4.6 Functional Design of Reactivity Control Systems

The control rod drive system (CRDS) consists of the control rods and related mechanical components that provide the means for mechanical movement. For the U.S. EPR, the CRDS consists of the control rod drive mechanisms (CRDM) and rod cluster control assemblies (RCCA). Additional systems, such as the protection system (PS), the reactor control surveillance and limitation (RCSL) system, and the control rod drive control system (CRDCS) support the CRDS by providing the control logic and electrical power for CRDS movement and trips.

As addressed in Sections 4.6.1 through 4.6.5, the CRDS design satisfies the following GDC of 10 CFR 50, Appendix A:

- GDC 4, which requires the CRDS to remain functional and provide reactor shutdown capabilities under adverse environmental conditions and after postulated accidents. Verification of the adequacy of the control rod drive mechanisms to perform their mechanical functions (e.g., rod insertion and withdrawal, scram operation and time) and to maintain the reactor coolant pressure boundary is performed under Section 3.9.4. Verification that the design and requirements are met, as applicable to the assigned safety class and seismic category, is performed under Section 3.2.1 and Section 3.2.2. Postulated piping failures inside the containment, including their associated locations and dynamic effects, are evaluated in Section 3.6.2, as they relate to the protection of SSC against such effects.

- GDC 23, which requires the CRDS to fail in an acceptable condition, even under adverse conditions, to prevent damage to the fuel cladding and excessive reactivity changes during failure.

- GDC 25, which requires the design of reactivity control systems to prevent a single malfunction of the CRDS from causing acceptable fuel design limits to be exceeded.

- GDC 26, which requires the CRDS to provide sufficient operational control and reliability during reactivity changes under normal operation and anticipated operational occurrences (AOO).

- GDC 27, which requires the combined capability of CRDS and the safety injection system (SIS) to reliably control the reactivity changes establishing the capability of cooling the core under postulated accident conditions.

- GDC 28, which requires the CRDS to prevent reactivity accidents from damaging the reactor coolant pressure boundary (RCPB), or resulting in sufficient damage to the core or support structures to significantly impair reactor cooling capability.

- GDC 29, which requires the CRDS to provide an extremely high probability of functioning during AOOs.

In addition to the CRDS, reactivity control systems that operate under shutdown conditions, normal operating conditions, transients, or postulated accident conditions include:

- Chemical and volume control system (CVCS).
- Extra borating system (EBS).
- SIS.

4.6.1 Information for Control Rod Drive System

The U.S. EPR contains 89 electromagnetic jack type CRDMs, each consisting of a drive rod, pressure housing, latch unit, and coil housing assembly. The CRDMs use natural air circulation, convection cooling; therefore a separate, dedicated liquid or forced air cooling system is not required. Natural convection cooling maintains the temperature of the CRDMs below design operating temperature. CRDM equipment is designed and qualified to operate in the reactor vessel cavity environment. Details of these CRDM components and how the components operate are provided in Section 3.9.4, and a diagram of the CRDM assembly is shown in Figure 3.9.4-1. An overview of the CRDM penetrations into the reactor pressure vessel is provided in Figure 3.9.5-1, and the layout of RCCA control and shutdown banks within the core is provided in Figure 4.3-34. The RCCAs are described in Section 4.2. The instrumentation and control (I&C) systems providing rod control are described in Section 7.7, which includes the CRDCS and RCSL systems.

The CRDMs are mounted on top of the reactor pressure vessel head and are protected from potential tornado-generated missile damage by being housed in a Seismic Category 1 structure (i.e., containment). The CRDMs are protected from internally generated missiles by the concrete secondary shield wall and by reinforced concrete missile shield slabs mounted above the reactor vessel. The CRDMs are seismically restrained by the reactor pressure vessel closure head equipment as addressed in Section 5.4.14.

The I&C systems associated with RCCA control count CRDM movement steps to provide a digital measurement of RCCA position. The CRDMs are also equipped with position indicator coils that provide analog RCCA position measurements. As such, the RCCA position is measured over the height of the core by two diverse methods:

- The digital measurement is non-safety related.
- The analog measurement, using position indicator coils, is safety related.

Additionally, a safety related rod position limit sensor provides input to the PS when the RCCA is at the bottom position and a non-safety related upper position limit sensor provides indication when the RCCA is at the top position.

Section 7.2 describes the PS, including I&C for CRDS trip functions.

4.6.2 Evaluation of the Control Rod Drive System

The safety-related function of the CRDS is to perform a rod drop and put the reactor in a subcritical condition. As described in Section 3.9.4, the CRDMs fail in an acceptable condition in accordance with GDC 23. When power is interrupted, the CRDMs insert the RCCA into the core by gravity. Therefore, the power supply to the operating coils of the CRDM is non-safety related. Additionally, the CRDS is part of the environmental qualification program as described in Section 3.11 and in Table 3.11-1, so that the CRDS remains functional and provides reactor shutdown capabilities under adverse environmental conditions. As noted in Section 3.1, in the event of a high or moderate energy pipe failure within the plant, adequate protection is provided so that essential structures, systems, and components are not impacted by the adverse effects of postulated piping failure. Within the support structure, the reactor vent lines and in-core instrumentation lines are high energy lines and are designed to comply with ASME Section III. These lines are less than or equal to one inch nominal pipe size (NPS) and as addressed in Section 3.6.2.1.3, are not postulated for line breaks or leakage cracks and therefore, do not represent a credible failure mode. As addressed in Section 3.5.1.2.2, a CRDM pressure housing failure, sufficient to create a missile from a piece of the housing or to allow a control rod to be ejected rapidly from the core, is non-credible. The U.S. EPR design also prevents the dynamic effects of postulated pipe ruptures based on the application of the leak before break approach.

The CRDS design follows the guidance of IEEE 384-1992 (Reference 3) and RG 1.75 with respect to physical independence and electrical isolation between essential and non-essential components. Physical separation, or barriers utilized to achieve the physical separation, and approved electrical isolation devices are utilized to implement electrical isolation. As addressed in Section 7.1, the safety-related I&C systems and components are designed to accommodate the effects of, and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, which include loss-of-coolant accidents (LOCA) and from events and conditions outside the plant in accordance with GDC 4. Section 7.1 also addresses I&C architecture implementation of several design strategies such as defense-in-depth, functional diversity, priority, and redundancy that optimize plant safety.

The PS conforms to IEEE Std 603-1998 (Reference 2) as described in Sections 7.1, 7.2 and 7.3. To conform to this standard, the PS design was evaluated against numerous criteria, including but not limited to the following:

- Single failure criteria.
- Environmental and seismic qualification.
- Independence.

- Reliability.
- Common cause failure.

As described in Section 7.2, the PS is designed to fail into a safe state or into a state that has been demonstrated to be acceptable in accordance with GDC 23. Each protective function has different requirements and therefore different criteria are used to achieve a fail safe state. The PS divisions are physically separated in their respective Safeguard Buildings. The four divisionally separated rooms containing the PS equipment are in different fire zones. Therefore, the consequences of internal hazards, such as fire, would impact only one PS division. The analog position indicator coils and the bottom position limit sensors, which provide input measurements to the PS, are the only instrumentation required of the CRDM and supporting systems to safely operate. Failure of the position indicator coils or the bottom position limit sensors to operate properly would not prevent the RCCAs from being inserted into the core or result in inadvertent withdrawal from the core. The PS has also been evaluated in the probabilistic risk assessment (PRA) and determined to be of high reliability because of its diverse signals and redundant channels and divisions. Chapter 19 provides a summary of the PRA. The PS is environmentally and seismically qualified to perform its designed safety functions while exposed to normal, abnormal, test, and post-event environmental conditions, as addressed in Section 7.2. As noted in Sections 7.1 and 7.7, there is independence between safety-related equipment of the PS and non-safety-related equipment, and failure of the non-safety-related portions of the CRDCS can not affect the safety-related function of the trip contactors.

A failure modes and effects analysis of the PS, as described in Section 7.2, verifies that the PS will initiate a reactor trip when required even with a credible failure of a single active component.

4.6.3 Testing and Verification of the Control Rod Drive System

The CRDS operability assurance program is described in Section 3.9.4.4. Testing of the CRDS verifies system operability and is conducted in several stages:

- Prototype tests and manufacturer tests prior to initial installation.
- Preoperational and initial startup tests.
- Inservice tests.
- Tests following maintenance and fuel movement.

Abstracts of CRDS tests performed as part of the initial test program are provided in Section 14.2. Also, the Technical Specifications and Section 3.1 provide requirements for surveillance and testing of reactivity control systems.

4.6.4 Information for Combined Performance of Reactivity Systems

The U.S. EPR contains two independent reactivity control systems in accordance with GDC 26 and GDC 27:

- For GDC 26, two independent reactivity control systems are the control rods and the soluble boron in the coolant from the CVCS.
- For GDC 27, the independent reactivity control systems are control rods, SIS, or EBS system, depending on the event.

Under normal operation and anticipated operational occurrences (AOO), control rods compensate for reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full load to no load. In addition, the control rod system provides a minimum shutdown margin during AOOs and is capable of making the core subcritical to prevent exceeding acceptable fuel damage limits, assuming that the highest worth control rod is in the fully withdrawn position. Soluble boron in the reactor coolant compensates for xenon burnout reactivity changes and maintains the core reactivity within the shutdown requirements for the cold shutdown condition.

CVCS is described in Section 9.3.4 and is an operational system used to maintain RCS boron concentration during normal plant operating modes. CVCS and CRDS work together to maintain reactivity control during normal plant operations. As addressed in Section 15.4.6, during normal operation, administrative controls preclude dilution events through procedures that limit the rate and duration of dilution. In addition, CVCS is designed to limit the rate of boron dilution, provide alarms, and take certain protective actions (refer to Section 9.3.4) to mitigate an inadvertent dilution event. Section 15.4.6.2 addresses analyses that show anti-dilution, safety-related protection channels provide effective protection by automatically eliminating the dilution source.

Under postulated accident conditions described in Chapter 15, except for large break LOCA, no credit is taken for reactivity control systems other than reactor trip to mitigate the events to achieve a stable plant condition. For large break LOCA, reactor trip is not credited during the initial mitigation of the event. Shutdown occurs through voiding of the core. Borated water from the accumulators and SIS provide the necessary boration to maintain the shutdown margin during the refilling of the core. Insertion of the control rods is credited to provide additional shutdown margin during long-term cooling. For plant events that go from a stable plant condition to cold shutdown condition, EBS is credited for boron addition. Information on the CRDS is provided in Section 3.9.4. In addition to CRDS, the SIS, and EBS systems contribute to the combined performance of reactivity control systems:

- SIS is described in Section 6.3. SIS is designed to meet single failure criterion. The system consists of four independent 100 percent capacity trains with each train

located in a separate Safeguards Building, as further described in Section 6.3.2. The SIS limits fuel assembly damage during core flooding (via accumulators) and emergency core cooling following a LOCA. This separation and independence provides protection from physical damage due to natural phenomena and hazards, and it allows fulfillment of the system safety function in the event of a single failure. See Figure 6.3-1—Safety Injection System Overview for a system layout.

- EBS is described in Section 6.8 and is available to inject high-pressure borated water into the reactor coolant system to support reactor shutdown. The EBS is a safety-related system and is used for reactivity control during postaccident cooldown after Postulated Accidents, including small break LOCAs and non-LOCA events where cooldown to cold shutdown conditions is the final design end state. The EBS performs its safety functions assuming the most limiting single active failure concurrent with a loss of offsite power. EBS consists of two redundant trains. Except for the injection lines that enter the reactor building, the two EBS trains are housed in separate divisions within the Fuel Building. Within the Fuel Building, each EBS train is physically separated by a wall, and the common suction and outlet lines are protected from each other and from high energy piping in other systems. The EBS is designed to withstand the effects of natural phenomena within the plant design basis without losing the capability to perform its safety functions. Redundant pumps and injection paths are installed in separate fire zones. Divisional separation protects these injection loops against dynamic effects that may result from equipment failures in accordance with GDC 4. See Table 6.8-1.

For the Chapter 15 analyses involving a reactor trip, the single, highest worth RCCA is postulated to remain untripped in a fully withdrawn position to satisfy the stuck rod criterion. Analyses specifically related to the CRDS failure or misoperation are provided in Section 15.4:

- Uncontrolled rod assembly withdrawal in Sections 15.4.1 and 15.4.2.
- Control rod misoperation in Section 15.4.3.
- Rod ejections in Section 15.4.8.

Mechanical failure or overheating of the CRDM causes failure of only one RCCA from inserting into the core by gravity, and the other CRDMs remain functional. Table 4.3-6 shows that more than 100 percent shutdown margin is available for reactor shutdown. This demonstrates that the CRDS maintains the reactor in a subcritical condition assuming a credible failure of a single active component and the CRDS has a high probability of functioning during AOOs and other accidents in accordance with GDC 29. As addressed in Sections 7.2 and 7.7, the PS and RCSL are designed with sufficient reliability to perform their functions in the event of AOOs. RCSL performs limitation functions to help reduce the risk of actuating a protective action as a result of an AOO. In the event an AOO leads to conditions requiring protective actions, the PS is designed to initiate reactor trip and ESF functions to protect the core and RCPB in accordance with GDC 29.

4.6.5 Evaluation of Combined Performance

For reactor trip functions, there are diverse means of tripping the reactor by dropping control rods even if a postulated common cause failure were to disable the PS. An automatic diverse actuation system and a manual hardwired trip function are provided as described in Section 7.8 and Section 7.2.

The CRDS reactivity insertion rates are described in Section 4.3.

The maximum reactivity change rate for normal operations and postulated accidental withdrawal of control banks prevent the peak heat generation rate and departure from nucleate boiling ratio from exceeding the maximum allowable values in accordance with GDC 25. The PS is designed to protect the fuel design limits in the presence of any single malfunction of the reactivity control systems. Additional information is provided in Section 7.1. The PS contains the functionality required to establish that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems in accordance with GDC 25.

- The maximum reactivity worth of control rods and the maximum rates of reactivity insertion employing control rods are limited to preclude rupture of the coolant pressure boundary or disruption of the core internals to a degree which would impair core cooling capacity during a rod withdrawal or ejection accident, as described in Section 15.4.

- Following a reactivity accident, such as rod ejection or steam line break, the reactor can be brought to the shutdown condition, and the core will maintain acceptable heat transfer geometry in accordance with GDC 28. The RCSL system is designed with sufficient reliability to perform automatic control and limitation of primary parameters associated with the reactor core and RCS. The PS is designed to protect against damage to the RCPB in the event of a postulated reactivity accident, as described in Section 7.2 and in accordance with GDC 28.

- Reactivity addition associated with an accidental withdrawal of a control bank or banks is limited by the maximum rod speed (i.e., 29.52 inches per minute) and by the worth of the banks.

The CRDS is constructed to have a combined capability, in conjunction with boration by the emergency core cooling system (i.e., SIS or EBS), of reliably controlling reactivity changes to establish that under postulated accident conditions the capability to cool the core is maintained. The SIS has been evaluated as described in Section 6.3 and in the Chapter 15 safety analyses. These analyses demonstrate that the CRDS and SIS and EBS systems reliably control reactivity changes to cool the core under postulated accidents in accordance with GDC 27.

4.6.6 References

1. ANP-10309P, Revision 3, "U.S. EPR Protection System Technical Report," June 2011.

2. IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1998.

3. IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers, Inc., 1992.