROTECTION SUBSYSTEM DESIGN DESCRIPTION	☐ R & D ☐ DV & S ☒ DESIGN	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 1986	J.Zgliczynski J.Bauer	C.Rodriguez Interface Assurance F.A.Silady	G.P.Connors	G.Bramblett		Initial issue (HFD-43202 Rev. 0) 6352-320-103

~~APPLIED TECHNOLOGY~~

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

CONTINUE ON GA FORM 1485-1

Cover Sheets = 2 (Unnumbered

Issue Summary	1,1a		
ii	through xvii	15	
1-1	through 1-31	31	
2-1	through 2-26	26	
3-1		1	
4-1	through 4-4	4	
5-1	through 5-3	3	
6-1	through 6-11	11	
7-1		1	
8-1		1	
9-1		1	
A-1	through A-7	7	
B-1		1	
C-1		1	
D-1		1	
E-1		1	
F-1		1	
Total		111	

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 1

ISSUE	DATE	PREPARED BY	APPROVAL				ISSUE DESCRIPTION/ CWBS NO.
			ENGINEERING	QA	FUNDING PROJECT	APPLICABLE PROJECT	
1	SEP 09 1986	J.Zgliczynski for J.Zgliczynski	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
		J.Bauer					

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

CONTENTS (Continued)

CONTENTS (continued)

CONTENTS (continued)

LIST OF APPENDICES

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

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

DEFINITIONS*

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

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

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

Associated Circuits: Non-Class 1E circuits not physically separated or electrically isolated from Class 1E circuits by acceptable separation distance, safety class structures, barriers, or isolation devices.

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

---

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

DEFINITIONS (Continued)

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

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

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

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

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

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

DEFINITIONS (Continued)

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

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

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

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

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

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

DEFINITIONS (Continued)

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

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

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

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

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

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

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

PREFACE

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

1. Maintain Safe Plant Operation
1.1 Maintain Safe Energy Production
1.2 Maintain Safe Plant Shutdown
1.3 Maintain Safe Plant Refueling
1.4 Maintain Safe Plant Startup/Shutdown

2. Maintain Plant Protection (in the event that plant operation cannot be maintained in the normal operating envelope)
2.1 Protect the capability to maintain safe energy production
2.2 Protect the capability to maintain safe plant shutdown
2.3 Protect the capability to maintain safe plant refueling
2.4 Protect the capability to maintain safe plant startup/shutdown

3. Maintain Control of Radionuclide Release (in the low probability event of failure to maintain plant protection).
3.1 Control radiation
3.2 Control personnel access

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

The OPDS is the top-level technical document for the HTGR plant. The OPDS (based on owner requirements and regulatory requirements) establishes the overall performance, functional, institutional, operational, safety, maintenance, inspection and decommissioning requirements for design of the plant.

In response to the OPDS, SDDs and SSDDs are prepared which describe and control the individual system and subsystem designs. Traceability from plant-level requirements to equipment-level requirements is maintained throughout this hierarchy of design documents.

SUMMARY

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

This document defines the functions of the 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	Minimum Accuracy	Minimum Range
Primary Coolant Pressure (Safety-Related)	{2 s}*	{±1%} of span	(600-1100 psia)}
Receptive Subsystems: Reactor Trip using outer control rods			
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	{40 s} (constant at all loads and includes 25 s sample transit time and 5 s sensor time constant)	{±140 ppmv}	Not Applicable
Receptive Subsystems: Reactor Trip using outer control rods			
Steam Generator Inlet Helium Temperature	{20.0 s} time constant at 100% power	{±30°F}	{[350-2200°F}
Receptive Subsystem: Reactor Trip using outer control rods			

*{ } = 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	Sensor Channel Parameters: Minimum Accuracy	Sensor Channel Parameters: 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.			

Fig. 1-1 Weekly Load Following Cycle

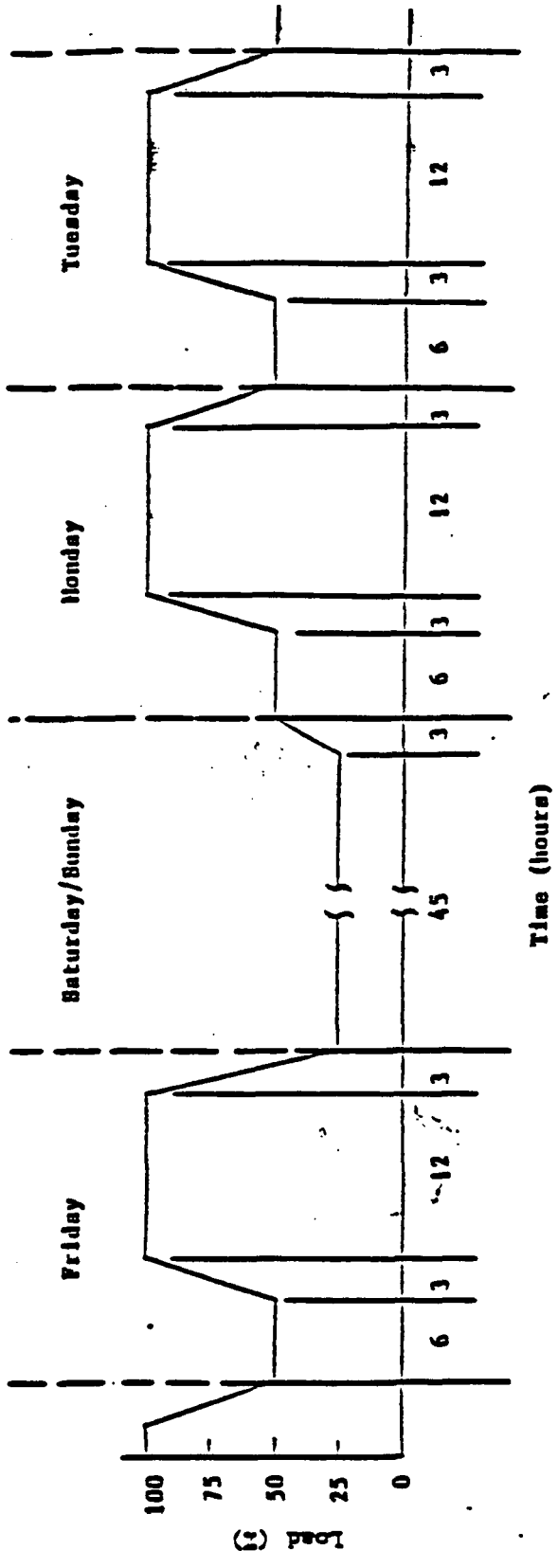


Table 1-2

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)

Subsystem	Unavailability			Reliability		Allocation	
	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.

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:

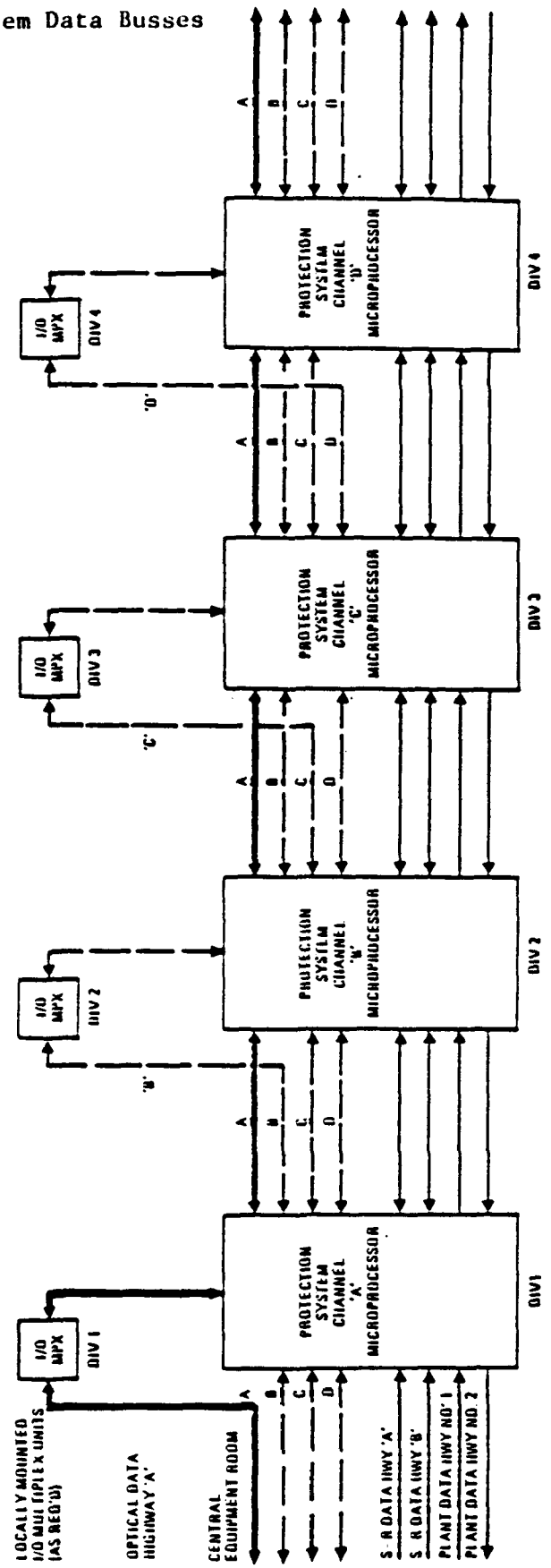
1. Reactor trip using outer control rods.
2. Reactor trip using reserve shutdown system.

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



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

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	1.90 and	1.80 and	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
		time delay ≤50 s and	50 s time delay	30 s time delay	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

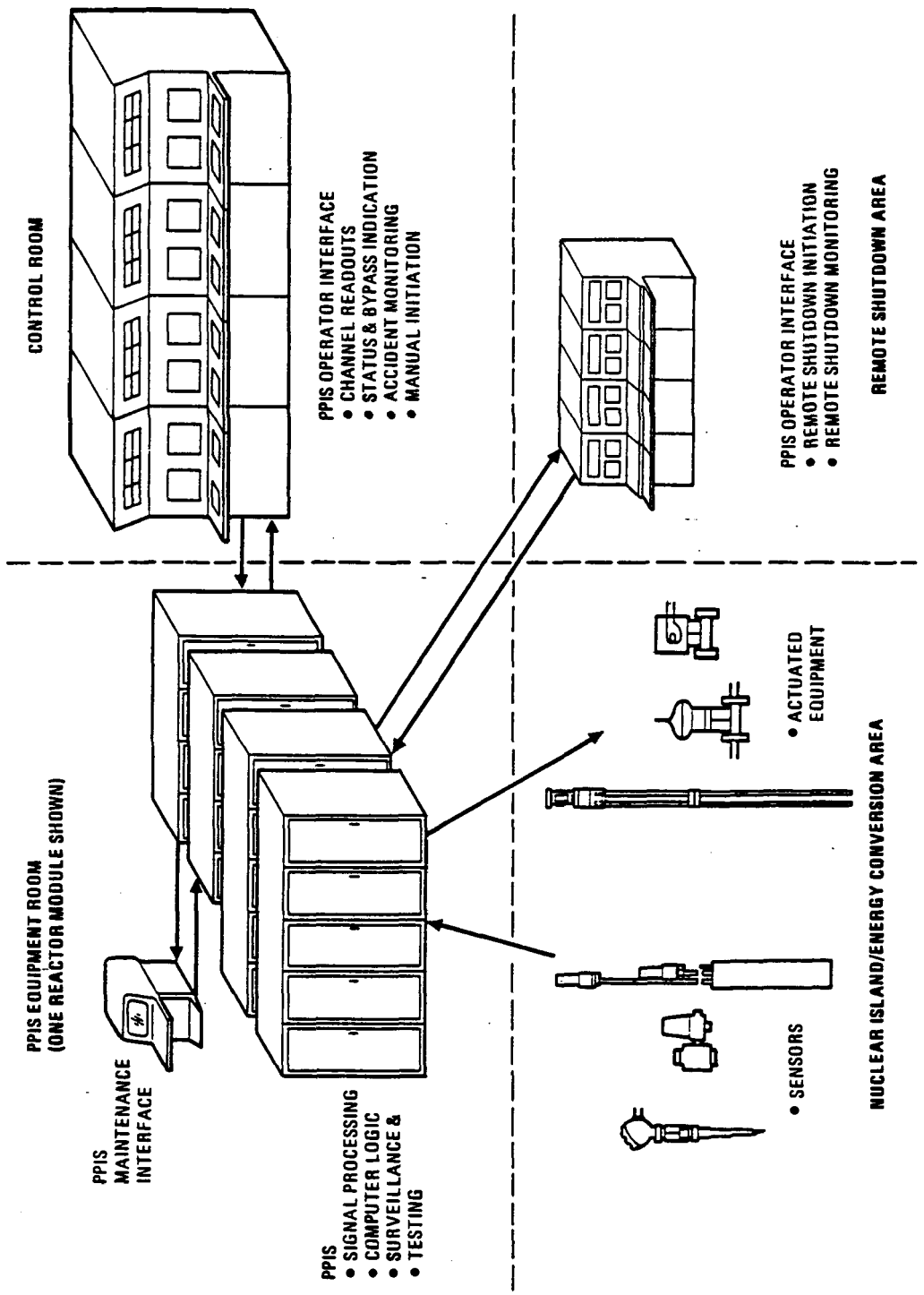


Table 2-7

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)

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)

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.

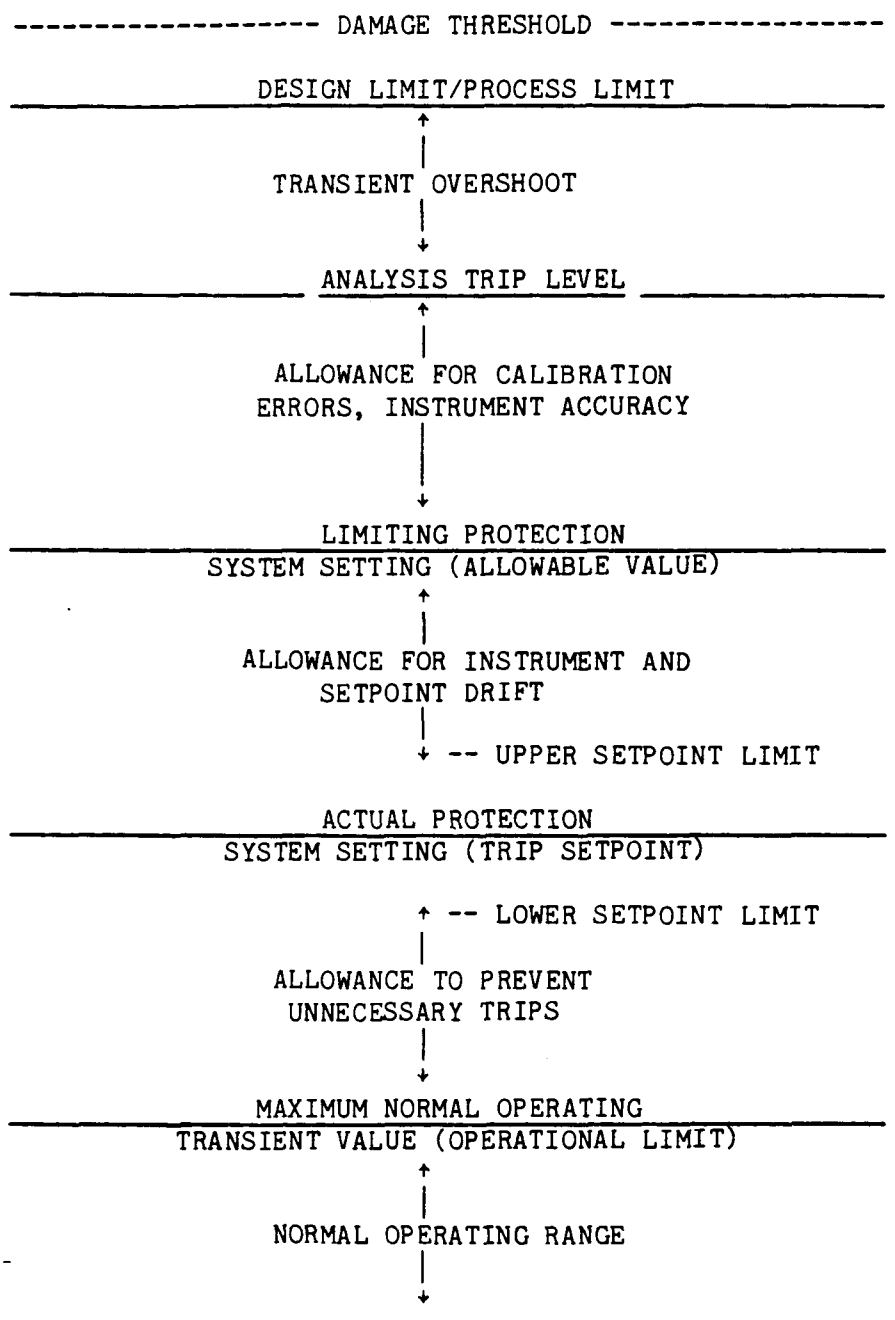


Figure 6-1 RELATIONSHIP BETWEEN SETPOINTS AND COMPONENT DAMAGE LIMITS

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.

Table 6-1

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 Ref.	Description/Reference 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]