DOE/HTGR--87-026

HFD-43007

SECURITY MONITORING
SUBSYSTEM DESIGN DESCRIPTION

4 x 350 MW(t) MODULAR HTGR PLANT

DISCLAIMER

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

Author/Contractor

Stone & Webster Engineering Corporation

~~DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED~~ HH

Issued By:
Stone & Webster Engineering Corporation
Under Subcontract to Gas-Cooled Reactor Associates
For the Department of Energy
Contract DE-AC03-78SF02034

June 1986

MASTER

7572-1488436-B4

HFD-43007

CONTENTS

	<u>Page</u>
LIST OF EFFECTIVE PAGES	iv
LIST OF ACRONYMS.	v
LIST OF DEFINITIONS	vi
LIST OF ILLUSTRATIONS	viii
LIST OF TABLES.	ix
LIST OF APPENDICES (TBD)	-
PREFACE	x
SUMMARY	xi
 1 SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS.	 1-1
1.1 Subsystem Functions	1-1
1.2 Subsystem Design Requirements.	1-1
1.2.1 Subsystem Configuration and Essential Features Requirements	 1-1
1.2.2 Operational Requirements.	1-1
1.2.3 Structural Requirements	1-1
1.2.4 Environmental Requirements.	1-1
1.2.5 Instrumentation and Control Requirements.	1-2
1.2.6 Surveillance and In-Service Inspection Requirements	 1-2
1.2.7 Availability Assurance Requirements	1-2
1.2.8 Maintenance Requirements	1-2
1.2.9 Safety Requirements	1-2
1.2.10 Codes and Standards Requirements	1-3
1.2.11 Quality Assurance Requirements	1-3
1.2.12 Construction Requirements	1-3
1.2.13 Decommissioning Requirements (TBD)	1-3
 2 DESIGN DESCRIPTION	 2-1
2.1 Summary Description	2-1
2.2 Subsystem Configuration	2-1
2.3 Subsystem Performance Characteristics	2-4
2.3.1 Subsystem Operating Modes	2-4
2.3.2 Subsystem Steady-State Performance	2-5
2.3.3 Subsystem Response to Plant Transients	2-5
2.3.4 Subsystem Failure Modes and Effects	2-5
2.4 Subsystem Arrangement	2-5
2.5 Instrumentation and Control	2-5

DISCLAIMER

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

CONTENTS (continued)

	<u>Page</u>
3 COMPONENT FUNCTIONS AND DESIGN REQUIREMENTS (TBD)	-
3.1 Component Functions (TBD)	-
3.1.1 Central Processing Unit Component Functions (TBD)	-
3.1.2 Multiplexers Component Functions (TBD)	-
3.1.3 Field Devices Component Functions (TBD)	-
3.1.4 Alarm Station Console Component Functions (TBD)	-
3.2 Component Design Requirements (TBD)	-
3.2.1 Central Processing Unit Component Design Requirements (TBD)	-
3.2.2 Multiplexers Component Design Requirements (TBD)	-
3.2.3 Field Devices Component Design Requirements (TBD)	-
3.2.4 Alarm Station Console Component Design Requirements (TBD)	-
4 SUBSYSTEM INTERFACES	4-1
4.1 Subsystem Interface Requirements	4-1
4.1.1 Interface Requirements Imposed on Other Systems	4-1
4.1.2 Interface Requirements Imposed on Subsystems Within the System	4-1
4.2 Component Boundary Definition (TBD)	4-1
5 SUBSYSTEM CONSTRUCTION (TBD)	-
5.1 Packaging and Shipping (TBD)	-
5.2 Handling at Delivery (TBD)	-
5.3 Receiving Inspection (TBD)	-
5.4 Storage (TBD)	-
5.5 Access to Buildings (TBD)	-
5.6 Installation and/or Field Fabrication (TBD)	-
5.7 Construction Testing (TBD)	-
5.8 As-Built Drawings (TBD)	-
6 SUBSYSTEM OPERATION (TBD)	-
6.1 Subsystem Limitations, Set Points, and Precautions (TBD)	-
6.1.1 Subsystem Limitations and Set Points (TBD)	-
6.1.2 Precautions (TBD)	-

CONTENTS (continued)

	<u>Page</u>
6.2 Preoperational Checkout (TBD)	-
6.3 Startup/Shutdown (TBD)	-
6.3.1 Startup to 25 percent Steam Flow.	-
6.3.2 Startup from 25 percent Steam Flow.	-
6.4 Normal Operation (TBD)	-
6.5 Refueling (TBD)	-
6.6 Shutdown (TBD)	-
6.7 Abnormal Operation (TBD)	-
6.8 Casualty Events and Recovery Procedures (TBD)	-
6.8.1 Casualty Events (TBD)	-
6.8.2 Design Features to Mitigate Effects of Casualty Events (TBD)	-
6.8.3 Recovery Procedures (TBD)	-
7 SUBSYSTEM MAINTENANCE (TBD)	-
7.1 Maintenance Approach (TBD)	-
7.2 Corrective Maintenance (TBD)	-
7.3 Preventive Maintenance (TBD)	-
7.4 In-Service Inspection (TBD)	-
7.5 Surveillance (TBD)	-
8 SUBSYSTEM DECOMMISSIONING (TBD)	-
9 REFERENCES	9-1

LIST OF EFFECTIVE PAGES

Page(s)	Rev	Date
Title page	0	6/86
i through xi	0	6/86
1-1 through 1-6	0	6/86
2-1 through 2-10	0	6/86
4-1 through 4-4	0	6/86
9-1	0	6/86

LIST OF ACRONYMS

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BSDD	Buildings and Structures Design Description
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CDS	Component Design Specification
CPU	Central Processing Station
DOE	Department of Energy
GHA	Guardhouse Access Detection
IEEE	Institute of Electrical and Electronics Engineers
MUX	Multiplexer
NFPA	National Fire Protection Association
NSSS	Nuclear Steam Supply System
OPDS	Overall Plant Design Specification
PDS	Perimeter Detection System
SAS	Secondary Alarm Station
SDD	System Design Description
SNM	Special Nuclear Material
SSDD	Subsystem Design Description
TID	Total Integrated Dose
TS	Tamper Switch
VMA	Vital and Material Areas

LIST OF DEFINITIONS

Authorized Individual	Any individual who has been designated in writing to have responsibility for surveillance of, or control over, special nuclear material or to have unescorted access to areas where special nuclear material is used or stored.
Alarm Response Force	Local law enforcement officers that provide the primary response for the protected facility and serve as the secondary response for those facilities using proprietary or commercial guards.
Controlled Access Area	Any temporarily or permanently established area which is clearly demarcated and access to this area is controlled, and which affords isolation of the material or persons within it.
Guard	A uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft, the protection of a plant against radiological sabotage, or both.
Intrusion Alarm	A tamper indicating electrical, electro-mechanical, electro-optical, electronic, or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and will alert guards or watchmen by means of actuated visible and audible signals.
Isolation Zone	Any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.
Material Access Area	Any location which contains special nuclear material within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.
Physical Barrier	Fence constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire, or similar material, on brackets angled outward between 30 degrees and 45 degrees from the vertical, with an overall height of not less than 8 ft, including the barbed topping;

LIST OF DEFINITIONS (continued)

Physical Barrier (cont)

Building walls, ceilings, and floors constructed of stone, brick, cinder block, concrete, steel, or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described above, with a height of not less than 8 ft; or

Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

Protected Area

An area encompassed by physical barriers and to which access to Nuclear Island is controlled.

Vital Area

Any area which contains vital equipment.

Vital Equipment

Any equipment, system, device, or material; the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

Security Force

A group of individuals or agencies equipped and trained to respond to security threats.

LIST OF ILLUSTRATIONS

<u>TITLE</u>	<u>PAGE</u>
2-1 Multiplexed Computer Based Security System.	2-9
2-2 CCTV Secondary Alarm Station (SAS).	2-10

LIST OF TABLES

	<u>TITLE</u>	<u>PAGE</u>
1-1	Environmental Conditions	1-4
1-2	Regulatory Requirements	1-5
1-3	Industry Codes and Standards	1-6
2-1	Security Monitoring Sensors	2-7
2-2	Plant/Subsystem Operating Relationships	2-8
4-1	Interface Requirements Imposed on Other Systems	4-2
4-2	Interface Requirements Imposed on Subsystems Within the System	4-4

PREFACE

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

1. Maintain Safe Plant Operation
 - 1.1 Maintain Safe Energy Production
 - 1.2 Maintain Safe Plant Shutdown
 - 1.3 Maintain Safe Plant Refueling
 - 1.4 Maintain Safe Plant Startup/Shutdown
2. Maintain Plant Protection (in the event that plant operation cannot be maintained in the normal operating envelope)
 - 2.1 Protect the Capability to Maintain Safe Energy Production
 - 2.2 Protect the Capability to Maintain Safe Plant Shutdown
 - 2.3 Protect the Capability to Maintain Safe Plant Refueling
 - 2.4 Protect the Capability to Maintain Safe Plant Startup/Shutdown
3. Maintain Control of Radionuclide Release (in the low probability event of failure to maintain plant protection)
 - 3.1 Control Radiation
 - 3.2 Control Personnel Access
4. Maintain Emergency Preparedness (in the extremely low probability of failure to maintain control of release of radionuclides)

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

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

SUMMARY

Security Monitoring acquires and processes sensor data for use by security personnel in the performance of their function. Security Monitoring is designed and implemented as a part of an overall security plan which is classified as Safeguards Information under 10CFR73.21.

SECTION 1

SUBSYSTEM FUNCTIONS AND DESIGN REQUIREMENTS

1.1 SUBSYSTEM FUNCTIONS

The function of Security Monitoring is to detect and assess through sensory, video, and alarm equipment unauthorized entry and tampering within the plant protected area to secure the plant and ensure public safety for all states of plant operation to maintain safety energy production, shutdown, refueling, and startup/shutdown.

1.2 SUBSYSTEM DESIGN REQUIREMENTS

1.2.1 Subsystem Configuration and Essential Features Requirements

Security Monitoring shall be a stand-alone system designed for independent and reliable operation. This subsystem shall be configured such that no single event or failure to any component or cable will degrade the operation of the subsystem.

(3007.0121.001)

1.2.2 Operational Requirements

Security Monitoring shall operate on a continuous basis through all plant modes. This subsystem shall be self-monitoring, reporting any subsystem failures as well as the presence of security breaches.

(3007.0122.001)

Security Monitoring equipment shall be designed to reject radio interference from hand-held, two-way communications equipment.

(3007.0122.002)

Security Monitoring equipment shall not malfunction in the environment of the power station and shall be capable of passing all specified tests.

(3007.0122.003)

1.2.3 Structural Requirements

Security Monitoring shall be located in both Non-Seismic Category I and Seismic Category I structures, and shall be seismically supported within Seismic Category I structures.

(3007.0123.001)

1.2.4 Environmental Requirements

Security Monitoring equipment shall be capable of operating within the normal and abnormal environmental conditions of temperature, pressure, humidity, and radiation for the design life of the equipment, as indicated in Table 1-1.

(3007.0124.001)

1.2.5 Instrumentation and Control Requirements

Security Monitoring shall provide annunciation (audible or visual) to the alarm stations.

(3007.0125.001)

All subsystem alarms and abnormal indications shall be annunciated at the alarm stations and a hard copy record made.

(3007.0125.002)

1.2.6 Surveillance and In-Service Inspection Requirements

The design of Security Monitoring and its components shall incorporate, to the greatest degree practicable, those features necessary for status monitoring and implementing in-service inspection functions with the plant in operation.

(3007.0126.001)

The status of all major Security Monitoring components shall be monitored, and when in-service inspection activities require removal of equipment from service, design features shall be included to minimize the out-of-service time.

(3007.0126.002)

1.2.7 Availability Assurance Requirements

Security Monitoring shall not be necessary for electrical generation.

(3007.0127.001)

1.2.8 Maintenance Requirements

Security Monitoring shall be designed to facilitate in-place or on-line maintenance to the greatest degree practicable.

(3007.0128.001)

The Security Monitoring components shall be provided with periodic maintenance consistent with the manufacturer's recommendations. In addition, adequate floor space and maintenance clearances shall be provided around these components to permit in-place maintenance and facilitate dismantling, removal, or replacement of equipment.

(3007.0128.002)

1.2.9 Safety Regulations

Security Monitoring shall be non-safety related for component design and Non-Seismic Category I for equipment support in non-Class 1E areas, and Seismic Category I for equipment support in Class 1E areas.

(3007.0129.001)

1.2.10 Codes and Standards Requirements

Security Monitoring shall be designed and constructed in accordance with the regulatory requirements and the industry codes and standards that are listed in Tables 1-2 and 1-3. Deviations from these requirements may be proposed for review and approval by the Project Office.

(3007.01210.001)

1.2.11 Quality Assurance Requirements

Items designated nonsafety-related are QAL II or QAL III. QAL II items shall come under a quality assurance program which complies with selected basic requirements and supplements of ANSI/ASME NQA-1 and the four additional supplements from NEF2-10, regarding engineering holds, engineering drawing lists, design review, and management assessment which shall be implemented on activities that affect the quality of such items. QAL III items shall come under a quality assurance program which complies with selected basic requirements of NQA-1 and the four additional supplements identified above.

(3007.01211.001)

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

(3007.01211.002)

1.2.12 Construction Requirements

Security Monitoring arrangement features shall facilitate the installation, removal, and reinstallation of equipment.

(3007.01212.001)

The Security Monitoring design shall utilize shop, factory, or field fabrication, assembly, or erection as appropriate to minimize erection costs and maintain quality control.

(3007.01212.002)

The design of Security Monitoring components shall incorporate materials and processes, as required, to meet all packaging, shipping, receiving, storage, handling, construction, and operational functions. Level B and Housekeeping Zone IV is provided from shop fabrication through plant startup.

(3007.01212.003)

1.2.13 Decommissioning Requirements

(TBD)

TABLE 1-1

SECURITY MONITORING ENVIRONMENTAL CONDITIONS

A. Normal Environment

Temperature, °C (°F)	15.6 -40 (60-104)
Pressure, psia	Atmospheric
Humidity, percent	20 - 80
Radiation, rad*	(TBD)
Aging, days/yr	(TBD)
Operating cycles	(TBD)

B. Abnormal Environment

Temperature, °C (°F)	48.9 (120)
Humidity, percent	10 - 90
Aging, days/yr	(TBD)

NOTES:

- * 40 yr total integrated dose (TID)

TABLE 1-2
REGULATORY REQUIREMENTS

A. Regulatory Guidance Documents

1.	RG 1.17	Protection of Nuclear Power Plants Against Industrial Sabotage
2.	RG 5.12	General Use of Locks in the Protection and Control of Facilities and Special Nuclear Material
3.	RG 5.20	Training, Equipping, and Qualifying of Guards and Watchmen
4.	RG 5.44	Perimeter Intrusion Alarm Systems

B. Codes of Federal Register

1.	10CFR50	Licensing of Production and Utilization Facilities
2.	10CFR73	Physical Protection of Plants and Materials

TABLE 1-3
INDUSTRY CODES AND STANDARDS

A. American National Standards Institute

1. ANSI N18.17 Industrial Security for Nuclear Power Plants

B. Institute of Electrical and Electronic Engineers

1. IEEE 472 Surge Withstand Capability Test

SECTION 2

DESIGN DESCRIPTION

2.1 SUMMARY DESCRIPTION

Security Monitoring is an integrated system of sensors for perimeter and interior intrusion detection and alarm, with CCTV used for assessment. Supervisory circuits are used to detect tampering and internal system faults. Security Monitoring meets the requirements established in 10CFR50 and 10CFR73.

2.2 SUBSYSTEM CONFIGURATION

The Security Monitoring configuration incorporates multiple detector types and CCTV into a logic multiplex system reporting to central redundant processors and consoles, as shown in Figures 2-1 and 2-2.

All detector alarm points are designed to initiate an alarm signal under any of the following conditions:

1. When sensing a stimulus or condition for which it was designed to react.
2. If primary power fails and secondary power does not take over properly.
3. If the detector's circuitry is opened, shortened, or grounded and if such condition is capable of compromising the device's normal operation.
4. If a tamper switch or triggering mechanism is activated.

Intrusion detection of the Nuclear Island perimeter is provided with the use of the following devices:

- Perimeter (fence) disturbance sensors such as electromechanical switches, piezoelectric transducers, geophones, and electret cables are used to detect intruder penetrations through perimeter fences. They detect mechanical vibrations generated in the fence when an intruder climbs over, cuts through, or lifts up the fence fabric to crawl under.
- Electric field sensors are used to detect fence penetrations when mounted to a perimeter fence, or boundary penetrations when installed in a stand-alone configuration along a zone between the perimeter and the item or structure being protected. They generate an electrostatic field along a combination of parallel field and sense wires. The field and sense wires are either secured to separate fence posts to form a stand-alone electric field fence or they are secured to existing fence posts to form a protected barrier that is part of the existing fence. As an intruder approaches the electric field sensor, his body distorts the electrostatic field generated by the field wire. The resulting field distortions alter the normal electrical

signals on the sense wire. When the change in the signal characteristics satisfies the detector alarm criteria, an alarm is initiated.

- Microwave sensors are invisible barrier detectors used to detect intrusion in the exterior perimeter. These sensors are part of a microwave system composed of a transmitter, receiver, power supply, interconnecting wiring, and alarm annunciator. The microwave transmitter produces a beam-like pattern of microwave energy directed to the receiver, which senses the microwave beam. A partial or total interruption of the beam causes an alarm condition. The microwave beam is modulated to reduce interference from spurious sources of radio frequency energy, to increase sensitivity, and to decrease the vulnerability to defeat from "capture" of the receiver by a false microwave source. Successive microwave links are overlapped so as not to leave gaps.
- Infrared sensors are invisible barrier detectors used to detect intrusion in the exterior perimeter. These sensors are part of an infrared system composed of a transmitter, receiver, power supply, interconnecting wiring, and alarm annunciator. The transmitter directs a narrow beam to a receiver. If the infrared beam between the transmitter and receiver is interrupted, an alarm signal is generated. The infrared beam is modulated. Since it does not diverge significantly, multiple infrared beams between transmitter and receiver are used to define a "wall." If this "wall" is penetrated by an individual, an alarm results.
- Ferrous metal detectors are used to detect perimeter intrusion. These detectors are part of a metal detector system which consists of buried electrical cables, amplifiers, inhibitors, and alarm annunciator. The system is passive and is susceptible to changes in the ambient magnetic field. Such changes are caused either by electromagnetic disturbances or by ferrous metal being carried over the buried cables. The change in the local magnetic field induces a current in the buried cable which is filtered and sensed by the electronics. If the change exceeds a predetermined threshold, an alarm is generated. To reduce nuisance alarms from external electromagnetic sources (e.g., electrical power transmission lines), the electrical cable is laid in loops which are transposed at regular intervals. The inhibitor, buried under a cable loop, senses strong temporary electromagnetic interference (e.g., lightning) and disables the alarm system for approximately one second, thus reducing nuisance alarms.
- Pressure-sensitive sensors/transducers are used to detect small variations in the mechanical stress exerted on the surrounding soil by the presence of an individual passing above the sensor. The signals produced by the transducers are amplified and compared with a pre-established threshold. If the signal exceeds the threshold, an alarm occurs. The transducer is a set of piezoelectric crystals, a fluid-filled flexible tube, or a specially fabricated electrical cable. The sensitive area consists of a narrow corridor, about one meter in width.

- Closed-circuit television (CCTV) cameras are used to observe all areas of the isolation zone. CCTV cameras have pan, tilt, and zoom capabilities, as necessary, with the controls and monitors located in the CAS and SAS.
- CCTV motion detectors are used to detect the presence of an intruder by electronically comparing successive scenes for differences in images. An alarm is initiated when the compared images differ by more than 6 percent. The detectors are capable of desensitizing portions of the viewed area where naturally moving objects occur.
- Balanced magnetic switches are installed on each gate in the perimeter fence and all doors in the protected area. An alarm is initiated with the opening of a gate or door, since the magnetic field is decreased, closing a contact. An alarm is also initiated with an attempted substitution of an external magnetic field, since the magnetic field is increased, closing a contact.

Intrusion detection of all vital and material access areas in the Nuclear Island is provided with the use of the following electronic devices:

- Balanced magnetic switches are installed on all doors leading to vital and material access areas, and entrances to the plant from outside.
- CCTV cameras are located at access ways to vital and material access areas, and in the areas themselves. Visual observation via CCTV provides a positive means of assuring that only individuals who have authorized access to an area pass through the access point into the area. Also, the movements of personnel inside those areas can be followed.
- Ultrasonic motion detectors are used to detect movement of an individual within the area for a distance of 5 ft or less at any velocity between 20 fpm and 600 fpm which causes the control unit to initiate an alarm signal. They consist of transmitter/receiver elements and the necessary control circuitry. The detector senses disturbances in a field of acoustic energy above a frequency of 18 kHz.
- Radiation monitors are used as nuclear material detectors and are located in access passageways to material access areas. These monitors assist in the search of individuals for concealed nuclear material and measure the amount of any radioactive contamination of individuals exiting from a material access area.
- Microwave motion detectors are used to detect movement of man-sized objects in the area. They consist of transmitter/receiver elements and the necessary control circuitry. The detectors operate on the Doppler principle, comparing shifts in frequency in the 2 GHz region between transmitter and receiver.

- Vibration detectors are used to protect walls, ceilings, and floors from forceful entry. The detectors consist of contact microphones and associated electronics for threshold and counting processing.
- Infrared sensors are installed in passageways leading to vital and material access areas. A description of the infrared system is provided under the perimeter intrusion detection and alarm system.

Intrusion detection within the access portal located in the operations center for searching of personnel prior to entry into the protected area is provided with the use of the following devices:

- Metal detectors are located in the secure access passageway so that all individuals entering the protected area pass through the detector. The detectors are walk-through stations. A hand-held metal detector is used to pinpoint the exact location of any metal on a subject.
- X-ray detectors are provided for examination of packages prior to entry to the protected area. The package is placed on a conveyor which passes it by an x-ray generator. The package is either fully exposed to the x-ray beam and the image shown on a fluoroscope screen, or exposed to a sweeping x-ray pencil beam which, through the detector, allows the image to be stored in "memory."
- Explosive detectors are used to search individuals for concealed explosives. They are capable of detecting dynamite, TNT, and similar nitrogen compounds. The guard passes the explosive detectors of the hand-held "sniffer" variety over the individual being searched.
- Radiation monitor/Special Nuclear Material (SNM) detectors are used to provide an efficient, sensitive, and reasonably unobtrusive means of searching individuals for concealed SNM, or measuring the amount of any radioactive contamination of individuals exiting from the protected area. They are composed of a detector unit, associated electronics, and alarm logic. The detector unit is sensitive to the radiations which emanate from a contaminated individual or from SNM, and responds to these radiations by generating current pulses. These pulses are amplified, filtered, and fed to alarm logic which interprets the number (or rate) of pulses in some period of time. If the number (or rate) of pulses exceeds a set level, an alarm condition ensues.

The Security Monitoring sensors, their quantity, and location are listed in Table 2-1.

2.3 SUBSYSTEM PERFORMANCE CHARACTERISTICS

2.3.1 Subsystem Operating Modes

Security Monitoring operates continuously under all plant conditions regardless of plant status. The relationship between system operating modes and plant conditions is shown in Table 2-2.

2.3.2 Subsystem Steady-State Performance

Security Monitoring appears dormant in the steady-state, while providing continuous status of vital and protected areas.

2.3.3 Subsystem Response to Plant Transients

Security Monitoring is oblivious to all other plant systems and operations.

2.3.4 Subsystem Failure Modes and Effects

NOT APPLICABLE

2.4 SUBSYSTEM ARRANGEMENT

Security Monitoring sensors are located at the perimeter fence, the vital and material access areas, and the operations center.

All of the Security Monitoring equipment for the Nuclear Island is housed within the Central Alarm Station (CAS) located within the protected area and the redundant Secondary Alarm Station (SAS) located in the operations center. The CAS is a vital area, isolated by controlled access doors with walls, windows, and doors designed to resist penetration by means of small arms fire, liquids, abrasives, or fire. This room has its own ventilation system separated from the system serving the rest of the building to ensure a secure environment for the personnel attending the security monitors.

The perimeter, vital and material access areas, and access portal detection alarm points are annunciated in the CAS and SAS. The annunciation of a perimeter alarm or an access portal detection alarm indicates the type of alarm (such as microwave system or metal detector) and location. The perimeter alarm annunciates via a graphic display as well as on a printer, while the access portal detection alarm actuates the printer only.

An alarm printer is provided in the CAS and SAS to indicate and log all security-related alarms, location, type, and time of alarm.

All enclosures, housing components which could compromise or neutralize the system, are equipped with tamper switches or triggering mechanism compatible with the alarm systems. The electronics are designed so that tamper-indicating devices remain in operation even though the system itself may be placed in the access mode. All controls that affect the sensitivity of the alarm system are located within a tamper-resistant enclosure. All signal lines connecting the alarm points with alarm monitors are supervised.

2.5 INSTRUMENTATION AND CONTROL

To the extent feasible, each Security Monitoring device is designed to initiate an alarm if any part or component fails, or ages to the extent to render the detector ineffective.

Terminals are located within each detector enclosure and readily accessible to permit wiring for required combinations of detector units. All controls and

terminals which are not required for operation of the detector are not readily accessible.

TABLE 2-1
SECURITY MONITORING SENSORS

<u>Parameter</u>	<u>Quantity</u>	<u>Location</u>
Microwave Detectors	(TBD)	Perimeter fence
Microwave Motion Detectors	(TBD)	Vital and material access areas
Infrared Detectors	(TBD)	Perimeter fence and vital and material access areas
Ferrous Metal Detectors	(TBD)	Perimeter fence
Pressure Transducers	(TBD)	Perimeter fence
Vibration or Stress Detectors	(TBD)	Perimeter fence and meteorological tower
Vibration Detectors	(TBD)	Vital and material access areas
CCTV Cameras	(TBD)	Perimeter fence and vital material access areas
CCTV Motion Detectors	(TBD)	Perimeter fence
Balanced Magnetic Switches	(TBD)	Perimeter fence and vital material access areas
Ultrasonic Motion Detectors	(TBD)	Vital material access areas
Radiation Monitors/SNM Detectors	(TBD)	Vital material access areas and access portal
Metal Detectors	(TBD)	Access portal
X-ray Detectors	(TBD)	Access portal
Explosive Detectors	(TBD)	Access portal

TABLE 2-2

PLANT/SUBSYSTEM OPERATING RELATIONSHIPS

<u>Plant Conditions</u>	<u>Initial Steady-State Mode</u>	<u>Final Steady-State Mode</u>	<u>Remarks</u>
(1) Startup	Operating	Operating	Continuous operation
(2) Shutdown	Operating	Operating	Continuous operation
(3) Normal Operation	Operating	Operating	Continuous operation
(4) Abnormal Operation	Operating	Operating	Continuous operation

LEGEND

I/O - INPUTS AND OUTPUTS

CAS - CENTRAL ALARM STATION

SAS - SECONDARY ALARM STATION

μP - MICROPROCESSOR

PDS - PERIMETER DETECTION SYSTEM

GHA - GUARDHOUSE ACCESS DETECTION

VMA - VITAL AND MATERIAL ACCESS DETECTION

TS - TAMPER SWITCH

Figure 2-1
MULTIPLEXED COMPUTER-BASED SECURITY SYSTEM

LEGEND

CAS - CENTRAL ALARM STATION
 SAS - SECONDARY ALARM STATION
 VMD - VIDEO MOTION DETECTOR
 PTZ - PAN, TILT, ZOOM
 CRT - CATHODE RAY TUBE

Figure 2-2
 CCVT SECONDARY ALARM STATION

SECTION 4

SUBSYSTEM AND COMPONENT INTERFACES

4.1 SUBSYSTEM INTERFACE REQUIREMENTS

4.1.1 Interface Requirements Imposed on Other Systems

Interface requirements at the system level are presented in Table 4-1 showing the interfacing systems with subsystem identification on which the requirements are imposed, the nature of interface, the interfacing components, and the interface requirements.

4.1.2 Interface Requirements Imposed on Subsystems Within the System

Interface requirements at the subsystem level are presented in Table 4-2 showing the interfacing subsystems within the Miscellaneous Control and Instrumentation Group on which the requirements are imposed, the nature of interface, the interfacing component, and the interface requirements.

4.2 COMPONENT BOUNDARY DEFINITIONS

(TBD)

TABLE 4-1
INTERFACE REQUIREMENTS IMPOSED ON OTHER SYSTEMS

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
1. <u>Reactor System</u> (10)	No interface	NA	NA
2. <u>Vessel System</u> (11)	No interface	NA	NA
3. <u>Reactor Services Group</u> (20)	No interface	NA	NA
4. <u>Heat Transport System</u> (21)	No interface	NA	NA
5. <u>Miscellaneous Control and Instrumentation Group</u> (30)	See Table 4-2 for interface requirements imposed on subsystems within the Miscellaneous Control and Instrumentation Group.		
6. <u>Plant Protection and Instrumentation System</u> (32)	No interface	NA	NA
7. <u>Fuel Handling, Storage and Shipping System</u> (34)	No interface	NA	NA
8. <u>Plant Control, Data and Instrumentation System</u> (37)	No interface	NA	NA

TABLE 4-1 (continued)

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
9. <u>Power Conversion Group</u> (50)	No interface	NA	NA
10. <u>Heat Rejection Group</u> (52)	No interface	NA	NA
11. <u>Reactor Cavity Cooling System</u> (56)	No interface	NA	NA
12. <u>Shutdown Cooling System</u> (57)	No interface	NA	NA
13. <u>Building Structures and Building Service Group</u> (70)	See Table 2-1 for interface requirements on Building Services.		
14. <u>Mechanical Services System</u> (90)	No interface	NA	NA
15. <u>Electrical Group</u> (92)			
(Non Class IE AC Distribution)	Provides ac power	Non-Class IE MCC	480 V, 60 Hz 3 phase
(Plant Security)	Alarm Accessibility	Multiplexers	TBD
(Grounding, Lightning, Heat Tracing, and Cathodic Protection)	Provides grounding for equipment	Equipment enclosures	TBD

TABLE 4-2

INTERFACE REQUIREMENTS IMPOSED ON
SUBSYSTEMS WITHIN THE SYSTEM

Interfacing Systems (with Subsystem/Identification)	Nature of Interface	Interfacing Component	Interface Requirements
<u>Miscellaneous Control And Instrumentation Group (30)</u>			
(NSSS Analytical Instruments)	No interface	NA	NA
(Radiation Monitoring)	No interface	NA	
(Seismic Monitoring)	No interface	NA	NA
(Meteorological Monitoring)	Provides detection	Meteorological Building and guy wires	TBD
(Fire Detection and Alarm)	No interface	NA	NA

SECTION 9

REFERENCES

1. Gas-Cooled Reactor Associates (GCRA). Utility/User Design Requirements for Modular High Temperature Gas-Cooled Reactor Plant, GCRA-86-002, Rev. 1. GCRA, San Diego, CA, March 1986.
2. GA Technologies, Inc. (GA) et al. Overall Plant Design Specification Modular High Temperature Gas-Cooled Reactor, HTGR-86-004, Rev. 1. GA, San Diego, CA, February 1986.
3. GA Technologies, Inc. (GA). NSSS/BOP Interface Requirements for the 4 x 350 MW(t) Modular HTGR Plant, HTGR-86-007, GA, San Diego, CA, April 1986
4. Stone & Webster Engineering Corporation (SWEC). Meteorological Monitoring, HFD-43005, SWEC, Boston, MA, June 1986.
5. Quality Assurance Requirements, HCP-20801, Rev.1. September 1984.