Enclosure 1

Changes to Hermes PSAR Chapter 7

(Non-Proprietary)

SSC Name	Safety Classification	Seismic Classification	Quality Program	SAR Section	Plant Area
Tritium Management System	Non-safety related	SDC-2	Not Quality-Related	9.1.3	SR and NSR areas
Inventory Management System	Non-safety related	SDC-2	Not Quality-Related	9.1.4	SR area
Instrumentation and Control Systems					
Reactor Protection System, including field sensors, cabinets and associated wiring except for Cabling to the RPS trip devices and manual reactor trip switches	Safety-related	SDC-3	Quality-Related	7.1 7.5	SR area
Cabling to the RPS trip devices and manual reactor trip switches	Non-safety related	SDC-2	Not Quality-Related	7.3	SR and NSR areas
Plant Control System, including field sensors, cabinets and associated wiring	Non-safety related	SDC-2	Not Quality-Related	7.2 7.5	SR and NSR areas
Main Control Room	Non-safety related	SDC-2	Not Quality-Related	7.4	Auxiliary Building
Remote Onsite Shutdown Panel	Non-safety-related	SDC-2	Not Quality-Related	7.4	SR area
Plant Auxiliary Systems					
Remote Maintenance System	Non-safety related	SDC-2	Not Quality-Related	9.8	SR and NSR areas
Fire Protection System	Non-safety related	SDC-2	Not Quality-Related	9.4	SR and NSR areas
Radioactive Waste Handling Systems	Non-safety related	SDC-2	Not Quality-Related	11.2.2	SR and NSR areas

CHAPTER 7 INSTRUMENTATION AND CONTROLS

7.1 INSTRUMENTATION AND CONTROLS OVERVIEW

7.1.1 Summary Description

The instrumentation and control (I&C) systems monitor and control plant operations during normal operations and planned transients. The systems also monitor and actuate protection systems in the event of unplanned transients. I&C is comprised of four parts, described in the bulleted list below. Each of the four parts are described in further detail in subsequent subsections of this chapter. The architectural design of the system accounts for interconnection interfaces for plant I&C structures, systems, and components (SSCs). Figure 7.1-1 provides an overview of the I&C system architecture.

- The plant control system (PCS) provides the capability to reliably control the plant systems during normal, steady state, and planned transient power operations, including normal plant startup, power maneuvering, and shutdown (see Section 7.2).
- The reactor protection system (RPS) provides protection for reactor operations by initiating signals to mitigate the consequences of postulated events and to ensure safe shutdown (see Section 7.3).
- The main control room and remote onsite shutdown panel provide the capability for plant operators to monitor plant systems, control plant systems, and to initiate plant shutdown (see Section 7.4).
- Sensors provide input to multiple control and protection systems (see Section 7.5).

The I&C system implements IEEE Standard 603-2018 (Reference 1) and IEEE Standard 7-4.3.2-2003 (Reference 2) and other consensus standards for safety-related I&C functions. The particular application of consensus standards is discussed for each I&C subsystem in the following sections.

The I&C system incorporates the principles of independence, redundancy, and diversity. Features reflecting those principles are discussed in the specific subsystem descriptions. The RPS is the safety-related system credited for tripping the reactor and actuating engineered safety features. Accordingly, the RPS is isolated and independent from the other I&C systems and uses input signals from independent instrumentation. RPS instrumentation signals are provided to the PCS via a data diode, which is a part of the RPS hardware platform (see Section 7.3.3). The RPS incorporates redundancy and diversity in the system design as discussed in Section 7.3. The I&C system includes the capability for both manual and automatic control.

Section 7.5 describes the sensors used at the facility. Sensors for temperature, pressure, neutron count rates, level, flow, radiation level, and other analog and digital field detectors provide input to the plant control system and reactor protection system. Independent instruments are provided for RPS and PCS. Each section about specific I&C subsystems includes a discussion of the instruments that support that subsystem and the type of instrumentation used (i.e., analog or digital).

7.1.2 Calibration of Trips, Interlocks, and Annunciators

Safety limits (or analytical limits (ALs)) are defined by the operating limits in the plant safety analysis.

Systems having significant safety functions (for example technical specification limiting conditions for operation) that do not directly protect a plant safety limit, will be analyzed in the same fashion as those having safety limits. The technical specifications are described in Chapter 14.

Setpoints for safety-related instrumentation will be calculated in accordance with the guidance of ANSI/ISA 67.04.01-2018 (Reference 3). The setpoint nomenclature as defined in the Regulatory Information Summary RIS-2006-17 (Reference 4), will be applied to setpoint calculations developed to support licensing activities. Operational considerations such as drift, linearity, hysteresis, and

operational margins are considered in the development of specific instrument loop setpoints. Consideration is also given to fixed instrument errors and environmental affects in the selection of instrument setpoints.

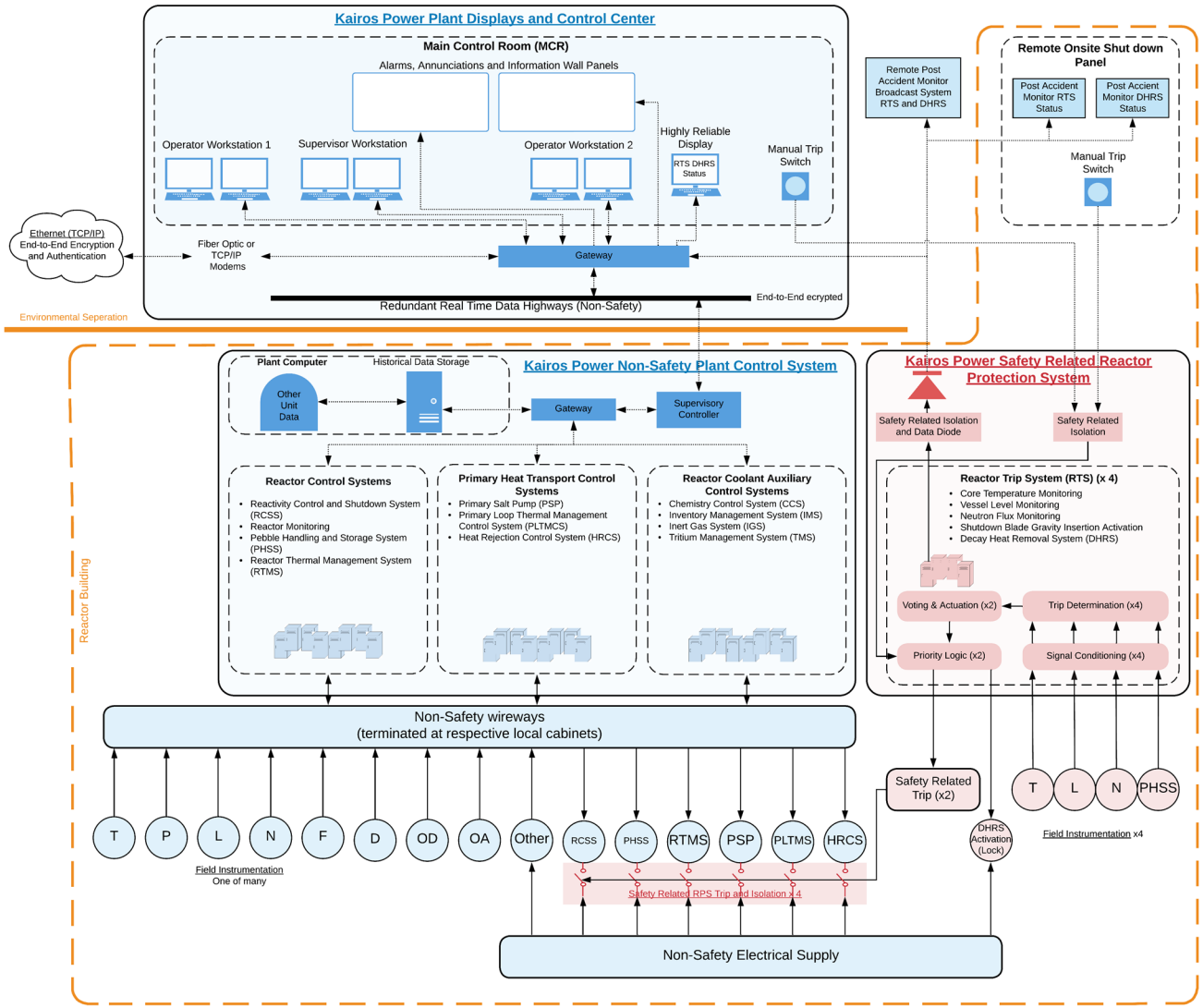
The ~~PCS and~~ RPS includes sensors, trips, and~~,~~ interlocks~~, and annunciations~~ to ~~monitor the operation of the process control systems~~shut down the reactor when operating parameters exceed operational limits. ~~For the RPS, t~~This includes release of the control and shutdown elements within a set of defined parameters after the onset of a postulated event. Specific trips and~~,~~ interlocks~~, and annunciations for each system~~ are discussed in Section~~s 7.2 and~~ 7.3. However,~~ for both systems, activation and~~ RPS actuation setpoints for trips and~~,~~ interlocks~~, and alarms~~ are calculated based on the following design principles:

- Simulation models: Time to reach operational limits based on system qualification (environments, process conditions, etc.) as demonstrated by actual empirical data collected during simulation testing
- ~~Control System~~RPS Technical Specifications: Measurement time, process parameters as informed by safety case assumptions and bounded by Technical Specification limits
- Mechanical design and testing - response time for actuation to complete: Time to detect, process, and actuate the required controls; this time should be less than the time between event onset and parameter reaching a limiting condition for continued operation
- Tiered (graded) approach to protection: ~~In all cases the PCS utilizes early detection monitoring of parameters that are non-safety related to inform risk for continued operation or trip status for investment protection.~~ The RPS utilizes highly reliable safety-related parameters as the final level of protection for public health and safety~~ as well as investment protection~~.
- ~~Annunciators are used to inform operations of the changing process parameters that will require system control response or potential operator intervention in order to maintain parameters within the normal operating envelope.~~

7.1.3 References

1. Institute of Electrical and Electronics Engineers, Standard IEEE 603, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations.” 2018.
2. Institute of Electrical and Electronics Engineers, IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations." 2003.
3. Instrument Society of America, ANSI/ISA-67.04.01, “Setpoints for Nuclear Safety-Related Instrumentation.” 2018.
4. Nuclear Regulatory Commission, Regulatory Issue Summary 2006-17, “NRC Staff Position on The Requirements of 10 CFR 50.36, ‘Technical Specifications,’ Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels.” August 24, 2006.

Figure 7.1-1: Instrumentation and Controls System Architecture



T Temperature

P Pressure

L Level

F Flow

N Neutronics

R Radiation Monitor

D Discrete (Digital Input of Output/Actuation)

~~A Analog (Modulating Output/Actuation)~~

OA Other analog field instruments

OD Other digital field instruments

7.2 PLANT CONTROL SYSTEM

7.2.1 Description

The PCS is a non-safety related control system which controls reactor startup, changes in power levels, and shuts down the reactor. The PCS implements these functions through a series of subsystems which include:

- Reactor control system (RCS)
- Reactor coolant auxiliary control system (RCACS)
- Primary heat transport control system (PHTCS)
- Primary heat rejection control system (PHRCS)

The PCS maintains plant parameters within the normal operating envelope. This system also provides data to the control consoles located in the main control room (see Section 7.4). Figure 7.1-1 shows the elements of the PCS.

The PCS is a microprocessor-based distributed control system that individually controls plant systems using applicable inputs. The subsystems listed above are integrated into the PCS using non-safety related signal wireways which are terminated at local cabinets and using redundant, non-safety, real time data highways.

The plantwide sensor inputs are used to verify interlock and permissive rules for the various plant states. The sensor data is also used to provide feedback and alarms to the operators via the control consoles. The PCS is powered by AC and DC power supplies which are discussed in Chapter 8.

The PCS uses non-safety related sensor inputs as well as safety-related sensor inputs from the plant protection system ~~via a data diode~~(See Section 7.3.3). The PCS includes the input parameters shown in Table 7.2-1. The sensors are described in Section 7.5. The instrumentation provides input signals using non-safety related signal wireways that are terminated at local cabinets.

Control outputs are generated using a control transfer function based on the sensor inputs and setpoints provided by the control system. The setpoints are adjusted automatically based on the plant operating mode, or in some cases by the operator via the main control room consoles. Plant operators do not directly control PCS outputs.

The PCS does not provide any safety-related functions during any mode of operation or postulated event. The PCS is electrically and functionally isolated from the safety-related RPS (see Section 7.3) using a safety-related isolation device as shown in Figure 7.1-1. The RPS isolation devices ensure electrical isolation between the electrical system and the non-safety related SSCs that PCS normally controls that are deactivated by the RPS when a reactor trip is demanded.

The subsystems of the PCS are described below.

7.2.1.1 Reactor Control System

The RCS controls and monitors systems and components that support normal operation, planned transients, and normal shutdown of the reactor. The RCS controls the systems listed in Figure 7.1-1 and supports the following capabilities:

- Reactivity control and planned transients/adjustments in power level
- Monitoring of core neutronics
- Pebble handling and storage
- Monitoring and control of temperature in the reactor

- Primary loop draining, filling, and piping monitoring, including PHTS external piping

The purpose of the PHTCS is to control the transport of primary coolant through the PHTS, to maintain the primary coolant in a liquid state, and to monitor the inventory of primary coolant in the PHTS. The PHTCS maintains the parameters in the PHTS within the normal operating envelope. The PHTCS controls the primary salt pump (PSP) and the primary loop auxiliary heating system. The sensors used by the PHTCS are discussed in Section 7.5.

The PHTCS provides control signal for the PSP (see Chapter 5). The control system manipulates the primary coolant flow rate by variable frequency to maintain PHTS parameters within the normal operating range. The PHTCS does not provide a safety function; however, as discussed in Section 7.3, the RPS trips the PSP on a reactor trip, as a protection feature for the reactor system related to the pump.

The PHTCS maintains the primary coolant in liquid phase throughout the PHTS to prevent localized over- or under-heating. The control system uses temperature as input to provide control signal to the PHTS auxiliary heaters.

7.2.1.4 Primary Heat Rejection Control System

The PHRCS controls and monitors systems and components that support normal operation of the intermediate loop which removes heat from the primary loop. The system supports the following capabilities:

- Control of the flow rate through the intermediate loop
- Intermediate loop heating
- Intermediate loop draining, filling, and piping monitoring

The purpose of the PHRCS is to control the transport of intermediate coolant through the intermediate loop, to maintain the intermediate coolant in a liquid state, and to monitor the inventory of intermediate coolant in the intermediate loop. The PHRCS does not perform a safety function. The PHRCS maintains the parameters in the intermediate loop within the normal operating envelope.

The PHRCS controls the intermediate salt pump (ISP), the intermediate loop auxiliary heating system, the intermediate coolant inventory system, the intermediate loop chemistry control system, the intermediate loop cover gas system, and the heat rejection blower. The PHRCS controls the ISP by changing the intermediate coolant flow rate by variable frequency to maintain intermediate loop parameters within the normal operating range. The PHRCS controls the intermediate loop auxiliary heating system to maintain the intermediate coolant in liquid phase throughout the intermediate loop to prevent localized over- or under-heating. The control system uses temperature information as input to provide control signal to the intermediate loop auxiliary heaters.

7.2.2 Design Bases

Consistent with Principal Design Criteria (PDC) 13, the PCS is designed to monitor variables and systems over their anticipated ranges for normal operation, and over the range defined in postulated events.

7.2.3 System Evaluation

The PCS is designed to monitor plant parameters and maintain systems within normal operating range. The PCS is also designed to control planned transients associated with anticipated operational occurrences and maintain the reactor in a shutdown state. These functions are consistent with PDC 13. The PCS does not perform a safety-related function. Finally, the PCS is designed so that it cannot interfere with the RPS's ability to perform its safety functions; see Section 7.3 for more information about the isolation of the RPS from the PCS.

The PCS is a digital system that controls the reactor power about a point set by the operator. The control system uses linear average temperature and flow rate in the primary system as variable inputs to control power level so that it remains within the normal operating envelope. The system design meets the applicable portions International Electrotechnical Commission (IEC) standard 61131 for industrial controllers (Reference 1), and the applicable portions of the cyber security standard IEC 62443 (Reference 2). Table 7.2-2 lists other standards applied to the PCS. Applicable portions of IEEE 1012-2017 (Reference 3) are used for verification and validation of PCS components, which is consistent with the non-safety related classification of the PCS.

Action in the PCS is designed to accurately and reliably provide control signal for all modes of normal operation. The PCS is also designed to provide timely control signals, with further analysis of timeliness to be provided in an application for the Operating License.

The PCS includes interlocks and inhibits that prohibit or restrict operation of the reactor and PHSS unless certain operating conditions are met. The following interlocks are included in the control system design:

- An interlock that prohibits reactivity control element withdrawal until there is sufficient neutron count rate to ensure that nuclear instruments are responding to neutrons.
- Interlocks are also provided related to startup power level and pebble handling as detailed in Table 7.2-3.

~~PCS actuation setpoints are established and calibrated using the method described in Section 7.1.2. The final design of SSCs controlled by the PCS affect the acceptance criteria to establish PCS actuation setpoints. Accordingly, the Operating License application will include a description of the acceptance criteria to establish and calibrate actuation setpoints or interlock functions, which will reflect the setpoint method described in Section 7.1.2.~~

The plant controls are grouped and located on a single operating panel in the main control room so that operators can easily reach and manipulate the controls. Displays of the results of operator actions are readily observable. See Section 7.4 for more information about the human interface for the PCS.

The PCS is not safety-related and no safety-related SSCs cross the seismic isolation moat, discussed in Section 3.5. However, any portion of the PCS that crosses the moat includes flexible design features to accommodate design displacements from postulated seismic events to the extent necessary to prevent damage of SSCs in the PCS from affecting a safety-related SSC's ability to perform its safety function. Specific design features and the SSCs to which they are applied, will be provided in the Operating License application.

Additional information about the PCS that is dependent on the final design of the reactor SSCs will be provided in the Operating License Application, including: (1) further specifics about the hardware and software, (2) software flow diagrams for digital computer systems, (3) a description of how the operational and support requirements will be met, and (4) the basis for reliability of PCS systems and reliability targets.

7.2.4 Testing and Inspection

Functional tests will be performed prior to initial startup and tests and inspections consistent with the standards discussed in Section 7.2.3.

7.2.5 References

1. International Electrotechnical Commission, IEC 61131, "Programmable Controllers." 2020.
2. International Electrotechnical Commission, IEC 62443, “Cybersecurity.” 2015

Table 7.2-3: Plant Control System Interlocks and Inhibits

Input Signal to the Plant Control System	Interlock or Inhibit
High radiation detected in pebble handling area	Movement of pebbles stops within a specified time delay *Purpose*: Minimize effects of a PHSS transfer line break
Abnormal positioning of pebble in PHSS	Movement of pebbles stops within a specified time delay *Purpose*: Prevent damage to PHSS system
Neutron Flux detected on Source Range and is below 0.5 count/second	Block reactivity control element withdrawal *Purpose:* Prevent inadvertent rapid positive reactivity insertion
DHRS operating	~~Reactor auxiliary heating system (RAHS~~RTMS~~)~~ blocked from operating *Purpose*: Prevent inadvertent actuation of ~~RAHS~~RTMS.

7.3 REACTOR PROTECTION SYSTEM

7.3.1 Description

The RPS provides protection for reactor operations by initiating signals to mitigate the consequences of postulated events and to ensure safe shutdown. The RPS is the only portion of the I&C system that is safety-related and that is credited for tripping the reactor and actuating engineered safety features. The purpose of the RPS is to actuate upon receipt of a trip signal in response to out-of-normal conditions and provide automatic initiating signals to protection functions. There are three possible trip sources that can cause the RPS to actuate and three protection functions that result from RPS actuation, shown below in Figure 7.3-1. The three possible trip sources are:

- Process variables reach or exceed specified setpoints, as measured by RPS sensors
- Manual initiation from the main control room or remote onsite shutdown panel
- Plant electric power is lost (with a time delay)

The three KP-FHR protection functions that result from RPS actuation are:

- ~~Activate~~ Actuate the RCSS that inserts control and shutdown elements into the reactor core
- Inhibit actions from the PCS so that it does not interfere with the functioning of the RPS
- Ensure ~~activation~~ an actuation of the decay heat removal system (DHRS) that passively removes heat from the PHTS to the atmosphere

Actuation of the RPS to trip the reactor includes several actuations that stop specific non-safety related SSCs, normally controlled by PCS, to ensure that those non-safety related SSCs to do not prevent a safety-related SSC from performing its safety function. The non-safety related functions that are stopped are shown in Figure 7.1-1. RCSS element withdrawal is inhibited after a loss of power, to prevent inadvertent positive reactivity insertion when power returns (see also Table 7.3-2). The PSP is stopped to maintain Flibe inventory in the core. ISP is stopped to prevent a pressure differential between the primary and intermediate systems. Pebble extraction and insertion in the PHSS is stopped to prevent removing pebbles from the core in the event of a PHSS extraction line break. Finally, RAHS actuation is prohibited to prevent a challenge to the heat removal capability of the DHRS. These inhibitions are accomplished through safety-related trip devices as shown in Figure 7.1-1.

The RPS is built on a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic implementation using discrete components and field programmable gate array (FPGA) technology. The RPS is isolated from other I&C systems, including the main control room and the remote onsite shutdown panel, using safety-related isolation hardware ~~gateways~~. Isolation is achieved at the point of signal generation either through features built into the hardware platform or through separate isolation devices. The RPS includes the following safety-related (except as noted otherwise) elements:

- Separate channels of sensor electronics and input devices
- Redundant and separate groups of signal conditioning
- Redundant and separate groups of trip determination
- Manual reactor trip switches in the main control room (switches are non-safety related)
- Safety-related components to provide electrical isolation from the non-safety-related highly reliable DC power system power supply
- ~~Power supplies for safety-related sensors and RPS components, which also provide isolation from the non-safety-related highly reliable DC power system power supply~~
- ~~Redundant voltage sensors for detecting loss of 120 VAC to the uninterruptible power supply system~~
- Multiple reactor trip devices and associated cabling (cabling is non-safety related)

- ~~Two non-safety related~~ RPS ~~gateways~~isolation hardware
- Two divisions of reactor trip system (RTS) voting and actuation equipment

Reactor trip functions are hardcoded into FPGA logic and are not dependent on plant operating state. Operating conditions are compared against the trip setpoints and actuate protection functions according to established programmable logic. The RPS cabinets are located within the safety-related portion of the Reactor Building within an environmentally separated enclosure, discussed further in Section 7.3.3.

The RPS performs safety-related functions as shown in Figure 7.1-1 which include RTS actuation and ensuring actuation of the DHRS. Both functions are described in more detail in Sections 7.3.1.1 and 7.3.1.2. Operator interface for the RPS is discussed in Section 7.4. The RPS uses inputs from the reactor core temperature, reactor vessel level, and source and power range neutron detectors. The sensors that provide input to the RPS are safety-related and described further in Section 7.5.

7.3.1.1 Reactor Trip System

The RTS ~~activates~~ actuates the RCSS that allow for insertion of control and shutdown elements into the reactor core. Upon receipt of a trip signal, the RTS removes power from coils on the reactivity shutdown elements which drop by gravity into the reactor (See Section 4.2.2 for more information about the shutdown elements). The RTS receives trip signals generated from automatic or manual sources.

The RTS is built on a logic-based platform that does not utilize software or microprocessors for operation. It is composed of logic implementation using discrete components and FPGA technology. The RTS is isolated from other I&C systems using safety-related isolation ~~gateways~~~~isolation~~ hardware.

The RTS receives input from sensors through hardwired, analog, safety-related signal wireways that are terminated at local cabinets. Section 7.5 provides additional information about the sensors that provide input to the RTS. Using the inputs from the sensors, the RTS automatically opens the reactor trip devices when setpoints are reached. The system uses both undervoltage coils as well as shunt trip coils to provide the means to open the trip devices. The reactivity shutdown element position coils fail open on loss of power.

The main control room and the remote onsite shutdown panel each have the capability to provide a manual trip signal to the RTS. Section 7.4 includes a discussion of the human interface with the RTS.

Table 7.3-2 provides a list of interlocks implemented for RPS systems. If normal power is not available and the RPS does not detect a transfer to backup power within a defined time period, the RPS removes power from the RTS, causing the control and shutdown elements to drop into the core. The RPS includes an interlock that inhibits movement of reactivity control elements, and a manual reset is required before reactivity control elements can be withdrawn. The purpose of this interlock is to prevent inadvertent insertion of positive reactivity when normal power is lost and subsequently restored.

On ~~activation~~actuation, the RTS will trip the PSP. A manual reset prevents the pump from inadvertently restarting after power return. To ensure positive pressure between the primary and intermediate coolant loops within the heat exchangers, the ISP trips concurrently with the PSP. An interlock prevents starting the ISP if the PSP is not running.

7.3.1.2 Decay Heat Removal System

The DHRS provides passive residual heat removal that requires no electrical power to operate, as discussed in Section 6.3. Although the DHRS is always operating above a certain threshold of fission product accumulation level, the decay heat removal portion of the RPS provides actuation signal to DHRS to ensure the DHRS is operating when there is a RPS actuation signal. The RPS actuation signal to

The RPS is designed with sufficient functional and component diversity to prevent the loss of function for the RPS.

- Upon loss of electrical power or detection of adverse environmental conditions, the RPS fails to a safe state, consistent with PDC 23.
- The RPS system functionally independent from the control systems, consistent with PDC 24.
- Consistent with PDC 25, the RPS is designed to ensure that radionuclide release design limits are not exceeded upon reactor trip actuation, including in the event of a single failure of the reactivity control system.
- Consistent with PDC 28, the RPS setpoints are designed to limit the potential amount and rate of reactivity to ensure sufficient protection from postulated events involving reactivity transients. The limits are set such that reactivity events cannot result in damage to the reactor coolant boundary greater than limited local yielding, and cannot sufficiently disturb the core, its support structures, or other reactor vessel internals to impair significantly the capability to cool the core.
- The RPS is designed to be redundant and diverse to assure there is a high probability of accomplishing its safety-related functions in postulated events, consistent with PDC 29.
- Consistent with 10 CFR 50.55(i), RPS is designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the safety function to be performed.
- Consistent with 10 CFR 50.55a(h)(3), the RPS is designed in accordance with IEEE Std 603-2018 (Reference 1). The RPS implements the 2018 edition of IEEE Std 603 as an alternative code to IEEE Std 603-1991 (Reference 2) and the correction sheet dated January 30, 1995.

7.3.3 System Evaluation

The RPS provides automatic reactor trip (1) if plant parameters exceed the normal operation envelope (PDC 20), (2) in the event of station blackout, and (3) manually using signal from the main control room or remote onsite shutdown panel. The RPS also ensures that the DHRS is running when the reactor trips. The RPS is consistent with 10 CFR 50.55a(h)(3) and NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” by meeting IEEE 603-2018. Table 7.3-1 provides a list of the consensus standards to which the RPS is designed.

Chapter 13 describes the postulated events to which the RPS is designed to respond. The RPS uses the same set of operating parameters in the trip and actuation logic for all modes of reactor operation. The setpoints are established to ensure that the design conditions of the reactor coolant boundary are not exceeded during operation within the design basis. This is consistent with PDC 25 because maintaining the reactor coolant boundary within design basis bounds will ensure that radionuclide release design limits are not exceeded. The setpoints are established and calibrated using the method described in Section 7.1.2.

Consistent with 10 CFR 50.55a(h)(3), reactor trips implemented by the RPS meet IEEE 603-2018, Section 4. The primary plant trip signal is based on average core temperature measurement. In addition, the plant will also have a trip signal for high flux rate based on input from the neutron detector sensors and a trip of the reactor upon detection of a break in the PHSS extraction line. When the temperature or flux rate are outside the normal operating range or when a PHSS extraction line break is detected, the primary plant trip deenergizes the RSS trip device, the DHRS loop trip device, and the PCS inhibitor trip device. Redundant trip devices are provided for each signal pathway. Note that the cabling to the trip devices is not classified as safety-related because the trip devices accomplish their safety function without reliance on the input cabling. However, the cables to the trip devices are designed to IEEE 603-2018.-See Figure 7.3-1 for a schematic of the RPS trip logic. Trip setpoints are established and calibrated using the methods described in Section 7.1.2. The PCS inhibitor trip device functionally isolates the RPS

from the PCS. This includes tripping the PSP, discussed in Section 7.2.1.3. The RPS also provides alarm signals to the main control room, which will be described in the Operating License application.

Consistent with PDCs 10, 15, and 20, the RPS provides reactor trip and decay heat removal actuation to ensure that the design conditions of the reactor coolant boundary are not exceeded during normal operation, including anticipated operational occurrences. With power, the RPS provides a trip actuation which opens a trip device, removing power from the reactor protection features (shut down elements and decay heat removal), as discussed in Sections 7.3.1.1 and 7.3.1.2. In the event that the RPS loses power, the RPS fails to a safe state, consistent with PDC 23. With loss of power, the RPS trip devices fail open, and power is removed from the aforementioned reactor protection features.

The reliability of the RPS is such that there is a high probability the RPS will accomplish its safety-related functions if a postulated event occurs, consistent with PDCs 22 and 29. No single failure results in loss of the RPS protective functions, consistent with PDC 21 and Section 5 of IEEE 603-2018. Specifics of the minimum redundancy in the RPS to permit periodic testing without compromising the function of the RPS will be provided in an application for the Operating License.

The RPS is functionally independent from the PCS, consistent with PDC 24 and Section 6 of IEEE 603-2018. The system does not share components with the PCS and takes inputs from separate, dedicated sensors. However, safety-related sensors that provide input to the RPS also provide signals to the PCS via a safety-related data diode that uses one-way fiber optic channels. -The data diode is integrated into the RPS hardware platform. Consistent with PDC 13, the system uses sensors that monitor variables and systems over their anticipated ranges for normal operation and for postulated event conditions. As discussed in Sections 7.3.1, the RPS uses as input core temperature and vessel level from safety-related sensors. The sensors are discussed in Section 7.5, including the range over which the sensors monitor reactor variables.

Consistent with PDC 3, the RPS is designed to perform its safety function in the event of a fire hazard. The RPS is designed and located to minimize the probability and effect of fires and explosions by the use of low combustible materials and physical separation. These design features, in conjunction with the fire protection program described in Section 9.4, provide assurance that the RPS conforms to PDC 3.

Consistent with PDC 4 and 22, the RPS is designed for the environmental conditions associated with normal operation, maintenance, testing, and postulated events. A description of how the operational and support requirements will be met, including a description of the enclosure that houses the RPS cabinets, will be provided in an application for the Operating License.

The RPS is located in the safety-related portion of the Reactor Building. The Reactor Building is designed to protect internal SSCs from external hazards as discussed in Chapter 3. Consistent with PDC 22, the RPS's location in the safety-related portion of the Reactor Building ensures that natural phenomena will not result in a loss of protection for the RPS.

No portion of the RPS that performs a safety function crosses the seismic isolation moat that is described in Section 3.5. The RPS includes a block to the PCS to prevent any PCS SSCs from interfering with a safety-related SSC's performance of its safety function. The RPS block is accomplished by removing power to a safety-related relay. The safety-related relay is also located in the safety-related portion of the Reactor Building, so no other flexible design features to address differential displacement are required for the RPS to accomplish the block to the PCS during postulated seismic events. This is consistent with PDCs 2 and 4.

The RPS is under the Quality Assurance Program as described in Section 12.9 which is consistent with PDC 1 and 10 CFR 50.55(i).

Table 7.3-2: Reactor Protection System Interlocks and Inhibits

Input Signal to the Reactor Protection System	Interlock or Trip
Fission product accumulation in the core exceeds a defined level	DHRS is actuated~~activated~~ *Purpose*: ensure decay heat removal
Fission product accumulation in the core exceeds a defined level	Manual reset for DHRS prohibited *Purpose*: DHRS cannot be disengaged while the core generates decay heat
Low power level AND a minimum defined fission product accumulation in the core is reached*	Manual reset for DHRS available *Purpose:* Prevent overcooling while shutdown
DHRS manual reset is available after RPS actuation~~activation~~ NOTE: see row above for the initial conditions for DHRS manual reset availability	Reactor Auxiliary Heating System actuation~~activation~~ available. *Purpose*: Allow additional thermal management capabilities following a reactor trip
Loss of normal power AND No transfer to backup power within a defined time period	Movement of reactivity control elements inhibited with manual reset required *Purpose*: prevent inadvertent positive reactivity addition to the core by preventing withdrawal of reactivity control elements when power returns following a reactor trip
Loss of normal power AND Actuation~~Activation~~ of the RTS	After the RTS trips the PSP, manual reset is required to restart the PSP *Purpose*: Prevent inadvertent restart of the PSP when power is restored
Actuation~~Activation~~ of the RTS	After the RTS trips the PSP and ISP, the ISP is prevented from restarting unless the PSP is running *Purpose*: ensure positive pressure between the primary and intermediate coolant loops
PSP not running	Trip the ISP and lock out restart of the ISP until the PSP is running. *Purpose*: prevent ingress of nitrate into the primary loop above a certain threshold
Detection of a break in the PHSS extraction line	Trip the pebble extraction and insertion machines

* The fission product accumulation is based on the operating time and power level relationship.

7.4 MAIN CONTROL ROOM AND REMOTE ONSITE SHUTDOWN PANEL

7.4.1 Description

The main control room (MCR) provides means for operators to monitor the behavior of the plant, control performance of the plant, and manage the response to postulated event conditions in the plant. The remote onsite shutdown panel (ROSP) provides separate means to shut down the plant and monitor plant parameters in response to postulated event conditions. Figure 7.4-1 shows the architecture of the MCR and ROSP.

7.4.1.1 Main Control Room

The MCR contains equipment related to normal operation of the plant. These include operator and supervisor workstation terminals which provide alarms, annunciations, personnel and equipment interlocks, and process information. These pieces of equipment are the main point of interaction (human/system interface (HSI)) between operators and the PCS and the information coming from the RPS. The terminals are connected to the main plant network through a network switch. The system uses redundant fiber optic communication channels between the PCS and the MCR. Communication from the RPS to the MCR utilizes ~~a~~the data diode discussed in Section 7.3.3 ~~fiber optic channel~~ for one-way communication.

The MCR console displays plant parameters to allow operators to monitor conditions during and following postulated events. The MCR console contains a manual trip switch that propagates through a gateway and through safety-related isolation, which allows operators to initiate a plant trip, but this is not a credited safety-related function nor credited in the accident analyses (see Chapter 13).

The MCR also contains a central alarm panel for the fire protection system so that operators can monitor the status of fire protection equipment inside the Reactor Building. The central alarm panel includes controls for the ventilation and extinguishing systems related to the response to fires.

7.4.1.2 Remote Onsite Shutdown Panel

The ROSP provides a HSI for plant staff to monitor indications from the reactor protection system including operating status of the RTS and the DHRS in the event that the MCR becomes inaccessible or uninhabitable. The ROSP features one-way (read-only) communication with reactor protection system instrumentation signals and the ability to initiate a trip signal from the manual trip button that actuates~~activates~~ reactor protection systems. The ROSP is not safety-related and is located in the safety related portion of the Reactor Building.

7.4.2 Design Bases

Consistent with PDC 19:

- The design of the main control room allows actions to be taken to operate the reactor under normal operating conditions and to monitor it under postulated event conditions.
- The main control room is designed to provide radiation protection allowing access and occupancy of the control room under postulated event conditions without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent (TEDE) for the duration of the event.
- The main control room is designed to be habitable, allowing access and occupancy of the main control room during normal operations and under postulated event conditions.
- An ROSP is located outside the control room that (1) provides the capability to promptly shutdown the reactor and includes instrumentation and controls to monitor the unit during shutdown, and (2) provides the capability for subsequent safe shutdown of the reactor through the use of suitable procedures.

7.4.3 System Evaluation

7.4.3.1 Main Control Room

The MCR is located in an ~~Auxiliary~~ auxiliary ~~Building~~ building~~(see Section 3.5)~~ separate from the Reactor Building. There are no operator actions performed nor safety-related SSCs located in the MCR that are credited for mitigating the consequences of postulated events described in Chapter 13. Therefore, the MCR and ~~Auxiliary~~ the building~~Building~~ that houses the MCR are designed to local building code standards.

The MCR consoles are designed to allow operators to manipulate plant parameters to control the reactor within an acceptable envelope during normal operating conditions, including planned transients. However, no operator actions are credited in the safety analysis of postulated events described in Chapter 13. Although the controls in the MCR are not credited in the safety analysis, the MCR consoles are designed as follows:

- MCR displays implements the guidance from NUREG-1537, Section 7.6, with respect to ease of operators use. The plant controls are grouped and located in the MCR so that operators can easily reach and manipulate the controls. Displays of the results of an operator's actions are readily observable.
- The screen element organization and appearance of the consoles are designed to allow operators to perform actions to operate the reactor under normal operating conditions and to monitor it under postulated event conditions, consistent with PDC 19.
- The MCR consoles are digital interfaces that consider IEEE 7-4.3.2-2003 (Reference 1), as it relates to hardware design, and Regulatory Guide 1.152, Revision 2 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." The control consoles in the MCR are designed to display plant parameters that indicate plant status. The MCR consoles display the following information:
    - Plant sensor data and digitally processed parameter outputs based on plant sensor data
    - Indications of PCS and RPS system and equipment status
    - Current and past operating parameter and system information for a duration relevant to inform process and maintenance trending
- Administrative controls are applied to the consoles in the main control room to prevent unauthorized access. MCR console screens are password-protected and include interlocks such as swipe cards and multi-operator coordinated logins to prevent unauthorized access and systems actuation.

The MCR is located at a distance from the Reactor Building such that the radiological consequences of unfiltered air in the MCR during postulated events does not exceed 5 rem TEDE for the duration of the event. The environmental control features for the MCR are separate from the environmental control features for the Reactor Building. ~~See Section 3.5 for more information about the Auxiliary Building that contains the MCR.~~ The analysis of operator dose depends on the final design of the reactor's safety-related SSCs and the analysis will reflect the methods described in Chapter 13. Accordingly, a description of the analysis of operator dose will be provided in the application of the Operating License.

Further, Section 2.2 describes potential chemical hazards related to anhydrous ammonia and chlorine from offsite highway traffic. Sensors are provided for the MCR for anhydrous ammonia and chlorine. When levels of either of those chemicals are detected to be above a threshold value, the ventilation system for the MCR will be turned off and administrative procedures applied until the hazard dissipates.

The design features described above demonstrate conformance with PDC 19.

Figure 7.4-1: Architecture of the Main Control Room and the Remote Shutdown Onsite Panel