U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPOWER™ iPWR DESIGN

7.0 INSTRUMENTATION AND CONTROLS – INTRODUCTION AND OVERVIEW OF REVIEW PROCESS

This design-specific review standard (DSRS) section provides guidance to the staff of the U.S. Nuclear Regulatory Commission (NRC) to use in reviewing the instrumentation and control (I&C) design of the Babcock and Wilcox (B&W) mPower™ nuclear power reactor. This guidance will assist the staff in determining whether the design complies with the applicable regulatory requirements and whether the applicant has demonstrated that there is reasonable assurance that the design will provide adequate protection of public health and safety. This DSRS was developed as a pilot initiative for the mPower™ design, and is not applicable to other designs unless specifically addressed in DSRS document for that design center because this guidance focuses on B&W mPower™ design-specific technical matters.

Major Differences Between the DSRS and the Standard Review Plan

The guidance in this DSRS chapter differs from the guidance in Chapter 7 of the Standard Review Plan (SRP) (NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," issued in 2007). This DSRS chapter reflects a number of important lessons the staff learned when using the SRP to review new large light-water reactor (LWR) designs.

The staff has incorporated the following lessons learned into this guidance:

1. This guidance emphasizes fundamental I&C design principles such as independence, redundancy, predictability and repeatability, and diversity and defense-in-depth. The staff intends to verify that an applicant has shown the I&C design incorporates these principles through analysis, such as hazard analysis. These principles are cornerstones of the staff's review in this area. The current SRP guidance is system-focused and does not take advantage of such a unifying framework. This guidance aims to address all the significant aspects of the I&C design in a unified manner through this framework.

2. This guidance highlights only those technical requirements and guidance applicable to the B&W mPower integral pressurized-water reactor (iPWR). The existing SRP discusses regulatory requirements that are inapplicable to the mPower™ design and guidance that is not used in this DSRS. For example, the SRP cites the Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard (Std.) 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," which is only applicable to nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999.

3. The structure of this guidance reflects an integrated I&C design using digital technology, which is common in new and advanced reactor design. In addition, the areas most significant to safety are discussed first. The current SRP guidance is system-based;

ADAMS Accession No. ML12314A197

therefore, many regulatory requirements and their supporting guidance are repeated in multiple subsections. The approach of this DSRS minimizes such repetition.

4. This guidance applies to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g., Field Programmable Gate Arrays (FPGAs)). This DSRS uses the term software to refer to such technology and complex logic. The staff considers the information in this guidance sufficient to form a basis for an NRC finding in the area of software. The current SRP guidance is not always clear on the subject of software development because it reflects the complete software development life cycle, which may not be fully implemented at the design certification (DC) review stage.

5. This guidance introduces the use of an integrated hazards analysis approach, which is a well-established safety engineering practice, to NRC I&C review practices. This approach consolidates the various methods discussed in the current SRP and provides a consistent, comprehensive, and systematic way to address the potential hazards associated with the I&C systems in a unified framework.

6. This guidance also provides an approach to evaluate whether simplicity has been considered in the design of the digital I&C system. Although no regulations, standards, or guidance explicitly address the concept of simplicity for digital I&C systems, recent experience in reviews of LWR applications has shown that complex I&C systems can challenge the demonstration of conformance with safety system design criteria such as independence. In this context, simplicity supports all fundamental design principles for developing I&C safety systems.

7. This guidance encompasses all relevant branch technical positions contained in the current SRP. This guidance also clarifies the interface between the I&C area and other disciplines, such as equipment qualification, (Chapter 3), human factors engineering (Chapter 18), quality assurance (Chapter 17), and reactor systems (Chapter 15).

I&C System Review Scope

The guidance contained in DSRS Chapter 7 covers all I&C safety systems and components (i.e., hardware, software, firmware, and other forms of complex logic). This guidance also covers those areas such as software tools and equipment that are used for the I&C design or are connected to the I&C systems or components for testing.

Most of the guidance contained in DSRS Chapter 7 is derived from IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which is an NRC requirement for I&C safety systems. The scope of IEEE Std. 603-1991 includes all I&C safety systems. While IEEE Std. 603-1991 does not establish requirements for I&C systems that are not safety-related, such as control systems and diverse I&C systems, the criteria in IEEE Std. 603-1991 can be applied to any I&C system. Consequently, the reviewer will use the concepts of IEEE Std. 603-1991 and the guidance contained in DSRS Chapter 7 in the review of I&C systems that are not safety-related but are risk-significant as a starting point, using a graded approach commensurate with the safety and risk significance of the system or component. Applicable review considerations include, for example, design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing.

The guidance in Chapter 7 of the DSRS applies to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g., Field Programmable Gate Arrays (FPGAs)). Careful consideration should be given to characteristics of software elements (e.g., software/logic development process, impact of design errors, translation of algorithms, etc.) and hardware elements (e.g., failure modes, electronic-level timing, electrical issues, type of processing, etc.) for each type of technology chosen by the applicant.

I&C System Review Objectives

The objective of all I&C safety system reviews is to confirm that (1) the I&C system design includes the functions necessary to assure adequate safety during operation of a nuclear power plant under normal conditions and under accident conditions, (2) these functions, and the I&C systems and equipment have been properly classified, and (3) an application demonstrates that appropriate quality standards will be used for the design, fabrication, construction, and testing of I&C systems and equipment commensurate with the importance of the I&C safety functions to be performed.

To ensure the review objectives are met, the reviewer should confirm that (1) variables and systems are properly monitored to assure a safe state, (2) variables and systems are maintained within their prescribed operating ranges, (3) variables and systems in an abnormal condition are identified and such an abnormal condition is communicated to the respective destinations credited in the safety analysis, (4) systems and components are automatically initiated to assure that fuel design limits are not exceeded as a result of AOOs, and (5) systems are capable of operating under accident conditions.

DSRS Chapter 7 covers the following topics:

1. DSRS Section 7.1 provides guidance to I&C reviewers that is used to confirm that the application contains sufficiently detailed design information, in the form of functional block diagrams, descriptions of operation, architectural descriptions, and other design details, to demonstrate that the hardware and software for digital I&C architectures incorporate the fundamental design principles, namely independence; redundancy; predictability and repeatability; and diversity and defense-in-depth.

2. DSRS Section 7.2 provides guidance associated with major functional and design characteristics, including IEEE Std. 603-1991 performance requirements, general arrangements, and materials of construction of I&C systems and components, that I&C reviewers will use to confirm that the final design will conform to the design bases with adequate margin.

3. Sections 7.1, 7.2, and Appendices A, B, and C of the DSRS are used in the review of an application to confirm that all safety functions allocated to I&C safety related systems, including the computer software supporting system operation, and all functions, information, and resources upon which these are dependent, are identified and analyzed in Chapter 7 in the application. The safety systems and functions supported by the I&C system are identified and described in other sections of the application (particularly in Chapters 5, 6, 8, 9, 10, 15, and 18). The review of these systems is coordinated (as described above) with the organizations that have primary review responsibility for the supported systems.

4. For design certification (DC) and combined license (COL) reviews, the staff reviews the applicant's proposed ITAAC associated with the SSCs related to this design-specific review

standard (DSRS) section in accordance with DSRS Section 14.3, "Inspections, Tests, Analyses, and Acceptance Criteria." The staff recognizes that the review of ITAAC cannot be completed until after the rest of this portion of the application has been reviewed against acceptance criteria contained in this DSRS section. Furthermore, the staff reviews the ITAAC to ensure that all SSCs in this area of review are identified and addressed as appropriate in accordance with DSRS Sections 14.3 and 14.3.5.

DSRS Table 7-1 lists all regulatory requirements associated with I&C safety systems, the applicable DSRS section, and I&C review responsibilities.

When an application takes exception to the guidelines applicable to I&C safety systems, the bases for such an exception is reviewed to confirm that it is acceptable. The bases for each exception to the guidelines should demonstrate that the exception does not result in a significant reduction in the margin of safety or in nonconformance with applicable requirements.

I&C System Review Interfaces

I&C systems provide for the collection, integration, and dissemination of information and the subsequent control actions needed to assure adequate safety during plant operation. These I&C functions involve numerous interfaces and interactions with other plant systems, necessitating corresponding interactions between the I&C discipline with other disciplines for review of a nuclear power plant design. Emphasis among these interfaces is the one with Chapter 15, in which design-basis accidents (DBAs) and AOOs analyses are presented. These analyses establish the bases for safety system design and associated safety margins. For example, the Chapter 15 portion of the applicant's final safety analysis report (FSAR) identifies the variables to be monitored, the suitability of the monitored variables for generating signals to initiate automatic protective actions, and the credited automatic protective actions. The organization responsible for reviewing Chapter 15 of the application is the lead for completing this review, and confirms that all the safety functions required from this perspective are adequately identified and will request assistance from the I&C organization if needed.

Several other DSRS chapters identify additional variables and control features with respect to a wide variety of structures, systems, and components (SSCs). The organizations responsible for these reviews have the lead for completing them and will request assistance from the I&C organization if needed.

The reviews associated with Chapter 7 confirm that the I&C system requirements, including those related to parameters and control features identified in other chapters of the DSRS, are allocated to the protection and control systems. In some cases, I&C system components must meet specialized requirements (such as environmental qualifications), requiring those components to be reviewed by other organizations. These organizations have the lead for completing the special requirement reviews and will request assistance from the I&C organization if needed.

The following organizations provide the lead role in evaluating the interface and interactions described. I&C reviewers support these reviews when requested by the lead organization. Specific technical questions on safety or compliance with requirements may warrant additional interactions between organizations to resolve the concerns.

1. The organization responsible for the review of transients and accidents analyses evaluates the adequacy of limiting conditions for operation, limiting safety system

settings, and design descriptions for safety-related components and systems. The I&C reviewer ensures that the application lists the settings of all the protection and safety system functions that are credited in the safety analysis and that the variables monitored to support these functions are appropriate.

2. The organization responsible for the review of reactor systems evaluates the adequacy of protective, control, display, and interlock functions and confirms that they are consistent with the accident analysis, the operation of the I&C systems, and the requirements of General Design Criteria (GDCs) 10, 15, 28, 33, 34, and 35.

3. The organization responsible for the review of plant systems evaluates the adequacy of the auxiliary supporting features and other auxiliary features to assure that they satisfy the applicable acceptance criteria. These features include, for example, compressed (instrument) air, cooling water, systems for boration of reactor or spent fuel pool makeup water, lighting, heating, and air conditioning. This review confirms that (1) the design of the auxiliary supporting features and other auxiliary features ensure that these components, equipment, and systems do not degrade the I&C safety systems below an acceptable level, and (2) the auxiliary supporting features and other auxiliary features will maintain the environmental conditions in the areas containing I&C equipment as specified in the FSAR. This review includes the design criteria and testing methods employed in the seismic design and installation of equipment implementing auxiliary supporting features and other auxiliary features. The organization responsible for review of plant systems also evaluates the adequacy of protective, control, display, and interlock functions, and confirms that they are consistent with the operation of the supported system credited in the safety analysis and the requirements of GDCs 41 and 44.

4. The organization responsible for the review of containment systems reviews the containment ventilation and atmospheric control systems provided to maintain environmental conditions for I&C equipment located inside containment. This organization also evaluates the adequacy of protective, control, display, and interlock functions associated with containment systems and severe accidents, and confirms they are consistent with the accident analysis, operation of containment features, and the requirements of GDCs 16 and 38.

5. The organization responsible for the review of electrical systems (1) evaluates the adequacy of physical separation criteria for cabling and electrical power equipment, (2) determines whether power supplied to redundant systems is supplied by appropriately redundant sources, and (3) confirms the adequacy of design features associated with the proper functioning of the onsite and offsite power systems, such as protective devices. The guidance of DSRS Section 7 also applies to any protective device, such as a circuit breaker or relay with digital logic built into it. The guidance of DSRS Section 7 also applies to any grounding paths from an I&C element in a safety system to a ground through the electrical power network.

6. The organization responsible for the review of environmental qualification reviews the environmental qualification of I&C equipment. The organization responsible for the review of electrical systems (1) evaluates the adequacy of physical separation criteria for cabling and electrical power equipment, (2) determines whether power supplied to redundant systems is supplied by appropriately redundant sources, and (3) confirms the adequacy of instrumentation associated with the proper functioning of the onsite and

offsite power systems, such as protective devices.

7. The organization responsible for the review of environmental qualification reviews the environmental qualification of I&C equipment. The scope of this review includes the design criteria and qualification testing methods and procedures for I&C equipment consistent with GDC 4, Title 10 of the Code of Federal Regulations (CFR), Section 50.49, and Section 5.4 of IEEE Std. 603-1991.

8. The organization responsible for the review of seismic qualification reviews the seismic qualification demonstration for I&C equipment, including the design criteria and qualification testing methods and procedures consistent with 10 CFR Part 50, Appendix B, Criterion III. The organization responsible for the review of human-machine interface evaluates the adequacy of the arrangement and location of I&C, and confirms that the functions allocated to the operators can be successfully accomplished.

9. The organization responsible for the review of quality assurance reviews general quality assurance programs.

10. The organization responsible for the review of probabilistic risk analysis and severe accidents evaluates the adequacy of the models and methods used for the probabilistic risk analysis and strategies for handling severe accidents, including aspects associated with I&C.

DSRS Chapter 7 Acceptance Criteria and Review Process

1. Regulatory Requirements

   10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” including the correction sheet dated January 30, 1995, which is referenced in 10 CFR 50.55a(h)(2) and (3). The standard sets forth design and functional requirements that are discussed in this DSRS. In addition, IEEE Std. 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," in place 6 months before the docket date of the application as endorsed by Regulatory Guide (RG) 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," provides specific guidance for the application of IEEE 603-1991 criteria to computer-based I&C systems.

   In accordance with 10 CFR 50.55a(a)(3), an applicant can propose alternatives to the requirements of 10 CFR 50.55a(h), but the applicant must demonstrate that the proposed alternative would provide an acceptable level of quality and safety or that compliance with the specified requirements of 10 CFR 50.55a(h) would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety. In accordance with 10 CFR 52.47(a)(8),(21), and (22), for new reactor license applications submitted under Part 52, the applicant is required to include the following information: (1) the proposed technical resolution of unresolved safety issues (USIs) and medium- and high-priority generic safety issues (GSIs) that are identified in the version of NUREG-0933 current on the date 6 months before the docket date of the application and that are technically relevant to the design; (2) the information necessary to demonstrate how operating experience insights have been incorporated into the plant design; and, (3) the information necessary to demonstrate compliance with any technically relevant portions of the TMI requirements set forth in 10 CFR 50.34(f), except

paragraphs (f)(1)(xii), (f)(2)(ix), and (f)(3)(v). These cross-cutting review areas should be addressed by the reviewer for each technical subsection and relevant conclusions documented in the corresponding safety evaluation report (SER) section.

2. DSRS Acceptance Criteria

   Each DSRS subsection identifies specific DSRS acceptance criteria which the staff has determined to provide an acceptable approach for satisfying the applicable requirements. The types of guidance documents include but are not limited to: Regulatory Guides, Commission policy as described in SECY papers and corresponding Staff Requirements Memoranda (SRM), certain technical reports (e.g., NUREGs), and specific staff positions that set forth solutions and approaches previously determined to be acceptable by the staff in dealing with a similar safety or design matter. The DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the requirements in 10 CFR 52.47(a)(9), "Contents of applications; technical information." The same approach may be used to meet the requirements of 10 CFR 52.79(a)(41) for COL applications.

3. Level of Review Applied To I&C Systems

   As stated in Commission Paper SECY-11-0024, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," the level of review for a particular system, structure, or component (SSC) is derived from both the SSC's safety importance (i.e., safety-related or nonsafety-related) and risk significance. The introduction to NUREG-0800, "Introduction," Part 2, describes the licensing review philosophy and framework to be applied by the staff for new iPWR design certification and combined license applications under 10 CFR Part 52. With the incorporation of risk insights, I&C systems may be classified as:

   Safety-related risk-significant (A1)
   Safety-related nonrisk-significant (A2)
   Nonsafety-related risk-significant (B1)
   Nonsafety-related nonrisk-significant (B2)

   The staff expects that the mPower™ application will include the classification of SSCs, a list of risk-significant SSCs, and a list of SSCs subject to Regulatory Treatment of Non-Safety Systems (RTNSS) (called RTNSS SSCs). The I&C staff will support a review of RTNSS SSCs with other technical organizations in accordance with the guidance in DSRS Section 3.2 and SRP Sections 17.4 and 19.3 to confirm that nonsafety-related SSCs that perform risk-significant functions are included within the scope of the RTNSS process. With this determination, the review framework for I&C systems will be implemented as follows:

   A. For SSCs determined to be **safety-related risk-significant (A1), and safety-related nonrisk-significant (A2)**, the level of review will involve detailed analyses and evaluation techniques to satisfy the acceptance criteria contained in the DSRS. This includes Sections 7.1, 7.2 and Appendices A, B, and C of Chapter 7 of the DSRS. In addition, the review will identify those programmatic requirements applicable to I&C

systems in order to augment the review scope and to support the overall safety review of the application.

In the context of I&C, the term "safety system" is used to include all systems that are safety-related. Protection systems are I&C safety systems that initiate actions to assure that fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and respond to design basis events (DBEs). During safe shutdown[1], reactivity control systems must be capable of maintaining the core in a subcritical condition under cold conditions, and residual heat removal systems must be capable of maintaining adequate cooling of the core.

i. The reactor trip system (RTS) initiates rapid control rod insertion to mitigate the consequences of AOOs and DBEs.

ii. The engineered safety features actuation system (ESFAS) initiates and controls safety equipment that removes heat or otherwise assists with maintaining the integrity of the physical barriers to radioactive release (e.g., fuel cladding, reactor coolant pressure boundary, and containment). Typical engineered safety features (ESF) systems include:

- Containment and reactor vessel isolation systems.
- Emergency core cooling systems (ECCSs).
- Containment heat removal and depressurization systems.
- Pressurized-water reactor (PWR) auxiliary feedwater systems.
- Emergency boration systems.
- Containment air purification and cleanup systems.
- Containment combustible gas control systems.
- Control room isolation and emergency heating, ventilating, and air conditioning (HVAC).

iii. Safe shutdown systems function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include I&C systems used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions, as defined in SECY94-084 "Policy and Technical Issues Associated with the Regulatory Treatment of Non-safety Systems in Passive Plant Designs," Typical safe shutdown functions include:

- Reactivity control.
- Reactor coolant makeup.
- Reactor pressure control.
- Decay heat removal.

To the extent that ESF systems are used to achieve and maintain safe shutdown, the review of these systems is limited to those features that are unique to safe shutdown and not rcredited for accident mitigation.

[1] The NRC considers a "safe stable shutdown condition" for advanced passive LWRs to be:
A condition by which all plant conditions are stable and within regulatory limits and the reactor coolant system pressure is stabilized and reactor coolant temperature is at value less than or equal to 420 degrees F.

iv. Auxiliary supporting features and other auxiliary features are systems or components of systems that provide support functions necessary for the safety systems to accomplish their safety functions. Figure 3 of IEEE Std. 603-1991, "Examples of Equipment Fitted to Safety System Scope Diagram," provides a matrix with an extensive list of auxiliary supporting features and other auxiliary features. Heating, ventilation, and air conditioning systems and electrical power systems are examples of auxiliary supporting features. Auxiliary supporting features are discussed primarily in Chapters 8 and 9 of the Safety Analysis Report. Examples of other auxiliary features include built-in test equipment and isolation devices. The I&C aspects of auxiliary supporting features and other auxiliary features are addressed in the review of those SAR sections which discuss the systems or components that provide these functions. To the extent that the operation of auxiliary supporting features or other auxiliary features are initiated by the protection system, this aspect is included in the review of I&C safety systems.

B. For SSCs determined to be **nonsafety-related risk-significant (B1)**, the level of review will shift from applying analyses and evaluation techniques to identifying those programmatic requirements applicable to I&C systems that satisfy the acceptance criteria contained in the DSRS. The objectives of the review are to confirm that B1systems are capable of controlling variables within prescribed operating ranges, and to confirm that the effects of operation or failures of these systems are bounded by the accident analyses in Chapter 15 of the DSRS.

Staff expects RTNSS systems to be in the scope of the B1 systems. Not all B1 systems are RTNSS, but the B1 acceptance criteria outlined below will be used for systems and functions that are considered risk-significant. The RTNSS criteria used to determine risk-significant SSC functions are contained in Section 19.3 of the SRP. The I&C technical staff assist in the review of those SSC functions associated with the following RTNSS categories:

RTNSS "A" – SSC functions relied on to meet beyond design basis deterministic performance requirements such as those set forth in Title 10 of the Code of Federal Regulations (10 CFR) 50.62 for mitigating Anticipated Transients Without Scram (ATWS) and in 10 CFR 50.63 for Station Blackout (SBO). The I&C review scope includes the diverse actuation system (DAS) which is used to actuate plant systems for ATWS mitigation.

RTNSS "B" – SSC functions relied on to ensure long-term safety (beyond 72 hours) and to address seismic events. The I&C review scope includes post-accident monitoring (PAM) systems, including safety-related displays in the control room, emergency lighting, control room cooling to remove heat generated by personnel, and monitoring equipment.

RTNSS "C" – SSC functions relied on under power-operating and shutdown conditions to meet the Commission's safety goal guidelines of a core damage frequency (CDF) of less than 1x10-4 each reactor year and a large release frequency (LRF) of less than 1x10-6 each reactor year.

RTNSS “D” – SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents.

RTNSS “E” – SSC functions relied on to prevent significant adverse systems interactions between passive safety systems and active non-safety SSCs. The I&C review scope includes evaluations of the potential for adverse interaction between passive safety-related and active non-safety-related systems to confirm that any non-safety-related design features or functional capabilities relied upon to prevent non-safety-related systems from adversely impacting a safety function have been included in the scope of RTNSS.

There may be other nonsafety-related SSCs whose functions could impact plant safety and control that are not considered within the scope of RTNSS. Examples include systems used for reactivity control of the reactor through the positioning of the control rods, systems used to control the feedwater to the reactor vessel and feedwater temperature, and systems used to regulate reactor steam flow and pressure. These systems can affect the performance of safety-related functions either through normal operation, inadvertent operation, or various AOOs that could be considered candidates for regulatory oversight. If such systems and functions are considered risk-significant, the I&C staff will conduct a review using the review criteria for B1 SSCs.

The I&C review of B1 SSCs will emphasize the following specific topics from Section 19.3 of the SRP and selected topics from Sections 7.1, 7.2 and Appendices A, B, and C of Chapter 7 of the DSRS:

i. The reviewer should help with the identification of SSC functions based on the RTNSS criteria listed above.

ii. The reviewer should review the functional design of RTNSS SSCs, including the adequacy of functional design and design improvements to minimize adverse interaction between passive and non-safety-related active systems. The reviewer will confirm the following:

- The reviewer should confirm that the nonsafety-related systems meet the reliability and availability goals assumed for the system and that a single point of failure of the nonsafety system would not result in consequences more severe than those described in the analysis in Chapter 15 of the SAR.

- The reviewer should review the bases for the nonsafety-related systems’ design to confirm the necessary features for manual and automatic control of process variables within prescribed normal operating limits.

- The reviewer should confirm that the plant accident analysis in Chapter 15 of the SAR does not rely on the operability of any nonsafety-related system function to assure that regulatory limits are met.

- For nonsafety-related system elements credited in the diversity and defense-in-depth analysis, the reviewer should use the review criteria for diverse I&C systems in DSRS Section 7.1.5.

- The reviewer should confirm that the safety analysis includes consideration of the effects of both nonsafety-related system action and inaction in assessing the transient response of the plant for postulated accidents and anticipated operational occurrences.

- The reviewer should confirm that the failure of any nonsafety-related system component or any auxiliary supporting system for nonsafety-related systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the application. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures (the evaluation of multiple independent failures is not intended).

- The reviewer should confirm that the consequential effects of anticipated operational occurrences and postulated accidents do not lead to nonsafety-related system failures that would result in consequences more severe than those described in the analysis in Chapter 15 of the SAR.

- The reviewer should confirm that I&C systems include environmental control as necessary to protect equipment from environmental extremes. This would include, for example, heat tracing of instruments and instrument sensing lines as discussed in RG 1.151, “Instrument Sensing Lines,” and cabinet cooling fans.

- With respect to an I&C system that is not safety-related, the reviewer will confirm that the application describes quality measures commensurate with the importance of the system function to be accomplished. Refer to DSRS section 7.2.1 for additional guidance. To satisfy GDC 1, an applicant may choose to apply its Appendix B QA program to I&C systems that are not safety-related. In any case, the development of a software-based I&C system that is not safety-related should follow a structured system and software development framework consistent with the guidance in this section.

- The reviewer should use the review criteria for independence in DSRS 7.1.2 to confirm adequate independence of safety systems from nonsafety-related systems.

- The nonsafety-related systems design should minimize the potential for inadvertent actuation and challenges to safety-related systems.

- The reviewer should use the review criteria for access control in DSRS 7.2.9 to confirm adequate physical and electronic control of access to digital computer-based nonsafety-related system software and data to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

iii. The reviewer should review the proposed regulatory treatment proposed for SSCs in the scope of the RTNSS program to confirm that the oversight is

commensurate with the risk-significance of each SSC's reliability/availability mission.

Note that for SSCs determined to be highly risk-significant, it may be appropriate to perform a more detailed review using Sections 7.1, 7.2 and Appendices A, B, and C of Chapter 7 of the DSRS.

C. For SSCs determined to be **nonsafety-related nonrisk-significant (B2)**, both the design-related review and the programmatic requirements are anticipated to be minimal. For the performance-oriented acceptance criteria, the review is focused on identifying those performance-based activities (e.g., tests or inspections) within the applicable programmatic requirements which can be used to satisfy the acceptance criteria from the DSRS.

TABLE 7.1 INSTRUMENTATION AND CONTROLS – MAPPING OF REGULATORY REQUIREMENTS AND DSRS REVIEW CRITERIA

Regulations	Location in DSRS	Review Responsibilities
10 CFR 50.55a(h)		
IEEE Std. 603-1991, Section 4, "Safety System Designation"	7.1.1 Safety System Design Basis 7.1.4 Predictability and Repeatability (covers Section 4.10)	Full
IEEE Std. 603-1991, Section 5.1, "Single-Failure Criterion"	7.1.3 Redundancy 7.1.5 Diversity and Defense-in-Depth	Full
IEEE Std. 603-1991, Section 5.2, "Completion of Protective Action"	7.2.3 Reliability, Integrity, and Completion of Protective Action	Full
IEEE Std. 603-1991, Section 5.3, "Quality"	Covered in Chapter 17 of the DSRS	Partial, [1]
IEEE Std. 603-1991, Section 5.4, "Equipment Qualification"	7.2.2 Equipment Qualification	Partial, [2]
IEEE Std. 603-1991, Section 5.5, "System Integrity"	7.2.3 Reliability, Integrity, and Completion of Protective Action	Full

Regulations	Location in DSRS	Review Responsibilities
IEEE Std. 603-1991, Section 5.6, “Independence”	7.1.2 Independence	Full
IEEE Std. 603-1991, Section 5.7, “Capability for Test and Calibration”	7.2.15 Capability for Test and Calibration	Full
IEEE Std. 603-1991, Section 5.8, “Information Displays”	7.2.4 Operating and Maintenance Bypasses 7.2.13 Displays and Monitoring	Full
IEEE Std. 603-1991, Section 5.9, “Control of Access”	7.2.9 Control of Access, Identification, and Repair	Full
IEEE Std. 603-1991, Section 5.10, “Repair”	7.2.9 Control of Access, Identification, and Repair	Full
IEEE Std. 603-1991, Section 5.11, “Identification”	7.2.9 Control of Access, Identification, and Repair	Full
IEEE Std. 603-1991, Section 5.12, “Auxiliary Features”	7.2.8 Auxiliary Features	Full

Regulations	Location in DSRS	Review Responsibilities
IEEE Std. 603-1991, Section 5.13, "Multi-Unit Stations"	7.2.11 Multi-Unit Stations	Full
IEEE Std. 603-1991, Section 5.14, "Human Factors Considerations"	7.2.14 Human Factors Considerations	Full
IEEE Std. 603-1991, Section 5.15, "Reliability"	7.2.3 Reliability, Integrity, and Completion of Protective Action	Full
IEEE Std. 603-1991, Section 6.1, "Automatic Control"	7.2.12 Automatic and Manual Control	Full
IEEE Std. 603-1991, Section 6.2, "Manual Control"	7.2.12 Automatic and Manual Control	Full
IEEE Std. 603-1991, Section 6.3, "Interaction Between the Sense and Command Features and Other Systems"	7.2.10 Interaction between Sense and Command Features and Other Systems	Full
IEEE Std. 603-1991, Section 6.4, "Derivation of System Inputs"	7.2.6 Derivation of System Inputs	Full
IEEE Std. 603-1991, Section 6.5, "Capability for Testing and Calibration"	7.2.15 Capability for Test and Calibration	Full

Regulations	Location in DSRS	Review Responsibilities
IEEE Std. 603-1991, Section 6.6, "Operating Bypasses"	7.2.4 Operating and Maintenance Bypasses	Full
IEEE Std. 603-1991, Section 6.7, "Maintenance Bypass"	7.2.4 Operating and Maintenance Bypasses	Full
IEEE Std. 603-1991, Section 6.8, "Setpoints"	7.2.7 Setpoints	Full
IEEE Std. 603-1991, Section 7.1, "Automatic Control"	7.2.12 Automatic and Manual Control	Full
IEEE Std. 603-1991, Section 7.2, "Manual Control"	7.2.12 Automatic and Manual Control	Full
IEEE Std. 603-1991, Section 7.3, "Completion of Protective Action"	7.2.3 Reliability, Integrity, and Completion of Protective Action	Full
IEEE Std. 603-1991, Section 7.4, "Operating Bypass"	7.2.4 Operating and Maintenance Bypasses	Full
IEEE Std. 603-1991, Section 7.5, "Maintenance Bypass"	7.2.4 Operating and Maintenance Bypasses	Full

Regulations	Location in DSRS	Review Responsibilities
10 CFR Part 50, Appendix A, GDC		
GDC 1, “Quality standards and records”	Covered in Chapter 17 of the DSRS	Partial, [1]
GDC 2, “Design bases for protection against natural phenomena”	7.2.2 Equipment Qualification Coordinated with Chapter 3 of the DSRS	Partial, [3]
GDC 4, “Environmental and dynamic effects design bases”	7.2.2 Equipment Qualification Coordinated with Chapter 3 of the DSRS	Partial, [4]
GDC 10, “Reactor design”	Coordinated with Chapter 15 of the DSRS	Partial, [5]
GDC 13, “Instrumentation and control”	Sections 7.1 and 7.2 of the DSRS	Full, [6]
GDC 15, “Reactor coolant system design”	Coordinated with Chapter 15 of the DSRS	Partial, [7]
GDC 16, “Containment design”	Coordinated with Chapter 6 of the DSRS	Partial, [8]

Regulations	Location in DSRS	Review Responsibilities
GDC 19, “Control room”	Sections 7.1 and 7.2 of the DSRS Coordinated with Chapter 6 of the DSRS Coordinated with Chapter 18 of the DSRS	Full, [9], [25], [26]
GDC 20, “Protection system functions”	Sections 7.1 and 7.2 of the DSRS	Full, [10]
GDC 21, “Protection system reliability and testability”	7.1.2 Independence 7.1.3 Redundancy 7.1.4 Predictability and Repeatability	Full, [11]
GDC 22, “Protection System Independence”	7.1.2 Independence 7.1.5 Diversity and Defense-in-Depth	Full, [12]
GDC 23, “Protection system failure modes”	7.1.1 Safety System Design Basis Appendix A, Hazard Analysis	Full, [13]
GDC 24, “Separation of Protection and Control Systems”	7.1.2 Independence 7.1.3 Redundancy 7.1.5 Diversity and Defense-in-Depth	Full, [14]

Regulations	Location in DSRS	Review Responsibilities
GDC 25, “Protection system requirements for reactivity control malfunctions”	Coordinated with Chapter 15 of the DSRS	Partial, [15]
GDC 28, “Reactivity limits”	Coordinated with Chapter 15 of the DSRS	Partial, [16]
GDC 29, “Protection against Anticipated Operational Occurrences”	7.1.4 Predictability and Repeatability	Full, [17]
GDC 64, “Monitoring Radioactivity Releases ”	7.2.13 Displays and Monitoring	Full
10 CFR 50.34(f)(2), which addresses Three Mile Island (TMI) requirements		
10 CFR 50.34(f)(2)(iv) (Safety Parameter Display Console)	7.2.13 Displays and Monitoring	Full
10 CFR 50.34(f)(2)(v) (Bypass and Inoperable Status Indication)	7.2.4 Operating and Maintenance Bypasses 7.2.13 Displays and Monitoring	Full, [18]

Regulations	Location in DSRS	Review Responsibilities
10 CFR 50.34(f)(2)(xi) (Direct Indication of Relief and Safety Valve Position)	7.2.13 Displays and Monitoring	Full, [19]
10 CFR 50.34(f)(2)(xii) (Auxiliary Feedwater System Automatic Initiation and Flow Indication)	7.2.13 Displays and Monitoring	Full, [20]
10 CFR 50.34(f)(2)(xvii) (Accident Monitoring Instrumentation)	7.2.13 Displays and Monitoring	Full
10 CFR 50.34(f)(2)(xviii) (Instrumentation for the Detection of Inadequate Core Cooling)	7.2.13 Displays and Monitoring	Full, [19]
10 CFR 50.34(f)(2)(xiv) (Containment Isolation Systems)	7.1.5 Diversity and Defense-in-Depth Paragraphs (B) and (D) of 50.34(f)(2)(xiv) should be coordinated with Chapter 6 of the DSRS	Partial, [21]
10 CFR 50.34(f)(2)(xix) (Instruments for Monitoring Plant Conditions Following Core Damage)	7.2.13 Displays and Monitoring	Full

Regulations	Location in DSRS	Review Responsibilities
10 CFR 50.34(f)(2)(xx) (Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves)	7.2.13 Displays and Monitoring Coordinated with Chapter 8 of the DSRS	Partial, [22]
10 CFR 50.34(f)(2)(xxii) (Failure Mode and Effect Analysis of Integrated Control System)	7.2.15 Capability for Test and Calibration	Full
10 CFR 50.34(f)(2) (xxiii) (Anticipatory Trip on Loss of Main Feedwater or Turbine Trip)	7.2.8 Auxiliary Features	Full
Other Regulations		
10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety"	Covered in Chapter 17 of the DSRS	Partial, [1]
10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants"	7.1.5 Diversity and Defense-in-Depth	Full, [23]

Regulations	Location in DSRS	Review Responsibilities
10 CFR 50.36(c)(1)(ii)(A) (Technical Specifications, Safety Limits, Limiting Safety System Settings, and Limiting Control Settings)	7.2.7 Setpoints	Full
10 CFR 50.36(c)(3), "Surveillance Requirements"	7.2.7 Setpoints 7.2.15 Capability for Test and Calibration	Full
10 CFR 50.34(b)(2)(i) (Contents of Applications; Technical Information, Final Safety Analysis Report)	7.2.8 Auxiliary Features	Full
10 CFR 52.47(b)(1)	DSRS Section 14.3.5	Full
10 CFR 52.80(a)	DSRS Section 14.3.5	Full
10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"	7.2.2 Equipment Qualification Coordinated with Chapter 3 of the DSRS	Partial, [24]

Regulations	Location in DSRS	Review Responsibilities
Regulatory Guides		
RG 1.22, "Periodic Testing of Protection System Actuation Functions"	7.2.15 Capability for Test and Calibration	
RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"	7.2.4 Operating and Maintenance Bypasses 7.2.13 Displays and Monitoring	
RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems"	7.1.2 Independence 7.1.3 Redundancy 7.1.5 Diversity and Defense-in-Depth 7.2.11 Multi-Unit Stations	
RG 1.62, "Manual Initiation of Protection Action"	7.1.5 Diversity and Defense-in-Depth 7.2.12 Automatic and Manual Control	
RG 1.75, "Criteria for Independence of Electrical Safety Systems"	7.1.2 Independence 7.2.9 Control of Access, Identification, and Repair	

Regulations	Location in DSRS	Review Responsibilities
RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”	7.2.13 Displays and Monitoring	
RG 1.105, “Setpoints for Safety-Related Instrumentation”	7.2.7 Setpoints	
RG 1.118, “Periodic Testing of Electric Power and Protection Systems”	7.2.15 Capability for Test and Calibration	
RG 1.151, “Instrument Sensing Lines”	7.2.2 Equipment Qualification	[2]
RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”	7.1.2 Independence 7.2.2 Equipment Qualification [2] 7.2.3 Reliability, Integrity, and Completion of Protective Action 7.2.5 Interlocks 7.2.9 Control of Access, Identification, and Repair 7.2.11 Multi-Unit Stations	

Regulations	Location in DSRS	Review Responsibilities
RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems”	7.2.2 Equipment Qualification	[2]
RG 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants”	7.2.2 Equipment Qualification	[2]
RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants”	7.2.2 Equipment Qualification	[2]

Notes:

[1] This regulation is applicable to all I&C systems and components important to safety. The reviewer should confirm that Chapter 17 identifies I&C safety systems and components that are subject to the QA requirements established in 10 CFR Part 50, Appendix B, 10 CFR 50.55a(a)(1), and GDC 1.

[2] The I&C review of equipment qualification is limited to a confirmation that I&C equipment (including isolation devices) subject to qualification requirements have been selected and identified in the application. Organizations responsible for seismic and environmental qualifications verify that the functional performance requirements described in DSRS Chapter 3 are met.

[3] This regulation is applicable to all I&C safety systems and supporting data communication systems. The I&C review for GDC 2 should confirm that the I&C systems important to safety are designed for protection against natural phenomena consistent with the analysis of these events as provided in Chapter 3 of the application, and that they are located and housed in structures consistent with these requirements. DSRS Section 7.2.2 addresses seismic qualification of I&C equipment, which is required by 10 CFR Part 50, Appendix B, Criterion III, 10 CFR 50.49, and Section 5.4 of IEEE Std. 603-1991.

[4] This regulation is applicable to all I&C safety systems and supporting data communication systems. The design bases should identify those systems and components that are designed to accommodate the effects of environmental conditions and that are protected from the dynamic effects of missiles, pipe whipping, and discharging fluids. If systems or components are qualified to survive the environmental effects of postulated accidents for limited periods of time, the bases for limited operability should be provided. The I&C systems needed for severe accidents must be designed so there is reasonable assurance they will operate in the severe accident environment for which they are intended and over the time span for which they are needed. The review of this requirement should be coordinated with the organization responsible for review of environmental qualification. DSRS Section 7.2.2 addresses environmental qualification of I&C equipment, which is required by 10 CFR 50.49 and Section 5.4 of IEEE Std. 603-1991.

[5] This regulation is applicable to I&C protection and control systems. The I&C review scope addresses the adequacy of I&C protective and control functions to confirm that I&C systems are designed with sufficient margin to assure that specified fuel design limits are not exceeded.

[6] This regulation is applicable to all I&C systems including supporting data communication systems. The review of GDC 13 should determine the adequacy of the information provided for the RTS, ESFAS, ESF, safe shutdown, interlock, control, and diverse I&C systems over the anticipated ranges for normal operation, AOOs, and accident conditions.

[7] This regulation is applicable to I&C protection and control systems. The I&C review scope addresses the adequacy of I&C protective and control functions to confirm that I&C systems are designed with sufficient margin to assure that the design conditions

of the reactor coolant pressure boundary are not exceeded. Evaluation of I&C system contributions to design margin for reactor coolant systems should be a part of the review of the adequacy of I&C protective and control functions.

[8] This regulation is applicable to ESF I&C systems. The review of GDC 16 should confirm that the I&C systems provide the functions, performance, and reliability necessary to support the containment system safety function. GDC 16 imposes functional requirements on ESF I&C systems to the extent that they support the requirement that the containment provide a leak tight barrier.

[9] This regulation is applicable to all I&C systems and supporting data communication systems.

[10] This regulation is applicable to I&C protection systems, RTS, and ESFAS.

[11] This regulation is applicable to I&C protection systems, RTS, ESFAS, and supporting data communication systems. Review of compliance with GDC 21 should address:

- Design basis
- Single-failure criterion
- Completion of protective action
- Quality
- System integrity
- Physical, electrical, and communications independence
- Capability for test and calibration
- Indication of bypass
- Control of access to safety system equipment
- Repair and troubleshooting provisions
- Identification of protection system equipment
- Auxiliary features
- Multi-unit stations
- Human factors considerations
- Reliability
- Manual controls
- Derivation of system inputs
- Operating bypasses
- Maintenance bypasses
- Setpoints

[12] This regulation is applicable to I&C protection systems, RTS, ESFAS, and supporting data communication systems. Review of compliance with GDC 22 should address:

- Design basis reliability
- Single-failure criterion
- Quality
- Equipment qualification
- System integrity
- Physical, electrical, and communications independence
- Manual controls
- Setpoints

[13] This regulation is applicable to I&C protection systems, RTS, ESFAS, and supporting data communication systems.

[14] This regulation is applicable to all I&C systems.

[15] This regulation is applicable to the RTS and reactivity control system interlocks. For the review of GDC 25, the staff should confirm that the protection system is designed for an appropriate spectrum of reactivity control system malfunctions as addressed in the review of protection system design basis. Chapter 15 of the application addresses the capability of the protection system to ensure that fuel design limits are not exceeded for events caused from malfunctions of the reactivity control systems.

[16] This regulation is applicable to I&C interlock and control systems. The review of GDC 28 should confirm that the I&C systems provide the functions, performance, and reliability necessary to limit reactivity increases.

[17] This regulation is applicable to the protection systems, reactivity control functions of control systems, and supporting data communication systems.

[18] For compliance with 10 CFR 50.34(f)(2)(v), the staff should address the characteristics of IEEE Std. 603-1991, Sections 5.6, 5.8, 5.12, and 6.3 for the safety system. Since the safety system will satisfy the requirements stated in DSRS Sections 7.1 and 7.2, as part of the staff's review, it meets the characteristics for 10 CFR 50.34(f)(2)(v). In addition, providing automatic indication of the bypassed and operable status of safety systems is covered as part of the staff's review of DSRS Section 7.2.13.

[19] NUREG-0737 provides additional guidance on conformance with this requirement.

[20] For compliance with 10 CFR 50.34(f)(2)(xii), the staff will, in addition to the review of DSRS Section 7.2.13, verify that automatic and manual auxiliary feedwater (AFW) system initiation has been provided and incorporated in the ESFAS and instrumentation systems design. NUREG-0737 provides additional guidance on conformance with this requirement.

[21] For conformance with paragraphs (C) and (E) of 10 CFR 50.34(f)(2)(xiv), the reviewer should use the following guidance:

- Ganged reopening of containment isolation valves is not acceptable. Reopening of isolation valves should be performed on a valve-by-valve or line-by-line basis, provided that electrical independence and the single-failure criterion for the ESFAS functions continue to be satisfied.

- Containment purge lines and other penetrations that provide a path to the environment should be isolated on a high radiation signal as one of the diverse isolation functions.

NUREG-0737 provides additional guidance on conformance with this requirement.

[22] The review of 10 CFR 50.34(f)(2)(xx) of power supplies is part of Chapter 8, titled “Electric Power,” and it is not reviewed in Chapter 7. The power supplies should conform with the guidance of NUREG-0737.

[23] The review of 10 CFR 50.62 should be coordinated with the organization responsible for the review of reactor systems, which evaluates whether the ATWS mitigation protective functions conform to the ATWS analysis referenced in Chapter 15 of the application, for AOOs, and to verify the adequacy of the design of mechanical systems used to mitigate ATWS.

[24] For the review of 10 CFR 50.49, the staff will coordinate with the organization responsible for the review of equipment qualification, which reviews mild environment qualification, including electromagnetic interference qualification of safety system I&C equipment, instrument sensing lines, lightning protection, and qualification for harsh environments.

[25] The evaluation of the habitability aspects of GDC 19 with respect to radiation protection is addressed in the review of DSRS Chapter 6.

[26] The adequacy of the human factor aspects of the control room design is addressed in the review of DSRS Chapter 18.