7 INSTRUMENTATION AND CONTROLS

The U.S. Nuclear Regulatory Commission (NRC) staff reviewed Chapter 7, "Instrumentation and Controls," of the Tennessee Valley Authority (hereinafter referred to as TVA or the applicant), Construction Permit Application (CPA), Preliminary Safety Analysis Report (PSAR), as supplemented, against applicable regulatory requirements using regulatory guidance and standards to assess the sufficiency of the preliminary information on the Instrumentation and Controls (I&C) design for the issuance of a construction permit (CP) in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 (TN249), "Domestic Licensing of Production and Utilization Facilities." As part of this review, the NRC staff evaluated information on the I&C system design, with special attention given to design and operating characteristics, unusual or novel design features, and principal safety considerations. The NRC staff evaluated the preliminary design of the I&C systems to ensure the design criteria, design bases, and information relative to construction is sufficient to provide reasonable assurance that the final design will conform to the design basis.

The NRC staff's reviews and evaluations for areas relevant to PSAR Chapter 7, including regulations and guidance used, a summary of the application information reviewed, and evaluation findings and conclusions, are discussed in the sections below for each specific review area. A summary and overall conclusions on the staff's technical evaluation of the instrumentation and controls are provided in Section 7.3, "Summary and Conclusions on Instrumentation and Controls."

7.1 Instrumentation and Control Introduction and Overview

The one-unit BWRX-300 SMR (hereinafter referred to as CRN-1) designed by GE-Vernova Hitachi Nuclear Energy utilizes an integrated digital-based I&C design. The I&C architecture is arranged to support a plant-level defense-in-depth (D-in-D) framework. The BWRX-300 D-in-D framework links to a classification scheme based on the importance of the individual defense lines (DLs). The applicant states that the BWRX-300 passive safety features require fewer automatic actuation functions that also eliminate required operator actions for design-basis accidents (DBAs) for 72 hours. The following subsections offer descriptions of the BWRX-300 I&C system design derived primarily from the applicant's Chapter 7 PSAR, which will be evaluated by the staff in later sections of the safety evaluation.

7.1.1 Relationship Between Instrumentation and Control Functions and Plant-Level Defense Lines

As further summarized in Sections 3.2.1 and 3.2.2 of this report, Defense Line 1 (DL1) includes the quality measures and design features employed to minimize potential for failures and initiating events to occur and to minimize potential for failures to occur in subsequent lines of defense. Accident monitoring instrumentation supports more than one DL and receives DL1 treatment by application of applicable industry standards for accident monitoring instrumentation.

Defense Line 2 (DL2) contains Safety Category 3 plant functions (e.g., anticipatory reactor trips) designed to detect and mitigate postulated initiating events (PIE) in the anticipated operational occurrences (AOO) frequency range category and prevent plant conditions from escalating to accident conditions. Safety Category 3 functions that normally operate to actively control reactor

parameters are also part of DL2 (e.g., reactor level and pressure control and control rod positioning). Safety Category 3 functions are supported by Safety Class 3 (SC3) equipment.

Defense Line 3 (DL3) contains safety-related Safety Category 1 functions that act to mitigate PIEs consisting of AOOs and DBAs that prevent core damage, maintain integrity of the physical barriers that prevent radiological release, and place the plant in a safe state. DL3 also includes functions that maintain the plant in a safe condition following mitigation of PIEs until normal operations are resumed. Safety Category 1 functions include reactor scram and actuation of engineered safety features. Safety Category 1 functions are needed when Safety Category 3 (DL2) functions are not effective at intercepting a PIE or when a PIE is beyond the capabilities of DL2 functions. Accordingly, DL3 provides D-in-D in mitigation for AOO PIEs. Safety Category 1 functions are credited for mitigating PIEs independent of Safety Category 2 and Safety Category 3 functions and are therefore required to be independent from Safety Category 2 and Safety Category 3 functions. Safety Category 1 functions are supported by Safety Class 1 (SC1) equipment.

Defense Line 4 (DL4) comprises two subsets, designated as Defense Line 4a (DL4a) and Defense Line 4b (DL4b).

DL4a includes Safety Category 2 functions required to place and maintain the plant in a safe state in case of PIEs and event sequences with failure of the Safety Category 1 functions (e.g., beyond design basis events (BDBE) or design extension conditions (DEC) without core damage). DL4a provides D-in-D for mitigation for DBA PIEs. Safety Category 2 functions detect and mitigate DECs and are used as a backup to Safety Category 1 (DL3) functions (e.g., common-cause failures (CCFs) postulated to occur in DL3 coincident with DBA PIEs). Safety Category 2 functions are supported by Safety Class 2 (SC2) equipment. Safety Category 2 functions are designed to work in tandem with Safety Category 3 functions to ensure AOOs and DBAs resulting from a single failure are mitigated by two DLs among DL2, DL3, and DL4a. Safety Category 2 functions can be used, along with unaffected Safety Category 3 functions, to mitigate a PIE as part of the same event sequence (i.e., to act as a single DL and not as two independent DLs in an DEC analysis). All AOOs and DBAs resulting from a single failure are required to be mitigated by Safety Category 1 functions and separately by either Safety Category 3 functions or Safety Category 2 functions, or by a combination of Safety Category 2 and Safety Category 3 functions.

DL4b contains Safety Category 3 functions that are explicitly provided to prevent or mitigate a severe accident while keeping radioactive releases to acceptable levels.

The DL independence requirements are consistent with the D-in-D strategy (i.e., the crediting of DLs in the fault evaluation and deterministic safety analyses). The only aspects of independence required between equipment performing Safety Category 2 and Safety Category 3 functions are required electrical isolation and physical separation for cable raceways and I&C cabinets. Equipment performing DL4b functions is independent of any equipment postulated to have failed in the event sequence those functions are mitigating.

Defense Line 5 (DL5) includes emergency preparedness measures to cope with potential unacceptable releases in case the first four DLs are not effective. These are offsite measures taken to protect the public in a scenario involving substantial release of radiation. DL5 is supported by accident monitoring instrumentation.

7.1.2 Instrumentation and Control System Classification

The BWRX-300 distributed control and information system (DCIS) is an integrated control and monitoring system for the plant. The DCIS is arranged in three safety-classified DCIS segments and a Non-Safety Class (SCN) segment with appropriate levels of hardware and software quality corresponding to the system functions they control and their equipment locations.

The Safety Category 1 functions are allocated to DL3 and implemented with SC1 equipment, with the following exceptions:

1. Structures, systems, and components (SSCs) only needed after the first 72 hours of the event are classified as SC2.
2. SSCs only needed after the first 7 days of the event are classified as SC3.

The Safety Category 2 functions allocated to DL4a are implemented in at least SC2 equipment. Safety Category 2 functions complete the safety objective via an independent and diverse means of logic and actuation if the Safety Category 1 function is not completed due to an SC1 equipment failure. SSCs that are only needed after the first 7 days of the event are classified as SC3.

The Safety Category 3 functions are allocated to DL2 and implemented in at least SC3 equipment. The Safety Category 3 functions need to be performed independently from diverse Safety Category 1 functions providing protection for the same event.

The Safety Category 3 functions allocated to DL4b are implemented in at least SC3 equipment unless other requirements are justified.

Accident monitoring is a DL1 provision and SC3 is assigned to functions that support monitoring and display of post-accident monitoring (PAM) Type D, E, and F variables.

SSCs that are not required to be SC1, SC2, or SC3 are classified as SCN. The SCN controller equipment is designed to prevent random I&C component failures from initiating plant transients. Vendor-supplied SCN equipment is integrated into the SC3 DCIS network through SC3 gateways.

The system designations of primary protection system as SC1, diverse protection system (DPS) as SC2, nuclear controllers as SC3, and balance of plant (BOP) controllers as SCN represent an initial decomposition of the overall I&C systems based on safety classification. Further refinement of the system decomposition, based on functional grouping within a Safety Class and equipment selection, is performed as the I&C architecture design process progresses. This process is described in the PSAR Section 7.4.2.2.

7.1.3 Instrumentation and Control Systems of Systems

The DCIS systems (i.e., primary protection system, DPS, nuclear controllers, and SCN controllers) are developed and integrated into an architecture that implements the BWRX-300 D-in-D strategy The applicant states the DCIS systems are networked using a managed network switch scheme that allows the parts to operate independently and prevent faults from propagating while appearing seamless to the plant operator. The BWRX-300 I&C segments are interconnected (networked) to support common services like alarming, visual display units (VDU), recording, and sending data to the emergency response facilities while maintaining

appropriate separation between the segments and providing for the necessary safety and security.

7.1.3.1 Distributed Control and Information System

The various DCIS systems are implemented on different hardware and software platforms appropriate to the safety classification of the functions they are performing, as indicated by the PSAR Figure 7.2-1:

- Safety Category 1 functions and SC1 equipment in DL3
- Safety Category 2 functions and SC2 equipment in DL4a
- Safety Category 3 functions and SC3 equipment in DL2 and DL4b
- Non-Safety Category functions and SCN equipment

Enterprise network consists of:

- rRedundant unit data highways (UDH)
- rRedundant plant data highways (PDH)
- oOptical fiber data links

PSAR Chapter 7 states the SC1 DCIS is comprised of three divisions that operate completely independently from each other (except for voting). It is completely isolated from the rest of the BWRX-300 DCIS except for the optically isolated data links provided through unidirectional boundary devices to SC3. Isolated information only flows through dedicated connections in one direction through isolating boundary devices to the SC3 networks so that SC1 system information may be alarmed, monitored, and recorded (but not controlled) with SC2 and SC3 equipment (e.g., VDUs, printers, alarm system, and historians). They can also be monitored by the VDUs associated with the SC1 systems. The SC1 DCIS divisions are separately powered by the three divisions of the SC1 electrical system.

DL4a performs Safety Category 2 diverse protection system (DPS) functions using SC2 equipment. Safety Category 2 DPS actuation logic operates on a digital I&C platform that is diverse and independent from the SC1 equipment. It communicates status and diagnostic information to the SC3 DCIS portion via isolated one-way optical data link.

DL2 performs Safety Category 3 nuclear controller functions using SC3 equipment. The SC3 DCIS is redundant and segmented into two parts. The two network segments are the nuclear segment and the BOP segment. The two bus segments are classified as SC3. The nuclear segment uses controllers classified as SC3. The SC3 BOP segment interfaces with the SCN controllers to acquire information to support human-system interface (HSI) integration in the SC3 DCIS. Both segments have their own redundant unit data highway (UDH), and each independently provides the control and monitoring capability of nuclear and BOP I&C for their segment. Each segment has their own redundant network-managed switches classified as SC3. Each segment can operate independently of the other. Each segment has associated VDUs, historians, and an alarm system. The SC3 segments use triple modular redundant (TMR) and redundant controller architectures for various functions to support reliability goals or prevent adverse actuations for anticipated hardware component failures.

The nuclear segment supports the SC3 controllers (which include the major reactor control systems) by acquiring SC1 data from the SC1 controllers via unidirectional boundary devices.

The SC3 BOP segment provides for control of the plant equipment with no safety category (SC) function and controllers used for power generation. It also provides SC3 gateways to interface non-native controllers to the SC3 BOP segment. Although lower classified equipment, these functions use TMR controller architectures (referred to hereafter as TMR controllers) to prevent random I&C component failures from causing plant transients.

7.1.3.2 Unit Data Highway Network

The SC3 and SCN DCIS components are connected to the two UDH networks shown in PSAR Figure 7.2-1 using the general switch arrangement shown in PSAR Figure 7.2-2. Each component is connected to redundant network switches. Either connection to the network for the component and either network switch provides full functionality, making failovers seamless. The controllers are either dual redundant or TMR and the UDH network connections and switches are dual redundant. The UDH network design is fault tolerant, and components and connections are monitored and alarmed. The various components can be replaced online without affecting either safety or power generation. The UDH provides for control and monitoring capability of nuclear and BOP I&C systems. Any SC3 VDU can monitor or control any SC3 or SCN equipment.

7.1.3.3 Network Managed Switches

The SC3 data networks are a rapid spanning tree network of managed Ethernet switches as shown on PSAR Figure 7.2-3. In addition to providing standard Ethernet switch capability, each managed network switch provides security features. These include identification of authorized equipment addresses, the ability to ignore or not uplink to other segments, the ability to control which nodes are allowed to communicate and the ability to alarm abnormal network traffic.

No switch or network failure can adversely affect SC1 functions because the SC1 equipment is isolated from these networks by unidirectional boundary devices. The BWRX-300 I&C data networks are fault tolerant such that no single network failure can adversely affect plant operation.

7.1.3.4 Plant Data Highway Network

Formatted: Body Text

The PDH, as shown on PSAR Figure 7.2-1, is used for important, but non-essential and non-control services like printers, plotters, long-term data storage, etc. Information is sent outside the plant network through the unidirectional boundary devices (firewall) to the utility servers. Various lower cyber security levels of users are connected to these servers, including the onsite or offsite emergency response facilities and utility business or engineering networks that may have their own cyber security restrictions. Only the utility server can respond to requests for information from outside the plant network, and the only information it has is the plant data sent to it through the firewall. No plant DCIS component receives or is able to respond to a data request from outside the plant network. No component outside the plant network can access the PDH. The managed switches do not allow any such communication to reach the PDH, SC3 UDH, or SCN UDH. The PDH is designed to function as a communication channel that is reliable and responsive for displaying process information.

7.1.4 Distributed Control and Information System Functions

The reactor mode switch is used as an input to the DCIS to insert or remove operating bypasses for the actuation of Safety Category 1, Safety Category 2, and Safety Category 3 functions. The reactor mode switch is classified as a SC1 component and is a four-position switch with the following positions:

- RUN
- STARTUP
- SHUTDOWN
- REFUEL

The reactor mode switch is manually positioned by the reactor operator as the reactor is transitioned from cold (REFUEL) to rated power (RUN). The switch position determines and provides information to the various controllers needing the reactor mode switch position information to provide the correct operating bypasses for system operation. The reactor mode switch is in the main control room (MCR) to support normal plant operation.

The reactor mode switch provides the necessary electrical isolation between each segment to maintain divisional independence or isolation between different SCs. The reactor mode switch position information is sent to the following functions:

- SC1 Protection System (Three Divisions)
- SC2 DPS
- SC3 Nuclear Controllers (including the Anticipatory Trip System)
- SC3 Automatic Power Regulator (APR)
- SC3 Rod Control and Information System (RC&IS)

As shown in PSAR Figure 7.3-1, the multideck reactor mode switch signals are sent to the independent functions from the physically separated rotary switch segments. Each of the three SC1 divisions performing Safety Category 1 functions receive independent electrically separated reactor mode switch information, and each of the systems performing Safety Category 2 and Safety Category 3 functions receive the reactor mode switch information three times to allow for validation. The receiving system logic determines the resolution of valid or faulty switch positions. For example, the Safety Category 1 fail-safe safety functions trip for multiple switch positions or no switch positions. Fail-as-is systems alarm and stop their processes. The APR takes the plant out of automation and the RC&IS blocks control rod motion. An alarm is provided for inaccurate switch positions.

7.1.4.1 Primary Protection System - DL3/SC1

The SC1 Primary Protection System acquires the plant information from the sensors specified for systems performing Safety Category 1 functions. The plant information acquired is displayed on the associated VDUs and provided through qualified isolation devices to the SC3 integrated plant displays.

Systems Architecture

The SC1 I&C systems have three independent divisions that are powered by three separate divisions of the SC1 electrical system. Each of the three divisions uses two uninterruptible power supply (UPS) that are backed by a 72-hour battery. The UPS and the battery chargers can be powered by offsite power or either of the standby diesel generators. The SC1 I&C system automatic actuation functions are designed to be fail-safe (except for isolation condenser system (ICS) isolation). On loss of power or loss of data communication, the reactor scrams, and the ICS is automatically initiated to remove decay heat. The automatic and manual controls for the ICS reactor isolation valves (RIVs) are fail-as-is. Each division of DCIS cabinets and associated UPS, battery chargers, and batteries are located in separate, fire barrier rooms in the reactor building (RB). Each division of instrument racks are located in separate fire barrier rooms in the RB. Primary functions of the Safety Category 1 functional logic are:

- reactor scram
- reactor and containment isolation
- ICS initiation functions

The three independent divisions of the I&C system receive plant process input signals from SC1 sensors of their respective division. Uninterruptible power for the sensors and signal conditioning is provided by the associated division of the I&C system. As shown in PSAR Figure 7.3-2, “Safety Class 1 Functional Architecture,” the field input and output signals are hardwired per division to the I&C cabinets. Remote data acquisition multiplexers are not required for performance of the Safety Category 1 functions.

As shown in PSAR Figure 7.3-3, “BWRX-300 Safety Category 1 Actuation Logic,” the three independent divisions communicate among themselves to determine whether there has been a trip in two-out-of-three (2oo3) divisions. Each division independently makes the 2oo3 trip decision. The voting communication between divisions contains message authentication and divisional or parameter trip status, and if there is a loss of communication from a division, the receiving division assumes a trip. The divisions have additional logic to support monitoring and can include alarms for predetermined parameters on the associated VDUs. This design supports accident monitoring using signals acquired by SC1 equipment and the corresponding divisional support systems like SC1 electrical supply status. The SC1 divisions export plant process, accident monitoring, and diagnostic data via dedicated, unidirectional boundary devices to the SC3 systems. Reactor scram, reactor and containment isolation, and ICS initiation can also be initiated without software via hard switches in either plant control room.

System Design Bases and Associated Safety Functions

The design bases of the SC1 I&C systems are to mitigate the effects of a PIE (i.e., AOO or DBA and most DECs) assuming no credit for Safety Category 2 or Safety Category 3 functions (e.g., CCF). The SC1 I&C system design includes instrumentation to monitor plant variables and systems over the respective ranges for operational states and PIEs. Safety Category 1 functions operate alone ensuring that no AOO or DBA cause a radiation release greater than regulatory requirements consistent with safety analysis assumptions described in Chapter 15 of this report. Safety Category 1 functions operate independently of Safety Category 3 functions using diverse equipment to perform required Safety Category 1 functions. The SC1 I&C system is designed to be available during all modes of plant operation. The DL3 functions categorized as Safety Category 1 and implemented in SC1 I&C equipment are:

1. Hydraulic scram—SC1 I&C initiates a trip when a measured parameter exceeds a predefined setpoint and initiates a hydraulic scram with a 2oo3 voting logic using the same parameter. The trip logic is used to scram the reactor by hydraulically inserting the control rod blades. Hydraulic control units (HCUs) are pressurized accumulators used to forcibly drive the control rod blade into the core. Scram initiation is enabled by de-energizing two scram solenoid valves to vent air holding the HCU scram valve closed against a spring force. When the HCU scram valve is opened, two control rod blades are inserted into the core except for one HCU that inserts a single control rod blade. As listed in PSAR Table 7.3-1, the following SC1 process parameters initiate hydraulic scram function:

    a. HIGH Reactor Pressure Vessel (RPV) pressure (HP1)
    b. LOW RPV pressure (LP1)
    c. LOW RPV water level (L3)
    d. HIGH average power range monitor (APRM) neutron flux (RUN setpoint)
    e. HIGH Simulated Thermal Power (STP)
    f. HIGH containment pressure
    g. HIGH APRM neutron flux (STARTUP setpoint)
    h. Indication of a line break (main steam line (MSL) or FW)

    The SC1 hydraulic scram uses divisional load drivers to de-energize the HCU scram solenoid valves. As the SC1 hydraulic scram is initiated, a scram follow signal is sent to SC2 equipment to have each fine motor control rod drive (FMCRD) motor drive its ball nut upward to a position just below the fully inserted and latched hollow piston that is coupled to the control rod blade. This signal is sent whenever a hydraulic scram is demanded by SC1 I&C regardless of whether the hydraulic scram actuation has been successful.

2. Power Range Neutron Monitoring (PRNM)—SC1 I&C acquires and processes the PRNM neutron monitoring power signals to support the SC1 hydraulic scram function. The PRNM acquires signals from 13 vertical “strings” of local power range monitors (LPRM) and gamma thermometers (GT) arranged radially throughout the BWRX-300 core. Each string has four LPRM detectors and eight GT distributed vertically over the length of the wet tube rod assembly. The LPRM signals are averaged per division to produce an APRM signal. The average signal is normalized to thermal power in percent and used for high-power APRM flux trips. PRNM also provides the high simulated thermal power (STP) signal. The PRNM also provides signals for accident monitoring purposes to the three-dimensional (3-D) core thermal power distribution monitor, and to the SC3 control rod blocking systems. These additional functions are not required to support any SC1 function; however, SC1 sensor signals are used to acquire the process parameter inputs.
3. Reactor, Containment, and System Isolation—SC1 I&C performs the Safety Category 1 functions for RPV and containment isolation by closing the main steam reactor isolation valves (MSRIV), main steam containment isolation valves (MSCIV), feedwater reactor isolation valves (FWRIV), feedwater containment isolation valves (FWCIV), and other valves identified in PSAR Subsection 6.2.4, to limit line break effects both inside and outside containment. The isolation functions and initiation signals are listed in PSAR Table 7.3-1. The different isolation functions are initiated when 2oo3 divisions agree on an isolation demand.
4. ICS Actuation—SC1 I&C performs the Safety Category 1 function of initiating ICS, which is comprised of three Isolation Condensers (IC) that are each a simple loop including the RPV steam supply piping to the heat exchangers submerged in the ICS pools, and a line to return the condensed steam to the RPV. The ICS is initiated by opening a normally closed condensate return valve per IC. The Safety Category 1 I&C logic activates each IC

Formatted: Indent: Left: -0.06", Space After: 12 pt

separately using 2oo3 voting logic. When initiated by high reactor pressure, a different initiation setpoint is used for each IC. When the 2oo3 voting logic is satisfied, a pair of load drivers de-energize the solenoids that are being used to hold the fail-open valve closed. The ICS functions and initiation signals are listed in PSAR Table 7.3-1.

5. Diverse ICS Isolation—Because the ICS is part of the reactor coolant pressure boundary (RCPB), a break in an ICS line necessitates that the RIVs for that train's steam supply and condensate return lines be closed to quickly terminate a loss of coolant. To ensure that a common cause failure of the control system cannot spuriously isolate the three ICS trains, the isolation functions for Trains A and C are allocated to one SC1 I&C system while the isolation functions for Train B are allocated to a second independent and diverse SC1 I&C system. Each train is provided with its own leak detection instrumentation and isolation valves such that no single control failure results in isolation of all three trains.
6. Accident Monitoring—SC1 I&C acquires accident monitoring information associated with Type B and C accident monitoring variables, as defined in IEC 63147:2017:2017/IEEE 497-2016, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." Type A variables provide the primary information required to permit the operating staff to take specific required manual actions for which no automatic control is provided. The BWRX-300 does not have any Type A variables, as noted in PSAR Table 7.3-2. Type B variables provide the primary information to the accident management personnel to assess the plant safety functions. These safety functions include accomplishing or maintaining reactivity control, core cooling, reactor coolant system integrity, and containment integrity (including radioactive effluent control). Type C variables provide the primary information to the accident management personnel to indicate the potential for breach or the actual breach of fission product barriers (e.g., fuel cladding, reactor coolant pressure boundary, and containment pressure boundary). Type B and C variables are categorized as SC3.
7. Communications—Digital data is used to acquire the process, diagnostic, and monitoring signals within the divisional SC1 I&C components and organize them into a predefined message protocol. The divisional communication messaging is then isolated using SC1 hardware and converted into two optical fiber message streams per division. The three redundant pairs of divisional optical fiber message streams are sent through unidirectional boundary devices to two SC3 gateways and then to the SC3 networks. These gateways are redundant such that if one fails, the three divisions of SC1 I&C signals are still available for alarming, recording, and monitoring in the lesser classified I&C systems.

The design bases of Safety Category 1 functions are to act when Safety Category 3 functions are not effective at intercepting a transient or when an event is beyond the capabilities of the Safety Category 3 functions. If Safety Category 1 functions completely fail, Safety Category 2 functions are designed to prevent core damage. For common physical parameters measured by the DLs, the Safety Category 3 function setpoints are set to act first, consistent with the SC3 design bases, i.e., to mitigate/prevent SC1 from needing to respond.

The BWRX-300 does not use interlocks to prevent over-pressurization of low-pressure systems or of the reactor coolant system during low temperature conditions, nor does it use interlocks to isolate SC systems from SCN systems or to preclude inadvertent interconnections between redundant or diverse safety systems for the purposes of testing or maintenance. No interlocks are required because the BWRX-300 design minimizes piping systems, major system components (e.g., pumps and valves), and subsystems connected to the RCPB, and connected systems are designed to full reactor coolant pressure.

Fundamental Design Properties in the System Design

The applicant states that the SC1 I&C system design includes DL1 properties that represent the quality measures implemented to minimize the potential for failures to occur by the use of conservatism in design and analyses. These DL1 properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed in the following five subsections.

Equipment Qualification

The applicant states that the SC1 I&C equipment is designed to operate in the environment that is to be expected during both normal operations and anticipated off-normal conditions. The SC1 I&C equipment is qualified to perform its intended functions. Qualification addresses both hardware and software aspects of the SC1 I&C system. The SC1 I&C design and manufacturing processes are of sufficient quality to ensure I&C systems can reliably perform their credited protection functions. Additional information on equipment qualification can be found in Section 3.11 of this report.

Reliability

The applicant states its SC1 I&C systems have the required reliability to perform its intended functions. The reliability of the SC1 I&C system will be demonstrated as part of the final design. The SC1 I&C systems use digital technology consisting of three divisions with 2oo3 voting logic for trips and safety function initiations, which prevents spurious actuations due to single hardware failures. This I&C design allows one division of sensors to be bypassed or one division of logic to be bypassed to support maintenance or testing. It is physically only possible to bypass one division of sensors or one division of logic at a time, which retains the capability to provide required safety actuations. When a bypass is used, the 2oo3 logic behaves as the equivalent of two-out-of-two (2oo2) to initiate a protection function. Correct functioning of the SC1 digital I&C platforms is continuously monitored by self-testing features. Critical faults detected by self-testing features trip the outputs of the platform and other faults are alarmed. The SC1 I&C system uses dual power supplies and dual power feeds per chassis to increase system reliability and availability.

Redundant divisions of sensors are monitored for deviations by an automated function that is performed continuously in the TS monitor. Deviations greater than a specified value are alarmed.

For each pair of HCU scram solenoids, one scram solenoid uses a load driver from Division 1 and the other load driver from Division 2. Division 1 and Division 2 load drivers open on a 2oo3 vote from the three divisions communicated via optical fiber. Both scram solenoids in the HCU are de-energized to initiate a scram. The HCU scram design allows surveillance testing of each division through to the solenoid without causing a scram in normal operation. Testing provisions that are permanently connected to safety systems are classified the same as the safety system. The arrangement of the scram solenoid control and power is shown as PSAR Figure 7.3-4. In addition, the reactor can also be shut down with the complete failure of SC1 hydraulic scram function with the diverse backup of Safety Category 2 functions.

The reactor and containment isolation valves are closed by de-energizing two solenoid valves mounted on the isolation valve actuators. One of the isolation solenoids uses a load driver and uninterruptible power from Division 1 and the other solenoid is powered from Division 2. Division

1 and Division 2 load drivers open on a 2oo3 vote from the three divisions communicated via optical fiber. Both solenoid valves of the isolation valve are de-energized to initiate a valve closure. This valve design allows surveillance testing of each division through to the solenoid without causing an isolation during normal operation. The arrangement of the isolation solenoid control and power is shown in PSAR Figure 7.3-5.

The ICS actuation circuits have two normally energized solenoids on the IC valve that keep the valve normally closed. One of the solenoid valves is in Division 1 and the other solenoid valve is in Division 2. Each solenoid has a normally closed load driver that opens on a 2oo3 vote from the three divisions communicated via optical fiber. Both solenoids per ICS actuation valve are de-energized to initiate a valve opening. This solenoid valve arrangement allows surveillance testing of each division through to the solenoid without causing ICS initiation during normal operation.

Each IC isolation valve is designed with three divisional solenoids, and 2oo3 solenoids need a change in state for the valve to open or close. Reliable isolation and prevention of inadvertent isolation is achieved by the assignment of the SC1 I&C divisions to solenoid valves that control each IC isolation valve and the mechanical arrangement of the solenoid valves to ensure that a single failure does not result in the unwanted isolation of an IC or prevent a required isolation of an IC. Manual actuation of the IC isolation function can be performed on a train-by-train basis. This manual isolation is a Safety Category 2 function; however, it is implemented via SC1 equipment because no lower classified equipment can have the ability to isolate an IC train (which potentially prevents SC1 actuation of that train).

Robustness

Robustness of the SC1 I&C design is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions. The SC1 I&C design requirements address the full range of operating environments associated with normal operation, transient, and accident conditions, as well as foreseeable internal and external hazards. The applicant states the SC1 I&C systems have the required separation and independence to perform their intended functions. The SC1 equipment is located in three separate divisional fire barrier rooms in the reactor building (RB). The equipment is separated from the SC3 equipment that is located in a separate fire barrier room in the control building (CB). The SC1 I&C system uses sensors and actuators independent of the SC2 DPS. The SC1 I&C system provides trip communication between divisions for voting using optical fiber. A unidirectional boundary device provides for isolated optical communications to SC3 systems through the SC3 gateways to prevent communication from lower SC systems from affecting SC1 I&C systems. The isolation devices are classified as SC1. The logic used to rapidly scram the reactor by hydraulically inserting the control rod blades is separate and independent of the normal FMCRD positioning controls using the RC&IS. Each LPRM/GT string has four LPRMs equally spaced vertically along the approximate 12 ft height of the core. PSAR Figure 7.3-6 indicates the LPRM/GT locations in the BWRX-300 core. Each LPRM is individually powered and signal conditioned by its associated division.

The SC1 I&C systems are designed with three divisions with 2oo3 voting logic for trips, isolations, and initiations. This redundancy ensures that the protection functions can be actuated even with an assumed single failure. The SC1 I&C system has the required fail-safe design features to perform its intended functions. Deliberate operator action is required to return the SC1 I&C system to normal after actuation.

The SC1 hydraulic scram, PRNM, and reactor and containment isolation functions use only fail-safe logic (including loss of sensor and communications data). The SC1 hydraulic scram logic is also equipped with individual manual scram switches in Division 1 and Division 2. These switches interrupt the power to the scram solenoids independently of the SC1 hydraulic scram logic and do not use any software. The switches are included in the secondary control room (SCR) and both switches are required to be operated to cause a scram. A loss of uninterruptible power or logic power causes an SC1 hydraulic scram, ICS actuation, and RPV and containment isolation but does not close the IC RIVs. The SC1 PRNM logic provides flux-related trip signals to initiate a SC1 hydraulic scram.

The SC1 ICS actuation logic initiates the three ICs separately (using 2oo3 voting logic) for both reliability reasons and to allow different initiation setpoints for each IC. A loss of power initiates all three trains of the ICS. The condensate return valves are open/close only and are operated by SC1 functional logic. The logic is similar to the SC1 hydraulic scram function logic.

The ICS isolations do not use a fail-safe design. Instead, the IC steam supply and IC condensate return isolation valves are designed to fail-as-is to minimize the potential for inadvertent isolation. The SC1 I&C logic actively energizes the IC isolation valve solenoids to isolate an IC and each IC is isolated independently and only upon indication of a line break for that IC. Unlike fail-safe logic, which treats an invalid input or loss of communication as a vote to trip, fail-as-is logic ignores invalid inputs such that the logic always requires two valid trip votes prior to actuation. If logic or valve solenoid power is lost or the logic fails self-diagnostic monitoring, the isolation valves remain at their last position. The divisional logic outputs change state (open or close the isolation valves) only with active power. Logic and sensor diagnostics are alarmed but do not initiate isolation. The isolation is active and latching to fail-as-is. Three solenoids are provided on each isolation valve and energizing any 2oo3 solenoids cause the valve to change position and latch. The three solenoids provide single failure tolerance because the fail-as-is design requires power from at least two divisions. Reliable isolation, when required, is achieved by requiring 2oo3 solenoids and 2oo3 divisional logics to initiate an isolation. The 2oo3 logic minimizes the potential for inadvertent isolation for random I&C component failures. The IC isolation controls are placed into two groups to prevent a CCF in SC1 equipment within a group from causing all three ICs to be spuriously isolated. One group has the isolation controls for two ICs and the second group has the isolation controls for the remaining IC. For the first IC group, the main SC1 hardware and software platform performs the IC isolation function. For the second group (one IC) separate and diverse hardware and software perform the isolation function. The ICS design ensures that even with a postulated CCF of the primary SC1 I&C platform, at least one IC is maintained operational, and one IC is sufficient to mitigate AOOs.

Secure Development & Operational Environment

The SC1 I&C systems have features that adequately address access control to limit cyber security vulnerabilities and ensure the system can perform its intended functions. The SC1 I&C design incorporates access control features to support the establishment of a secure operational environment. The SC1 I&C software is produced in a secure development environment that prevents the insertion of undocumented code. The SC1 I&C systems are installed and maintained in accordance with the station administrative procedures and control of access programs.

The SC1 I&C network is isolated from the rest of the BWRX-300 DCIS. The three SC1 DCIS divisions operate completely independently from the SC2 and SC3 DCIS. Information only flows through unidirectional boundary devices from SC1 I&C to the SC3 networks when the system is

in operation. Two-way data flow can be used with appropriate access control features to support LPRM calibration. The SC3 nuclear segment includes the SC2 gateways that receive isolated SC1 signals through a unidirectional boundary device and provide them to the SC3 nuclear segment. Measured parameters, setpoints, logic and trip status, and diagnostic information are continuously sent through these gateways to the SC3 nuclear segment TS Monitor, which can perform online surveillance testing, alarm on discrepancies, and additionally alarm on loss of these expected communications.

Diversity and Defense-In-Depth

The SC1 I&C system provides the main line of protection for AOOs and DBAs. The SC3 nuclear segment provides anticipatory trip functions to support the BWRX-300 D-in-D strategy. Safety Category 3 functions are designed to prevent or mitigate AOOs before either Safety Category 1 or Safety Category 2 functions are required. The design bases of Safety Category 2 functions provide diversity and D-in-D for the complete failure of the Safety Category 1 function . Safety Category 2 functions independently provide comparable Safety Category 1 functions using diverse platforms from those used in SC1 equipment. Diversity measures are incorporated within the SC1 I&C system design as an additional level of protection for potential systematic faults caused by design and implementation defects within redundant divisions of the system. The IC isolation controls are designed to prevent a CCF of a Safety Category 1 function causing all three ICs to be spuriously isolated. These diversity measures ensure that at least one IC remains operational for any CCF affecting the IC isolation features and one IC is enough to mitigate AOOs.

The hydraulic scram is equipped with individual manual scram switches in Division 1 and Division 2. These hard-wired switches interrupt the power to the scram solenoids independently of the automatic actuation logic. The switches are included in the secondary control room (SCR) and both switches are required to be operated to cause a scram. The SC1 ICS initiation logic is equipped with individual switches in Division 1 and Division 2 to open the ICS condensate return line valves. These hard-wired switches open the valves. The switches are included in the SCR and both switches are required to be operated to cause an ICS Initiation.

The SC1 I&C reactor, containment, and system isolation logic is equipped with individual switches in Division 1 and Division 2 to close the MSRIV, MSCIV, FWRIV, and FWCIV. These switches use a software-free method to close the valves. The switches are included in the SCR and both switches are required to be operated to close these valves. SC1 manual switches are provided in the SCR to open and close ICS RIVs.

Operator Interface and Accident Monitoring

Data from the SC1 I&C systems is available on appropriate displays. Redundant video display units (VDUs) are located in the MCR, SCR, and locally in the SC1 I&C equipment rooms. The displays also include an alarm system to provide operator awareness and to prompt to the displays containing further information relating to the alarm. SC1 I&C system bypass conditions are alarmed in the MCR. Reactor scram, ICS initiation, and reactor, containment, and system isolation can be manually initiated by switches in the MCR and the SCR. Manual actuation of the IC isolation function can be performed on a train-by-train basis. Signals monitored by the SC1 I&C systems are recorded, alarmed, and displayed to the operator on an appropriate display. Self-diagnostics of the SC1 I&C signals and the various SC1 I&C components are alarmed. The monitored parameters required to be available for 72 hours are supported by the SC1 UPS and batteries without the need for offsite power. Data from the SC1 I&C system is

also transmitted through a unidirectional boundary device to SC3 DCIS and SC3 equipment qualified for SC3 accident monitoring functions, where the signals are recorded, alarmed, and displayed. The associated monitoring also includes signals needed to monitor divisional support equipment like the UPS and battery chargers, as well as the SC1 equipment room temperatures. The operator can view the information for the SC1 I&C system on the associated VDUs even if the SC3 DCIS is not operational. The SC1 I&C system acquires and displays accident monitoring information associated with PAM Type B and C variables.

The BWRX-300 passive reactor design automatically actuates SC1 functions to mitigate a design basis event (i.e., AOOs or postulated accidents). The BWRX-300 does not require manual actions to mitigate any design basis events. Therefore, no Type A PAM variables are required. The simplicity of the BWRX-300 safety features to mitigate design basis events and safely shut the plant down, when coupled with the BWRX-300 D-in-D framework, ensures the capability to mitigate the effects of AOOs and DBAs even with a coincident loss of a complete DL. For the BWRX-300, Type B and C PAM variables are only used for immediate verification that DL safety category functions have actuated. They are not needed for subsequent operator actions to realign or control more complicated engineered safety features after the initial actuation phase. The multiple DLs and their capability to accommodate the loss of a complete DL eliminate the need for an immediate operator action to respond to equipment failures for successful accident management. The Type B and C PAM variables are displayed in both the MCR located in the CB and the SCR located in the RB. A preliminary list of the Type B and C PAM variables is provided in PSAR Table 7.3-2.

7.1.4.2 Diverse Protection System—DL4a/SC2

The SC2 system acquires the plant information from the sensors specified for systems performing Safety Category 2 functions. The plant information acquired is displayed on the SC3 integrated plant displays.

Systems Architecture

As shown in PSAR Figure 7.3-8, the SC2 DPS is arranged into a segmented architecture. Three channels of input signals are acquired and compared to setpoints to produce trip or initiating signals using a 2oo3 voting logic. As shown in Figure 7.3-9, SC2 analog signal splitter per each process signal is used for shared sensors. A representative DPS block diagram for a reactor scram is shown in PSAR Figures 7.3-10 and 7.3-4.

Protection function signals within the SC2 equipment do not use the plant data networks. The reactor control and information system (RC&IS) communicates with the FMCRD motor controllers on a dedicated redundant network. The FMCRD network is independent from the plant DCIS network, which is not required for any Safety Category 2 function, nor does it interfere with any Safety Category 2 function.

System Design Bases and Associated Safety Functions

The design bases for Safety Category 2 functions assume the complete failure of Safety Category 1 functions. Safety Category 2 functions are implemented in SC2 equipment that is independent and diverse from the SC1 equipment. The SC2 equipment design for systems implementing Safety Category 2 functions include provisions for instrumentation to monitor plant variables and systems over the respective ranges for operational states and PIEs in order to ensure adequate information can be obtained on plant status. SC2 equipment is designed to be

in-service during all modes of plant operation. Specific safety functions are mode dependent, as determined by the Fault Evaluation process in described in PSAR Section15.2 and the initiating signals are enabled based on the Reactor Mode Switch position.

The system functions performed by SC2 equipment are:

1. Diverse Protection System (DPS)—The SC2 DPS is implemented on a technology diverse from the SC1 equipment and segmented into three channels. The DPS channel trip and initiation signals are based on 2oo3 votes and are fault tolerant to avoid inadvertent actuations. The DPS functions include:
    a. hydraulic scram independent of Safety Category 1 functions
    b. RPV, containment and system isolations independent of Safety Category 1 functions
    c. ICS initiation independent of Safety Category 1 functions
    d. FMCRD fast motor run-in
    e. alternate rod insertion (ARI) pilot valve actuation
    f. feedwater (FW) and condensate pumps trip
    g. cavity pool makeup from ICS pools

    The hydraulic scram and ARI signals are initiated whenever a Safety Category 2 scram function is demanded regardless of whether it has been successful. The Safety Category 2 fast motor run-in function occurs on any hydraulic scram signal followed by a reactor power level indicating that the hydraulic scram was not successful. The DPS functions and initiation signals are listed in PSAR Table 7.3-3. The DPS provides the capability for manual initiations using switches located in the MCR. These are separate from the switches associated with SC1 I&C which are located in the SCR. The setpoints for SC2 DPS actuation logic are determined using the final analytical limits from the plant safety analyses and the measurement uncertainties associated with the DPS. Safety Category 2 functions are designed to prevent core damage for PIE assuming the complete failure of a Safety Category 1 function.
2. Gamma Thermometers—Provide electrical signals from the GTs based on local gamma flux which is representative of core thermal power. The GT represents a completely diverse technology to the neutron detecting LPRMs used by the SC1 system. The DPS acquires signals from 13 vertical LPRM/GT “strings” arranged radially throughout the BWRX-300 core. Each string has four LPRM detectors and eight GTs distributed vertically over the length of the wet tube rod assembly. The GT signals are apportioned to four cabinets such that each cabinet gets a similar allocation of radial and axial GT signals.
3. FMCRD Motor Control—There are 57 FMCRDs in the BWRX-300 and each one has an individual motor and an individual motor controller. The motor controllers are allocated to SC2 equipment and interface with DPS, emergency rod insertion panels (ERIP), and RC&IS. Each motor controller uses software to supply the appropriate commands to the FMCRD motors using individual position controllers. Control rod position indication is provided to RC&IS. Normally the FMCRDs are individually (or in gangs) positioned by the RC&IS to control reactor power in response to either operator or automation system insert and withdraw commands. The FMCRD motor controller software is required for the fast motor run-in, but the DPS actuated hydraulic scram is independent from this function and does not rely on this software.
4. Emergency Rod Insertion Panels (ERIP) and Emergency Rod Insertion Control Panels (ERICP)—There are four SC2 ERIPs that have two functions. The first is to multiply the scram demand signals from the SC3 and SC1 systems, as well as fast motor run-in demand signals from the SC2 DPS to each of the 57 FMCRD motor controllers. The second is to

multiply the multi-channel rod block monitor (MRBM) rod block demand signals to each of the 57 FMCRD motor controllers. The MRBM rod block stops the rods from being able to withdraw and the motor run-in has priority. The circuit design ensures control rod insertion is always available. The scram follow motor run-in is automatically initiated upon receipt of a valid hydraulic scram demand from any of the interfacing systems.

These panels are contact multipliers that each receive manual scram signals, three rod motor withdraw power block signals, and three motor run-in signals from the ERICP. The three motor run-in signals and three motor withdraw power block signals are decoded using 2oo3 logic to pick up additional actuation devices, 29 in one panel and 28 in the other panel. The design ensures that a failure of an actuation device can only affect one FMCRD. The motor run-in actuation devices are sealed in once energized long enough to ensure the motors have time to drive the rods full in.

The ERICP sends the manual scram and motor run-in and motor power block signals to the ERIP. The scram follow motor run-in is automatically initiated whenever SC3 anticipatory trip system (ATS), SC2 DPS, or SC 1 hydraulic scram function initiates a hydraulic scram.

The first two SC1 hydraulic scram, and SC3 anticipatory hydraulic scram initiation signals are shared with SC2 equipment to generate an FMCRD scram follow motor run-in. Simultaneous with the initiation of the SC1 and SC3 hydraulic scram functions, the scram follow function drives each FMCRD motor upward, stopping just short of re-engaging the control rod blade. This, in addition to the SC1 internal control rod blade full in rod latches, prevents the control rod blade from dropping out of the reactor post-scram. This also ensures that any rod scram failure (due to a failed HCU component, for instance) is inserted into the reactor within minutes of the scram signal. The Safety Category 2 DPS fast motor run-in is completely independent of the scrams initiated by Safety Category 1 and Safety Category 3 functions and serves as the backup to the complete failure of the hydraulic scram in case of complete failure of the mechanical/hydraulic portions of the CRD system. This function is performed by the ERICP sending signals to DPS to indicate that a hydraulic scram has been initiated from any source. After receiving such signals, the DPS logic expects its GT inputs to show a decreasing power due to a hydraulic scram. If the GT measurements do not decrease sufficiently within a short time, the DPS generates outputs to the ERICP to order a fast motor run-in. The FMCRD motors should have already started in their scram follow capacity and the DPS signal to the ERICP causes the motors to increase insertion speed.

5. FMCRD Motor UPS—These UPS are dedicated to the FMCRD motor controllers and motors and are not part of the SC1 or SC2/SC3 normal DCIS UPS. The FMCRD motors and controllers have four dedicated UPS that can supply the FMCRD motors in the absence of offsite power or the absence of standby diesel generator power. The FMCRDs are divided into four groups distributed throughout the core. Each of the four groups of motor and motor controller has its own UPS that has a capacity that is at least twice as long as the duration of a motor run-in.

Fundamental Design Properties in the System Design

The applicant states that the SC2 system includes DL1 properties that represent the quality measures implemented to minimize potential for failures to occur by the use of conservatism in design and analyses. These DL1 properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed in the following five subsections.

Equipment Qualification

The applicant states that SC2 equipment is designed to operate in the environment that is to be expected during both normal operations and anticipated off-normal conditions. Qualification addresses both hardware and software aspects of the SC2 equipment. The design and manufacturing processes are of sufficient quality to ensure I&C systems can reliably perform their credited Safety Category 2 protection functions. The SC2 equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The SC2 equipment qualification measures confirm the I&C systems and equipment are capable of reliably performing the design bases functions for which they are credited over the range of environmental conditions postulated for the area in which they are located. Additional information on equipment qualification can be found in Section 3.11 of this report.

Reliability

The applicant states the SC2 equipment has the required reliability to perform its intended functions. The reliability assessment of the final design will be used to optimize goals such as minimizing out-of-service time for repair and reducing the frequency of surveillance. The DPS provides self-diagnostics to SC3 DCIS for equipment status monitoring through qualified SC2 isolation features. FMCRD motor controller self-diagnostics and rod separation signals are also used by RC&IS.

The SC2 DPS is designed to support required surveillance testing without affecting plant operation. It provides the capability for signal and channel bypass to support maintenance and testing. Bypass conditions are alarmed in the MCR. The SC2 design provides for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device. The use of measuring and test equipment that can impair a Safety Category 2 function requires deliberate manual intervention via hardware interlock features at the system interfaces. Testing provisions permanently connected to safety systems are classified the same as the safety system.

The GT system supports averaging the four groups of GT signals and normalizing the average to core thermal power. The GT system provides the capability for bypassing individual GTs. Bypass conditions are alarmed in the MCR. The GT system provides for the calibration of the GTs. The GT system is designed to support required surveillance testing without affecting plant operation. It also provides the GT system self-diagnostics to the SC3 DCIS for display. The SC2 DPS, GTs, and ERIPs are redundantly and uninterruptedly powered by the SC2/SC3 electrical system load groups. The FMCRD motor controllers are normally powered from the SC2/SC3 electrical system and have dedicated SC2 UPS. The FMCRD UPS has a capacity that is at least twice as long as the duration of a motor run-in. The DPS, GTs, and ERIP UPS are backed by two load groups of batteries. The UPS and the battery chargers can be powered by offsite power or either of the SC3 standby diesel generators.

Robustness

The SC2 DPS proposed design reflects the use of design methods and adherence to engineering best practices to ensure that the protection functions are achieved for the specified conditions. The applicant states the SC2 systems have the required separation and independence to perform their intended functions as a diverse backup to SC1 equipment. The majority of the SC2 equipment is located in a separate fire barrier room in the CB with the remainder located in compartmentalized fire barrier rooms in the RB. It is separated from SC1 equipment that is located in three separate divisional fire barrier rooms in the RB. The SC2

equipment is powered by separate power supplies than the SC1 equipment. The four ERIPs are located in the RB near the cabinets housing the FMCRD motor controllers. The SC2 DPS uses sensors and actuators that are independent of SC1 equipment. Only isolated one-way communication is allowed from SC1 equipment to SC2 equipment. This communication cannot prevent either DLs from fulfilling its protection functions. SC2 equipment is independent from SC3 equipment to an extent that is practicable in that shared sensors are not credited with mitigation for the same PIE. As shown in PSAR Figure 7.3-8, some signals shared between SC2 and SC3 equipment, are used by both SC2 and SC3 TMR controllers allocated to each parameter performing SC2 and SC3 functions. The splitters for redundant signals are located in separate cabinets. The shared signals are developed using TMR architectures. Signal sharing is accomplished using non-software, analog splitters that are powered with redundant uninterruptable power supplies. The SC2 splitter technology supplies isolated outputs. The splitter design ensures a splitter output is unable to adversely affect the other outputs. The three channels of the SC2 DPS receive signals from separate SC2 splitters to be used by the 2oo3 voting logic for trips and initiations. The FMCRD motor controllers receive normal control signals from RC&IS; however, the ERIPs and DPS actuation signals have priority over the RC&IS control signal to run the rods in. The control rods and motors are located inside containment in the RB. The FMCRD motor controllers are organized into four groups located in four separate rooms in the RB outside containment. Four dedicated SC2 FMCRD UPSs provide the necessary independent power to operate the motors and monitor system operation. The power sources are also independent of the normal SC2 UPS that power the SC2 and SC3 DCIS. The ERIPs, FMCRD motor controllers, and the UPS to power them are arranged in four independent and separately located groups.

The DPS is monitored digitally through unidirectional isolated signals without adversely affecting SC2 functions. The digital monitoring checks for inconsistencies between redundant signals, performs sensor range checks, and monitors actuator, communication, and power supply status. The ERIP logic is designed to ensure that an actuation device failure can only affect one FMCRD. Motor run-in is initiated when a manual scram is initiated from either control room. The motor run-in actuation devices are sealed in for at least 4 minutes once energized to ensure the motors have time to drive the rods full in. The SC2 DPS has the required fail-as-is design features to perform its intended functions and avoid spurious actuations. The fail-as-is, energize to actuate, design is used to prevent lesser classified DPS from creating unnecessary challenges to plant safety requiring action by Safety Category 1 functions. Deliberate operator action is required to return the Safety Category 2 functions to normal after actuation. SC2 equipment operating by itself (or in combination with Safety Category 3 functions unaffected by the PIE) and assuming a complete failure of a Safety Category 1 function, ensures that no AOO or DBA causes a radiation release greater than regulatory requirements consistent with safety analysis assumptions described in Chapter 15 of this report. No SC1 equipment can prevent a scram, reactor isolation, containment isolation, or ICS initiation from SC2 equipment or vice versa. DPS initiates hydraulic scrams, isolations, and ICS using the same solenoids as Safety Category 1 functions but using actuation devices instead of load drivers. For diversity, the SC2 equipment is able to independently shut down the plant using the FMCRD motors. The SC2 ERIPs receive isolated hydraulic scram demand signals initiated by the Safety Category 1 hydraulic scram function, and Safety Category 3 anticipatory hydraulic scram functions to also initiate reactor shutdown using the FMCRD motors. The motor run-in inserts rods even if the hydraulic scram does not work or the entire SC1 system fails.

GTs provide a diverse technology to the neutron detecting LPRMs used in the SC1 system. The GT system segment supplies two types of outputs: average power signals and digital signals of individual sensor measurements. The GT signals are sent to four GT data acquisition cabinets

located in four separate rooms of the RB. The signals are apportioned to the four cabinets such that each cabinet gets a similar allocation of radial and axial GT signals. The digital GT signals are sent to SC3 equipment via the SC3 DCIS network.

Secure Development & Operational Environment

The applicant states that SC2 DPS and FMCRD software is produced in a secure development environment that prevents the insertion of undocumented code and precludes their use. The SC2 equipment adequately addresses access control to limit cyber security vulnerabilities and ensure the system can perform its intended functions. The SC2 DPS and FMCRD designs incorporate features to support establishment of a secure operational environment. The SC2 digital equipment is installed and maintained in accordance with the station administrative procedures and control of access programs. SC2 equipment diagnostics and internal data are available to the SC3 networks and controllers.

Diversity and Defense-In-Depth

The SC2 systems provide diverse protection functions to place and maintain the plant in a safe state in the event of PIE concurrent with failure of Safety Category 1 functions to support the D-in-D strategy. The design bases of the SC2 systems provide diversity and D-in-D for the complete failure of a Safety Category 1 function (i.e., CCF). Safety Category 2 functions independently provide safety functions comparable to the Safety Category 1 functions using diverse platforms from the SC1 equipment. The SC2 sensors are selected to be as diverse as practical from SC1 sensors. The ERICP provides diversity and D-in-D by sending the manual scram, Safety Category 1 hydraulic scram, and Safety Category 3 anticipatory hydraulic scram signals to the ERIPs to drive in rods by the FMCRDs. The Safety Category 2 method of actuation is diverse from the method of actuation implemented by the Safety Category 1 hydraulic scram function. The SC2 actuation relays are configured as energize to actuate whereas SC1 I&C load drivers are configured as de-energize to actuate which provides functional diversity in these actuation circuits. The ARI pilot valves described in PSAR Section 4.6 are energized to actuate and provide an alternate path to vent control air and open scram valves resulting in hydraulic insertion of control rods. The FMCRD motor controllers are required to be diverse from the SC1 I&C platform equipment and credited as a required mitigating function for a failure of Safety Category 1 hydraulic scram function due to CCF. A motor run-in results from scrams manually initiated via the MCR or the SCR to the ERIPs, with no involvement of RC&IS software. The FMCRD UPS provides additional D-in-D if normal power is lost.

Operator Interface and Accident Monitoring

Data obtained by the SC2 equipment is sent to the SC3 DCIS for display, recording, monitoring, and alarming. SC2 system bypass conditions are alarmed in the MCR. A reactor scram can be manually initiated by switches in the MCR or the SCR. SC2 sensors signals shared with SC3 equipment provide measurements that are diverse from SC1 sensors for selected parameters.

7.1.4.3 Nuclear Controllers including Anticipatory Trip System—DL2/SC3/Nuclear Segment

The SC3 nuclear segment, which contains the SC3 ATS, major reactor control, and the control rod blocking safety functions, complements the SC1 and SC2 I&C systems to provide D-in-D for the plant protection functions. The SC3 system acquires plant information from the sensors

specified for systems performing SC3 functions or from isolated signals shared from SC1 and SC3 systems. The plant information acquired is displayed on the SC3 integrated plant displays.

System Architecture

PSAR Figure 7.3-11 shows the preliminary functional architecture for the SC3 nuclear segment. Depending on final DCIS design and processor loading, multiple functions may be combined and implemented on a common controller. A representative block diagram for the Safety Category 3 anticipatory scram functions is shown in PSAR Figure 7.3-12. As shown in PSAR Figure 7.3-11, the SC3 nuclear segment employs TMR and redundant controller architectures for processing units to improve reliability or eliminate spurious control actions caused by a single hardware failure. Protection function and control signals needed between controllers for their functions use point-to-point wire or optical fiber connections. The SC3 nuclear segment of the DCIS provides both control and monitoring functions and supports both local and remote data acquisition.

System Design Bases and Associated Safety Functions

The design bases of the Safety Category 3 functions are to prevent or mitigate AOOs before either Safety Category 1 or Safety Category 2 functions are required. The SC3 hardware and software are diverse from SC1 equipment. The SC3 system design includes provision of instrumentation to monitor plant variables and systems over the respective ranges for operational states and during PIE. SC3 equipment is designed to be in service during all modes of plant operation. Specific safety functions are mode dependent, as determined by the Fault Evaluation process in Chapter 15 and specified by the Mode Switch position. As described in PSAR Section 7.3.3.2, the primary SC3 nuclear segment functions are:

1. Anticipatory Trip System (ATS)—The ATS is designed to perform the Safety Category 3 functions which are mitigating transients and providing investment protection for expected transients by tripping the plant in advance of any required Safety Category 1 or Safety Category 2 response. A failure in ATS does not adversely affect the Safety Category 1 or Safety Category 2 functions. The ATS uses logic like the Safety Category 1 hydraulic scram function and DPS. An ATS malfunction cannot prevent Safety Category 1 hydraulic scram nor can the Safety Category 1 hydraulic scram stop a Safety Category 3 ATS scram function. The ATS scram initiation and rod block signals are listed in PSAR Table 7.3-4. Simultaneously with the ATS hydraulic scram demand, a scram follow signal is generated for FMCRD motor run in. This signal is sent to the FMCRD whenever a hydraulic scram is demanded by ATS regardless of whether the hydraulic scram actuation has been successful. The ATS is designed to perform Safety Category 3 non-scram functions, including:

a. turbine trip on low main condenser vacuum
b. turbine bypass valves closure on low main condenser vacuum
c. turbine bypass valves fast open on fast closure of turbine control valve/turbine stop valve demand
d. MSRIV/MSCIV isolation on low main condenser vacuum
e. standby diesel generator start on low electrical bus voltage
f. FW and condensate pumps trip on high RPV level
g. FW isolation on High-High RPV level
h. ICS pressure control on high reactor pressure

The setpoints for SC3 ATS actuation logic are selected to act before Safety Category 1 functions, since its design bases are to mitigate/prevent Safety Category 1 functions from needing to respond.

2. Plant Automation System (PAS)—The PAS coordinates automatic reactor power control as part of a larger automation scheme, including coordination of SC3 control systems (for control of nuclear equipment) and coordination of SCN control systems (for control of BOP equipment). The SC3 and SCN control systems need to individually be put into automatic mode by the operator for this automation to be functional; without this operator action, any commands originating from the PAS are ignored. The PAS provides batch control of the steps needed to automate the plant systems used to bring the reactor from cold conditions to rated power.
3. Reactor Level Control (RLC)—The RLC provides reactor level monitoring and control from cold conditions through pressurization and heat up to power operation. This system controls reactor level at greater than 10–15 percent power by adjusting the frequency of the adjustable speed drives of the FW pump motors. At lower powers, the system uses a low flow control valve supplied with either a condensate pump or feed pump operating at fixed speeds, depending upon reactor pressure. The RLC also operates level control valves in the shutdown cooling system (SDC) and the reactor water cleanup system (CUW) when water is rejected from the reactor vessel during cold and heat up operations.
4. Feedwater Temperature Control—The feedwater temperature control controls the feedwater temperature delivered to the reactor by the sixth stage FW heater by measuring the heater exit temperature and modulating a steam heating valve as required to meet the demanded temperature setpoint. The FW temperature is programmed as a function of reactor power and the temperature is held constant between 90 and 100 percent thermal power and then decreased as power is further reduced. Appropriate function logic features are provided to keep the FW nozzle temperatures from changing too rapidly. The controller also provides the sixth stage FW heater level control necessary to keep the FW heater level at the optimum setpoint for best heat transfer.
5. Reactor Pressure Control (RPC)—RPC provides control from a cold vessel through pressurization and heat up to power operation. During plant operation this system normally controls reactor pressure by sending a flow demand signal to the turbine controller. During plant startup or at other times when the turbine is off-line, RPC adjusts reactor pressure by sending a flow demand signal to the turbine bypass valves.
6. IC Pressure Control—Three BWRX-300 ICs have a very large capacity for reactor pressure reduction. While desirable in safety systems, this capacity can result in exceeding the normal allowed cooldown rate for the reactor vessel. The ICs are each initiated by opening either of two condensate return valves that are installed in parallel. Both valves are “open or close” and can be actuated by the SC1 protection system and the SC2 DPS. One valve is also controlled by SC3 I&C system.
7. Turbine-Generator Control—In addition to performing the normal function of controlling positions of the turbine control valves and bypass valves, the turbine-generator controller

provides the turbine protection functions (e.g., turbine overspeed protection). The turbine-generator controller also provides trip and load rejection signals to the ATS and similar signals to the RPC to quickly open the bypass valves. The turbine-generator controller is used in plant automation to allow the turbine to be rolled, synchronized, and initially loaded.

8. Rod Control and Information System (RC&IS)—The RC&IS provides the control logic and positions control rods using the fine motion drive motors. RC&IS is supervised by blocking functions to ensure that the sequences are followed, and no thermal limits or fuel operating guidelines are exceeded. In the automatic mode, RC&IS accepts insert and withdraw commands from automatic power regulator (APR). The automatic thermal limit monitor (ATLM) and multi-channel rod block monitor (MRBM) are always functioning to supervise and block control rod motion. At higher thermal power levels, manual movement commands deviating from the sequence are alarmed. RC&IS moves the control rods to a predefined rod pattern (by insertion only) when a selected control rod run-in (SCRRI) demand is issued. The SCRRI rod pattern is chosen to achieve a specific reactor power. The RC&IS provides position demands to the control rod motor controllers and drives which are in SC2 equipment. The SC2 design features allow the FMCRDs to be commanded to full in or to be blocked by disabling rod withdrawal regardless of RC&IS status or RC&IS positioning demand signals. The design allows a Safety Category 3 function to give commands to an SC2 system because the SC3 system is supervised by the blocking systems.
9. Containment Inerting/Nuclear Boiler Control—The containment inerting function provides monitoring and control for the generation and storage of nitrogen gas to do the initial containment fill and thereafter to make up for the small long-term losses. It also supplies nitrogen to any inside containment pneumatic valves. The I&C nuclear boiler function acquires signals from the nuclear boiler system into the SC3 DCIS to provide monitoring and control functions for nuclear boiler system SC3 equipment.
10. Shutdown Cooling Control (SDC)—The shutdown cooling function provides separate controllers for monitoring and control for the SDC system to remove decay heat from the reactor. There are two separate SDC controllers that respectively operate the redundant SDC. The SDC controllers can receive commands from the PAS or can be manually operated.
11. Containment Cooling Control—The containment cooling function provides redundant monitoring and control of the redundant containment air handling units with chilled water cooling during normal operation or during an outage.
12. IC and Fuel Pool Cooling and Cleanup System (FPC) Control—The IC and fuel pool cooling, and cleanup function provides monitoring and control for the ICS pool, ICS redundant heat exchangers, ICS pumps and their associated valves, and the FPC. The controller interfaces with redundant pumps and heat exchangers and filter demineralizers. The controller also includes logic to start a standby pump if an operating pump trips.
13. Service water (SW), plant cooling water (PCW), and chilled water equipment (CWE) control —The SW, PCW, and CWE function provides redundant monitoring and control for the SW, PCW, and CWE pumps and valves.
14. SC2/SC3 Electric System Control—The SC2/SC3 electric system feeder breakers, load center breakers, motor control center breakers, and diesel generator breakers interface with the two SC2/SC3 electric system controllers for control and monitoring. These breakers perform their protection functions independently of I&C control. The diesel generator breakers close automatically after a loss of associated bus power. The SC2/SC3 electric system controllers control the sequencing of the standby diesel generator loads to minimize operator involvement. These controllers also provide monitoring of the electric system parameters and for the SC2 UPS, battery chargers, and batteries.

15. SC2/SC3 Protective Relay Monitoring—The SC2/SC3 protective relay monitoring function is to interface with the relays through gateways as necessary, so data is available to I&C to support operator displays and alarms of electrical system status and for advanced condition monitoring.
16. RB and CB Heating, Ventilation, and Cooling System (HVS) Control—The RB and CB HVS provides redundant monitoring and control for automatic operation of the normal RB and CB HVS requirements by controlling the redundant cooling of the various RB and CB air handling units, building intake and exhaust fans, recirculating fans, damper, and chilled water control valve operation.
17. Process Radiation Monitoring—The SC3 controller is used for the acquisition of the various process radiation measurements, alarms, and diagnostics, and transmission of these data to the SC3 nuclear segment networks with appropriate isolation or using appropriate safety class equipment to generate and transmit the data.
18. SC3 Gateways—The SC3 gateways are used to bring data-linked signals to the SC3 nuclear segment networks. The signals from SC1 systems are isolated with SC1 isolators at the source. The two SC3 gateways perform three functions: (1) provide another layer of isolation that prevents communication back to the SC1 sources, (2) provide protocol conversion of the signals from SC1 systems to be compatible with the plant networks and package the data into messages for specific SC3 controllers, and (3) accept data links from SC2, SC3, or SCN sources that are input to the SC3 nuclear segment.
19. Automatic Thermal Limit Monitor (ATLM)—The ATLM function provides redundant protection against critical power ratio (a fuel heat flux to flow consideration) and linear heat generation rate (maximum heat flux through the fuel clad) design limits. This online monitoring of thermal limits and fuel operating guidelines uses LPRM and APRM data sent via qualified isolation devices. The fuel operating guidelines keep the fuel duty per node below previously conditioned power levels to prevent fuel failures. Operation above the preconditioned envelope per node is constrained to slow power changes. The ATLM rod blocks are automatically operative at higher reactor powers. The ATLM receives online LPRM data and uses it with previously stored and periodically updated 3-D power distribution and RC&IS data for current rod positions and the next selected rods to be moved. This data is used to predict the resulting thermal limits and nodal powers for the fuel operating guidelines. If the prediction anticipates a thermal limits or soft duty guideline violation, the control rod motion is blocked.
20. Multi-Channel Rod Block Monitor (MRBM)—The MRBM provides redundant protection against critical power ratio and linear heat generation rate design limits. The MRBM rod blocks are automatically operative at higher reactor powers. The redundant MRBMs use LPRM and APRM data received from qualified isolation devices and control rod status from RC&IS. The MRBMs operate after receiving a signal from RC&IS that rods have been selected for motion. The MRBMs, using the real time LPRM information received, identify the LPRMs around the selected rods and normalize their average to a nominal value. As the selected rods are being withdrawn, the LPRM average around the selected rods increases in value. If the ratio of the withdrawing average to the initial average increases by too great an amount, it indicates that the local power has increased by an amount that would violate fuel thermal limits. Under those circumstances, the MRBMs issue a rod block.
21. Wide Range Neutron Monitor (WRNM)—The WRNM function provides redundant monitoring of the fixed neutron monitoring detectors in the core. The main use of the detector data is to determine reactor period per detector. These period data are representative of the whole core and are used for monitoring and by APR. Both the operator and APR use the data when starting the reactor. Either WRNM can cause a control rod withdrawal block (unless bypassed) for a short period and either can cause a hydraulic scram (when reactor mode switch is in STARTUP) via the ATS for a shorter period.

22. Safety Parameter Display System (SPDS)—The SPDS provides an overview display of plant parameters during transients and accidents. The SPDS functionality is included within the SC3 equipment. The SPDS presents sufficient information on safety-critical parameters and includes display and trending of the parameters associated with the emergency procedure guidelines for the plant.
23. Technical Specifications (TS) Monitor—The TS monitor monitors signals and alarm deviations from plant TS requirements. Redundant input signals from the SC1 divisions used for safety actuation are continuously compared by the TS monitors during operation and alarmed for deviations outside of established tolerance. The TS monitors are a redundant pair of processing units, which communicate among themselves for validation of determinations. The TS monitors have their own self-diagnostics, and the loss of a TS monitor is alarmed.
24. Core Thermal Power/Flow Monitor—The core thermal power/flow monitors use redundant pairs of processing units that calculate reactor thermal power and core flow. The thermal power is calculated once per second. The lowest power levels are estimated from the WRNM system and the intermediate power levels from the low flow FW system and bypass valve position. In the normal power range (approximately 10 to 100 percent thermal power), the calculation is done using a heat balance. All the heat balance parameters are measured and, in most cases, redundant. The most important measurements, FW flow, FW temperature and reactor pressure are triply redundant. Natural circulation core flow is calculated by a heat balance around the core inlet. Alarms are provided if sensed parameters are missing or inconsistent. The core thermal power/flow monitors have their own self-diagnostics. The loss of a monitor results in an alarm.
25. Three-dimensional Core Thermal Power Distribution Monitor—The redundant 3-D core thermal power distribution monitor computers each provide core monitoring, fuel operating guidelines, and thermal limit information. These computers use thermal power calculation, core flow calculation, LPRM data, GT data, and control rod position data to determine the core 3-D power distribution. The program runs periodically (typically every hour), and on-demand from the operator or ATLM. Thermal limits and other diagnostics are alarmed, and data are recorded in the plant historians. The core monitors have their own self-diagnostics, and the loss of a monitor results in an alarm.
26. Plant Alarm System—The plant alarm system provides aggregated process alarms and self-diagnostic data from the plant control and monitoring systems. The alarms and data are prioritized and filtered by plant mode and events. The alarm system also provides annunciator displays integrated into the MCR video displays. The alarms are available to the operator and recorded in the plant historians. Alarm information is available in both control rooms and to perform the technical support center function. The alarm systems are redundant pairs of processing units that each monitor plant data. The alarms are available even with a single alarm system failure.
27. Plant Historians and Monitoring—The plant historians and monitoring computer provides archiving of the plant control, alarm, and monitoring system information. The data are recorded at least once per second, depending on the parameter. The recording capacity is designed to at least collect data from a fuel cycle. The historians allow archival storage and playback while the plant is online and support operator-initiated data trending on control room displays or report printouts. The historians are redundant pairs of processing units that each monitor plant data. The stored data is still available even with a single historian failure.
28. Fiber Optic Relay Panels—The fiber optic relay panels provide the capability to send data across SC boundaries when the use of data links and networks is not indicated. These relay panels containing optical fiber transmitters and receivers can transmit either analog or discrete contact signals without the use of any software.

Fundamental Design Properties in the System Design

The SC3 system includes DL1 properties that represent the quality measures implemented to minimize potential for failures and initiating events to occur in the first place. These DL1 properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed below.

Equipment Qualification

The applicant stated that SC3 equipment is designed to operate in the postulated environment during normal operations and anticipated off-normal conditions. The SC3 equipment is qualified to perform its intended functions and meets the applicable IEC standards for Class 3 systems. The SC3 equipment is qualified for seismic interaction if required for mitigation of seismic-related events. The SC3 equipment is qualified for electromagnetic compatibility. Additional information on equipment qualification can be found in Section 3.11 of this report.

Reliability

The applicant states that its SC3 nuclear segment has the required reliability to perform its intended functions. SC3 hardware platform uses TMR controllers for the major plant control systems. The TMR controllers are designed to prevent random I&C component failures from causing plant transients. The TMR controller outputs are dual ported to the plant SC3 nuclear segment network. Where a mechanical system has safety functions and is redundant (i.e., “A” and “B”), two controllers are furnished so the redundant components may be operated separately, and the system is not affected by a single failure. For the functions with TMR controllers, single controller failures (and some double failures) have no adverse effect on system or plant operation, and failed controller parts may be replaced online. The SC3 equipment is designed with a specific intent that no random controller failure initiates an AOO. SC3 nuclear segment rod block functions are implemented on redundant processors for reliability. Normally both redundancies are online, and their data continuously compared. Any one redundancy can be bypassed at a time but, if bypassed, it takes the plant out of automation mode. Design reliability assurance program and reliability, availability, and maintainability plan documents are used to quantify the required failure rates of the DCIS to assure plant safety and plant availability goals. Extensive hardware and software diagnostics are provided for the TMR controllers to provide operator monitoring and alarms. The SC3 equipment is powered by the SC2/SC3 electrical system which provides redundant UPS and power feeds.

Robustness

Robustness of the SC3 nuclear segment is the degree to which it can function correctly in the presence of invalid inputs or stressful environmental conditions. The SC3 nuclear segment has the required separation and independence to perform its intended functions. SC3 equipment is independent from SC1 equipment. SC3 functions are also independent from SC2 functions to an extent that is practicable in that shared sensors are not credited with mitigation of the same PIE. SC2 and SC3 functions share support equipment. SC3 functions are designed to ensure that they cannot adversely affect SC1 or SC2 functions from fulfilling their protection functions. The SC3 equipment is located in two separate fire barrier rooms in the CB. There is no communication from SC3 equipment to SC1 equipment. Only rod block or motor run-in initiation (dry contact) communication for SC3 segment is sent to the SC2 ERIPs. The SC3 nuclear segment has the required fail-as-is design features to perform its intended functions and avoid spurious actuation. The fail-as-is, energize to actuate, design is used to prevent lesser classified

systems (e.g., anticipatory trip system) from creating unnecessary challenges to plant safety (e.g., spurious actuations for expected failures) requiring action by SC1 functions. Software-based SC3 equipment includes watchdog timers, sensor range checks, and monitoring of power supplies, communications, and actuators. ATS and reactor control system TMR controller uses three signals from SC2 splitters, and a fourth SC3 signal. Typically, these parameters include containment pressure, reactor level, reactor pressure, and condenser vacuum scrams. Each ATS controller and reactor control system validates the analog signal with a range and consistency check, compares each of the four signals to a common setpoint, and then indicates the analog value and trip status. For example, the reactor level and pressure controller analog validation algorithms use the three splitter signals from SC2 equipment, and the fourth signal dedicated to SC3 functions to make a fault tolerant control signal that functions even if the splitter signals are lost. This scheme is used to provide reliable trips and avoid inadvertent trips.

Secure Development and Operational Environment

The SC3 nuclear segment design incorporates features to support establishment of a secure operational environment. It is installed and maintained in accordance with the station administrative procedures and control of access programs. Communications on the nuclear segment UDHs are rigorously controlled and monitored and information sent outside the plant network is through unidirectional boundary devices. The SC3 nuclear segment adequately addresses security to limit cyber security vulnerabilities and ensure the system can perform its intended functions.

Diversity and Defense-In-Depth

The SC3 nuclear segment provides anticipatory trip functions to support the D-in-D strategy. The SC3 hardware and software are diverse from SC1 equipment. The SC3 ATS actuation relays are configured as energize to actuate whereas the SC1 I&C load drivers are configured as de-energize to actuate, which provides functional diversity in these actuation circuits. Diversity measures are incorporated within the SC3 nuclear segment design as an additional level of protection for potential systematic faults caused by design and implementation defects when equipment is credited as a backup in the safety analyses. The use of a fourth SC3 signal provides immunity against loss of control signals due to the postulated CCF of the SC2 signal splitters. Safety Category 3 functions can initiate hydraulic scram, automatically and manually initiate isolations, and operate the ICS. SC3 equipment cannot prevent a scram, isolation, or ICS initiation actuated from SC1 or SC2 systems. Similarly, Safety Category 1 and Safety Category 2 functions cannot adversely affect Safety Category 3 functions. SC3 equipment is powered by UPS with battery backups, the power supply is redundant, and a single failure does not affect an SC3 function or segment. Power feeds to equipment performing Safety Category 2 or Safety Category 3 functions are not shared with SC1 equipment. The processing units used for the control rod blocking functions are implemented in equipment diverse from the SC1 equipment if it is credited as a backup in the safety analyses. The turbine overspeed protection control logic uses two diverse and independent systems to provide sufficient reliability to eliminate the risk of turbine missile generation and to avoid the need for a mechanical overspeed trip. These turbine overspeed protection systems use TMR control architecture to eliminate random hardware vulnerabilities that could result in spurious turbine trips.

Operator Interface and Accident Monitoring

The SC3 data are available on their appropriate displays in the MCR, SCR, and locally in the SC3 equipment rooms. The SC3 displays also include an alarm system. SC3 system bypass

conditions are alarmed in the MCR. The SC3 system acquires accident monitoring information associated with Type B and C accident monitoring variables from the SC1 I&C system. Type D, E, and F accident monitoring variables are implemented in the SC3 and SCN equipment. The aggregated SC3 displays of accident monitoring information are provided to the MCR and the SCR. Type D, E, and F variables are categorized as SC3. A preliminary list of the Type D, E, and F accident monitoring variables is provided in PSAR Table 7.3-2.

7.1.4.4 Balance of Plant Controllers – SCN/BOP Segment

The SCN BOP controllers that feed the SC3 BOP segment contains the control and monitoring systems associated with power generation and support systems.

Systems Architecture

PSAR Figure 7.3-13 shows the functional architecture of the SCN BOP controllers. The functions shown using TMR controllers are dual ported to the plant SC3 BOP segment network. The other functions are packaged systems provided by an equipment vendor. Control signals needed between controllers for their functions are point-to-point wire or optical fiber. The signals needed by a controller for its functions are radially connected to the controller and do not use plant networks.

System Design Bases and Associated Safety Functions

The design bases of the SCN BOP controllers are to provide for the control and monitoring of the SCN power generation and support equipment. This equipment is not credited for protection functions, although it may be available for beyond design basis events and severe accident scenarios.

The main functions of the SCN I&C system are described in the PSAR Section 7.3.4.2 and include the following SSCs:

1. condensate and FW
2. FW Heater Drains and Extraction Steam
3. condenser
4. turbine auxiliaries
5. generator auxiliaries
6. moisture separator reheater
7. turbine bypass valves
8. reactor water cleanup system (CUW)
9. circulating water
10. intake structure
11. turbine and radwaste building HVS
12. service air, instrument air, and plant gas systems
13. condensate polishing system
14. SCN electric system
15. SCN protective relaying
16. condensate storage and transfer
17. equipment and floor drains system
18. potable water and sewage
19. hydrogen water chemistry and noble metal injection
20. liquid and solid waste management and offgas

21. BOP gateways – the applicant states that the BWRX-300 uses many packaged systems bought from vendors instead of being designed and implemented by GVH. These vendor systems are integrated into the plant DCIS for both monitoring and control purposes.
22. fire protection (packaged)
23. water treatment (packaged)
24. clock (packaged)
25. equipment condition monitoring (packaged)
26. seismic monitoring system (packaged)
27. area radiation monitoring system (packaged)
28. meteorological monitoring system (packaged)
29. environmental monitoring system (packaged)

Fundamental Design Properties in the System Design

The SCN system properties are based on the quality measures implemented to minimize the potential for failures and initiating events to occur. The SCN systems are conservatively designed and analyzed.

These SCN system properties of qualification, reliability, robustness, security, diversity, and other D-in-D features are discussed below:

Equipment Qualification

The applicant states that SCN BOP controllers are designed to operate in the environment that is to be expected during normal operations. The SCN BOP controller design and manufacturing processes are of sufficient quality to ensure that I&C systems can reliably perform their design bases functions. The SCN BOP controller equipment is designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The SCN BOP controller equipment is assessed as a potential hazard when it is located near safety classified equipment and, if necessary, qualified for electromagnetic compatibility only for emissions.

Reliability

The applicant states that the SCN BOP controllers have the required reliability to perform their intended functions. It further states that the reliability analysis of the SC3 BOP segment demonstrates it meets its reliability goals using qualitative and quantitative performance measures or criteria, as appropriate. Separately, the SCN BOP controllers have the required reliability to perform their intended functions. SCN BOP controllers are implemented with redundancy as appropriate to ensure that single controller failures have no adverse effect on system or plant operation. The controllers have a specific reliability requirement goal which ensures that the frequency of failures is not more than once per 100 years. The intent is that no random controller failure initiates an AOO. Extensive hardware and software diagnostics are provided for the TMR controllers to provide operator monitoring and alarms. The main SCN BOP controller platform's control and monitor design support both local and remote data acquisition. The intent is that the failure of a SCN controller does not initiate an AOO.

Robustness

The SCN BOP controllers have no direct connections (i.e., commands or communication) with the SC1 systems. The SCN BOP controller equipment is in different rooms than the SC3

nuclear segment rooms and physically separated from SC1 and SC2 equipment rooms. Vendor supplied SCN hardware is connected through an SC3 gateway.

Security

The SCN BOP controller design incorporates features to support establishment of a secure operational environment. This equipment is installed and maintained in accordance with the station administrative procedures and control of access programs. The vendor-packaged SCN BOP controllers are interfaced to the SC3 BOP segment through SC3 gateways to provide communication protocol conversion and eliminate cyber security vulnerabilities.

7.1.5 Digital Instrumentation and Control System Development Processes

PSAR Section 7.4 and Figures 7.4-1 and 7.4-2 outline the development process for the digital I&C control system. The software-related development process is summarized in PSAR Section 7.4.3 and Figure 7.4-3.

7.2 Regulatory Requirements, Regulatory Guidance, and Industry Standards

In PSAR Section 7.1.3.1, the applicant states that the content of PSAR Chapter 7 is aligned with the review guidance in "Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews" (NRC 2021-TN13282~~ML21011A140~~). Although the DRG is primarily intended for review of the non-LWR I&C system designs, it is technology inclusive and the applicant specifically requested that the DRG be used as an alternate approach to the NUREG-0800, Chapter 7, SRPs. Since the DRG can apply to LWR designs, it can be used for the review of the CRN-1 I&C design, including the implementation of safety classifications, as described by NEDC-33934P, "BWRX-300 Safety Strategy" GE Hitachi Nuclear Energy Americas LLC, Revision 2, March 2026 (GE Hitachi 2026-TN13283~~ML26077A383~~, non-proprietary, ML26077A382, proprietary). Further, I&C designs are inherently technology inclusive, given that they function as a product of common parameters shared among all reactor designs.

Commented [TC1]: Reference Team

7.2.1 Introduction

Chapter 7 of the PSAR describes the CRN-1 integrated I&C systems of systems designed as Distributed Control and Information System (DCIS). I&C functional requirements and performance objectives are identified based on the level of protection offered by each defensive line and are discussed in SE S~~s~~ection 7.1.2.

7.2.2 Regulatory Evaluation

Listed below are the applicable regulatory requirements and guidance that form the acceptance criteria for the NRC staff's review of the CRN-1 I&C systems. It should be noted that the NRC staff evaluated the information provided in PSAR Section 7.2, against the applicable portions of Standard Review Plan (SRP) Chapter 7 and applicable NRC regulations and guidance.

Regulatory Requirements:

- 10 CFR 50.34(f)(2)(iv) (TN249), related to safety parameter display console with respect to displays and monitoring requirements

- 10 CFR 50.34(f)(2)(v), related to bypass and inoperable status indication with respect to operating bypass, maintenance bypass, and displays and monitoring requirements
- 10 CFR 50.34(f)(2)(xiv), related to containment isolation systems with respect to actuation system requirements
- 10 CFR 50.34(f)(2)(xvii), related to accident monitoring instrumentation
- 10 CFR 50.34(f)(2)(xviii), related to instrumentation for the detection of inadequate core cooling
- 10 CFR 50.34(f)(2)(xix), related to instruments for monitoring plant conditions following core damage
- 10 CFR 50.34(f)(2)(xxiv), related to central reactor vessel water level recording
- 10 CFR 50.34(h), "Conformance with the Standard Review Plan," related to the NRC staff's review of the proposed I&C system
- 10 CFR 50.44(c)(4), related to combustible gas control monitoring
- 10 CFR 50.55a(h)(3), related to meeting requirements of IEEE Std 603-1991 and the correction sheet dated January 30, 1995
- 10 CFR 50.55a(z), "Alternatives to codes and standards requirements," allows use of alternatives to the requirements of 10 CFR 50.55a(h), when authorized by the NRC
- 10 CFR 50.62(c)(3), related to requirements for reduction of risk from anticipated transients without scram (ATWS) events
- 10 CFR Part 50, Appendix A, "General Design Criteria (GDC) for Nuclear Power Plants," applicable to the CRN-1 I&C systems:
  - GDC 1 – Quality standards and records
  - GDC 2 – Design bases for protection against natural phenomena
  - GDC 4 – Environmental and dynamic effects design bases
  - GDC 10 – Reactor design
  - GDC 13 – Instrumentation and control
  - GDC 15 – Reactor coolant system design
  - GDC 16 – Containment design
  - PDC 19 – Control room
  - GDC 20 – Protection system functions
  - GDC 21 – Protection system reliability and testability
  - GDC 22 – Protection system independence
  - GDC 23 – Protection system failure modes
  - GDC 24 – Separation of protection and control systems
  - GDC 25 – Protection system requirements for reactivity control malfunctions
  - GDC 26 – Reactivity control system redundancy and capability
  - GDC 28 – Reactivity limits

- GDC 29 – Protection against anticipated operational occurrences
- GDC 33 – Reactor coolant makeup
- GDC 34 – Residual heat removal
- GDC 35 – Emergency core cooling
- GDC 63 – Monitoring fuel and waste storage
- GDC 64 – Monitoring radioactivity releases

Commission Policy

Formatted: Space After: 12 pt

- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, item II.Q, as clarified by SRM-SECY-93-087, "SECY-93-087 – Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993, item 18, describes the NRC's position on defense against potential common-mode failures in DI&C systems
- SRM-SECY-22-0076, "Staff Requirements – SECY-22-0076 – Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems," dated May 25, 2023

Regulatory Guidance and Industry Standards

The CRN-1 I&C systems are designed to conform to several NRC-endorsed standards as well as to some alternative industry standards in lieu of NRC-endorsed standards. With respect to NRC-endorsed standards, the CRN-1 I&C systems are designed to conform to:

- Design Review Guide (DRG), "Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews," February 26, 2021
- RG 1.89, Rev. 2 (NRC 2023-TN10967), "Equipment Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," issued April 2023
- RG 1.180, Rev.2 (NRC 2019-TN12943), "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," issued December 2019

In addition to conformance with the above NRC-endorsed standards, the CRN-1 I&C systems are designed to conform to alternative Institute of Electrical and Electronics Engineers (IEEE) standards and International Electrotechnical Commission (IEC) standards instead of certain NRC-endorsed standards applicable to I&C systems as described by various regulatory guides. PSAR Tables 1.9-20 and 7.1-3 identify conformance to the alternative industry standards instead of the standards endorsed by the NRC in the following regulatory guides:

Formatted: Left

Table 7.2-1~~Table 7.2-1~~ ~~–~~ Alignment of Regulatory Guides to BWRX-300 Alternative Industry Standards

Reg. Guide	Reg. Guide Title	Alternative Industry Standard
1.22	Periodic Testing of Protection System Actuation Functions	IEC 60671:2007 IEC 62385:2007

Reg. Guide	Reg. Guide Title	Alternative Industry Standard
1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	IEEE Std 603-2018
1.53	Application of the Single-Failure Criterion to Safety Systems	IEEE Std 379-2014 IEEE Std 603-2018
1.62	Manual Initiation of Protective Actions	IEEE Std 603-2018
1.75	Criteria for Independence of Electrical Safety Systems	IEC 60709:2018 IEC 62808:2018
1.97	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	IEC 63147:2017/IEEE 497-2016
1.100	Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants	IEC/IEEE 60980-344:2020
1.105	Setpoints for Safety-Related Instrumentation	IEC 61888:2002
1.118	Periodic Testing of Electric Power and Protection Systems	IEC 60671:2007 IEC 62385:2007
1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.153	Criteria for Safety Systems	IEEE Std 603-2018
1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018

Reg. Guide	Reg. Guide Title	Alternative Industry Standard
1.170	Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant	System and Software Development IEC 61513:2011 IEC 60880:2006 IEC 62566:2012 IEC 62138:2018 SDOE IEC 62645:2019 IEC 62859:2016 Communication Independence IEC 61500:2018
1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	IEC/IEEE 60780-323:2016
1.227	Wide-Range Spent Fuel Pool Level Instrumentation	IEC 63147/IEEE 497:2017

7.2.3 Technical Evaluation

The NRC staff used the guidance in “Design Review Guide (DRG): Instrumentation and Controls for Non-LWR Reviews,” to evaluate the CRN-1 I&C systems design. Interim Staff

Guidance DNRL-ISG-2022-01, “Safety Review of Light-Water Power Reactor Construction Permit Applications,” also provides guidance to facilitate the NRC staff’s safety review of light-water power reactor CPAs. I&C design-specific review guidance provided in Appendix A of DNRL-ISG-2022-01 states that in evaluating a CPA, the NRC staff should focus on the following elements of the I&C design:

- An overall I&C architecture that demonstrates adherence to the fundamental I&C design principles.
- Plant safety functions allocated to each of the safety-related I&C systems.
- Proposed communications between safety-related and non-safety-related I&C systems.
- Regulations that the applicant intends to comply with for the I&C design.
- Regulations that the applicant intends to take exemption from or deems not applicable to its design.
- Topical reports incorporated by reference in the application.

Assessment of I&C Architecture

The architecture of the overall CRN-1 I&C system is described in PSAR Sections 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.3.1.1, 7.3.2.1, 7.3.3.1, and 7.3.4.1, and depicted in PSAR Figures 7.2-1, 7.2-2, and 7.2-3. Based on the I&C architecture information provided in the PSAR and the discussion in Sections 7.1.3 and 7.1.4 of this SE, the NRC staff finds that the preliminary I&C architecture appears sufficiently robust, reliable, and reflects the fundamental I&C design principles of independence, redundancy, diversity in support of D-in-D, and deterministic behavior (predictability and repeatability) necessary for the CP stage and that final determination will occur during the FSAR review. The architecture description of each individual I&C system includes (1) the I&C functions allocated to the system that support implementation of the overall I&C architecture design; (2) the identification of the redundancy (i.e., divisions) within each safety-related system to support meeting the single-failure criterion; and (3) the identification of all physical and logical interfaces and the purpose of each interface.

Diagrams of the overall I&C architecture illustrate the I&C system architecture principles and concepts. As discussed in Sections 7.1.3, 7.1.4, and 7.1.5 of this SE, sufficient detail is provided in the PSAR figures as follows:

- all the safety-related I&C systems and all the I&C systems that are not safety-related
- connections between the above systems
- interfaces and means of communication between the individual I&C systems
- identification of signal and isolation devices
- signal and data flow paths

Allocation of Important to Safety Functions

PSAR Section 3.2.1 describes assignment of safety categories to functions, and PSAR Section 3.2.2 describes safety class to components. Categories of safety functions (associated with fundamental safety functions [FSFs]) assigned to the applicable safety class of I&C systems as described in PSAR Section 7.3 are outlined below.

The FSFs for CRN-1 are:

- control of reactivity
- removal of heat from the fuel (in the reactor, during fuel storage and including long-term heat removal)
- confinement of radioactive material, shielding against radiation, and control of planned radioactive releases, as well as limitation of accidental radioactive releases

Table 7.2-2~~Table 7.2-2~~ I&C System Safety Classification

Important to Safety Function	I&C System Safety Class
Safety Category 3 DL2 functions—Actively control key plant parameters associated with FSFs and detect and mitigate AOO PIEs.	Anticipatory Trip System – Safety Class 3 (SC3)
Safety Category 1 DL3 functions—Detect and mitigate DBA PIEs and event sequences comprising AOO PIEs and failure of DL2 functions	Primary Protection System – Safety Class 1 (SC1)
Safety Category 2 DL4a functions—Detect and mitigate design extension conditions (DEC) or BDBE, including event sequences associated with some DBA PIEs and failure of DL3 functions.	Diverse Protections System – Safety Class 2 (SC2)
Safety Category 3 DL4b Functions—Detect and mitigate DECs to prevent core damage or mitigate the consequences of core damage events (severe accidents).	To be determined in the final safety analysis report (FSAR) – Safety Class 3 (SC3)

The DL3 functions, categorized as Safety Category 1 and implemented in SC1 I&C equipment, are discussed above in Section 7.1.4.1 of this SE.
The DL4a functions, categorized as Safety Category 2 and implemented in SC3 I&C equipment, are discussed above in Section 7.1.4.2 of this SE.
The DL2 functions, categorized as Safety Category 3 and implemented in SC3 I&C equipment, are discussed above in Section 7.1.4.3 of this SE.

Communications between safety-related and non-safety-related I&C systems

As discussed in Section 7.1.4.1~~7.1.4.1~~ of this report, the SC1 signals are hardwired per division to the SC1 cabinets, and the cabinet outputs are hardwired to their actuators. Remote data acquisition multiplexers are not required because the SC1 I&C system and SC1 signals are mostly located in the RB. The voting communication between divisions contains message authentication and divisional or parameter trip status, and if there is a loss of communication from a division, the receiving division assumes a trip. The data acquisition functions are implemented on SC1 I&C hardware and software platforms in the SC1 cabinets with a common backbone to the SC1 communications function. The backbone ensures that SC1 I&C platforms in a division have access to the SC1 signals in that division and the communication function ensures that divisional data are isolated and sent through a unidirectional boundary device to the SC3 gateways.

As discussed in Section 7.1.4.2~~7.1.4.2~~ of this report, protection function signals within the SC2 equipment do not use the plant networks. The RC&IS communicates with the FMCRD motor controllers (which perform a Safety Category 2 function) on a dedicated redundant network. The FMCRD network is not part of the plant DCIS network and does not go through the network managed switches. This communication is not required for any Safety Category 2 function, nor could it interfere with any Safety Category 2 function. The splitter arrangement used for shared SC2 sensors is shown in PSAR Figure 7.3-9. These SC2 classified splitters are analog and

provide both input/output isolation and isolation between outputs. As shown in FSAR Figure 7.2-1, DL4a/SC2 data are isolated and sent through a unidirectional boundary device to the SC3 DPS diagnostics system.

As discussed in Section 7.1.4.3 of this report, SC3 control signals needed between controllers for their Safety Category 3 functions are point-to-point wire or optical fiber. As discussed in Section 7.1.3.2 of this SE and shown in PSAR Figure 7.2-1, SC3 I&C systems communicate via SC3 UDH Nuclear Segment.

Compliance with Applicable Regulatory Requirements

Listed below are the GDCs in 10 CFR Part 50 (TN249), Appendix A, that are applicable to the CRN-1 I&C systems, along with the NRC staff's evaluation of the compliance of the CRN-1 I&C systems with those GDCs.

GDC 1——Quality standards and records

GDC 1 requires in part that, "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to ensure a quality product in keeping with the required safety function."

Formatted: Body Text

The applicant states that to meet, in part, the requirements of GDC 1, it cites IEEE Std. 603-2018 as an alternative approach to those standards cited in multiple RGs (refer to Section 7.2.2 Regulatory Evaluation of this SE). The staff will evaluate each of these alternatives to verify that each meets the intent of the cited reference in the specific RG at both the CP stage and the operating license submittal. The staff notes that during the staff's review of the PSAR, to satisfy RG 1.62 (NRC 2010-TN12944), it uses IEEE Std. 603-2018 as an alternative to IEEE Std. 603-1991.

IEEE 603-2018 Clause 6.2, *Manual Control*, addresses requirements for manual control. The PSAR states the preliminary design includes manual scram switches located in the SCR and does not include details on manual scram capability from the MCR. Further information from the applicant at the operating license stage will be required to fully demonstrate compliance with Clause 6.2, but the overall information to support GDC 1 is sufficient for the CP stage.

PSAR Section 7.1.3.4 states that the CRN-1 I&C systems comply with the GDC 1, which have plant-wide applicability, as discussed in Section 3.1 of the PSAR. It also states the SC1, SC2, and SC3 I&C systems design complies with GDC 1. Based on the information provided in the PSAR, the staff finds the preliminary design adequately addresses GDC 1.

GDC 2——Design bases for protection against natural phenomena

PSAR Section 7.1.3.4 states that the CRN-1 I&C systems comply with the GDC 2, which have plant-wide applicability, as discussed in Section 3.1 of the PSAR. It also states the SC1 I&C system design complies with GDC 2. Based on the information provided in the PSAR, the staff finds the preliminary design adequately addresses GDC 2.

Formatted: Body Text

GDC 4—Environmental and dynamic effects design bases

PSAR Section 7.1.3.4 states that the CRN-1 I&C systems comply with the GDC 4, which have plant-wide applicability, as discussed in Section 3.1 of the PSAR. It also states the SC1, SC2, and SC3 I&C systems design complies with GDC 4. Based on the information provided in the PSAR, the NRC staff finds the preliminary information adequately addresses the requirements GDC 4.

GDC 10—Reactor design

GDC 10 requires the reactor core and associated coolant, control, and protection systems to be designed with appropriate margin to ensure that specified acceptable fuel design limits (SAFDL) are not exceeded during any condition of normal operation, including the effects of AOOs. PSAR Section 7.1.3.4 states that the SC3 I&C systems include the control, electrical, mechanical, and measurement elements that support DL2 functions during normal operations and AOOs. These functions are designed to ensure that SAFDL are protected with margin appropriate for AOO PIEs. Based on the information provided in the PSAR, specifically that, “the SC1 I&C system provide the main line of protection for AOOS and DBAs (as described in Section 7.3.1.3.5 of the PSAR), the NRC staff finds the preliminary design adequately addresses GDC 10.

GDC 13—Instrumentation and control

GDC 13 requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary (RCPB), and the containment and its associated systems. PSAR Section 7.1.3.4 states that DL3 functions are performed by independent and diverse SC1 I&C systems to maintain the specified variables by automatic safety actuations to ensure adequate safety. The lower classified information displays associated with the SC1 I&C systems provide monitored parameters during normal operation and for accident monitoring by the operators. The SC3 I&C systems perform DL2 functions to monitor plant variables in the reactor core, RCPB, containment and supporting systems. Normal and off-normal operating ranges are defined to support process control during normal operation and the automatic initiation of control functions to maintain the specified variables within prescribed operating ranges through normal control or, when required, by automatic safety actuations to assure adequate safety and accident monitoring in the event of AOOs or DBAs. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 13.

GDC 15—Reactor coolant system design

GDC 15 requires the reactor coolant system and associated auxiliary, control, and protection systems to be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. PSAR Section 7.1.3.4 states that the SC3 I&C systems perform DL2 functions to automatically initiate

hydraulic scram and pressure control functions so that the reactor coolant pressure design limits are not exceeded during AOOs. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 15.

GDC 16——Containment design

GDC 16 requires the reactor containment and associated systems to be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require. PSAR Section 7.1.3.4 states that SC1 I&C systems perform the DL3 functions for reactor, containment, and system isolation to limit line break effects both inside and outside containment. Diverse SC2 I&C systems perform the DL4a functions for reactor, containment, and system isolation to limit line break effects both inside and outside containment. However, during the OL stage of licensing review the staff will likely verify the applicant's information in Section 7.1 that states in part, "Accordingly, DL4a is not required to be independent and diverse from DL2", which may contract the reliability statements of the DL4a system if the two DLs are not sufficiently independent of each other Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 16.

PDC 19——Control room

The evaluation of PDC 19 is provided in section 6.4.3 of this report. PDC 19 requires a control room to be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and AOOs, and to maintain it in a safe condition during DBAs. Adequate radiation protection shall be provided to permit access and occupancy of the control room during DBAs without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent as defined in 10 CFR 50.2. Equipment at appropriate locations outside the control room shall be provided with a design capability for safe shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe shutdown condition. PSAR Section 7.1.3.4 states that the SC1 I&C systems provide lower classified operator interfaces in the MCR and SCR for display of Type B and C accident monitoring parameters and provide the ability to place and maintain the reactor in safe shutdown in the event of an MCR evacuation event. Prior to evacuating the MCR, operators would trip the reactor and initiate the ICS and containment isolation. The CRN-1 design does not rely on operator action, instrumentation, or controls outside of the MCR to maintain safe shutdown. The design includes Type B and C accident monitoring parameters displayed in the SCR to allow operators to monitor the reactor for safe shutdown condition. Based on the information provided in the Chapter 7 PSAR related to the ability to operate the nuclear power unit safely under normal conditions, AOOs and DBAs, the NRC staff finds the preliminary design adequately addresses PDC 19 for the purposes of the CP. Additional discussion related to the radiological aspects of PDC 19 are found in section 5.10 of this report.

GDC 20——Protection system functions

GDC 20 requires the protection system to be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to ensure that SAFDL are not exceeded as a result of AOOs, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety. PSAR Section 7.1.3.4 states that the SC1 I&C systems are designed to provide timely protection in sensing accident conditions and initiating the required DL3 functions. The SC3 I&C systems automatically initiate the DL2 functions to

ensure that AOO acceptance criteria, including SAFDL, are not exceeded. Also, PSAR Section 7.3.1.3.5 states that it is the SC1 I&C system that provides the main line of protection for both AOOs and DBAs. Additionally, the SC3 I&C systems sense DBA conditions and automatically initiate DL2 functions to ensure that DBA acceptance criteria are met. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 20.

GDC 21———Protection system reliability and testability

GDC 21 requires that the protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to ensure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. PSAR Sections 3.1.3.2 and 7.1.3.4 state that SC1 I&C system functions provide assurance that, through redundancy and independent divisions of equipment, the SC1 I&C system has sufficient reliability to fulfill the single-failure criterion. No single component failure, intentional bypass maintenance operation, calibration operation, or test to verify operational availability, impairs the ability of the system to perform its intended DL3 functions. Independence between redundant divisions prevents failures occurring in one division from impairing the ability of the other divisions to function correctly. With one division inoperable, the required minimum redundancy is temporarily lost.

Acceptable reliability of operation is established by limiting the time such a condition can exist through Technical Specifications. Design features, such as self-testing routines in digital equipment, that permit in-service testing are included in the design and the Safety Category 1 functions can be tested during reactor operation. The BWRX-300 Safety Strategy, NEDC-33934P explain that the systems implementing Safety Category 3 protection functions are designed to ensure acceptable reliability of operation. Each Safety Category 3 DL function uses triple modular redundant (TMR) controllers for a majority of DL2 functions (control rod block functions are implemented in dual redundant hardware and are designed to fail-safe), as well as triple redundant input sensors. TMR controller inputs and outputs use dedicated communication paths; execution of these Safety Category 3 functions does not rely on the UDH. TMR is a fault tolerant technique where three controllers perform the same process simultaneously. The CRN-1 design uses sensor inputs in triplicates. The results from controllers are then processed by a majority voting system producing a single output. This means that if one of the three sensors (or their associated communication path) or one of the TMR controllers fails, the other two can still provide the correct output, ensuring reliability. SSCs performing Safety Category 3 protection functions are redundantly powered from battery-backed feeds supplied by the SC3 preferred power 250 VDC subsystem. This redundancy improves reliability, ensuring that a single power feed failure does not result in the loss of a protection function. The criteria to ensure acceptable reliability of operation for Safety Category 3 protection functions are:

- No single sensor or controller failure results in the loss of a protection function.
- Removal of a single sensor or controller from service does not result in the loss of a protection function.
- No single power feed failure results in the loss of a protection function.

- Removal of a single power feed from service does not result in the loss of a protection function.

The SC3 hardware does not have the same types of independence between redundancies as in the SC1 systems; however, this is accounted for in calculating the reliability achieved for the DL2 functions. Acceptable reliability and availability of operation is established by monitoring DL2 functions in accordance with the Availability Controls Manual. Extensive hardware and software diagnostics are performed continuously during operation to detect and alarm individual failures that may occur. Cross-checks between redundant sensor measurements are performed continuously during operation to detect single sensor failures that may occur during operation.

Based on the information provided in the PSAR, the staff finds that GDC 21 establishes a qualitative expectation for high functional reliability of the protection system but does not prescribe specific numerical reliability targets as provided in the applicant's PSAR.
The applicant references a numerical reliability target (e.g., 1E-02 failures per demand) for the DL2 protection system as part of its safety strategy. However, the staff notes that demonstrating conformance with a specified numerical reliability target alone does not, by itself, ensure high functional reliability. As discussed further in SE Section 15.1, the applicant uses defense line reliability targets to structure event sequence frequencies and transitions between licensing basis event categories on a per-sequence basis, but does not evaluate the integrated and cumulative contribution of structures, systems, and components (SSCs) across all applicable scenarios.

Formatted: Body Text

For that reason, the staff's review does not rely on, or constitute approval of, predefined numerical reliability targets for individual defense lines, SSCs, or specific functions. Instead, the staff's assessment of compliance with GDC 21 is based on the overall design attributes of the protection system, including redundancy, independence, diversity, testability, and the ability to perform required safety functions under anticipated conditions.

Formatted: Body Text

While the staff finds the information provided by the applicant at the CP stage acceptable for satisfying GDC 21, at the operating license stage, the staff will review the detailed design and performance characteristics of the DL2 protection system to confirm that these attributes collectively provide high functional reliability. To the extent that quantitative reliability analyses are used to support this demonstration, they will be considered as supporting information and evaluated in the context of uncertainties, assumptions, and the overall system design, rather than as standalone acceptance criteria.

GDC 22——Protection system independence

GDC 22 requires that the protection system shall be designed to ensure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. PSAR Sections 3.1.3.3 and 7.1.3.4

Formatted: Body Text

state that the SC1 equipment that performs DL3 functions is implemented with independence between redundant equipment such that the effects of natural phenomena, and of normal operation, maintenance, testing, and postulated accident conditions do not result in loss of the minimum redundancy required for successful performance of DL3 functions. Redundant SC1 sensors are designed to be electrically and physically separated, and only circuits of the same division can be run in the same raceway. Signals required to cross divisional boundaries to implement the 2 out of 3 voting logic use fiber optic communication pathways to maintain electrical isolation between divisions. SC1 equipment is also seismically and environmentally qualified to function in the expected environments resulting from natural phenomena events or accidents. The SC1 I&C systems are designed to permit maintenance and diagnostic work while the reactor is operating, without restricting the plant operation or hindering the output of safety functions. Operational system testing can be performed using independent input for each division. When a monitored variable supporting a Safety Category 1 function exceeds its scram trip point, it is sensed by three independent sensors, each located in a separate instrumentation channel.

The staff notes the DL2 functions do not have the same level of independence that exists within DL3 functions; however the applicant states that DL2 functions are implemented with independence adequate to meet their reliability requirement pursuant to an “other defined basis” described in GDC 22. TMR controllers are used for majority of DL2 functions, as well as triple redundant input sensors, except control rod block functions are implemented in dual redundant hardware. SSCs performing a DL2 function are designed to operate in the environment expected during normal operations and in response to AOOs relying on the DL2 function for mitigation. The resulting reliability of DL2 functions in the final system design will need to be adequate to provide confidence that these functions will be performed when needed. Additionally, per the information provided by the applicant, CRN-1 systems making up the protection system have layers of protection with both DL2 and DL3 functions that are able to mitigate AOOs to within the acceptance criteria described in PSAR Table 15.3-1 and Table 15.3-2, respectively. The applicant identified that there is independence between these layers, as SC3 equipment is independent from SC1 equipment except in cases where sharing of in-core components (e.g., LPRMs data is utilized to initiate Safety Category 1 hydraulic scram functions and Safety Category 3 rod block functions) is necessary due to practical limitations. Additionally, the applicant describes that a level of diversity exists among these DLs, as the SC1 I&C systems are diverse from other I&C systems (i.e., hardware platforms are diverse). The independence and diversity between layers of protective functions are delineated by the applicant stating that they will achieve high plant-level protection reliability. The SC3 I&C systems are designed to ensure they cannot adversely affect SC1 I&C systems from fulfilling their Safety Category 1 protection functions. Additionally, there is no communication from SC3 equipment to online SC1 equipment and Safety Category 3 functions may use signals from SC1 equipment sent via qualified isolation devices for some control purposes. The physical separation and signal isolation devices for the SC3 I&C systems are designed to meet the requirements of IEC 60709.

Formatted: Body Text

Based on the information provided in the PSAR, the staff finds the preliminary design information adequately addresses GDC 22 for the CP stage. At the operating license stage, the staff will review the detailed design and performance characteristics of the protective system(s) to ensure that GDC 22’s protection systems’ independence criteria are met such that the protection system(s) is (are) designed in a reliable manner such that it will not result in the loss of protective function, or shall be demonstrated to be acceptable on some other defined basis.

Formatted: Body Text

GDC 23——Protection system failure modes

GDC 23 requires that the protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. PSAR Sections 3.1.3.4 and 7.1.3.4 state that the SC1 I&C systems implementing DL3 functions are designed to fail into a safe state if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced. Use of independent divisions allows the system to sustain any single divisional failure without preventing redundant divisions from initiating the Safety Category 1 protection functions. The environmental conditions in which the SC1 I&C systems must operate are considered in establishing the component specifications. Instrumentation specifications are based on the worst expected ambient conditions in which the instruments must operate. The applicant describes that the SC3 I&C systems have the required fail-as-is design features to perform intended functions and avoid spurious actuations. The fail-as-is, energize to actuate design is used to prevent lesser classified systems from creating unnecessary challenges to plant safety (e.g., spurious actuations for expected failures) requiring action by Safety Category 1 functions. Where software is used for SC3 equipment diagnostics, the SC3 equipment includes watchdog timers, sensor range checks, and monitoring of power supplies, communications, and actuators. The SC3 equipment is designed to operate in the environment that is to be expected during both normal operations and anticipated off-normal conditions, and the equipment is qualified to perform its intended functions and meets IEC 61513 requirements and the equipment standards requirements for Class 3 systems defined in Section 7 of IEC 61226. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 23.

GDC 24——Separation of protection and control systems

GDC 24 requires that the protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. PSAR Sections 3.1.3.5 and 7.1.3.4 state that the Safety Category 3 protection, reactor control, and rod block functions are implemented in separate systems with dedicated controllers. Safety Category 3 control functions are allocated to separate control processors (referred to as separate control segments) than the Safety Category 3 protection functions. The control functions and protection functions may use common input sensors. These sensors are triple redundant such that single failure of any sensor does not prevent either the control or protection function from being performed. Safety Category 3 protective functions are implemented separate from the Safety Category 3 control functions to the extent that any of the following failures leaves intact a group of equipment satisfying all reliability and independence requirements for Safety Category 3 functions:

- failure of any single sensor performing Safety Category 3 control and protective functions;
- failure of any single processor performing Safety Category 3 control or protective functions; or

- removal from service of any single component that supports both Safety Category 3 control and protective functions.

SC1 DL3 functions are implemented separately from the SC3 DL2 functions to the extent that any failure leaves intact a group of equipment satisfying all reliability and independence requirements necessary to ensure performance of the DL3 functions for DBAs. Interconnections between equipment performing DL2 functions and DL3 functions is limited such that either the DL3 or DL2 functions remain available in the presence of any credible single failure, or credible CCF, postulated to affect mitigation capabilities of either SC. The SC1 signals are electrically isolated and physically separated from SC3 I&C systems. Sensor signal outputs may be shared, but each signal is optically isolated before entering a redundant or lower classified channel interface. The independence features prevent faults in a lower classified system from propagating to a higher classified system. Based on the information provided in the PSAR, the NRC staff finds that the preliminary design adequately addresses GDC 24.

GDC 25——Protection system requirements for reactivity control malfunctions

GDC 25 requires that the protection system shall be designed to ensure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods. PSAR Section 7.1.3.4 states that SC3 DL2 I&C system functions, along with other mitigating design features, ensure that SAFDL are not exceeded for reactivity control malfunctions. To prevent a rod withdrawal error, the rod control system has redundancy to limit the effect of single failures. Additionally, the rod patterns are enforced for rod withdrawals. If there is a malfunction of the rod control system that results in a rod withdrawal error during startup, a DL2 rod block is initiated based upon a wide range neutron monitor (WRNM) short reactor period signal. If the rod withdrawal error were to result in a further decrease to the WRNM short reactor period based setpoint, a reactor scram would occur. If a rod withdrawal error were to occur at higher power, the APRM scram would terminate the event if it were to continue to its setpoint. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 25.

PDC 26——Reactivity control system redundancy and capability

PDC 26 requires that two reactivity control systems of different design principles shall be provided. One system shall use two diverse means of inserting control rods. The system shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including AOOs, and with appropriate margin for malfunctions such as stuck rods, SAFDL are not exceeded. The second reactivity control system shall be capable of inserting negative reactivity into the core to assure a reactor shutdown from full power operating conditions if both diverse means of inserting control rods were to fail. PSAR Section 7.1.3.4 states that the SC1 I&C system, diverse SC2 I&C system, and the SC3 anticipatory trip system separately initiate DL2, DL3, and DL4a hydraulic scram functions. Each of these hydraulic scram functions also initiate a scram follow signal to the SC2 FMCRD control system, which inserts the control rods with the motors operating at normal speed. A DL4a fast motor run-in function is initiated if the SC2 I&C system does not obtain positive confirmation of successful hydraulic scram. A boron injection system (BIS) is also provided for reactivity control diversity if the control rods were to fail to insert. PSAR Table 3A-1 notes that instrumentation associated with the BIS is classified as SC3. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses PDC 26.

GDC 28——Reactivity limits

GDC 28 requires that the reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding, nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold-water addition. PSAR Section 7.1.3.4 states that the SC1 I&C system implements DL3 functions to provide timely protection against the onset and consequences of conditions that threaten the integrity of the fuel barrier and RCPB. The SC3 DL2 functions provide the control logic and position the control rods using the SC2 FMCRD control system. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 28.

PDC 29——Protection against anticipated operational occurrences

The applicant's proposed PDC 29 requires that the protection and reactivity control systems be designed to ensure: (1) an extremely high probability of accomplishing their safety functions in the event of AOOs and (2) a high probability that the SAFDLs are not exceeded as a result of AOOs. The staff finds PDC 29 incorporates the minimum requirements of GDC 29 because it includes the language related to providing an extremely high probability of accomplishing safety functions in the event of an AOO and also establishes a defense-in-depth approach for mitigating AOOs. PSAR Sections 3.1.3.10 and 7.1.3.4 state that the CRN-1 design provides two layers of defense for AOOs; and the applicant states that Safety Category 3 functions ensure SAFDLs are not exceeded, Safety Category 1 functions ensure FSF are met. The applicant continues, the combination of Safety Category 3 functions and independent Safety Category 1 functions, arranged in DLs providing layered protection against AOO PIEs, results in extremely high functional reliability for performance of FSFs during and after DBEs, including AOOs.

The staff notes that these SC3 functions appear to constitute the primary line of defense for AOO mitigation, although in Section 7.3.1.3.5, "Diversity and Defense-in-Depth", the applicant states that it is the SC1 I&C system that provides the main line of protection for AOOs and DBAs. For SC3 functions as part its safety strategy, the applicant assigns a numerical reliability target of 1E-02 failures per demand for SC3 functions to support a high probability that SAFDLs are not exceeded during AOOs. However, meeting a specified numerical reliability target alone will not by itself provide assurance that the systems are capable of performing their safety functions.

Formatted: Body Text

Section 15.1 of this report, and its subsections, further describe how the applicant uses defense line reliability targets to structure event sequence frequencies and transitions between licensing basis event categories based on individual sequences and the acceptability of that approach. The design also includes a second and independent layer of defense consisting of SC1 protection and reactivity control functions that are credited for mitigation of DBAs. These SC1 systems provide independent protection to ensure that fundamental safety functions are maintained if the preceding defense line, (i.e., DL2) does not perform as assumed.

Formatted: Body Text

At the operating license stage, consistent with the principles described in PDC 29, the staff will review the detailed design and performance characteristics of the protection and reactivity control systems supporting AOO mitigation to verify that either the SC3 instrumentation and control systems have sufficient capability, independence, and reliability to ensure that SAFDLs are not exceeded as a result of AOOs during the lifetime of the facility or that through an analysis it can be demonstrated that even if the SC3 system were to fail, sufficient time exists for the SC1 system and/or the operators to manage any AOOs prior to any safety limits being exceeded. Depending on the applicant's final design, the staff may also evaluate the independence and capability of the SC1 protection systems that provide a subsequent layer of defense. Based on the information provided in the PSAR, the staff finds that the preliminary design approach adequately addresses PDC 29.

GDC 33——Reactor coolant makeup

GDC 33 requires that a system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to ensure that SAFDL are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation. PSAR Section 7.1.3.4 states that for normal operational leakage, the SC3 I&C system performs the DL2 functions to maintain reactor coolant system level. For breaks, the SC1 I&C system performs the DL3 function to actuate RIVs. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 33.

GDC 34——Residual heat removal

GDC 34 requires a system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that SAFDL and the design conditions of the reactor coolant pressure boundary are not exceeded. Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure. PSAR Section 7.1.3.4 states that the SC1 I&C system actuates DL3 ICS functions to provide the necessary residual heat removal capability for ensuring SAFDL are met, and RCPB design conditions are not exceeded. Evaluation of the electrical power portion of the GDC is discussed in Section 8.3 of this SE. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 34.

GDC 35——Emergency core cooling

GDC 35 requires a system to provide abundant emergency core cooling. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling

is prevented, and (2) clad metal-water reaction is limited to negligible amounts. Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure. PSAR Section 7.1.3.4 states that SC1 I&C system performs the DL3 functions to initiate ICS and reactor, containment, and system isolation functions. The ICS design includes features that provide redundancy in components, because the worst-case single failure can only affect one ICS train or RIV. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 35.

GDC 63—Monitoring fuel and waste storage

GDC 63 requires that appropriate systems shall be provided in fuel storage and radioactive waste systems and associated handling areas (1) to detect conditions that may result in loss of residual heat removal capability and excessive radiation levels, and (2) to initiate appropriate safety actions. PSAR Section 7.1.3.4 states that the SC3 I&C systems provide monitoring and control for the spent fuel pool redundant heat exchangers and pumps and their associated valves to detect conditions that may result in loss of residual heat removal capability and implement appropriate DL2 functions. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 63.

GDC 64—Monitoring radioactivity releases

GDC 64 requires that means shall be provided for monitoring the reactor containment atmosphere, spaces containing components for recirculation of loss-of-coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents. PSAR Section 7.1.3.4 states that the CRN-1 I&C systems provide process radiation monitoring and area radiation monitoring subsystems (ARM) to monitor for radioactivity releases from normal operations, including from AOOs and DBAs. The SC3 DCIS provides displays in both the MCR and SCR as well as a SPDS function that provides a big picture overview display of plant parameters during transients and accidents. Based on the information provided in the PSAR, the NRC staff finds the preliminary design adequately addresses GDC 64.

Additional NRC Regulations

PSAR Section 7.1.3.2 states that the following additional NRC regulations that contain detailed design requirements related to the I&C design are applicable to the CRN-1 I&C design:

- 10 CFR 50.34(f)(2)(iv) (TN249), related to safety parameter display console with respect to displays and monitoring requirements
- 10 CFR 50.34(f)(2)(v), related to bypass and inoperable status indication with respect to operating bypass, maintenance bypass, and displays and monitoring requirements
- 10 CFR 50.34(f)(2)(xiv), related to containment isolation systems with respect to actuation system requirements
- 10 CFR 50.34(f)(2)(xvii), related to accident monitoring instrumentation

- 10 CFR 50.34(f)(2)(xviii), related to instrumentation for the detection of inadequate core cooling
- 10 CFR 50.34(f)(2)(xix), related to instruments for monitoring plant conditions following core damage
- 10 CFR 50.34(f)(2)(xxiv), related to central reactor vessel water level recording
- 10 CFR 50.34(h), "Conformance with the Standard Review Plan," related to the NRC staff's review of the proposed I&C system
- 10 CFR 50.44(c)(4), related to combustible gas control monitoring
- 10 CFR 50.55a)h)(3), related to meeting requirements of IEEE Std 603-1991 and the correction sheet dated January 30, 1995
- 10 CFR 50.55a(z), "Alternatives to codes and standards requirements," allows use of alternatives to the requirements of 10 CFR 50.55a(h), when authorized by the NRC
- 10 CFR 50.62(c)(3), related to requirements for reduction of risk from ATWS events

The CRN-1 design uses IEEE 603-2018, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to the IEEE 603-1991 version, to support a 3-division SC1 architecture. For use of alternative standards requirements, the applicant has indicated that it intends to seek NRC authorization to use alternative standards requirements under 10 CFR 50.55a(z). A request for NRC authorization for the use of the IEEE 603-2018 standard will be evaluated during the FSAR review if the applicant submits such a request.

As stated in 10 CFR 50.35(a)(2), such further technical or design information as may be required to complete the safety analysis, and which can reasonably be left for later consideration, will be supplied in the FSAR. As a result, compliance with the additional applicable regulations stated above will be evaluated at the OL stage during the FSAR review.

Formatted: Font: Bold, Underline

Formatted: Body Text

Reports referenced

NEDC-33934P, "BWRX-300 Safety Strategy," GE-Hitachi Nuclear Energy Americas,

LLC, Revision 2, March 2026.

Commission Policy

The PSAR application does not contain a digital I&C system CCF coping analysis required by the Commission in SECY-93-087, item II.Q, as clarified by SRM-SECY-93-087, item 18, and SRM-SECY-22-0076. As stated in 10 CFR 50.35(a)(2), such further technical or design information as may be required to complete the safety analysis, and which can reasonably be left for later consideration, will be supplied in the FSAR. The digital I&C system CCF coping analysis will be evaluated during the FSAR review at the OL stage.

Regulatory Guidance and Industry Standards

PSAR Table 7.1-3 outlines a set of alternative industry standards that have been endorsed by the NRC Regulatory Guides. As stated in 10 CFR 50.35(a)(2), such further technical or design information as may be required to complete the safety analysis, and which can reasonably be left for later consideration, will be supplied in the final safety analysis report. Use of these alternative standards for designing SC1, SC2, and SC3 I&C systems will be evaluated during the FSAR review at the OL stage.

7.2.4 Conclusion

The NRC staff reviewed the I&C systems design described in PSAR Chapter 7 and finds the information acceptable because (1) the PSAR provides an adequate discussion of the I&C system design to support conformance of the I&C system design with applicable GDCs and PDC; and (2) the contents of the PSAR are consistent with the guidance in the DRG and in DNRL-ISG-2022-01, and Commitments to Meeting the Requirements of 10 CFR 50.55a(h)(3) (TN249). Therefore, the NRC staff concludes that the preliminary information provided by the applicant is sufficient and meets the regulatory requirements of 10 CFR 50.34(a) for the I&C design and adequately supports issuance of a CP pursuant to the regulations in 10 CFR 50.35. A more detailed evaluation of the I&C design will occur during the review of the OLA, at which time the NRC staff will confirm that the final design conforms to this design and meets all applicable regulations.

7.3 Summary and Conclusion

The NRC staff evaluated the information on the I&C systems as described in PSAR Chapter 7 and finds that the preliminary information on, and design criteria of, the I&C systems, including the PDC's and GDCs, design bases, and information relating to materials of construction, general arrangement, and approximate dimensions is consistent with the DRG, "Instrumentation and Controls for Non-Light-Water Reactor Reviews." Therefore, the NRC staff concludes that the preliminary information provided by the applicant is sufficient and meets the regulatory requirements of 10 CFR 50.34(a) for the I&C design and adequately supports issuance of a CP pursuant to the regulations in 10 CFR 50.35.

During the NRC staff's review of the OLA, the NRC staff will evaluate 1) the digital I&C CCF coping analysis in accordance with the above stated Commission Policy; 2) the required reliabilities of DL2, DL3, and DL4a protection functions; and 3) the use of alternative industry standards (not previously endorsed by NRC Regulatory Guides) for designing the CRN-1 I&C systems.

7A&B Human Factors Engineering Program

7A&B.1 Introduction

Section 7A of the CRN-1 CPA describes the establishment of the human factors engineering (HFE) program for CRN-1 and Section 7B provides the associated HFE technical elements of a BWRX-300 facility. The final implementation of the HFE program will be included in the CRN-1 Final Safety Analysis Report (FSAR). The CRN-1 CPA describes an HFE program that would result in the following:

- Development of a HFE program plan (HEFPP) that defines a HFE program for a BWRX-300 standard plant design and site-specific design stage specifically for CRN-1 and forms the basis for any future site BWRX-300 design HFE programs.
- Applicability of the HFE program to plant conditions in the design basis, normal, outage abnormal, and emergency phases.
- Usage of HFE requirements management in accordance with a process that is standardized and applied across the entire plant design for CRN-1, including the use of best practices and compliance with regulatory guidelines that reflect state-of-the-art human factors guidelines, principles, and methods.
- Allocation of HFE process requirements that result in the HFEPP by incorporating how the HFE program is conducted and applied with interfaces among HFE and other disciplines.
- Implementation of HFE product requirements which are derived from HFE design standards, codes, and guidance or from HFE analyses as required to support task performance in the plant conditions described in the second bullet.
-

Formatted: List Bullet, Bulleted + Level: 1 + Aligned at: 0.35" + Indent at: 0.6"

7A&B.2 Regulatory Evaluation

The applicable regulatory requirements for the evaluation of the HFE are as follows:

- 10 CFR 50.34(a)(3)(i) (TN249)
- 10 CFR 50.34(f)[1]:
  - (2)(ii); (iii); (iv); (v); (xvii); (xviii); (xix); (xxi); (xxiv); (xxvi); and (xxvii)
  - (3)(i)

The applicable guidance documents for the evaluation of HFE are as follows:

1 As stated in DANU-ISG-2022-05, “The requirements here do not apply to 10 CFR Part 50 applicants not listed in 10 CFR 50.34(f). Rulemaking is underway to align the requirements of 10 CFR Part 50 and 10 CFR Part 52 that may make these requirements applicable to all 10 CFR Part 50 applicants. In the interim, the NRC staff should propose license conditions on 10 CFR Part 50 applications to address these regulations.”

- DNRL-ISG-2022-01, “Safety Review of Light-Water Power Reactor Construction Permit Applications,” October 2022 (NRC 2022-TN12894)
- Chapter 18 of NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” Revision 3, December 2016 (NRC 2021-TN8013)
- NUREG-0711, “Human Factors Engineering Program Review Model,” Revision 3, November 2012 (NRC 2012-TN12817)

7A&B.3 Technical Evaluation

The NRC staff evaluated Section 7A and Section 7B of the CRN-1 PSAR using the guidance and criteria as described in DNRL-ISG-2022-01, which specifies the use of NUREG-0800. Specifically for human factors engineering, Chapter 18 of NUREG-0800 is used to ensure that the application includes sufficient information, of a scope and level of depth appropriate for a CPA, to understand the development of the HFE program for the CRN-1 facility.

Formatted: Font: Bold

7A&B.3.1 Inclusion and Application of Appropriate PDC

Formatted: Body Text

10 CFR 50.34(a)(3)(i) states that an applicant for a CP must include in the PSAR the PDC for the facility. Appendix A to 10 CFR Part 50, “General Design Criteria for Nuclear Power Plants,” provides guidance to CP applicants in establishing PDC for nuclear power units. The applicant evaluated PDC 19 for the CRN-1 facility, which was included in Section 3.1.2.10 of the PSAR as follows:

> A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and anticipated operational occurrences, and to maintain it in a safe condition during design basis accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room during design basis accidents without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent as defined in 10 CFR 50.2.
>
> Equipment at appropriate locations outside the control room shall be provided with a design capability for safe shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe shutdown condition.

The applicant indicated in Section 3.1.2.10 that the BWRX-300 design meets the adequate radiation protection requirement of PDC 19 for the main control room (MCR) and secondary control room (SCR). The applicant also discussed that the BWRX-300 is designed to meet the PDC 19 requirement of providing a “safe shutdown” capability outside of the MCR in the event of an MCR evacuation. The operators will be directed to trip the reactor and initiate decay heat removal and containment isolation prior to evacuating the MCR if necessary for design basis accidents. The operators will also be capable of placing the reactor in safe shutdown in the SCR located in the Reactor Building. The following Clinch River PSAR sections also indicate compliance with PDC 19 as related to both the MCR and SCR:

- Control Room Habitability (PSAR Section 6.4.3.1)
- I&C Systems (PSAR Section 7.1.3.2)

- Control Room Heating, Ventilation, and Cooling System (PSAR Section 9.4.1.3)
- Reactor Building Heating, Ventilation, and Cooling System (PSAR Section 9.4.6.3)
- Radiation Monitoring (PSAR Section 11.5.3)
- Deterministic Safety Analysis Acceptance Criteria (PSAR Section 15.3.1)
- Description of the Computer Codes or Standards Used in the Safety Analyses (PSAR Section 15.5.1.2.7)
- Analysis of Fuel Handling Accident (PSAR Section 15.5.8)
- Analysis of Loss of Cooling Accidents Outside Containment (PSAR Section 15.5.9.1)

The NRC staff reviewed PDC 19 in the applicable sections of the CRN-1 PSAR and concluded that the CRN-1 MCR and SCR are both designed to operate under normal conditions, abnormal or outage conditions and DBA with radiation protection, state-of-the-art human factors principles, and control room habitability. The NRC staff finds that the CRN-1 PSAR complies with 10 CFR 50.34(a)(3)(i) by including a PDC specific to the designs of both the MCR and SCR.

7A&B.3.2 Technologically relevant HFE-related requirements of 50.34(f)

Section III in Chapter 18 of NUREG-0800 describes regulations that impact HFE design related to the MCR and applicable acceptance criteria to address the human factors portions of these regulatory requirements. Table 1.9-21 of the PSAR lists the additional Three Mile Island-related requirements under 10 CFR 50.34(f) (TN249). The applicant evaluated each of the regulations cited in NUREG-0800 in comparison to the HFE design implications for the MCR and SCR and assessed how each regulation will comply with the current PSAR or future FSAR, and which regulations are not applicable to the BWRX-300 design. The evaluations are discussed below:

- 50.34(f)(2)(ii)—The applicant indicated that a program being established to improve plant procedures from construction to operations will comply with this regulation by the issuance of the CRN-1 FSAR.
- 50.34(f)(2)(iii)—The applicant stated that the control room, designed with state-or-the-art human factors principles, will comply with this regulation by the issuance of the CRN-1 FSAR.
- 50.34(f)(2)(iv)—The applicant discussed in PSAR Section 7.1.3 that the I&C design, which includes the SPDS console for the control room, complies with this regulation. PSAR Section 7.3.3.2 describes the SPDS as providing sufficient information on safety-critical parameters and includes display and trending of the parameters associated with the emergency procedure guidelines for the plant.
- 50.34(f)(2)(v)—The applicant discussed in PSAR 8.1.2.1 that the automatic indication of bypassed and inoperable status of safety systems in the CRN-1 control room complies with this regulation and conforms to the regulatory guidance cited in RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems,” Revision 1, February 2010 (NRC 2010-TN12895).
- 50.34(f)(2)(xi)—The applicant stated that this regulation is not technically applicable to the BWRX-300 design since it does not have traditional relief valves. The direct indication in the control room is based on monitoring open relief valves for reactor

coolant loss. The passive design of the BWRX-300 ICS is used for overpressure protection and does not require relief valves for operation.

- 50.34(f)(2)(xii)—The applicant stated that this regulation is not applicable to the BWRX-300 design due to the auxiliary feedwater (AFW) system being associated only with pressurized water reactor designs. Therefore, no AFW system indication would be needed for the CRN-1 MCR.
- 50.34(f)(2)(xvii)—The applicant stated that this regulation is applicable for CRN-1 MCR due to the instrumentation described in PSAR Sections 6.2.1.3, 6.8, 7.1.3, 7.3.1, and 12.3.4. The MCR will display readouts of the containment pressure, water level, hydrogen concentration, radiation intensity, and noble gas effluents at all potential, accident release points. The instrumentation in the MCR will also provide continuous sampling of radioactive iodine and particulates in gaseous effluents.
- 50.34(f)(2)(xviii)—The applicant stated that the design of the instrumentation that will show signals from indicators of coolant level in the reactor vessel and in-core thermocouples in the MCR will comply with this regulation by the issuance of the CRN-1 FSAR.
- 50.34(f)(2)(xix)—The applicant stated that the MCR will provide instrumentation to monitor plant conditions following an accident as described in PSAR Sections 6.8, 7.1.3, and 7.3.1. Specifically, the design of the Containment Monitoring subsystem, which will monitor post-core damage accident plant conditions, complies with this regulation.
- 50.34(f)(2)(xxi)—The applicant discussed in PSAR Section 6.3.3 and 7.3.1.2 that the design of the ICS allows for automatic and manual initiation to remove decay heat from the reactor vessel. The ICS complies with this regulation.
- 50.34(f)(2)(xxiv)—The applicant indicated the MCR will have instrumentation to record the reactor vessel water level to meet normal post-accident recording requirements. A discussion of compliance with this regulation is provided in PSAR Section 7.1.3.2
- 50.34(f)(2)(xxvi)—The applicant discussed in PSAR Section 6.2.1 that the PCS has the capability to isolate containment and test for leak tightness and that the program for controlling leakage from systems that could contain radioactive fluids outside containment would be described in the CRN-1 FSAR. PSAR Section 5.4.7.3 described the SDC subsystem as having the capability of continuously monitoring leakage and providing system isolation as required. PSAR Section 6.3.3.1 described the ICS having the capability to control leakage outside of containment. All these systems show compliance with this regulation.
- 50.34(f)(2)(xxvii)—The applicant stated in PSAR Section 12.3.4.1.3 that the ARM subsystem as part of the process radiation and environmental monitoring system (PREMS) can provide in-plant radiation monitoring and airborne radioactivity. The ARM subsystem complies with this regulation.
- 50.34(f)(3)(i)—The applicant stated that procedures will be developed for the CRN-1 facility in evaluating operation, design, and construction experience. The applicant noted that compliance with this regulation will be provided in the CRN-1 FSAR.

The NRC staff reviewed each of the above items in comparison to each of the regulations stated for the MCR and concluded that the licensee provided information in the CRN-1 PSAR sections noted above sufficient to comply with the regulations. The NRC staff also reviewed the areas in

which the applicant indicated that compliance will be demonstrated in the CRN-1 FSAR and noted that further evaluation of the completed implementation of these areas can occur as part of the review of the FSAR prior to the operating licensing stage. The NRC staff finds that the MCR design associated with HFE can satisfy the requirements of 10 CFR 50.34(f)(2) listed above and 10 CFR 50.34(f)(3)(i).

7A&B.3.3 Development of the HFE Program

The applicant described, in Appendix 7A and 7B of the CRN-1 PSAR, the HFE program as being divided into the following 12 elements, consistent with the format used in NUREG-0711:

- HFE program management plan
- operating experience review (OER)
- functional requirements analysis (FRA) and function allocation (FA)
- task analysis (TA)
- staffing and qualification (S&Q)
- treatment of important human actions (TIHA)
- human-system interface (HSI) design
- procedure development
- training program development
- human factors verification and validation (V&V)
- design implementation
- human performance monitoring (HPM)

The applicant provided brief summaries of the technical HFE elements, highlighting the methodologies and processes for the formation of each element and their inclusion into the overall HFEPP. As stated in Appendix 7B of the PSAR, the applicant plans to submit a full description of these elements, the objectives and scope, methods, and results, and how they constitute a comprehensive and robust program of HFE integration across the plant design, in the CRN-1 FSAR, accompanied by subordinate documents, plans, strategies, processes, and analysis results.

The NRC staff evaluated each of the HFE elements in the PSAR and found that the overall methodology is generally consistent with a state-of-the-art approach to HFE, as described in NUREG-0711. Additionally, the NRC staff noted that a finding on the overall HFE acceptability of a design produced through implementation of the final HFEPP will require future NRC staff review of the information contained in the CRN-1 FSAR associated with the OLA. The NRC staff finds that the development of CRN-1 HFE program as described by the applicant can satisfy the requirements of PDC 19 to an extent appropriate for a CPA. However, the NRC staff also conclude that a complete evaluation of the adequacy of HFE within the CRN-1 design, including any associated finding related to 10 CFR 50.34(f)(2)(iii), will be deferred until the future OLA.

7A&B.4 Conclusion

The NRC staff reviewed the applicable PDC (i.e., PDC 19) for the CRN-1 MCR and SCR as required by 10 CFR 50.34(a)(3)(i) (TN249) and the applicable regulations for the development of the HFE program as required by 10 CFR 50.34(f)(2) and 10 CFR 50.34(f)(3). The NRC staff found that the applicant's development of the CRN-1 HFE program and MCR and SCR are in accordance with 10 CFR 50.34(f)(2) and 10 CFR 50.34(f)(3) and are acceptable for the purposes of the CP review. The NRC staff also found that the adoption of PDC 19 for the CRN-1 MCR and SCR designs are consistent with the requirements of 10 CFR 50.34(a)(3)(i). Based on its review, the NRC staff finds that the development of the HFE Program, as described in PSAR Appendix 7A and 7B, is consistent with the applicable regulatory guidance and can meet the regulatory requirements identified in 10 CFR 50.34(a)(3)(i), 10 CFR 50.34(f)(2), and 10 CFR 50.34(f)(3). Therefore, the NRC staff concludes that the preliminary information provided by the applicant adequately supports issuance of a CP pursuant to the regulations in 10 CFR 50.35 and 10 CFR 50.40. Further technical details and design information needed to complete the safety analysis can be left for later consideration and reviewed at the OL phase.

7.4 References

Chapter 18 of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Revision 3, December 2016 (ML16125A114)

NUREG-0711, "Human Factors Engineering Program Review Model," Revision 3, November 2012 (ML12324A013)

DNRL-ISG-2022-01, "Safety Review of Light-Water Power Reactor Construction Permit Applications," October 2022 (ML22189A099)

Commented [TC2]: Note to self: delete this section. The entire document will have one reference list after all the chapters are merged.

The references have been reconciled in the text above.

Reference Team