Chapter 7 – Instrumentation and Control Systems

ATOMIC ALCHEMY INC.

Non-Proprietary

Document Number	Revision	Approved By	Template
AAI-PSAR-07 (NP)	0	Digitally signed by Thomas Eiden Date: 2025.09.28 00:31:26 -06'00'	TEM-003 Rev 2 (05/14/2025)

CHAPTER 7
INSTRUMENTATION AND CONTROL SYSTEMS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TERMS

ACRONYMS AND ABBREVIATIONS

Common acronyms, abbreviations, and units of measurements may not be included here as it is assumed the reader is familiar with their meaning.

AAI	Atomic Alchemy Inc.
CIS	operator control and indications system
CRDM	control rod drive mechanisms
ESFs	engineered safety features
FCS	facility control system
HSIs	human-system interfaces
I&C	instrument and control
MCR	main control room
MHA	maximum hypothetical accident
NFM	neutron flux monitoring system
NPUF	Non-power Production and Utilization Facilities
OTS	off-the-shelf
PDC	Principal Design Criteria
RMS	radiation monitoring system
RPS	reactor protection system
SSCs	systems, structures, and components
VIPR	Versatile Isotope Production Reactor

GLOSSARY

Unique or clarified terms used in this document listed here. Each term is italicized upon first use and marked with (see Glossary) for identification.

Channel: a single, complete functional path within an I&C system from field input device to field output device which can employ a controller division. [AAI]

Division: One of the redundant segments of a system. A division includes its associated sensors, field wiring, cabinets, and electronics used to perform an action. It also includes the power source and actuation signals. [AAI]

7 INSTRUMENTATION AND CONTROL SYSTEMS

7.0 INTRODUCTION

Instrument and control (I&C) systems encompass the sensors, electronic circuitry, displays, and actuating devices that provide the information and means to safely control the Meitner-1 facility and assist to avoid or mitigate accidents.

Instruments are provided to monitor, indicate, and record operating parameters such as neutron flux density, coolant flow and temperature, and radiation intensities in selected areas around Meitner-1. I&C systems will automatically shut down the Versatile Isotope Production Reactor (VIPR) when a safety parameter reaches a predetermined set point limit. I&C subsystems may also be designed to actuate engineered safety features (ESFs) upon the detection of abnormal conditions.

7.1 I&C OVERVIEW

Chapter 7 applies I&C design to meet the functional performance and safety requirements of the reactor-related processes by describing the design characteristics, facility operations, system summaries, conformance to regulatory design criteria, and safety evaluations. The safety evaluation of each system will demonstrate that the system can be designed, installed, and operated in conformance with appropriate regulations, acceptance criterion, and industry codes that are applicable to Non-power Production and Utilization Facilities (NPUFs).

Inside the Meitner-1 facility, up to four 15 MWth reactors (VIPRs) interface with multiple I&C systems. I&C systems include the reactor protection system (RPS), the facility control system (FCS), the radiation monitoring system (RMS), and the operator controls and indications system (CIS). Operator interfaces are provided in the main control room (MCR) with secondary, backup stations throughout the facility.

The primary safety concern for this facility, unintentional release of radioactivity into the surrounding atmosphere from nuclear material, is achieved by maintaining reactor core fuel assembly temperatures below safety limits and by ensuring the safe handling of target capsules. This is accomplished by the I&C systems utilizing control rods and a neutron flux monitoring system (NFM) to control and promptly shutdown reactivity if necessary through the remote handling systems.

The VIPR reactor resembles traditional, open pool–type reactors. Its instrumentation and control systems apply established, regulator-accepted design principles proven in similar systems at currently operating facilities.

7.1.1 Objectives

I&C systems, structures, and components (SSCs) monitor parameters and systems over anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. The parameters and systems under the responsibility of I&C are those that can affect the fission process, the integrity of the reactor core, and radioactivity containment and its associated systems. The controls maintain these parameters and systems within prescribed operating ranges.

The primary safety objective of the I&C architecture design is to protect against uncontrolled radiation release from unsafe reactor operation and unsafe target handling related operations. I&C systems initiate protective actions to mitigate the consequences of design basis events via qualified SSCs.

I&C systems used to control the activities of the reactors will accomplish the following objectives informed by the Principal Design Criteria (PDCs):

- Confinement - prevent inadvertent radiation release
- Control of reactivity - maintain reactivity control of the reactors
- Removal of heat - maintain reactor core and used fuel cooling

The I&C system(s) of the VIPRs will employ designs and principles proven by industry practices to take advantage of previous regulatory recommendations and approvals.

7.1.2 Integration of Future Construction I&C SSC's

As explained in Chapter 1, VIPRs may be added incrementally after the initial installations are operating. The initial installation will include all SSCs of the final configuration for the reactor protection system (RPS) and facility control system (FCS) which will minimize the risk of later installations of I&C SSCs. Add-on I&C SSCs that interface to existing operating components comprise of sensors, actuators, and communication lines and will be isolated and partitioned such that no construction or commissioning related I&C activities can interfere in an unsafe manner with ongoing reactor operation and/or radioisotope production related activities. For I&C system integration or component connection and testing of new interfaces, existing operations will be temporarily halted.

Future integration of additional VIPRs and related I&C SSCs will be further defined in the operation license.

7.1.3 Summary of Major I&C Functions

The primary objective of the Atomic Alchemy Inc. instrumentation and control (I&C) systems is to maintain facility operation within prescribed design-basis limits. The safety analysis identifies the required I&C functions, which are then assigned to the appropriate systems. The assignment of functions to a system follows established design tenets. These principles ensure that safety is maintained as the highest priority and include:

- Safety is prioritized over process efficiency.
- Protective functions are designed as simply as possible.
- Safety-related SSC interactions with non-safety related SSCs are minimized so that the need for isolated inter-classification communications is minimized.
- Redundant and back-up components/systems do not share common failure characteristics with primary protection components/systems.

The following systems are described in greater detail including delineated functions in later sections.

7.1.3.1 The Reactor Protection System (RPS)

Safety Classification: safety-related

The RPS is designed to ensure reactor and personnel safety by maintaining operation within analyzed design-basis limits. The RPS also provides input to the ESF actuation system when instruments indicate abnormal or accident conditions could occur. It detects potential accident conditions or indications of imminent system or boundary failures and then actuates protective functions, primarily scramming the control rods to shut down the reactor.

The RPS, which includes neutron flux monitoring, is the I&C system primarily responsible for placing and maintaining the VIPR(s) in a safe state.

7.1.3.2 The Facility Control System (FCS)

Safety Classification: non-safety

The FCS provides control of non-safety processes and coordination of the Meitner-1 facility's functional interfaces. It is separate and isolated from the RPS but may monitor many of the same parameters. Control functions maintain the normal facility operating conditions and provide the operator with control of conditions like the reactor's power level.

7.1.3.3 The Operator Controls and Indications System (CIS)

Safety Classification: non-safety

The CIS provides operators with real-time operating parameters and system status information needed to monitor reactor operation and determine manual control actions. It also serves as the interface through which automatic and manual control actions are transmitted to the FCS for execution.

The CIS includes displays for reactor operators showing current parameter values, system and equipment status, and manual controls for commanding specific activities of the VIPR. These displays combine analog alarm indications with digital process visualizations.

7.1.3.4 Radiation Monitoring System (RMS)

Safety Classification: non-safety

The RMS monitors radiation levels in selected areas of the facility, transmits data to the FCS, provides alerts to support control of personnel radiation exposure, and tracks the release of radioactive material from the reactor and the facility.

The RMS indicates radiation intensity local to each sensor location and release of radioactive material to the environment. It informs reactor operations personnel if there is a need to actuate confinement systems and initiate personnel radiation protective actions. The system includes area radiation monitors, with displays near the instrument location and in the control room. The RMS monitors radioactive effluents to provide continuous air monitoring for airborne radioactivity in occupied spaces. RMS installations are located throughout the facility.

[ ]SEC,ECI

Figure 7-1: Reactor hall layout

[ ]SEC, ECI

Figure 7-2: Control room layout

7.1.3.5 Systems Architecture

The below architecture graphic represents the expected major systems and sub-systems. The interfacing connecting lines represent the functions employed within each system communicating with other systems. The arrows note one-way communications. The system central to the architecture which the other systems organize around is the four-channel reactor protection system. The RPS architecture is described in Section 7.5.4.

]PROP, ECI

Figure 7-3: RPS, FCS, RMS and CIS systems interfacing

Communications equipment is not shown here. The most conservative assumption is that complex devices such as network switches and data bus components will be classified as non-safety. Safety communications isolation devices such as data diodes, internal and external depending on the

technology selected, will be placed along safety-to-non-safety communication lines and considered part of the safety system qualification scope.

7.1.4 VIPRs: Open Pool Reactors

The Meitner-1 facility will use pool-type reactors to produce excess neutrons from fission. Each facility may employ from one to four reactors (VIPRs). These reactors are “non-power producing” and therefore the I&C systems used to monitor, control, and protect the reactors and surrounding facilities will meet the regulatory expectations of NUREG-1537 and follow selected guidance from Chapter 7 digital Interim Staff Guidance (ISG) documents. Field instrumentation and actuation devices will be placed throughout the facility. Non-safety control and indication systems will be located in the equipment room and other environmentally suitable areas. RS systems will be located in the equipment room with distributed components such as human-system interfaces (HSIs) in remote operational areas.

7.1.5 Operator Stations

Operator stations display both safety and non-safety parameters as well as manual controls. Their design is independent of the accident analyses in Chapter 13, which assume no operator actions are required on I&C systems.

7.1.5.1 Main Control Room

The facility has a single main control room (MCR) which interfaces with every I&C system of the four VIPRs.

The MCR includes potentially multiple operator consoles featuring digital graphic screens which provide soft controls, analog displays, and hardwired controls. The MCR primarily provides the operator with the capability to monitor and control reactivity and trip the reactor(s).

Human factors engineering concepts will be followed to design the console layout such as, but not limited to, a central operator focus on safety critical information and alarm color-coding and acknowledgement protocols.

The MCR is a controlled environment and therefore is a suitable environment to host the safety cabinets which contain sensitive electronic components of the reactor protection system.

7.2 DESIGN BASES AND REQUIREMENTS PER ACCIDENT ANALYSES

The I&C system design requirements are derived from the results of postulated accidents analyzed in Chapter 13 that could occur at the Meitner-1 facility.

The primary safety objective for all design bases requires that fuel assemblies and cladding integrity be maintained by ensuring that the temperatures remain below failure limits. The accidents listed below directly challenge fuel temperature and therefore integrity. The correlated design basis requirements are assigned to I&C systems of this chapter to mitigate those challenges.

7.2.1 Mishandling or Malfunction of Fuel

7.2.1.1 Maximum Hypothetical Accident

Chapter 13 Basis: The maximum hypothetical accident (MHA) for the Meitner-1 facility is cladding failure of every fuel pin in a single VIPR fuel assembly, assumed to be caused by a fuel handling accident in the reactor pool.

Chapter 7 Requirement: None. The analysis of the MHA establishes a bounding event that demonstrates safe reactor shutdown and protection to the public, staff, and environment are ensured without reliance on I&C systems, even under an incredible scenario involving the release of fission products to the atmosphere. There is no requirement applicable to Chapter 7 for the MHA.

7.2.1.2 Overheating of Fuel During Steady-Power Operation

This accident is bounded by the basis discussed in Section 7.2.1.1, above.

7.2.1.3 Dropping or Damaging Fuel

This accident is bounded by the basis discussed in Section 7.2.1.1, above.

7.2.1.4 Dropping of or Impacting with a Non-Fueled Component

This accident is bounded by the basis discussed in Section 7.2.1.1, above.

7.2.1.5 Operation with Damaged Fuel

This accident is bounded by the basis discussed in Section 7.2.1.1, above.

7.2.2 Reactor Power

7.2.2.1 Change of Rate of Reactivity

Chapter 13 Basis: The maximum rate of reactivity insertion allowed is 69 pcm/s (0.09 $/s), corresponding to the simultaneous movement of all control rod assemblies at 0.17 cm/s.

Chapter 7 Requirement: The RPS shall measure change of rate of reactivity and trip the reactor upon sensing 69pcm/s minus a setpoint safety margin.

Chapter 7 Requirement (non-safety): The FCS shall limit the rate of withdrawal of all control rod assemblies to a rate of 0.17cm/s minus a setpoint safety margin.

7.2.2.2 Reactor Power Licensed Operating Limit

Chapter 13 Basis: Though VIPR is licensed for a maximum thermal operating power of 16 MWth, it is intended to be operated at 15 MWth.

Chapter 7 Requirement: The RPS will monitor reactor power level via neutron flux monitoring channel(s) and trip the reactor upon sensing a reactor power level corresponding to the high setpoint defined in the FSAR.

7.2.2.3 Rapid Insertion of a Fuel Element into a Vacancy in the Core at the Most Reactive Position

Chapter 13 Basis: A rapid insertion of a fuel assembly into a vacancy in the core is postulated to occur from a fuel assembly, perched above the most reactive position in the VIPR core, falling into its fully

seated position. When this step insertion of reactivity occurs while the VIPR is at full power, excess reactivity causes the reactor to enter a supercritical configuration and begin a rapid power excursion.

Chapter 7 Requirement: The RPS will monitor reactor power level via neutron flux monitoring channels and trip the reactor upon sensing a reactor power level corresponding to the high setpoint defined in the FSAR.

7.2.2.4 Rapid Inadvertent Insertion of a Portion of All Excess Reactivity Loaded into the Reactor

This accident is bound by the basis discussed in Section 7.2.2.3, above.

7.2.2.5 Failure of an Experiment that Inserts Excess Reactivity

This accident is bound by the basis discussed in Section 7.2.2.3, above.

7.2.2.6 Rapid Increase in Reactivity as a Result of a Change in Operating Parameters

This accident is bound by the basis discussed in Section 7.2.2.3, above.

7.2.2.7 Ramp Insertion of Reactivity by Drive Motion of the Most Reactive Control Rods

Chapter 13 Basis: A ramp insertion of reactivity is caused by the continuous removal of the most reactive control rods from the VIPR in an uncontrolled fashion, without regard for reactor power or neutron flux levels within the core. When such a withdrawal occurs while the VIPR is at full power, excess reactivity causes the reactor to enter a supercritical configuration and begin a power excursion.

Chapter 7 Requirement: The RPS will monitor reactor power level via neutron flux monitoring channels and trip the reactor upon sensing a reactor power level corresponding to the high setpoint defined in the FSAR.

7.2.3 Radiation Release

7.2.3.1 Pool Radiation Release

Chapter 13 Basis: Radiation level increase in the reactor module will initiate an alarm for evacuation of the reactor confinement.

Chapter 7 Requirement: The RMS shall monitor radiation levels at each reactor module. Upon sensing high radiation, the RMS shall alarm throughout the facility.

7.2.4 Loss of Coolant

7.2.4.1 Pool Depth

Chapter 13 Basis: To maintain effective decontamination factors, the pool depth must be no less than [ ]^{PROP}.

Chapter 7 Requirement: The RPS shall monitor pool level and alarm at operating stations upon sensing a depth of [ ]^{PROP} meters plus a setpoint safety margin that will be defined in the FSAR.

7.2.4.2 Failure of the Primary Coolant Boundary

Chapter 13 Basis: The bounding loss of coolant event is caused by the failure of the PCS boundary, resulting in a rapid, large-scale loss of coolant accident. Specifically, a large piping break, such as a

double guillotine break, is assumed to occur in the cold leg of the primary coolant loop inside of the PCS pump and heat exchanger cavity in the auxiliary module.

Chapter 7 Requirement: The RPS shall monitor pool level and trip the reactor upon sensing a depth of [ ]^{PROP} meters plus a setpoint safety margin that will be defined in the FSAR.

7.2.4.3 Failure of a Component in the Primary Coolant Loop

This accident is bounded by the basis discussed in Section 7.2.4.2 above.

7.2.4.4 Failure in the Chemical and Volume Control System

This accident is bounded by the basis discussed in Section 7.2.4.2, above.

7.2.4.5 Failure of an Experimental Facility

This accident is bounded by the basis discussed in Section 7.2.4.2, above.

7.2.4.6 Failure of a Component in the Primary Coolant System

Chapter 13 Basis: The bounding loss of coolant flow event is caused by the failure of a component of the PCS, such that forced convection of coolant through the VIPR core immediately ceases. Operation of the VIPR at full power without the appropriate coolant flow, as occurs before the reactor is automatically shut down, increases the temperature of the fuel. This accident is considered separately from the loss of coolant accidents because the integrity of the PCS boundary is maintained and no coolant loss from the PCS is considered.

Chapter 7 Requirement: The RPS shall monitor flow in the primary coolant loop and trip the reactor upon sensing a flow rate of [ ]^{PROP,ECI} plus a setpoint safety margin that will be defined in the FSAR.

Chapter 7 Requirement: The RPS shall monitor temperature at the inlet of the primary coolant loop and trip the reactor upon sensing a temperature of [ ]^{PROP,ECI} minus setpoint safety margin that will be defined in the FSAR.

7.2.4.7 Blocking of One or More Fuel Coolant Channels

This accident is bounded by the basis discussed in Section 7.2.4.6, above.

7.2.5 Loss of Normal Electrical Power

Chapter 13 Basis: The loss of normal electrical power to one or all systems within the facility can be caused by a loss of power source outside of the facility or by electrical fault within the facility's power distribution system. Operation of the VIPR at full power without electrical power to the appropriate protective systems could defeat protective functions.

Chapter 7 Requirement: The RPS shall monitor flow in the primary coolant loop and trip the reactor upon sensing a flow rate of [ ]^{PROP,ECI} plus a setpoint safety margin.

Chapter 7 Requirement: The RPS shall monitor temperature at the inlet of the primary coolant loop and trip the reactor upon sensing a temperature of [ ]^{PROP,ECI} minus a setpoint safety margin.

Chapter 7 Requirement: Protective function actuations shall be designed as de-energize to trip.

Chapter 7 Requirement: The neutron flux monitoring channels shall use the same electrical power source as the control rod electro-magnets. A loss of normal electrical power to the channels shall also cause a scram of the control rods.

7.2.6 External Events

Chapter 13 Basis: Structures, systems, and components which perform a safety function are designed to withstand seismic events with heightened requirements; see Chapter 3, Section 3.5 for AAI's seismic classifications (importance factor). Seismic monitors, which are not credited with a safety function, will initiate safe shutdown of the reactor on the primary wave, well before the destructive secondary wave would reach the facility.

Chapter 7 Requirement: SSCs which must execute a protective function shall be designed considering potential interactions between different seismic categories of components to ensure that a failure does not compromise the protection SSC.

Chapter 7 Requirement: The RPS shall shutdown upon signal of significant seismic activity from a seismic monitor.

7.2.7 Mishandling or Malfunction of Equipment

7.2.7.1 Operator Error at the Controls

Chapter 13 Basis: Errors made by an operator at the controls could conceivably result in the continuous removal of a control rod assembly up to the maximum rate, a change in the operating parameters of the reactor coolant system, or the cessation of forced convective flow of the reactor coolant.

Chapter 7 Requirement: The RPS shall monitor flow in the primary coolant loop and trip the reactor upon sensing a flow rate of [ ]^{PROP,ECI} plus a setpoint safety margin.

Chapter 7 Requirement: The RPS shall monitor temperature at the inlet of the primary coolant loop and trip the reactor upon sensing a temperature of [ ]^{PROP,ECI} minus a setpoint safety margin.

Chapter 7 Requirement: The RPS will monitor reactor power level via neutron flux monitoring channel(s) and trip the reactor upon sensing the reactor power level high setpoint, which will be defined in the FSAR.

7.2.7.2 Other Operator Errors

Chapter 13 Basis: In addition to the initiating events discussed in Section 7.2.7.1, an operator could conceivably be responsible for the following:

- Rapid insertion of a fuel assembly into a core vacancy
- Damage to or failure of the reactor coolant boundary
- Blocking of one or more fuel coolant channels
- Dropping or damaging fuel, dropping non-fueled components, or operating with damaged fuel
- Experiment malfunction(s)

Chapter 7 Requirement: None. These accidents are bounded by their respective, previously discussed bases.

7.2.7.3 Malfunction or Loss of Safety-Related Instruments or Controls

Chapter 13 Basis: Malfunction of safety-related instruments or controls could conceivably result in consequences identical to those presented in Section 7.2.7.1.

Chapter 7 Requirement: Each protective function required by the accident analysis of this section shall be performed by independent, redundant channels.

Chapter 7 Requirement: Digital diagnostics shall detect faults within safety channels, including but not limited to redundant data incongruence among protective functions.

Chapter 7 Requirement: Protective function actuations shall be designed as de-energize to trip.

7.2.7.4 Electrical Fault in Control Rod Systems

Chapter 13 Basis: An electrical fault in the control rod systems could result in a loss of electrical power to one or more control rod systems.

Chapter 7 Requirement: An electro-magnet shall couple the control rod(s) to the control rod drive mechanism so that loss of or inadequate electricity due to an electrical fault will de-energize the coupling causing the control rods to drop which places the reactor in a safe shutdown state.

7.2.8 Analysis of Accidents with Radiological Consequences

This section analyzes the accidents with radiological consequences. Each defined accident does not directly lead to a release of radioactivity; therefore, consequences for those events are not applicable.

7.2.8.1 Mechanical Failure of a Fueled Experiment – Maximum Credible Accident

The rupture of an irradiated experiment capsule is the basis for the Maximum Credible Accident (MCA) scenario at the VIPR facility. The mechanical irradiation target failure is very similar to the fuel handling accident in that it involves special nuclear material, fission products, and release into the primary coolant. However, whereas the fuel handling accident involves a large amount of fuel, any experiment or irradiation target containing fissionable material is limited, in general, so that production of gaseous and volatile fission products results in releases lower than that considered in Chapter 13, Section 13.3.6.2. Therefore, experiment malfunction will not result in consequences more severe than those listed in the MHA.

Chapter 7 Requirement: None. This accident is bounded by the MHA analysis.

7.2.9 System Performance

7.2.9.1 Assumed Scram Delay

Chapter 13 Basis: VIPR accident analyses assumed a scram delay of one (1) second to allow for the execution of the Reactor Protection System protective functions. This delay encompasses the violation of any safety monitoring setpoint and the initiation of the reactor scram.

Chapter 7 Requirement: Upon sensing the crossing of a protective parameter's safety limit, the RPS shall initiate the actuation of the protective action within one (1) second.

7.3 SYSTEM-GENERIC, DESIGN CRITERIA-INFORMED DESIGN BASES

The PDCs of the Meitner-1 identify the SSCs that are critical in protecting public health and safety. The PDCs assigned in 7.1.1 provide criteria for developing the design bases of the Meitner-1 I&C SSCs.

These PDCs frame the design bases for setpoints, calibration requirements, monitoring functions, and the supporting subsections on testing and diagnostics, environmental qualification, and human–system interfaces, and Digital I&C design criteria .

7.3.1 Instrument Setpoints and Design Basis Limits

Design basis limits for I&C establish setpoints and operating ranges that ensure plant parameters remain within safety analysis assumptions. Instrument setpoints and acceptable operating ranges for systems will ensure that potentially unsafe or damaging process accidents are avoided and/or terminated before facility conditions exceed safety limits

Establishing and maintaining effective instrument setpoints serves to:

- Verify that calculation methods ensure protective actions are initiated before plant parameters exceed their analytical limits.
- Verify that control and monitoring setpoints are consistent with design and safety requirements.
- Confirm that calibration intervals and methods align with safety analysis assumptions.

Because analytical limits, as established by theoretical analyses, do include considerations for the accuracy (uncertainty) of as-installed instrumentation, additional testing is necessary to prove the as-installed limiting setpoint of each function. Accident analyses following the detailed design will establish specific setpoint limits for critical process parameters. The results of the analysis will be provided in the FSAR.

7.3.2 Setpoint Maintenance and Calibrations

The designed limits which I&C safety systems rely on to execute protective functions are based on instrument setpoints configured in the application logic. The ability to adjust these setpoints is necessary when, 1) the system transitions from analytical/theoretical design to practical field testing after installation, 2) when the circuit experiences drift, and 3) when facility processes change.

Both the protection and non-safety control systems shall be capable of automated calibration features. The protection system shall be capable of in-chassis, on-line manual calibration of setpoints and tuning of parameters without affecting the ability of the system to perform a protective action. Manual calibration and tuning activities are controlled by procedure and only possible while the affected functional logic is placed out of service.

7.3.3 Testing and Diagnostics

Online testing of the digital I&C systems consists of two types of tests: diagnostic built-in self-tests and manual surveillance tests. The self-diagnostic tests are built into the equipment and automatically perform comprehensive checks to validate that the equipment and software are performing their

functions correctly. Self-tests include online continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. On-line verification tests are manually initiated to verify that the safety system can perform its intended safety function.

Digital microprocessor-based I&C systems are inherently non-deterministic and therefore prone to different kinds of failures than traditional analog or FPGA-based systems. Surveillance testing must be combined with automatic self-testing to ensure comprehensive failure detection for all but latent software faults.

Refer to Section 7.5.6 for detailed description of the diagnostic and surveillance testing criteria placed on the RPS. Relevant descriptions of specific hardware and its associated software will be provided in the FSAR.

7.3.4 Environmental Qualification

The I&C systems' ability to function for the full range of reactor operation including maintenance and testing will be proven by environmental qualification. Conditions used for testing are based on anticipated facility environmental conditions. Refer to Chapter 2, "Site Characteristics", for a description and safety assessment of the construction site selected for the facility.

Environmental qualification acceptance of the systems will either be proven by testing per the criteria specific to the facility's requirements or credited by analysis of vendor-performed platform qualification.

7.3.4.1 Controlled Environment

The environmentally sensitive electronics of the control and protection systems will be located in the controlled environment of either the control room or the equipment room. Both areas are considered a mild environment because the conditions are postulated not to change because of an accident identified in the Chapter 13 accident analyses. No degrading environmental effects have been found that lead to common mode failure of equipment in either room. Sensitive electronics will be qualified as capable of functioning during and after normal and abnormal events and conditions that include:

- Wide temperature range of 40° to 120°F
- Noncondensing relative humidity up to 95 percent

7.3.4.2 Seismic Requirements & Testing

The I&C safety structures, panels, and platform hardware are designed to provide reasonable assurance that a postulated seismic event cannot cause an accident which would lead to failure of the reactor protection system to perform a safe shutdown of the reactor. Seismic monitors, which are not credited with a safety function, will initiate safe shutdown of the reactor on the primary wave, well before the destructive secondary wave would reach the facility.

7.3.4.2.1 Seismic Category II Over I Criteria

Location and placement of the safety I&C cabinets around SSCs will be evaluated for seismic "2 over 1" criteria.

7.3.4.3 Fire Damage

The fire control and protection functions are considered to be outside of the scope of this chapter. The cabinets which house RPS division cabinets will be rated to withstand fire damage for a duration which would allow operations staff to take appropriate action.

7.3.5 Human-System Interface (HSIs)

Operators will directly interact with I&C systems via HSIs of the operations control and indication system. The main operator I&C HSIs are

- engineering/maintenance workstations,
- status indications on control system components,
- field instrumentation displays,
- manual controls at the operator stations in the main control room, and
- analog and digital indications in the control room.

Safety I&C HSIs provide information to the plant operators for: (1) assessing plant conditions, safety system performance and making decisions related to plant responses to abnormal events, and (2) planned manual operator action related to accident mitigation. These HSIs also provide information to inform operator actions to mitigate the consequences of anticipated operational occurrences. No operator action is required or credited in the design bases of this chapter.

7.3.5.1 Human Factors Consideration

The layout of control and indication instruments of the main control room operating stations will be based on non-power utilization facility best-practice, human-factor principles.

An evaluation of the human action, and an integrated assessment will be made to determine the appropriate level of human factors engineering. The Meitner-1 facility requires indications from significantly fewer instruments than a standard nuclear power plant and therefore will have fewer console instruments. As such, the human factors evaluation is not expected to be as in-depth of an effort and therefore will only comply with select portions of NUREG-0711. The result of the evaluation will be provided in the FSAR.

7.3.6 Digital I&C Design Criteria

AAI has selected digital technology for the automated controls platform(s) which affords the benefit of extensive diagnostics. The RPS technology will be FPGA-based. The non-safety controls will be micro-processor-based. The difference between the two technologies may affect how the characteristics of each type of system can be credited with inherent safety features. Each type of system may therefore be tested and qualified differently.

Regulatory concerns related to general digital system technologies are discussed here.

7.3.6.1 Access Control and Cyber Security

A secure development and operational environment for digital safety systems serves to (1) prevent undocumented, unneeded, and unwanted modifications to the secured system and (2) protect against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of

connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

During development of the digital I&C systems appropriate physical, logical, and programmatic controls will be required of the vendor's facility. During on-line operations of the digital I&C systems appropriate physical, logical, and administrative controls will be set in place at the Meitner-1 facility. These secure development and operational environment protective measures may include adoption of design features into the digital safety system design to prevent inadvertent access to the system and protection against undesirable behavior from connected systems when operational.

Secured development measures taken at the vendor's facility include:

- Development of the program code, integration of the code with the hardware and testing of the integrated system in a secured area with physical locks.
- Cyber-hardening computer-based maintenance workstations that connect to the digital control system.
- Securing the program code during development and storage on a cyber-hardened laptop without the ability to connect to a network or internet, wirelessly or via cables.
- Transfer of the integrated system and all sensitive records from the vendor's facility to AAI via secured transport.

Secured operation measures taken at the Meitner-1 facility include:

- Physical locks and safe key storage for the digital control system panels.
- Procedures for securing access to the digital control system via a maintenance workstation.
- Password protection combined with multiple security levels and user accounts for computer-based maintenance workstations.
- Alarming of any connection or access to the digital control system to all operating stations displays.

7.3.6.2 Digital Communications

All I&C systems, both safety and non-safety, are expected to use digital controls platforms which take advantage of digital data communications employing various communications protocols. Systems may communicate internally among multiple redundant components, or externally to diverse and cross-safety class platforms.

7.3.6.2.1 Non-safety Data Communications

The non-safety data network is a high speed, redundant, real-time network that links the facility control Ssystem to the controls and displays of the main control room. The RPS feeds relevant information through the Facility Control System with communication protected through qualified isolation devices.

7.3.6.2.2 Safety Intra-Architecture Communications

The RPS architecture relies on redundant intra-division communication to meet single failure criterion and increased monitored data reliability. For the safety-related RPS this communication is considered relevant-to-safety. Isolation devices including fiber optic cabling and protocols such as

one-way controlled communications should be used to meet electrical isolation and independence requirements.

7.3.6.2.3 Safety to Non-safety Communications

The encompassing I&C architecture comprises non-safety controllers communicating with the non-safety real time data network and receiving data from reactor protection system divisions. Isolation devices such as data diodes and one-way communication protocols are used to secure the communications of safety systems to non-safety systems. The protection divisions send information through controlled one-way communications using qualified isolation devices. The design of this architecture meets electrical and communication isolation requirements.

7.4 THE FACILITY CONTROL SYSTEM (FCS)

The FCS oversees all normal operations of the facility from cold shutdown through full power operation of the VIPRs. The system primarily provides automatic regulation of reactor power but also maintains the reactor in a safe shutdown state, controls reactor startup via interlocks, changes power level based on operator commands, and provides defense-in-depth backup to the RPS for tripping the reactor. The system allows operators to control the facility's non-safety components from the main control room workstations. In addition to operating the VIPRs, the system facilitates operation of the radioisotope production related and radwaste processes.

The FCS interfaces with both safety and non-safety systems to provide process data to operator workstations from the RPS. The system processes and distributes data for non-safety alarms and displays for both normal and emergency facility operations, facility analysis, recorded logs, and retrieval of stored historical data in support of facility operations.

7.4.1 Design Criteria

7.4.2 Design Basis Requirements

- The system shall monitor the parameters detailed in Appendix A over their anticipated ranges for normal operation and for anticipated operational occurrences.
- The system's controller electronics shall be installed in an environmentally controlled room.
- The system's controller electronics and wiring shall be constructed of non-flammable or flame-retardant materials.
- Reactivity controls shall allow operators to maintain reactor power within prescribed operating ranges.
- The system shall provide the capability for automatic power level control of each VIPR's core reactivity.
- The system shall monitor core reactivity levels via neutron flux monitoring channels.
- The system shall use control rods and regulating rod(s), including a control rod drive mechanism, to control reactivity changes.

- The system shall limit the maximum speed by which the control rod drive mechanisms (CRDM) can raise and lower rods to 0.17cm/s to mitigate the potential amount and rate of unsafe reactivity increase as calculated from the accident analyses of Chapter 13.
- The system shall monitor and control the speeds of various pumps along the cooling system circuits.
- Any actuation of a reactor trip by the system diverse from the RPS shall be isolated via and independent channels.
- Any diverse trips from the system shall be wired to the de-energize-to-trip circuit in series so that it cannot defeat a trip from the RPS. Manipulation of the control rods via the CRDM shall not affect rod drop when power is removed from the CRDM electromagnets.
- The system shall have the capability to monitor, report, and maintain digital records of non-safety facility conditions.
- The system shall alarm critical facility parameters to the operator station. Refer to Appendix A of this chapter for parameters to be alarmed.
- The system shall monitor pool coolant temperature to inform pool coolant pump speed(s).
- The system shall control pool coolant flow to ensure adequate heat removal from the reactor core(s).

7.4.3 System Description

A single FCS comprises a central, non-safety distributed control system which receives data from field instrumentation and the safety RPS(s) of each VIPR. The FCS provides reactor power level control by reading neutron flux levels from the NFM and manipulating the CRDMs which control the incremental movement and position of each control and regulating rod. The FCS also controls pool coolant flow to constantly remove heat from the reactor core(s). The FCS communicates system and field instrument status to displays at operator stations and receives operator commands based on the displays. Field instrumentation includes control rod position gauges, primary coolant gauges, and those which interface via the RPS which include neutron flux monitoring detectors and core fuel assembly gauges. Operator controls primarily control reactor power level(s).

7.4.3.1 Reactor Power Control Function

The RPC function primarily regulates reactor power and power distribution by positioning clusters of control rods in the reactor core using the CRDMs. This function allows operators to lower and raise the four control rods and the single fine-tuning regulating rod in each VIPR.

Control rods are installed in each of the [ ]^{PROP} “inner” fuel assemblies, and the single regulating rod assembly is installed in one of the corner fuel assemblies (refer to Chapter 4, “Reactor Description”, for detailed rod locations). Redundancy is designed into the control rods to meet “single stuck rod” criterion. Each control rod assembly, consisting of multiple control rods connected to a common “spider” configuration, is controlled by a CRDM. Each CRDM raises/lowers its control rod assembly via a gear reduction screw drive. To prevent rapid insertion of reactivity, the maximum speed by which the CRDM can raise, and lower rods is 0.17cm/s. Limit switches at the CRDM provide rod position to the

operator stations. Limit switches indicate full-in or full-out status and protect the CRDM from reaching extreme positions.

Each control rod is electromagnetically attached to the CRDM. Because a trip has higher priority than a raise/lower command, loss of power to the electromagnet removes the capability of the CRDM to defeat the protective action when manipulating the position of the control rods.

7.4.3.2 Interfaces

The FCS interfaces with the following major systems.

The Reactor Protection System

The FCS receives data from each VIPR RPS via one-way communication which is sent from the RPS and not requested by the non-safety DCS. The communication lines are electrically isolated via a combination of fiber-optics and/or data diode technology to ensure a fault in the non-safety components cannot propagate via the interface to the RPS. This includes the Neutron Monitoring System.

Operator Control and Indication System

The FCS sends and receives non-safety data with the Operator Control and Indication System via two-way communication. The data includes alarms, control rod position, CRDM raise/lower commands.

7.4.3.3 Rod Control Interlocks

The following proposed interlocks restrict operation of the VIPR(s) from the Facility Control System functional logic.

- Neutron flux above a threshold to be defined in the FSAR prohibits automatic and manual control rod withdrawal.
- Margin-to-Overtemperature ΔT below a threshold to be defined in the FSAR prohibits automatic and manual control rod withdrawal.
- Margin-to-Overpower ΔT below a threshold to be defined in the FSAR prohibits automatic and manual control rod withdrawal.
- Bank control rod position above a threshold to be defined in the FSAR prohibits automatic rod withdrawal.
- Reactor coolant system T_{avg} below a threshold to be defined in the FSAR prohibits automatic and manual control rod withdrawal.
- Negative flux rate below a threshold to be defined in the FSAR prohibits automatic rod withdrawal.

7.4.3.4 Automatic Power Level Control

The FCS automatically maintains power level by comparing the signal from the wide range linear channel to a preset signal. It provides a shim-in or shim-out signal to the regulating rod drive controller to adjust power, as indicated by the wide range linear channel, to the preset level. The regulating rod control automatically shifts back to manual if the actual level drifts excessively from the preset level.

The regulating rod drive controller receives a signal from both the servo controller and the manual control switch on the rod control module.

7.4.3.5 Pool Coolant Flow

The FCS monitors and controls the speed of several pumps along the cooling system coolant circulating circuits. The cooling system consists of a primary circuit, a secondary circuit on the other side of the heat exchanger, and a tertiary circuit which contains the cooling towers and acts as the ultimate heat sink. The number of pumps and location along each circuit will be defined in the FSAR.

7.4.4 Significant Monitored Parameters

Refer to Chapter 7 Appendix A for a list of significant parameters which the system will monitor for each VIPR.

7.5 THE REACTOR PROTECTION SYSTEM

Protective functions ensure the safety of the facility by initiating protective actions as prescribed by the accident analyses of Chapter 13. The protective functions are grouped into 3 categories: reactor trip, facility protection, and shutdown of target handling processes, and can be actuated automatically by the control system or manually by an operator.

The reactor protection system is designed (1) to automatically initiate the operation of systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and initiate the operation of systems and components important to safety.

7.5.1 Design Criteria

7.5.2 Design Basis Requirements

- The System shall be designed so that the RPS will trip all VIPRs on sensing the effects of high-level seismic activity before the seismic effects can defeat the capability to perform protective functions.
- Sharing of protective function coincidence data among the RPS divisions will be secured through electrical isolation and data protocols such that the interface can be proven not to significantly impair the divisions' ability to perform their safety functions, including, in the event of an accident in the Meitner-1 facility, an orderly shutdown and cooldown of the remaining VIPR units as well as an orderly shutdown of the remaining radioisotope related processes when controlled by operations personnel.
- Setpoint limits of protective function parameters specified in Section 7.5.11, Design Basis Protective Functions, shall incorporate adequate margins including 1) that the temperature limit for fuel cladding damage includes an adequate safety margin, 2) that the related protected process parameter limit (e.g. – reactor power level) does not bring the fuel temperature to its calculated limit, 3) that the protected process parameter limit is protected by a calculated

safety margin, and 4) that the calculated limits are able to be tuned to actual performance when installed at the facility.

- The System's application logic setpoints shall provide an additional margin to the safety limits which are detailed in the bullet (? above. The setpoints margins shall also allow for uncertainties and instrument errors.
- The System shall monitor the parameters of Appendix A over their anticipated ranges for normal operation and for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those parameters and systems that can affect the reactor and radioisotope-related processes, the integrity of the reactor core, the spent fuel, the reactor coolant boundary, and the confinement boundaries and its associated systems.
- The System shall trip the reactor to prevent protective function parameters and systems from contributing to an unacceptably high risk to safety. Refer to the protective function parameters of Section 7.5.11.
- The System shall be designed (1) to automatically initiate the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.
- The System shall be designed so that anticipated operational occurrences cannot affect protective functionality of multiple, redundant channels.
- The System shall be designed to fail into a safe state as de-energized-to-trip which interrupts the trip circuit(s) and therefore electro-magnet control rod coupling power.
- The System shall sense an accident condition and activate the protective function in a duration of less than one (1) second.
- A single failure in a single RPS division, protective function sensor, or trip output signal shall not prevent actuation of protective functions.
- The System shall employ multiple, independent channels for each protective function of Section 7.5.11 to ensure high functional reliability and in-service testability commensurate with the safety functions to be performed.
- Removal from service of any component or channel does not result in the loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.
- The System shall use one-out-of-two coincidence logic to measure the protective function parameters of Section 7.5.11.
- During normal modes of operation, testing or maintenance, the System shall allow protective functions to be individually, manually bypassed/taken out-of-service as long as this does not result in the loss of the required minimum.

- The System shall be redundantly designed so that a single failure in the system shall not prevent a reactor trip.
- The System shall be designed to permit periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.
- Redundant divisions of the System shall be electrically independent including the downstream trip circuit(s) and upstream redundant sensors.
- The System shall permit bypassing of specific reactor power level trips and interlocks during the reactor start-up process.
- Due to the planned digital nature of the RPS and redundant divisions, diverse technology shall be implemented.
- The System shall receive individual trips for each reactor via either of two manual operator controls from main operator stations and shall receive a trip for all reactors from a gang switch at each operator station.
- The System shall trip the reactor upon sensing that the reactor overpower setpoint is reached. The trip uncouples control rods from the CRDM, dropping them into the core regardless of any single malfunction of the reactivity control functions and components.
- The System shall be separated from the FCS with the single exception of one communication line to each RPS division.
- Isolation devices and one-way communication protocols, from safety to non-safety, shall secure the independence of communication between each RPS division and the non-safety RCS.
- Once initiated, reactor protection functions all proceed to a singular action – reactor trip via falling control rods when decoupled from their respective CRDMs. No mechanism will be allowed to hinder a free-falling control rod from reaching its bottom depth in the reactor core or from forcing a control rod up without re-coupling to the CRDM.
- During return to normal operations, the System shall require deliberate operator actions to reset the reactor trip actuations.
- Recoupling of the control rods to their respective CRDMs via re-energized electromagnets by the trip circuit(s) shall only be allowed if all trip signals are cleared for that reactor.
- The System shall monitor reactor pool level and trip the respective reactor when coolant level is too low to ensure protection against radiological release.

7.5.3 System Description

The VIPR reactor protection system is designed to protect against unsafe reactor operation during steady state and accident conditions. The system initiates selected protective functions to mitigate the consequences of design-basis events and accidents, and to safely shut down the plant by either automatic means or manual actions. Changes to the normal operation of the reactors are monitored,

excursions that approach any predefined safety limit due to abnormal demands, system or component malfunctions, or accidents (as discussed in Chapter 13) cause the system to shut down the respective reactor.

The protection channels and protective responses are sufficient to ensure that no safety limit, limiting safety system settings, or reactor safety system limiting condition for operation will be exceeded. The system design ensures that the design bases can be achieved, and that the system can be readily tested and maintained in the designed operating condition.

The RPS consists of a digital controls platform which can initiate the instantaneous drop of the reactor control rods (reactor trip) by interrupting power to their electromagnets should a monitored parameter exceed a predetermined value. Neutron flux monitoring channels may be considered part of the RPS or may trip the reactor separately. A reactor scram may also be initiated manually by pressing a push button on the reactor control console.

7.5.3.1 Digital Safety System Qualified Platform

The safety systems will be based on a digital controls platform consisting of a set of commercial-grade hardware and pre-qualified digital components. The platform has been approved by way of a Safety Evaluation Report on the platform's qualification Topical Report by the NRC. Any additional testing required to satisfy the platform's qualification envelope coverage as applied to the unique environment of the facility will be managed by AAI's QA program.

7.5.4 System Reliability and Availability

Single failure criteria (Section 7.5.4.1) and independence (Section 7.5.5) are designed into the RPS to assure that (1) no single failure results in loss of protection function coverage and (2) controlled removal from service of selected components and channels does not result in loss of the required minimum redundancy to ensure performance of the safety function.

7.5.4.1 Single Failure Criteria

Supported by the safety analysis of Chapter 13, the inherent safety design of the VIPRs introduces negligible risk to the safety of the public and environment; therefore, single failure criteria is not required to be met on a regulatory commitment basis. However, due to the commercial needs of the facility of continual uptime of the reactors, the I&C protective functions are conservatively designed so that any single failure, while a function is in bypass, shall not prevent protective actuation at the system level. Field devices (sensors, actuators, and displays) and related communications lines which are relied on for safety will be at-minimum dual-redundant.

Each facility safety parameter will be monitored by triple-redundant sensors using two-out-of-two (2oo3) coincidence trip voting logic. Each sensor is monitored by dual-redundant RPS divisions using two-out-of-two (2oo2) coincidence logic during normal operation. Refer to Section 7.5.13.4 for more information on how bypassing channels affects redundancy. Refer to Section 7.5.11, Design Basis , for a list and description of protective functions required by accident analysis.

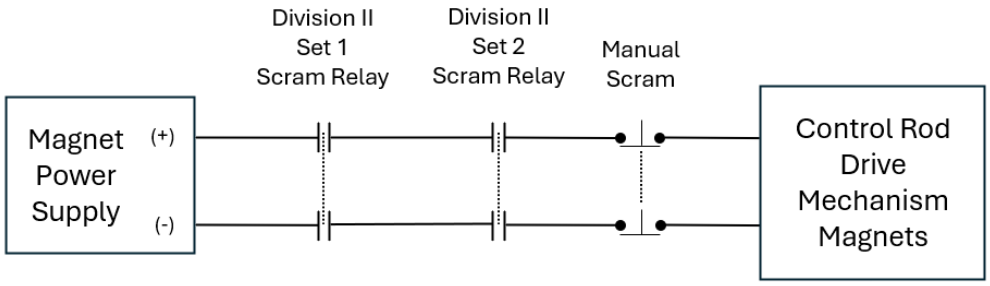

Figure 7-4: VIPR Scram Circuit

7.5.4.2 Architecture Redundancy

The reactor protection system will meet single failure criterion using fault-tolerant modules within dual-redundant, diverse, and independent divisions, each sensing the triple-redundant pairs of safety-related sensors. Each division is individually capable of actuating all protective functions of any VIPR by receiving protective function sensor inputs from all VIPRs and sharing the processed signals with the other division. This protects against a single failure or anticipated operational occurrence preventing the requisite safe shutdown of one or multiple VIPRs. The communication of processed data and protective function coincidence voting will employ isolation and communication safety protocols. Sharing of protective system data and functions will not significantly impair their ability to perform protective functions, including, in the event of an accident in one division, a safe shutdown of the remaining VIPRs performed by the other divisions.

Figure 7-5 represents the RPS architecture for a single VIPR, a single sensor of the VIPR, and the trip circuit of the single VIPR. In total, this dual-redundant architecture will cover four VIPRs, with dual-redundant sensors per VIPR, and one trip circuit per VIPR.

[ ]PROP, ECI

Figure 7-5: Dual division RPS architecture

7.5.4.3 Protective Function Parameter Redundancy

Table 7-1: RPS Monitored Parameters (per VIPR) lists the parameters which must be monitored by the RPS to perform the protective functions for a single VIPR as required by the accident analysis of Chapter 13. To meet single failure criterion while maintaining the ability of online surveillance testing, each of these parameters must be monitored by triple redundant sensors for each VIPR. VIPRs' sensors are monitored by dual-redundant RPS divisions.

Table 7-1: RPS Monitored Parameters (per VIPR)

RPS Parameter (per VIPR)	Sensor
Reactor pool coolant level *Reference section(s) 7.2.4.1; 7.2.4.2; 7.2.8.3; 7.2.10.1*	Float switches #1-3
Primary coolant loop inlet temperature *Reference section(s) 7.2.4.6; 7.2.6; 7.2.8.1; 7.2.8.3; 7.2.10.1*	Thermocouples #1-3
Primary coolant loop flow *Reference section(s) 7.2.4.6; 7.2.6; 7.2.8.1; 7.2.8.3; 7.2.10.1*	Flow meters #1-3

Table 7-2 lists the parameter(s) which must be monitored by the NFM to perform the protective functions for a single VIPR as required by the accident analysis of Chapter 13. To meet single failure criterion while maintaining the ability of online surveillance testing, each of these Parameters is monitored by an independent channel and detector.

Table 7-2: NFM monitored parameters (per VIPR)

NFM Parameter (per VIPR)	Channel 'A' Detector / Channel	Channel 'B' Detector / Channel	Channel 'C' Detector / Channel
Reactor power level *Reference section(s) 7.2.2.2; 7.2.2.3; 7.2.2.7; 7.2.8.1; 7.2.8.3; 7.2.10.1*	Compensated ion chamber / WR Linear channel	Uncompensated ion chamber / Safety channel	Fission chamber / WR log channel
Change of rate of reactivity *Reference section(s) 7.2.2.1; 7.2.8.3; 7.2.10.1*	Fission chamber / SR channel	none	none

Table 7-3 lists the components actuated by the RPS channels which ensure safe shutdown of reactor power for each VIPR. To meet single failure criterion while maintaining the ability of online surveillance testing, each of these components must be actuated by dual redundant devices for each VIPR. VIPRs' devices are actuated by the dual-redundant RPS divisions.

Table 7-3: Actuations (per VIPR)

Actuation	Division 'A' Component	Division 'B' Component
RPS de-energize trip circuit	Relay #A1 & Relay #A2	Relay #B1 & Relay #B2
Drop control rod assemblies	Control Rod CRDMs #1, #2, #3, & #4	

For a description of how single failure criterion is applied to online surveillance testing refer to Section 7.5.4.1, Single Failure Criteria.

7.5.4.3.1 *Electrical Redundancy*

Dual-redundant power to the RPS will be supplied by two physically independent circuits which each powering a division so that electrical fault or loss of power ensures at least one division remains operable.

7.5.4.4 Defense-in-Depth and Diversity

The I&C architecture design includes the principles of diversity and defense-in-depth for protective functions to ensure digital common-cause failure, and single point vulnerabilities do not prevent systems from executing protective functions. When a vendor's qualified digital platform for safety controls is selected, AAI will evaluate any defense-in-depth and diversity gaps and vulnerabilities of common-mode failures inherent to the selected technology to determine the safety layers and reinforcing mitigations to apply.

7.5.4.4.1 *Monitoring for Defense-in-Depth*

The primary design basis event is damage to the fuel cladding in the reactor core. Multiple parameters which have been analyzed to contribute to the risk of fuel cladding damage will be monitored. The depth of defense by I&C systems covers reactor power level, coolant level, coolant flow, coolant temperature, and operator action. Refer to Section 7.5.11, Design Basis , for a complete list and description of protective function monitored parameters.

7.5.4.4.2 *Diversity of Reactor Protection Divisions*

Depending on the digital safety controls platform selected, the RPS may use functional diversity (the implementation of different programming methods and logic design) and technological diversity (the implementation of varying computer chips or vendor platforms) to mitigate common mode failures and digital common cause failures.

7.5.5 Independence

Independence criteria include electrical, physical, communication and functional separation to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in the propagation of loss of protective functions. Electrical independence is designed among the RPS divisions and between the non-safety SSCs which interface with the RPS.

All VIPRs will share the redundant RPS divisions. Each RPS division monitors and actuates on other VIPRs, increasing single failure reliability. This provides multiple, independent protective functions for each monitored parameter where one system fault does not affect the protective functions of another channel. **See Figure** 7-3 for RPS inter-division communication.

Each VIPR has its own set of analog-based, triple-redundant nuclear instrumentation channels independent from the RPS controller divisions that monitor reactor power and provide direct trips to the trip circuit. Redundant field sensors shall be wired to independent modules within each RPS division.

The capability to independently test channels is described in Section 7.5.6.1, Manual Surveillance Testing.

Communication independence constraints among safety systems and with non-safety systems is described in Section 7.3.6.2, Digital Communications.

7.5.5.1 Isolation & Separation Criteria

Isolation devices are used to maintain electrical independence of divisions, and to prevent the non-safety system communications from affecting the safety system. These devices may be installed between systems or internal to the safety component; both configurations maintain independence among redundant channels and between safety and non-safety components which prevents faults from propagating among and between sub-systems. This includes the use of fiber-optic communications lines.

Each division of the RPS will be contained in a separate cabinet from the other division and from other control systems with separate, dedicated power supplies. RPS instrumentation will have adequate physical and electrical separation in the field and control room panels from non-safety instrumentation.

Each RPS division will communicate with shared field sensors of the other redundant RPS division. Isolation will be designed into the interfaces so that no electrical or communications fault can propagate through field devices among divisions.

7.5.6 Diagnostics & Surveillance Testing

7.5.6.1 Manual Surveillance Testing

As described in Section 7.5.1, the reactor protection system is designed to permit periodic testing of its functions during reactor operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. To support the commercial requirements for continuous reactor operation, all protective functions are designed for online testing while the reactor is at power.

The RPS design maintains compliance with single failure criteria during surveillance testing through the implementation of dual-redundant divisions. This architecture ensures that protective functions remain available and reliable throughout testing activities without compromising reactor safety.

7.5.6.2 Maintenance & Testing Bypasses

Bypass Configuration and Logic

Each protective channel within a division can be independently bypassed, with the exception of operator manual reactor trip functions. When a protective channel is placed in bypass, the remaining three divisions automatically reconfigure to operate under 2-out-of-3 (2oo3) coincidence voting logic until the bypassed channel is restored to service. This configuration maintains the single failure criterion requirements for the safety-related RPS throughout the bypass period.

Bypass Limitations and Controls

Maintenance procedures establish specific criteria governing bypass operations. The system enforces the following restrictions:

- Only one protective function of each monitored safety-related parameter type may be bypassed or tripped simultaneously
- If multiple protective functions of the same parameter type are tripped or bypassed concurrently, the system will automatically trip all Variable Impedance Power Regulators (VIPRs) that depend on that protective function type

Administrative controls prevent operators from bypassing the same safety channel across multiple divisions simultaneously. These controls are essential to maintaining single-failure criterion compliance, as simultaneous bypasses of identical channels could compromise the required redundancy.

Bypass Implementation

The bypass capability operates through software commands that remove a single protection channel from service while preserving dual redundancy and system availability. The resulting operable channels satisfy RPS single-failure criteria during bypass conditions. Importantly, the bypass function does not require physical modifications to the installed equipment, such as wire disconnections, jumper installations, or other hardware alterations.

7.5.6.3 Component Testing and Inspections

During reactor operation, the demonstrated reliability of shutdown actuation systems depends on successful completion of comprehensive, overlapping tests performed on RPS components. The testing program encompasses both automated diagnostics and manual surveillance activities to ensure continued system functionality.

Input and output field instrumentation within RPS channels requires regular surveillance testing and inspection beyond the built-in self-testing diagnostics. Field devices that directly execute protective functions are implemented with dual redundancy, enabling online troubleshooting and channel bypassing without reactor shutdown.

Administrative controls govern the placement of individual channels into bypass status, requiring that redundant channels providing identical protective functions remain operational throughout the bypass period. This approach ensures continuous protection while enabling necessary maintenance and testing activities.

The overlapping nature of these testing programs, combined with the inherent redundancy of the RPS design, provides high confidence in system reliability and availability for reactor protection functions during all operational modes.

7.5.6.4 Bypassed or Inoperable Status Indication

The Meitner-1 I&C systems will have the capability to permit testing of bypassed functions during operations. When the safety function is removed from service, either in bypass or trip, an alarm in the main control room and other operating stations informs the operator of bypassed or inoperable status indications for the reactor protection system.

7.5.6.5 Automatic Self-Testing

The Meitner-1 digital I&C systems will perform automated diagnostic and supervisory functions to continuously monitor the system for operational faults. Diagnostic functions monitor system operation and report faults of monitored functions to operators in the control room in addition to recording the fault events in digital storage.

7.5.6.5.1 Credited Diagnostics

Atomic Alchemy will select a digital controls platform with full-coverage diagnostic capability and will credit such diagnostics for maintaining system health and increasing the reliability of facility safety. Self-diagnostics capabilities of such a platform perform active monitoring to detect system I&C system issues. Most of the credited diagnostics will be provided from:

- Embedded in an off-the-shelf (OTS) product
- Available as an add-on to an OTS product
- Available as a free-standing product

The Meitner-1 diagnostics criteria include:

1) Built-in self-testing of control platforms.
   - Portable workstations may be connected to I&C equipment to retrieve diagnostic information, perform troubleshooting, and make configuration changes (in a safe, controlled state).
2) Configurable diagnostics to cover all detectable faults in the architecture.

7.5.6.5.2 OTS Built-in Diagnostics

I/O modules will be configured to calibrate analog inputs and outputs. Alarm and warning values for inputs will also be set for analog and digital inputs. Fail-state outputs to controlled field devices will be established. Controlled devices will be placed in a pre-programmed, alarmed fail-state if communication between other controllers and the I/O modules is interrupted.

7.5.6.5.3 Configurable Diagnostics

Online diagnostics will include (but are not limited to) the following capabilities:

- Analog input health monitoring (signal quality)
- Controller time synchronization monitoring (compared to system time)
- Hardware watchdog timers that detect failures that disrupt controller instruction execution

- Control algorithm execution task monitoring
- Monitoring of tasks critical to enabling the operator to supervise processes
- Divide by zero error detection
- Program execution infinite loop monitoring
- Communication monitoring and failover to alternate communications paths
- Detection and correction of single-bit memory errors not induced by hardware failures
- Detection and report of uncorrectable hardware single-bit memory errors
- Controller failure on multi-bit hardware memory errors

7.5.7 Reactor Trip Function

The reactor trip function has one objective which is intentionally kept as simple as possible for maximal reliability – to initiate the trip of the reactor core when critical parameter limits are crossed. The primary objectives of the reactor trip function are to actuate protective functions via safety end devices and communicate safety critical data and alarms to operators to help mitigate the consequences of accident conditions.

The reactor trip function monitors process parameters such as primary coolant flow and temperatures. Upon coincidence that multiple, redundant, directly measured process parameters or calculated parameters exceed setpoints, the reactor is shut down to protect against damage to the fuel cladding or loss of system integrity that could lead to the release of radioactive fission products.

7.5.8 Neutron Flux Monitoring

The NFM function provides the spectrum of neutron flux measurement from reactor full power level in a potentially harsh environment. It is designed to measure neutron flux with the detector in high gamma radiation and electrical noise environment. Each channel consists of a detector assembly near the core, qualified interconnecting cables, an amplifier assembly, and signal processing.

The NFM provides critical, trip actuation input data to the reactor protection system; as such, it will be qualified to the same level of rigor. Due to reliability concerns of inter-system communication and signal conversion faults, the reactor protection system and neutron flux monitoring function will be designed, created, and installed as one system. The NFM also provides reactor power levels to the FCS to support automatic power level regulation and operator stations for monitoring.

The NFM consists of independent, diverse channels to measure neutron flux in the reactor and to initiate protective action for specific conditions. The system consists of a source range and logarithmic channel, a wide-range linear channel, and a power channel. Their ranges overlap sufficiently to accurately monitor reactor power (neutron flux) from a few neutrons per second up to twenty megawatts.

7.5.8.1 Logarithmic Channel

The logarithmic (log) channel consists of a fission chamber, a preamp, amplifier, log meter, and neutron rate counter.

The channel contains two overlapping instruments. The low-range monitor provides source range power level by converting pulses from the fission chamber to a logarithmic power indication. The high-range monitor provides wide range power level by converting detector current to a logarithmic power indication. The instruments overlap to provide continuous indication. Although capable of providing indication over the entire range of steady state operation, the unit functions primarily as a start-up channel providing low power indication and providing necessary low power interlocks.

The source range channel employs a rod withdrawal inhibit interlock if count rate is <2 cps or $>9\times10^4$ cps. The <2 cps inhibit ensures that there is sufficient subcritical reactivity taking place and that sufficient counts are being measured to accurately indicate the fission rate in the core. The $>9\times10^4$ cps inhibit ensures the channel is not saturated by an excessively high-count rate.

The wide range log channel provides reactor power monitoring from source to power range levels. It combines the wide operating range of the log-based scales with the accuracy of a linear scale to provide accurate power measurement from milliwatt levels to full reactor power. The channel produces a reactor trip when reactor power exceeds a reactor power level high setpoint defined in the FSAR. It also provides calculated reactor period, which can produce a trip when reactor period is less than the number of seconds defined in the FSAR and not bypassed.

7.5.8.2 Wide Range Linear Channel

The wide range linear channel consists of a compensated ion chamber, a high voltage, a low voltage, and compensation voltage power supplies, and signal-processing circuits. The channel measures reactor power using multiple scales to provide wide range data during the approach to full power. It also provides input to the serve controller for automatic power control. See Section 7.4.3.4 for more information on automatic reactor power level control.

7.5.8.3 Safety Channel

The safety channel offers a diverse power level trip in addition to the logarithmic channel. This channel consists of an uncompensated ion chamber, signal processing circuits, and an external high-voltage power supply. It provides indication of power beginning at approximately 10 kW and produces a reactor trip when reactor power exceeds a reactor power level high setpoint defined in the FSAR.

7.5.9 Seismic Monitoring Function

The seismic monitoring must be kept operational during all modes of facility operation including administrative programs, maintenance, and repair procedures.

The safe shutdown system uses seismic monitoring instruments mounted to the building's foundation to monitor facility seismic activity. Upon detection of seismic activity exceeding the analyzed safety setpoint, a command is sent to trip the reactor and to bring the facility to a safe shutdown state.

7.5.10 Primary Coolant Monitoring Function

The primary coolant monitoring function monitors relevant-to-safety reactor coolant parameters that indicate a DNB and/or overstressing the reactor coolant system boundary. Reactor pool level is also credited with radiological confinement. Considerations such as light water pool level, temperatures,

RCS pump pressures and other reactor coolant system operating limits are monitored for protective action.

7.5.11 Design Basis Protective Functions

The following protective function trips are based on the accident analysis of Chapter 13.

7.5.11.1 Reactor Power Trips

Neutron Flux Monitoring Overpower Trip**:** High neutron flux trips the facility when the reactor power exceeds the high limit setpoint. The trip protects against excessive core power generation during normal operation and is active whenever the reactor is powered on.

Rate of Reactivity Trip**:** Rate of neutron flux change is calculated and trips the facility when a high rate setpoint is reached. The trip protects against maximum rate of reactivity insertion, 69 pcm/s (0.10 $/s).

7.5.11.2 Coolant Trips

Reactor Pool Coolant Level, Low Trip**:** This trip serves two functions in the event of low light water pool level: 1) to protect high fuel assembly temperature from damaging the fuel cladding, and 2) to ensure adequate dissolving of any escaped radionuclides. The function trips the reactor if level sensors at the pool's surface detect low coolant level.

Primary Coolant Flow, Low Trip**:** This trip protects the core from inadequate cooling. The function trips the reactor if the flow sensor(s) in the primary coolant loop detect a low rate of coolant flow.

Primary Coolant Loop Temperature, High Trip: The pool overtemperature ΔT trip protects high fuel assembly temperature from damaging the fuel cladding. The function trips the reactor if the temperature sensor(s) at the inlet of the primary coolant loop detects a high temperature.

7.5.12 Additional Protective Functions

The following protective function trips are **not** based in the accident analysis of Chapter 13.

7.5.12.1 Reactor Startup Trip

Source Range Neutron Flux, High Trip**:** High neutron flux trips the reactor when the source range channel exceeds the high limit setpoint. This trip provides protection during reactor startup and planned reactor shutdown. This function is delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious trip due to the short-term instability of the processed source range values.

7.5.12.2 Manual Reactor Trip

Manual Operator Trip**:** The manual operator trip command consists of two command controls per reactor in the main control room which act directly on the trip circuit breakers of the respective reactor.

7.5.12.3 Safeguards Trip

Reactor Trip on Protection System Actuation**:** A reactor trip is initiated with any signal that causes a facility safeguards actuation. This reactor trip occurs whether the safeguards actuation is commanded automatically or manually. This trip protects the core against adverse fuel conditions such as seismic activity, fire detection and high area radiation levels.

7.5.13 Reactor Trip Fail-safe Actuations

The reactor protection system is designed with de-energized-to-trip output signals. Any postulated adverse event that causes the reactor protection system to shut down or go offline will simulate a trip signal.

7.5.13.1 Trip Circuit

Each reactor is protected by redundant high-power circuit breakers connected in series capable of removing power from the control rod-affixed electromagnets. Once at least one of the redundant trip commands is actuated, the circuit breakers open dropping the control rods into the reactor core. Once the power to the magnets has been interrupted by a scram demand, a lockout circuit ensures that the current cannot be restored until the reactor operator manually resets the trip circuit. The trip circuit can only be reset and control rods re-coupled to the CRDMs if no trip signal is present.

7.5.13.2 Complete Loss of Electrical Power

The SSCs which execute I&C protective functions are designed so that a loss of power does not prevent prompt protective actions. Power loss to the following SSCs which are relied on for protective functions will initiate a trip of the reactor by other powered SSCs: NI channels including power displays relied on for manual trip, the RPS, any diverse actuation functions of the FCS, and the control rod electro-magnets. If all SSCs lose power, the RPS in combination with the control rod electro-magnets are designed as de-energize-to-trip.

7.5.13.3 Reactor Trip Bypasses

A number of bypasses will be developed for the FSAR to allow certain heavily controlled activities to occur that would otherwise cause a reactor trip. A non-exhaustive list of bypasses which may be developed include the following:

- Neutron flux above Intermediate Range setpoint
  - Allow manual block of source range reactor trip.
- Neutron flux below Intermediate Range setpoint
  - Automatically reset source range reactor trip.
- Reactor Power Range above setpoint
  - Allow bypass of power range (low setpoint) reactor trip.
  - Allow bypass of intermediate range reactor trip.
  - Automatically bypass source range reactor trip.
- Reactor Power Range below setpoint
  - Reset bypass of power range (low setpoint) reactor trip.
  - Reset bypass of intermediate range reactor trip.

- Allow manual reset of each source range channel reactor trip.
- Bypass reactor trip on low coolant flow.
- Bypass reactor trip on low reactor coolant pump speed.

7.5.14 Significant Monitored Parameters

Refer to Chapter 7, Appendix A for a list of significant parameters which the system will monitor for each VIPR.

7.6 THE ENGINEERED SAFETY FEATURE SYSTEM

AAI does not expect to implement automatic engineered safety feature actuations. The accident analysis of Chapter 13 showed no design basis need for I&C systems to perform an automatic engineered safety action.

7.7 OPERATIONS CONTROLS & DISPLAY SYSTEM

Control console and display instrument systems and equipment include displays for the reactor operator to view such operating information as current values of operating parameters and the status of systems and equipment. The system also enables the operator to control the reactor.

The operator uses safety displays to monitor and maintain the safety of the facility over the entire range of expected and anticipated operating conditions. Parameters will be analyzed and identified to establish the appropriate design bases and qualification criteria employed by the operator for monitoring conditions vital to maintaining the facility in a safe condition.

7.7.1 Design Criteria

Per the accident analysis of Chapter 13, no operator actions are necessary for a minimum of 72 hours following a design basis event. This includes no need to immediately ensure reactivity control, core heat removal, or reactor confinement control. Return to normal after a trip requires deliberate operation actions and cannot be reset while a trip command signal remains active.

7.7.2 Design Basis Requirements

- The system shall provide controls and displays to operate the nuclear reactor units safely under normal conditions and to maintain them in a safe condition under accident conditions, including loss of coolant accidents.
- The system shall monitor facility parameters over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those parameters and systems that can affect the reactor, the integrity of the reactor core, the spent fuel, the reactor coolant boundary, and the confinement boundaries and its associated systems.
- Appropriate controls shall be provided to maintain these parameters and systems within prescribed operating ranges.

- The system shall include controls at appropriate safe locations outside the control room which provide the capability for prompt shutdown of all the reactor units, including the necessary instrumentation and controls to maintain the facility in a safe shutdown condition indefinitely.
- The system shall require deliberate operator action to reset a trip and shall not allow reset while a trip command signal remains active.
- The system shall maintain digital records of timestamped process parameters for post-event analysis.

7.7.3 System Description

The operator controls and indication system (CIS) provides manual controls from which the operator can command specific activities of the VIPR. Indications allow the operator to monitor safety and non-safety parameters throughout the facility. These indications will be a combination of analog alarm indications and digital process visualizations.

The HSI components reside at the operator stations within the main control room. The number of operator stations in the control room will be defined in the FSAR.

The manual controls of the CIS primarily provide the operators with the ability to manually manipulate control and regulating rod height and individual or total trip of VIPRs. Secondary controls include adjusting process setpoints such as reactor coolant pump speed and valve positions.

The displays of the CIS primarily indicate reactor power levels, fuel assembly temperature, and facility alarms. Secondary displays include control and regulating rod positions, coolant flow speed, and pool level. Displays will be located adjacent to related manual controls if available.

7.7.3.1 Safety Parameter Displays

The safety critical display information is used by the operator to maintain the safety of the facility throughout operating conditions including anticipated operational occurrences and accident and post-accident conditions. Safety critical information will be displayed via highly reliable, qualified analog alarm annunciators and simple digital displays. These displays will be positioned at the center of the operator’s station to attract the majority of the operator’s focus.

7.7.3.2 Facility Data Displays

Non-safety facility process data will be displayed on digital screens which are an extension of the FCS. These displays will not be relied on for safety critical operator action and therefore will not be positioned as prominently as the alarm displays.

7.7.3.3 Manual Initiation of Protective Action Functions

Operators can manually initiate actuation of protective functions from the main control room. Once the protective function is actuated, the protective components move to a safe state. Upon removal of the system-level actuation, the facility components remain in their safe state until they are manually restored to a known baseline state by intentional operator action.

The manual actuations of protective functions are diverse actuations from the RPS initiated functions. The actuations are implemented from hard-wired controls located at the operating stations to the

protective field instruments, and do not interact with the application logic processing components of any I&C systems.

7.7.4 Significant Monitored Parameters

Refer to Chapter 7 Appendix A for a list of significant parameters which the system will monitor for each VIPR.

7.8 RADIATION MONITORING SYSTEM (RMS)

Radiation monitoring instruments detect radiation levels in critical areas in the facility and alert data to operations to help in the control of personnel radiation exposure and monitor the release of radioactive material within the facility.

7.8.1 Design Criteria

7.8.2 Design Basis

- The system shall monitor facility parameters over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those parameters and systems that can affect the reactor and target handling processes, the integrity of the reactor core, the spent fuel, the reactor coolant boundary, and the confinement boundaries and its associated systems.
- Appropriate controls shall be provided to maintain these parameters and systems within prescribed operating ranges.
- The system shall detect conditions that may result in excessive radiation levels.
- The system shall detect conditions in the reactor confinement and associated handling areas that may result in the loss of residual heat removal capability and excessive radiation levels.
- The system shall monitor the reactor confinement and radwaste modules atmosphere, spaces containing components for recirculation of loss of coolant accident fluids, effluent discharge paths, and the facility environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from design basis events.

7.8.3 System Description

The RMS primarily protects personnel from excessive radiation levels and mitigates release of radiation to the outside environment. The system indicates radiation intensity to reactor operations personnel to indicate the following: the need to actuate confinement systems; the need for personnel radiation protective actions; and the release of radioactive material to the environment. The system includes area radiation monitors, with displays near the instrument location and in the control room. The RMS monitors radioactive effluents to provide continuous air monitoring for airborne radioactivity in occupied spaces such as the reactor room. Portable radiation monitors and personal dosimetry systems are outside of the scope of I&C. This chapter coordinates with the basis for radiation protective instruments and measures as discussed in detail in Chapter 11, “Radiation Protection Program and Waste Management.” The objective of the radiation monitoring function is to provide

Meitner-1 facility control room operators with a continuous record and indication of radiation levels at locations where radioactive materials may be present, stored, handled, or inadvertently introduced.

The RMS monitors area radiation in the reactor confinement area, fuel storage area, and radwaste handling area for personnel protection and general surveillance. This includes the ventilation systems of each module building where a high radiation signal in a ventilation path closes the isolation damper or valve. The area monitor alarms locally and at each operator station. The system also uses portal monitoring for radiation in the reactor auxiliary module room.

Each RMS area installation has two setpoints – warning and alarm. A warning generates an annunciation on the control console to notify the operator of a potential problem. An alarm will automatically initiate evacuation. Appendix A details which parameters can initiate alarms, reactor trips, or both; warnings are not included in this listing.

7.8.4 Significant Monitored Parameters

Refer to Chapter 7, Appendix A for a list of significant parameters which the system will monitor for each VIPR.

Table 7-4 lists the parameter(s) which must be monitored by the RMS to perform the protective functions for a single VIPR as required by the accident analysis of Chapter 13. To meet single failure criterion while maintaining the ability of online surveillance testing, each of these parameters is monitored by an independent channel and detector.

NMS Parameter (per VIPR)	Channel 'A' Detector	Channel 'B' Detector
Pool radiation level *Reference section(s) 7.2.3.1*	Pool Radiation Monitor #1	Pool Radiation Monitor #2

Table 7-4: RMS Monitored Parameters (Per VIPR)

7.9 REFERENCES

Nuclear Regulatory Commission (NRC). 1996. NUREG-1537, Part 1, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content."

Nuclear Regulatory Commission (NRC). 2012. ISG to NUREG-1537, Rev. 0, "Final Interim Staff Guidance Augmenting NUREG-1537, Part 1, 'Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Format and Content,' for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors."

7.10 APPENDICES

Appendix A: I&C Monitored Parameters for an Individual VIPR

CHAPTER 7 – APPENDIX A
MONITORED PARAMETERS FOR AN INDIVIDUAL VIPR

I&C Monitored Parameters for an Individual VIPR

Facility Parameter	Instrument	I&C System/Channel	Alarm	Trip
Control Rod Assembly #1 Speed	Speed Sensor	Facility Control System	X	
Control Rod Assembly #2 Speed	Speed Sensor	Facility Control System	X	
Control Rod Assembly #3 Speed	Speed Sensor	Facility Control System	X	
Control Rod Assembly #4 Speed	Speed Sensor	Facility Control System	X	
Regulating Rod Speed	Speed Sensor	Facility Control System	X	
Fire Detection (Facility)	*Determined in the FSAR*	Facility Control System	X	X
Secondary Coolant Flow #1	Flow meter	Facility Control System	X	
Secondary Coolant Flow #2	Flow meter	Facility Control System	X	
Tertiary Coolant Flow #1	Flow meter	Facility Control System	X	
Tertiary Coolant Flow #2	Flow meter	Facility Control System	X	
Reactor Power Level (Log)	Fission chamber	N.M. Log Channel	X	X
Reactor Power Level (Linear)	Uncompensated ion chamber	N.M. Safety Channel	X	X
Neutron Count Rate	Fission chamber	N.M. Source Range Channel	X	X
Reactor Period	Fission chamber	N.M. Source Range Channel	X	X
Reactor Power Level (Linear)	Compensated ion chamber	N.M. Wide Range Linear Channel		
Reactor Pool Coolant Level #1	Fluid Level Sensor	Reactor Protection System	X	X
Reactor Pool Coolant Level #2	Fluid Level Sensor	Reactor Protection System	X	X
Reactor Pool Coolant Level #3	Fluid Level Sensor	Reactor Protection System	X	X
Primary Coolant Loop Inlet Temperature #1	Thermocouple	Reactor Protection System	X	X
Primary Coolant Loop Inlet Temperature #2	Thermocouple	Reactor Protection System	X	X
Primary Coolant Loop Inlet Temperature #3	Thermocouple	Reactor Protection System	X	X
VIPR Gang Scram (all VIPRs)	Pushbutton	Reactor Protection System		X
Manual Scram	Pushbutton	Reactor Protection System		X
Primary Coolant Loop Flow #1	Flow meter	Reactor Protection System	X	X
Primary Coolant Loop Flow #2	Flow meter	Reactor Protection System	X	X
Primary Coolant Loop Flow #3	Flow meter	Reactor Protection System	X	X
Seismic Activity (Facility)	Seismic Monitor	Reactor Protection System	X	X
Pool Radiation Level #1	Radiation monitor	Radiation Monitoring System	X	
Pool Radiation Level #2	Radiation monitor	Radiation Monitoring System	X	